VEILIG DIGITAAL

VEILIG DIGITAAL NASLAG

Inhoudsopgave

Hoofdstuk 1

Achterdeurtje

Een **achterdeurtje** (Engels: *backdoor*) is een bewust ingevoerde functie in programmatuur om een beveiligingsmechanisme te omzeilen.

1.1 Eigenschappen

De aanwezigheid van een achterdeurtje valt niet op tijdens normaal gebruik van het programma. Wie bekend is met het achterdeurtje, kan toegang krijgen tot de programmatuur zonder door de beveiliging te worden gehinderd. Kenmerkend voor het achterdeurtje is dat het niet in het functioneel ontwerp van een systeem is vermeld. Een achterdeurtje kan om goedaardige redenen in programmatuur worden ingebouwd, bijvoorbeeld de angst om een wachtwoord kwijt te raken. In dat geval is het hele concept van beveiliging niet juist uitgevoerd.

Veelal worden achterdeurtjes om kwaadaardige redenen ingebouwd. Mogelijkheden zijn dat krakers achterdeurtjes openzetten nadat zij een systeem gekraakt hebben om toegang in de toekomst te verzekeren en achterdeurtjes bewust in programma's ingebouwd worden om bepaalde partijen toegang tot de systemen van de gebruikers te geven.

1.2 Voorkomen

Het voorkomen van achterdeurtjes is niet eenvoudig. Mogelijke maatregelen zijn:

- het creëren van veiligheidsbewustzijn bij programmeurs;
- het hanteren van een fatsoenlijk wijzigingsbeheerproces;
- het beoordelen van de ontwikkelde code door vakgenoten;
- het beoordelen van de broncode door een onafhankelijke revisor.

Doordat een achterdeurtje in de regel niet is gedefinieerd in een Functioneel Ontwerp, zal de aanwezigheid door het uitvoeren van acceptatietests of penetratietests in de regel niet worden opgemerkt.

1.3 Trojaans paard

Een Trojaans paard is een programma met verborgen inhoud. Een Trojaans paard gebruikt een achterdeurtje om de kwaadaardige inhoud te activeren.

1.4 Easter egg

Het verschil met een Easter egg is dat een achterdeurtje bedoeld is om een beveiligingsmechanisme te omzeilen. Een achterdeurtje is meestal ingebouwd met kwaadwillige bijbedoelingen. Een easter egg is veelal een grapje of een bonus.

1.5 Externe link

- (en) Backdoor

Hoofdstuk 2

Adware

Adware of **advertentieondersteunde software** is een softwareapplicatie die advertenties weergeeft terwijl het draait. Deze applicaties bevatten ook codes die deze advertenties weergeven in een pop-up- of pop-undervenster of in een ander venster dat verschijnt op het computerscherm. Adware helpt ontwikkelkosten terugwinnen en de prijzen van de applicatie voor de gebruiker laag of zelfs gratis te houden. De inkomsten kan softwareontwikkelaars winst opleveren en motiveren om deze applicaties te blijven ontwikkelen en onderhouden.

Sommige adware is ook shareware, gebruikers kunnen dan ook kiezen voor een “geregistreerde” versie waar geen advertenties in voorkomen.

Sommige adwareprogramma’s bevatten ook een code die persoonlijke informatie van een gebruiker bijhoudt en doorgeeft aan derden, zonder de goedkeuring of kennis van de gebruiker. Dit wordt spyware genoemd. Andere adwareprogramma’s houden geen persoonlijke informatie bij van de gebruiker.

2.1 P2p-netwerken

Op verschillende p2p-netwerken zoals LimeWire en eDonkey duiken gevaarlijke muziekbestanden op. Bij het openen van een afgehaald mp3-nummer downloadt het bestand automatisch een Trojaans paard genaamd play_mp3.exe. Dit installeert op zijn beurt een valse muziekspeler vol adware.

Gevaarlijke bestanden op p2p-netwerken zijn niet nieuw, maar in dit geval is het onderscheid moeilijk te maken. Zoals bij echte muzieknummers verschillen de mp3-bestanden in grootte en naam. Zo duikt de malware op in een aantal populaire muzieknummers.

De zogezegde muziekspeler die het virus installeert, speelt een dubbelzinnig spel. Zo toont hij voor installatie een ellenlange gebruikersovereenkomst (End User Licence Agreement of EULA). Het programma vermeldt hier dat het extra software installeert, en de bewuste map bevat dan ook een duidelijke hint door zich in de map “Firefox_adware” te nestelen. Het programma is waardeloos. In praktijk is het niet meer dan een browservenster met een online muziekspeler die een handvol online liedjes bevat.[1]

2.2 Adware vs. adware

Sommige bedrijven die gratis te downloaden software aanbieden, hebben een geheime agenda: het verspreiden van adware. Deze 'meeliftende' software zorgt er vervolgens voor dat de argeloze surfer wordt bestookt met ongevraagde reclame.

In een poging zo veel mogelijk 'klanten' bij elkaar te krijgen, hebben deze adware-verspreiders een tactiek ontwikkeld: ze proberen elkanders software uit te schakelen of zelfs van pc’s te verwijderen. Zo claimt het bedrijf Avenue Media dat Internet Optimizer door concurrerende software van DirectRevenue wordt opgespoord en verwijderd, wanneer iemand beide programma’s op een pc installeert.

Avenue Media heeft DirectRevenue in 2004 voor de rechter gedaagd. Deze tactiek heeft het bedrijf één miljoen klanten gekost en loopt hierdoor zo'n tienduizend dollar aan inkomsten per dag mis.

Juridische experts noemen de rechtszaak van groot belang omdat deze - als Avenue Media in het gelijk wordt gesteld - meer duidelijkheid kan bieden over de rechten van softwarefabrikanten bij het veranderen van persoonlijke instellingen op pc’s.[2]

2.3 Adware vs. spyware

Er bestaan flink wat misverstanden over spyware. Spyware en adware worden vaak op één hoop gegooid.

Het woord spyware verwijst strikt genomen naar programma’s die bijvoorbeeld toetsaanslagen, surfgedrag en ander privacygevoelige informatie achterhalen. Intussen wordt de term gebruikt voor veel meer. Zo wordt adware vaak gemakshalve tot de spywarecategorie gerekend.

Antispywarebedrijven hebben een manifest waarin ze de verschillende categorieën programma’s definiëren. Daarin geven ze aan hoe ze met die groepen software omgaan. Maar soms lopen bedrijven met zulke classificaties

tegen problemen aan, zoals Microsoft in juli 2005 een aantal beruchte adwareprogramma's een lichtere classificatie toekende. Claria's GAIN hoorde bij de 'low threat' en de aanbevolen actie was daarmee verschoven van 'verwijderen' naar 'negeren'. Computergebruikers namen deze indeling niet serieus.

Om ruzie over interpretaties te voorkomen, heeft de Anti-Spyware Coalition (ASC), een consortium van softwarebedrijven en andere betrokkenen, een poging gedaan definities vast te leggen. Het is niet de eerste poging om spyware te definiëren. Een vroeger consortium, COAST geheten, viel uiteen nadat er een adwarebedrijf tussen was verschenen. De meeste leden van dat consortium zijn nu betrokken bij ASC, maar adwarebedrijven zijn niet van de partij.[3]

2.4 Referenties

[1] Adware valt aan via P2P-downloaders

[2] Adware valt adware aan

[3] Spyware en adware, wat is wat?: definities vastleggen

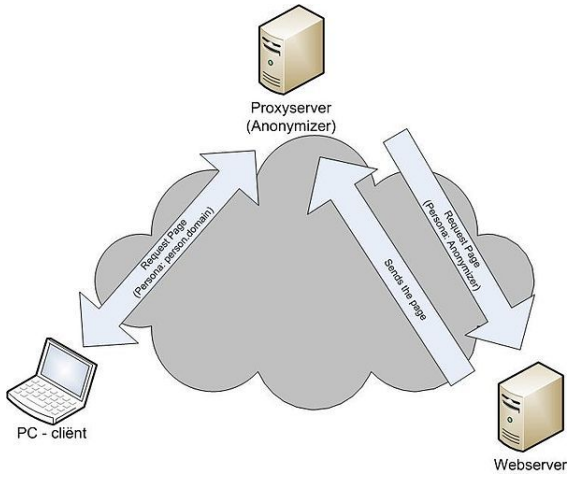
Hoofdstuk 3

Anoniem surfen

Anoniem surfen is een manier om het internet te benaderen waarbij zo veel mogelijk persoonlijke gegevens, zoals een IP-adres, verborgen blijven voor derden. Dit gebeurt via een proxy die als tussenpersoon dient en die zelf data van het internet opvraagt om die dan naar de gebruiker door te sturen.

3.1 Ontstaan

De eerste anonieme proxy Anonymizer.com kwam tot stand in 1997, aan de Universiteit van Californië-San Diego. In het teken van het Kosovo Privacy Project was het de bedoeling de mensen in de Kosovaarse oorlogszone de mogelijkheid te geven verslag uit te brengen zonder dat ze geïdentificeerd zouden worden en gestraft.[1]



Werking anoniem surfen zonder daisy-chaining.

3.2 Werking en doel

Wanneer een gebruiker een internetpagina opvraagt, heeft die website heel wat persoonlijke gegevens tot zijn beschikking. Zo wordt altijd het IP-adres meegestuurd, maar ook de browser, besturingssysteem, ISP en zelfs de locatie kunnen tot op zekere hoogte achterhaald worden.[2] Door anoniem te surfen, krijgt de server van de website enkel de gegevens van de anonieme proxy, omdat al het verkeer via de proxy loopt. Tevens wordt bij bepaalde diensten ook de verbinding geëncrypteerd waardoor de verstuurde informatie binnen het netwerk ook nog een extra beveiliging wordt toegekend. Dit maakt het mogelijk bijvoorbeeld websites op te roepen die geblokkeerd zijn door de eigen firewall of informatie van buitenaf te halen binnenin een repressief regime. Sommige proxy's kunnen ook cookies blokkeren.

Anderzijds worden anonieme proxy's ook gebruikt voor criminele doeleinden. Zo wordt kinderporno vaak geraadpleegd via dergelijke proxy's.

3.3 Risico's en nadelen

Hoewel anonieme proxy's beweren geen vertrouwelijke data bij te houden, is dit niet altijd het geval. Zo is het goed mogelijk dat een proxy logs bijhoudt van inkomende en uitgaande verbindingen die de IP-adressen bevatten. Zo'n proxy-server kan dan door de autoriteiten van het land waar de server zich bevindt, verplicht worden die logs vrij te geven. Het is echter mogelijk aan daisy-chaining te doen en dus meerdere anonieme proxy's na elkaar te gebruiken, hetgeen het opzoekwerk naar het werkelijke IP-adres erg bemoeilijkt.[3]

Een ander gevaar waaraan men aandacht moet schenken, is dat niet elke anonieme proxy te vertrouwen is. Omdat een anonieme proxy gebruikt wordt, worden de data daar onversleuteld naartoe gestuurd. Dit geeft de administrator van de proxy-server vrij spel in het achterhalen van gebruikersnamen, wachtwoorden en bankgegevens.[4]

Er zijn ook nadelen gekoppeld aan anoniem surfen die niet gerelateerd zijn aan veiligheid. Omdat de proxy-server zowel inkomende als uitgaande data moet verwerken, ligt de snelheid van het surfen vaak lager dan wanneer het niet-anoniem zou gebeuren. Dit heeft zeker een effect wanneer de server zowel een betalende als gratis dienst aanbiedt. In zo'n geval worden namelijk eerst de betalende gebruikers bediend. Daarnaast is het goed mogelijk dat een internetpagina niet correct of met foutmeldingen wordt weergegeven, gezien de proxy-server probeert verdachte onderdelen te verwijderen.[5]

3.4 Enkele voorbeelden

3.4.1 Tor-project

Het Tor-project is een specifiek voorbeeld van een manier waarop het daisy-chainen bij proxy-servers gebeurt. Het is een open netwerk en bestaat uit virtuele tunnels die zelfs door de U.S. Navy gebruikt worden. Het idee achter het Tor-netwerk is vrij simpel en omvat het distribueren van overdrachten over een willekeurig pad van verschillende plekken op het internet, zodat het praktisch onmogelijk wordt om te achterhalen waar het verkeer vandaan komt of naartoe gaat. Om zo'n pad uit te stippelen, maakt de cliënt verbinding met een directoryserver die dan een lijst van knooppunten aangeeft.

Tor is een onion routing systeem, wat inhoudt dat het verkeer uit verschillende lagen bestaat. Dit uit zich in de encryptie van de data. Zo haalt elk knooppunt in het pad telkens een laag van de encryptie af en weet die enkel van welk knooppunt het bestand komt en naar welk knooppunt het moet. Op die manier kent geen enkel knooppunt het volledige pad. Om efficiëntieredenen wordt dit pad een tiental minuten behouden, waarna het uit veiligheidsredenen opnieuw willekeurig wordt opgebouwd.[6]

Een groot aandachtspunt is dat er op het laatste knooppunt echter geen encryptie meer is. Wanneer iemand in het Tor-netwerk dus kwade bedoelingen heeft en het laatste knooppunt in een verbinding is, kan die alle data achterhalen. Dit is nog niet zo lang geleden gebeurd waardoor honderden gegevens zoals loginnamen en passwoorden van ministeries en ambassades uitgelekt waren. De bedoeling van het Tor-project is dan ook om te anonimiseren, niet om te beveiligen.[7]

3.4.2 I2P

I2P is vergelijkbaar met Tor, maar heeft geen enkel gecentraliseerd punt en is dus volledig gedistribueerd. Hierdoor is er ook geen plek waar data opgeëist kunnen worden, zoals bij proxy-servers. De gebruikers hebben daarnaast zelf de mogelijkheid om een middenweg tussen anonimiteit, betrouwbaarheid en snelheid te kiezen. I2P wordt over het algemeen vaker gebruikt voor peer-to-peer-toepassingen.

Net zoals bij Tor werkt I2P met knooppunten, die bestaan uit routers. Die maken hier echter geen tweerichtingspaden, want I2P heeft zowel een aparte inkomende tunnel als een uitgaande. Die tunnels blijven echter wel langer bestaan en worden aangemaakt door de routers, die via conventionele protocollen zoals TCP en UDP de links leggen. De data die door die verschillende knooppunten gaan, worden met elkaar vermengd en versleuteld. Een voordeel van I2P over Tor is dat de data tot en met de eindpersoon versleuteld zijn. Daarnaast maakt het gesplitste tweerichtingsverkeer het een stuk moeilijker om iemands identiteit te achterhalen.[8]

3.4.3 Freenet

Freenet is een computerprogramma waarmee je, na installatie, anoniem bestanden kan delen en surfen zonder enige vorm van censuur. Het is eigenlijk een parallelle internetomgeving waarin je geen echte websites gaat opvragen, maar 'freesites' – websites die door de gebruikers van Freenet online zijn geplaatst. Je bent verbonden met dit netwerk. Niet via een systeem dat alle verbindingen centraal beheert zoals bij meerdere peer-to-peer-applicaties maar via mensen die je vertrouwt, via vrienden. Die vrienden zijn op hun beurt ook weer met andere vrienden verbonden met dit netwerk. Dit zorgt ervoor dat het een netwerk is waarin iedereen de de verbonden vrienden moet vertrouwen. Die verbindingen zijn wel steeds versleuteld en gaan door verschillende nodes, wat het erg moeilijk maakt om te achterhalen vanwaar een bestand komt of waar het naartoe gaat.

De filosofie achter het Freenetsysteem is dat ieder een deeltje van zijn opslag en bandbreedte aanbiedt en dat gaat delen. De bestanden die op iemands computer staan, kan de persoon in kwestie niet lezen, die zijn namelijk versleuteld en alleen via het netwerk te openen. Zo kan het dus voorkomen dat je eigenlijk kinderporno of bestanden met illegale inhoud op het Freenet host. Dat zijn enkele van de risico's waarmee je rekening dient te houden wanneer je met anonimiteitsprojecten bezig bent.[9]

3.4.4 Remailer

Net zoals bij het surfen wordt ook bij het versturen van een e-mail erg veel informatie over je identiteit in de header gestopt. Een anonieme remailer kan al deze data wissen uit de header en hem daarna verder sturen en fungeert dus als tussenstation, net zoals een proxy server bij het anonieme surfen. Sommige systemen gaan hierin zelfs zo ver om je daadwerkelijk een anoniem adres aan te bieden en de daarop ontvangen post door te sturen naar je echte e-mailadres, zodat je constant anoniem kan werken.

Een eerste type van zulk een remailer is de Cypherpunk. Hierbij is het de bedoeling dat je een reeks remailers aanstelt om aan daisy-chaining te doen. De e-mail is met verschillende lagen versleuteld, waarvan elke remailer er een van kan afhalen, om te kijken wat het volgende adres is. Dit maakt het erg moeilijk om te achterhalen van waar de boodschap juist komt. Een tweede type is de Mixmaster. Deze gaat zo ver in het leveren van anonimiteit, dat hij ervan uitgaat dat het netwerk constant gemonitord wordt. Om verdachte patronen tegen te gaan, gaat hij eerder onverwachts te werk. In plaats van elke ontvangen boodschap meteen door te sturen, wordt er een variabele tijd gewacht. Hierna worden alle ontvangen e-mails gebundeld en in een keer verder verzonden.[10]

3.5 Privé browsen in een webbrowser

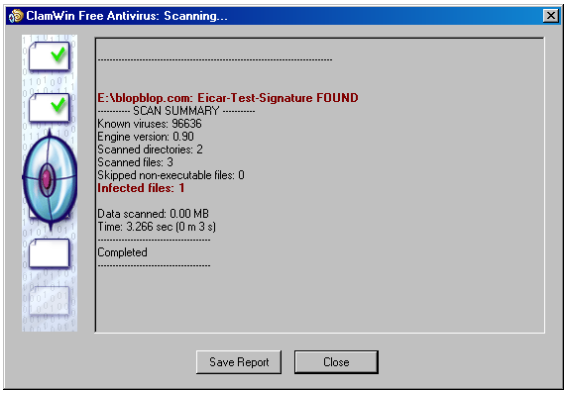
Anoniem surfen wordt in Google Chrome, Internet Explorer 8, Opera en de laatste Firefox-versie ook schijnbaar gepromoot door tijdens het surfen over te schakelen naar 'verborgen' status waarbij er geen bestanden in je geschiedenis of tijdelijke map worden aangemaakt. De opgeslagen favorieten en gedownloade bestanden blijven echter wel bestaan nadat u de browser sluit.

Deze vorm van privaat surfen heeft de namen "Incognito' (Chrome), "InPrivate" (Internet Explorer) en "Privénavigatie" (Firefox) op de markt gezet door ze te promoten als de ideale middelen om surfgedrag te verbergen voor degenen die na u dezelfde computer gebruiken.[11] Echter wordt de laatste tijd door cynici deze methode vergeleken met een techniek die een soort "porno-mode" verschaft.

Echter moet privaat surfen niet in dezelfde categorie gestopt worden als anoniem surfen aangezien deze niet voorkomt dat uw ISP of andere instellingen achter uw surfgedrag komen. Anderzijds beschermt dit evenmin uw gegevens wanneer u een site bezoekt waardoor kan besloten worden dat zaken zoals Incognito, InPrivate en Privénavigatie uw privacy kunnen garanderen op de lokale computer maar niet tegenover andere gebruikers op het World Wide Web.

Hoofdstuk 4

Antivirussoftware



Antivirusprogramma ClamWin

Antivirussoftware is programmatuur die probeert om computervirussen te identificeren, tegen te houden en te verwijderen.

Antivirussoftware gebruikt daarvoor twee verschillende technieken:

- Onderzoeken (scannen) van bestanden om te zoeken naar virussen die overeenkomen met de definities uit een lijst van bekende virussen.
- Identificeren van verdacht gedrag door eender welk computerprogramma, wat op een besmetting kan wijzen.

De meeste antivirusprogramma's gebruiken beide technieken, met de nadruk op de eerste aanpak. Er zijn ook programma's beschikbaar die enkel de eerste techniek gebruiken.

Tegenwoordig komt antivirussoftware op zich nog maar weinig voor, meestal is het samen met antispywarefunctionaliteit in antimalwaresoftware vervat. Dit soort beveiligingssoftware beschermt niet alleen tegen virussen, maar tegen alle vormen van kwaadaardige software (malware).

4.1 Methodes voor virusdetectie

4.1.1 Viruslijst

In de aanpak met viruslijsten, inspecteert de software een bestand en gebruikt daarbij een lijst van bekende virussen die door de makers van de software zijn geïdentificeerd. Wanneer een stuk code in het bestand overeenkomt met een virus uit de lijst, kan de software een van de volgende acties ondernemen (in volgorde waarin de actie verkozen wordt):

1. proberen het bestand te repareren door het virus zelf uit het bestand te verwijderen
2. het bestand in quarantaine plaatsen (zodat het bestand niet meer toegankelijk is voor andere programma's en het virus zich niet langer kan verspreiden)
3. het geïnfecteerde bestand verwijderen

Om deze aanpak op middellange en lange termijn succesvol te houden, worden de virusdefinities regelmatig bijgewerkt (meestal online). Bij nieuwe, geïdentificeerde virussen kunnen gebruikers en technici hun geïnfecteerde bestanden opsturen naar de auteurs van de antivirussoftware, om zo de informatie in toekomstige virusdefinities te verwerken.

De aanpak met virusdatabases onderzoekt typisch de bestanden wanneer het besturingssysteem deze aanmaakt, opent, sluit of verzendt via e-mail. Met als opzet om een virus onmiddellijk bij ontvangst te herkennen. Een systeembeheerder kan er ook voor zorgen dat de software op een regelmatig tijdstip alle bestanden op de harde schijf van de gebruiker scant.

Hoewel deze aanpak op een efficiënte manier de uitbraak van een virus tegenhoudt, omzeilen schrijvers van virussen de software door het schrijven van "oligomorfe", "polymorfe" en meer recent "metamorfe" virussen. Deze virussen encrypteren stukken van zichzelf of camoufleren zich zodat ze niet overeenkomen met hun bekende virusdefinities.

4.1.2 Detectie van verdacht gedrag

In plaats van bekende virussen te identificeren analyseert deze methode het gedrag van programma's. Wanneer bijvoorbeeld een programma gegevens schrijft naar een ander uitvoerbaar programma, kan de antivirussoftware dit als verdacht gedrag zien, de gebruiker waarschuwen en om een reactie vragen.

Deze vorm van antivirussoftware biedt bescherming tegen virussen die nog niet in de databases voorkomen. Dit zorgt voor een aantal fout-positieven, en gebruikers worden vlug achteloos voor de waarschuwingen. Wanneer een gebruiker elke waarschuwing wegklikt, heeft de antivirussoftware geen nut meer voor die gebruiker. Dit is een groeiend probleem, aangezien meer ontwerpen van niet kwaadaardige programma's andere .exe-bestanden aanpassen zonder deze fout-positiefkwestie in acht te nemen. Moderne antivirussoftware gebruikt deze techniek daarom steeds minder.

4.1.3 Andere methodes

Sommige antivirussoftware emuleren het begin van de code van een nieuw uitvoerbaar bestand dat het systeem aanroept, vooraleer het de controle aan het nieuwe bestand zelf overdraagt. Als het programma een zelfmodificerende code lijkt te gebruiken of op een andere manier het gedrag van een virus lijkt te vertonen (het zoekt bijvoorbeeld onmiddellijk naar andere uitvoerbare bestanden), wijst dit op een mogelijke infectie. Ook hier zijn er onschuldige bestanden die als malware aangeduid worden, zogenaamde *false positives*.

Bij nog een andere detectiemethode gebruikt men een sandbox. Een sandbox emuleert het besturingssysteem en voert het programma uit binnen deze simulatie. Nadat het programma is beëindigd, analyseert de software de sandbox op wijzigingen die op een virus kunnen wijzen. Vanwege prestatieproblemen vinden zulke detecties normaal gesproken enkel plaats tijdens manueel gestarte scans.

4.2 Aandachtspunten

- De verspreiding van e-mailvirussen (deze horen bij de meest destructieve en verspreide computervirussen) kan op een veel goedkopere en efficiëntere manier tegengegaan worden wanneer bugs in e-mailsoftware zouden hersteld worden, zonder dat de installatie van antivirussoftware nodig is. Deze fouten laten immers toe dat gedownloade code uitgevoerd kan worden, zich kan verspreiden en schade aanrichten.

- Het opleiden van de gebruikers is een meerwaarde boven op de antivirussoftware; de gebruikers wijzen op veilig omgaan met computers (zoals het niet downloaden en uitvoeren van onbekende programma's van het internet) vertraagt de verspreiding van virussen en vermindert de nood aan antivirussoftware.

- Computergebruikers zouden niet altijd hun machine mogen gebruiken als systeembeheerders. Als ze eenvoudigweg zouden werken in gebruikersmodus, zouden veel virustypes zich niet kunnen verspreiden (of hun schade zou minstens beperkt blijven). Dit is een van de verschillende redenen waarom virussen relatief zeldzaam zijn op UNIX-achtige systemen.

- De aanpak met lijsten om virussen te definiëren volstaat niet, wegens de voortdurende aanmaak van nieuwe virussen; maar ook het detecteren van verdacht gedrag werkt niet voldoende wegens het fout-positiefprobleem. Daarom kan de huidige kennis die ingebouwd is in antivirussoftware nooit alle computervirussen bestrijden.

- Er bestaan verschillende methodes om kwaadwillige software te encrypteren en te verpakken, zodat zelfs bekende virussen niet ontdekt kunnen worden door antivirussoftware. Om "gecamoufleerde" virussen op te sporen is een krachtige code nodig om deze bestanden te ontcijferen om later te kunnen onderzoeken. De meeste populaire antivirusprogramma's hebben dit niet en nemen vaak deze virussen niet waar.

- Het voortdurende schrijven en verspreiden van virussen en van de paniek eromheen, maakt dat de verkopers van antivirussoftware baat hebben bij het bestaan van virussen.

- Sommige antivirussoftware vermindert de systeemprestaties aanzienlijk. Gebruikers schakelen vaak de antivirusbescherming uit om dit prestatieverlies tegen te gaan en lopen zo een verhoogd risico op infectie op. Voor maximale bescherming moet de software altijd ingeschakeld zijn, wat vaak tot tragere prestaties leidt (zie ook Software bloat). Sommige antivirussoftware hebben minder invloed op de prestaties.

- Het is soms nodig om de virusbescherming uit te schakelen bij het uitvoeren van belangrijke updates, zoals de Windows Service Packs, of het updaten van de stuurprogramma's van de grafische kaart. Ingeschakelde antivirussoftware kan er tijdens een belangrijke installatie voor zorgen dat de update niet correct verloopt of helemaal niet lukt. Het komt voor dat de virusbescherming bij het installeren van degelijke updates automatisch tijdelijk wordt uitgeschakeld. Dit komt onder andere voor bij Microsoft Security Essentials (in Windows 8 Windows Defender), het antivirusprogramma van Microsoft.

4.3 Antivirussoftwarebedrijven

- Avira uit Duitsland
- AVAST Software uit Tsjechië, maker van avast!
- AVG Technologies makers van AVG Anti-virus uit Tsjechië
- BitDefender uit Roemenië
- Comodo Group uit de VS
- Computer Associates uit de VS
- Coranti uit Japan
- Defenx uit Zwitserland
- eScan, gemaakt door MicroWorld uit India
- Eset makers van NOD32 uit Slowakije
- F-Secure uit Finland
- G DATA Software uit Duitsland, makers van G DATA AntiVirus (voorheen AntiVirusKit)
- GFI Software
- H+BEDV, tegenwoordig bekend als Avira uit Duitsland, makers van AntiVir
- Intego, makers van VirusBarrier uit de VS
- Kaspersky Lab uit Rusland
- McAfee uit de VS
- Microsoft, de makers van Microsoft Security Essentials
- Norman uit Noorwegen
- Norton uit de VS
- Panda Security uit Spanje (voorheen Panda Software)
- Qihoo 360 uit China
- RAV Antivirus uit Roemenië (in 2003 gekocht van GECAD)
- Sophos uit het VK
- Softwin, maker van BitDefender uit Roemenië
- Stiller Research
- Symantec makers van Norton AntiVirus/Symantec Antivirus
- Trend Micro uit Japan (in naam uit Taiwan - VS)
- Zone Labs de makers van ZoneAlarm

4.4 Testorganisaties

Testorganisaties testen virusscanners en gerelateerde programma's. Voorbeelden hiervan zijn AV-Comparatives, AV-test.org, Virus Bulletin, ICSA Labs, West Coast Labs, GFI Software en EICAR.

4.5 Zie ook

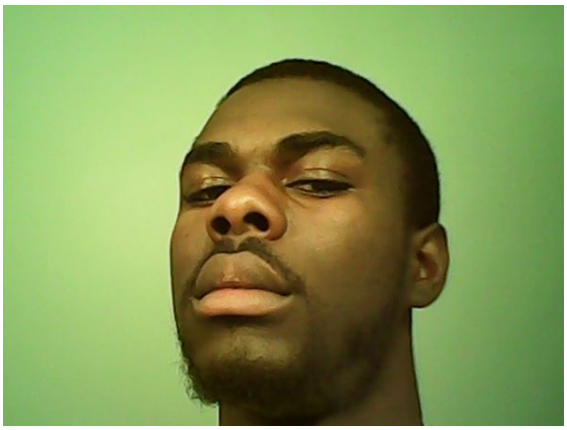
- Lijst van antivirussoftware

4.6 Externe links

- Project ***The Vaccine***
- (en) Carnegie Mellons CERT coordination center in het Internet Archive
- (en) European Institute for Computer Anti-Virus Research (EICAR)

Hoofdstuk 5

Avatar (computer)



Selfie als avatar

Vrouwelijke avatar in Second Life

Een **avatar** is een plaatje dat als gebruikersafbeelding op het internet gehanteerd wordt, bijvoorbeeld op internetforums als Twitter of in chatprogramma's als Windows Live Messenger. Deze afbeeldingen zijn meestal vrij klein, bijvoorbeeld tussen de 48x48 en 150x150 pixels (soms ook 100x100 of 100x200), maar kunnen soms vergroot worden door erop te klikken. Bij de sociale media worden regelmatig selfies gebruikt als avatar.

Avatars staan hier meestal naast of onder de nickname van een lid. Een avatar is dan de representatie van de persoon van vlees en bloed in de virtuele wereld of fantasiewereld. Op sommige spelsites zijn avatars geen realistische portretfoto of -tekening van de werkelijke persoon maar een simpele versiering of een pictogram dat uitdrukking geeft aan een visuele voorkeur van de gebruiker.

In vele hedendaagse videospellen wordt de avatar van de speler als een virtuele driedimensionale figuur uitgebeeld die door de speler kan worden bewogen en naar eigen smaak aangekleed en gestyled kan worden. Zo gebruiken 3D-platforms als Second Life en Habbo Hotel dit soort zeer realistische avatars.

Sommige weblogs maken gebruik van een systeem waarbij gravatars, ofwel *globally recognized avatars*, automatisch worden herkend en opgehaald uit een centrale database.

5.1 Etymologie

Het woord "avatar" komt uit het Sanskriet. In de hindoeïstische filosofie betekent het incarneren of verschijnen van een (abstracte) god in de wereld in de persoon van een levend wezen.

Hoofdstuk 6

Backbone

In de internetterminologie is een **backbone** een stelsel van zeer snelle computerverbindingen waarlangs het gegevensverkeer loopt van de netwerken die op de backbone zijn aangesloten. Een aangesloten netwerk kan zelf ook weer een backbone hebben.

Een voorbeeld is het Abilene-netwerk, dat fungeert als de backbone in het Internet2-project. In de beginjaren van het internet fungeerde het ARPANET als backbone.

Het woord *backbone* is het Engelse equivalent van ruggengraat.

6.1 Zie ook

- National Science Foundation Network

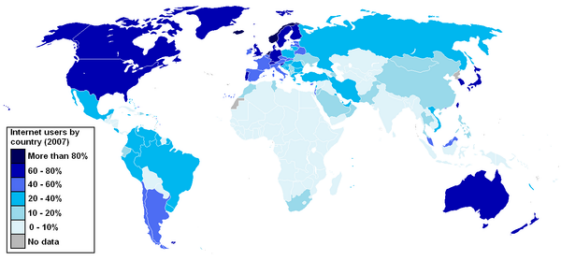
Hoofdstuk 7

Internet

Internet is een netwerk van computernetwerken (zie ook intranet en extranet). Een computernetwerk is over het algemeen alleen beschikbaar binnen een organisatie of gebouw, een beperking die opgeheven wordt door een internet. Om een internet goed te laten werken is het nodig om afspraken te maken over protocollen. Een bijna universeel gebruikt protocol is het zogenaamde Internetprotocol (IP). Computers in verschillende computernetwerken kunnen dankzij die afspraken met elkaar communiceren.

Het **internet** is de benaming voor een zeer groot, de hele aarde omspannend openbaar netwerk van computernetwerken, waarvan de afspraken worden beschreven in de Requests for Comments die worden beheerd door de Internet Engineering Task Force. De oorsprong van het internet is terug te voeren tot ARPANET, een in 1969 in de Verenigde Staten gebouwd militair netwerk, dat later voor algemeen gebruik geschikt is gemaakt vanuit Amerikaanse universiteiten. Inmiddels is het internet een mondiaal fenomeen, dat het karakter van massamedium heeft gekregen. Als een van de succesfactoren wordt wel genoemd dat het volledige internet eigendom van niemand is, terwijl de fysieke onderdelen wel degelijk een eigenaar hebben.

In het dagelijkse spraakgebruik wordt met internet vaak het World Wide Web bedoeld, maar dat is slechts een van de vele diensten die kunnen worden gebruikt via het internet. Andere bekende diensten zijn e-mail, VoIP, FTP en Usenet.



Percentages internetgebruikers per land in 2007

7.1 Het woord internet

De term *internet* was oorspronkelijk een bijvoeglijk naamwoord, namelijk een afkorting van *internetworking*, dat wil zeggen: netwerken onderling verbindend. In de oorspronkelijke specificatie van TCP/ IP, het basis-internetprotocol, uit 1974 is deze term al te vinden.[1] Men had het bijvoorbeeld over *internet-mail* en *internet-verkeer*. Hier betekende *internet*: werkend met TCP/IP, en het was een voorziening waar op sommige computernetwerken voor specifieke doeleinden bij tijd en wijle gebruik van werd gemaakt, als aanvulling op de faciliteiten van het computernetwerk zelf.

Door het ontstaan van een groot en explosief groeiend wereldwijd netwerk van via TCP/IP verbonden computers ging de term “internet” verwijzen naar dat specifieke netwerk, en het werd rond 1990 de officiële naam voor dat netwerk, een zelfstandig naamwoord, meestal met lidwoord en hoofdletter geschreven. In de daaropvolgende jaren werden alle andere vormen van computernetwerken naar de periferie verdrongen en groeide het internet uit tot een algemene voorziening zoals tv, radio en telefoon. De oorsprong van de voorziening en van de naam ervan verdwenen naar de achtergrond.

Sinds de nieuwe Nederlandse spelling van oktober 2005 wordt *internet* in het Nederlands in alle gevallen zonder hoofdletter geschreven.[2]

7.2 Geboorte van het internet

De grondslag voor het internet is ARPANET, een in 1969 door ARPA, een dienst van het Amerikaanse ministerie van Defensie, begonnen computernetwerk gebaseerd op packet switching. Men had ingezien dat met deze techniek en de toepassing van wachtrijtheorie en andere technieken voor gedistribueerde netwerken een erg robuust systeem op te zetten was. De term “Internet” werd in 1974 voor het eerst gebruikt in een document van Vinton Cerf en zijn manager, Bob Kahn, over TCP.

Op 1 januari 1983 stapte ARPANET over van NCP naar TCP/IP als netwerkprotocol (waarbij IP staat voor *Internet Protocol*), en daarmee was de geboorte van het

internet in zijn huidige technische vorm een feit. Het gebruik ervan verspreidde zich verder onder universiteiten en aan de overheid gelieerde instellingen, eerst in de Verenigde Staten, later ook in Canada, Europa en Japan. Het meeste gebruik vond plaats in de vorm van SMTP (e-mail), FTP (bestandsoverdracht) en telnet (tekstuele interactieve sessies).

Intussen ontwikkelde de verwerkingskracht van computers en netwerken zich zo sterk dat grafische gebruikersomgevingen op computers gemeengoed werden en het zelfs haalbaar werd om op deze manier documenten en applicaties op afstand over het internet beschikbaar te stellen. Het basisprincipe hierbij is hypertext, waarbij documenten aanklikbare verwijzingen naar elkaar bevatten.

Tim Berners-Lee en Robert Cailliau van het CERN zagen in dat hiervoor standaardtechnieken nodig waren die net als de TCP/IP-protocollen van het internet zelf platformafhankelijk zouden moeten zijn, en begonnen in 1991 het World Wide Web-project, waarin ze zulke standaarden ontwikkelden (HTTP en HTML), software schreven om ze te gebruiken, en die software vrijelijk aan de wereld beschikbaar stelden. Gebruikers en ontwikkelaars elders in de wereld volgden, en de ontwikkeling van de Mosaic-webbrowser in 1993 aan het NCSA was de definitieve doorbraak. Het gebruik van documenten en diensten over het internet werd hiermee enorm vereenvoudigd.

In 1993 werd het gebruik van het internet, tot dusverre voorbehouden aan overheid en onderwijs, door de Amerikaanse overheid opengesteld voor bedrijven en particulieren. Het gebruik nam nu explosief toe. Pizza Hut was in 1994 een van de eerste bedrijven ter wereld die het www commercieel inzetten door de mogelijkheid te bieden om bestellingen online te doen. In 1996 was het internet algemeen bekend bij het grote publiek, maar werd de term over het algemeen gebruikt als synoniem voor het World Wide Web.

7.3 Het huidige internet

Afgezien van de complexe fysieke verbindingen die de infrastructuur van internet vormen, wordt het internet bij elkaar gehouden door bi- en multilaterale commerciële contracten zoals peeringovereenkomsten en de technische standaarden die de te gebruiken protocollen beschrijven.

In tegenstelling tot oudere communicatieprotocollen is de set van protocollen die het internet gebruikt zo veel mogelijk onafhankelijk van het gebruikte fysieke medium. Hierdoor kan bijvoorbeeld TCP/IP-communicatie plaatsvinden over glasvezel-, koper- en radioverbindingen.

De basisprotocollen, zoals TCP/IP, worden vastgesteld door de Internet Engineering Taskforce (IETF). Deze komen tot stand via een publieke discussie. De IETF legt standaarden vast in documenten die RFC's worden genoemd. Sommige van deze worden door de Internet Architecture Board (IAB) verheven tot internetstandaard.

De meest gebruikte protocollen binnen internet zijn op dit moment IP, TCP, UDP, DNS, PPP, SLIP, ICMP, POP3, IMAP, SMTP, HTTP, HTTPS, SSH, Telnet, FTP, LDAP, SSL en TLS.

Populaire diensten die gebruikmaken van de hiervoor genoemde protocollen zijn bijvoorbeeld e-mail, Usenet, het World Wide Web, Gopher, IRC en MUD. Van deze diensten worden e-mail en het World Wide Web het meest gebruikt. Andere diensten bouwen hierop voort, zoals mailinglijsten en weblogs. e-mail en Usenet zijn echter niet toegangsafhankelijk van de bovenstaande protocollen, ze kunnen ook via andere netwerkprotocollen bereikt worden.

Andere populaire diensten zijn van oorsprong bedrijfseigen ontwikkelingen. Voorbeelden hiervan zijn Skype, ICQ en Gnutella.

7.4 Toegang tot het internet

Gebruikelijke methoden om toegang te krijgen tot het internet omvatten:

- Via een kabel, dus min of meer op een vaste plaats: de inbelverbinding, breedband (over een coaxiale kabel, glasvezelkabel of koperen kabel).
- Draadloos, via wifi-hotspots.
- Via het netwerk voor mobiele telefonie: mobiel internet (EDGE/2G/3G/4G).

Ook combinaties worden gebruikt, zoals thuis aangesloten zijn via een kabel, en daarmee een wifistation voor gebruik in huis creëren, of onderweg mobiel internet op een apparaat hebben, en van dat apparaat een wifistation maken (mobiele hotspot) voor gebruik op andere door de betreffende persoon en zijn eventuele gezelschap meegenomen apparaten.

Bij het, al of niet tegen betaling, beschikbaar stellen van internet, bijvoorbeeld aan bezoekers van een openbare gelegenheid, kan men onderscheiden:

- Het beschikbaar stellen van een computer met internetaansluiting. Dit gebeurt onder andere in bibliotheken en internetcafés.
- Het beschikbaar stellen van wifi. Dit gebeurt in/op sommige treinen, bussen, vliegvelden, stations, benzinestations, horecagelegenheden, en soms in de foyer van een bioscoop. Steeds meer luchtvaartmaatschappijen bieden op intercontinentale vluchten ook internet tegen betaling aan tijdens het vliegen.

Zo is in Nederland bijvoorbeeld bij de NS gratis wifi beschikbaar in veel intercity's (als onderdeel van On Board Information Services), en bij Arriva in alle treinen en een deel van de bussen.[3]

7.5 Robuustheid van het internet

Het internet is vanaf het begin zo gebouwd dat het netwerk stabiel is en blijft. Als een verbinding wegvalt, zullen de pakketten door de vele routers langs een ander pad gestuurd worden. Daarom wordt verondersteld dat de stabiliteit van het internet moeilijk te beïnvloeden is door terroristen. Als een kabel wordt doorgesneden of een knooppunt wordt opgeblazen, zullen de datapakketten zonder gegevensverlies een andere route kiezen. Dit bleek inderdaad zo te zijn bij de aanslagen op 11 september 2001 in New York. Onder het World Trade Center lag een belangrijk knooppunt van het internet maar er werd na de vernietiging hiervan geen noemenswaardige vertraging geconstateerd in het algemene internetverkeer.

Een kritische blik op het internet in Nederland leert echter wel dat bijna al het internationale verkeer via Amsterdam Internet Exchange ((AMS-IX)) in Amsterdam loopt, een van de drukste internetknooppunten ter wereld. Zo zijn er vanuit Amsterdam verbindingen met onder andere Londen en Hamburg (easynet), met Düsseldorf, New York en Kopenhagen (KPN) en met Chicago, Praag en Stockholm (Netherlight). Mochten onverhoopt alle verbindingen naar Amsterdam wegvallen, dan moet al het internationale internetverkeer van en naar Nederland een omweg via bijvoorbeeld Rotterdam en Antwerpen maken. Overbelasting van dat deel van het netwerk is dan een logisch gevolg. Het Amsterdamse internetknooppunt is overigens verdeeld over zeven verschillende locaties, waardoor de kans op algehele uitval klein is.

7.6 Risico's van het internet

"Internetbos", bedoeld om compensatie te bieden voor de CO_2-uitstoot die internetservers veroorzaken

De opmars van computernetwerken heeft ook zijn negatieve kanten:

- Via de talrijke verbindingen kunnen virussen en spyware zich snel verspreiden. Systemen die veel gebruikt worden, zoals Windows en Android, worden vaker geviseerd.
- Persoonlijke gegevens zijn vaak slecht beveiligd en daarmee gemakkelijk toegankelijk voor onbevoegden, wat gevolgen heeft voor de privacy van individuen.
- Eens gedeelde informatie op het internet is moeilijk weer te verwijderen.
- Het internet geeft een gevoel van anonimiteit, wat voor sommige mensen aanleiding is om extremer te reageren dan anders.
- Net als in de fysieke wereld heeft internet ook last van vandalen. Een goed voorbeeld hiervan zijn de "scriptkiddies".
- Ongewenste informatie, bijvoorbeeld een handleiding voor het vervaardigen van explosieven, kan ook eenvoudig verspreid worden.
- Het internet heeft indirect bijgedragen tot een enorme groei van het aantal servers die diensten verlenen over het internet en steeds meer elektriciteit vergen voor stroomvoorziening voor de elektronica en koeling. Een datacenter kan evenveel energie verbruiken als een fabriek.[4]

Men hoopt een aantal van bovenstaande problemen te verhelpen door nieuwe protocollen te ontwikkelen met een verbeterde authenticatie en een sterkere encryptie. Een voorbeeld daarvan is AS2. Het ontwikkelen van zuiniger computerchips en efficiëntere software moet het elektriciteitsverbruik van servers afremmen.

7.7 Zie ook

- Internet van A tot Z
- Informatica
- Telecommunicatie

7.7.1 Geschiedenis

- Geschiedenis van het internet
- Geschiedenis van het internet in Nederland

7.7.2 Algemeen

- Internetprovider
- Domeinnaam
- Communicatiesatelliet
- Globaal Brein

7.7.3 Internetdiensten

- Internet Relay Chat
- Webhosting

Aangeboden via internet

- E-mail
- Usenet

7.7.4 Gebruik

- User Agent
- browser
- Zoekmachine
- Nettiquette
- Internetjargon
- Nieuwsgroep
- Gebruikersgroep
- Portaal
- Weblog
- Mobiel internet
- Internetsoap
- Internetcensuur

7.7.5 Ontwikkelingen

- Internet der dingen

7.8 Externe links

- (nl) De geschiedenis van het internet
- (en) Internetlijnen over heel de wereld
- (en) I'm still here: back online after a year without the internet - artikel in The Verge, Paul Miller

Hoofdstuk 8

Besturingssysteem

Een **besturingssysteem** (ook wel: **bedrijfssysteem**, in het Engels **operating system** of afgekort **OS**) is een programma (meestal een geheel van samenwerkende programma's) dat na het opstarten van een computer in het geheugen geladen wordt en de hardware aanstuurt. Het fungeert als een medium tussen de hardware en de computergebruiker met als opzet dat de gebruiker programma's op een gemakkelijke en/of efficiënte manier kan uitvoeren.[1]

8.1 Kenmerken

Het besturingssysteem wordt meestal van de harde schijf gelezen, maar soms ook wel vanuit ROM-geheugen of als *live-system* vanaf een verwisselbaar medium zoals een diskette, cd-rom, dvd, solid state drive of (voor ingebedde systemen) een flashgeheugen. Een schijfloos systeem, dat wil zeggen een systeem zonder harde schijven, kan opstarten vanaf een netwerk in een zogenaamde *Thin client*-configuratie. De protocollen BootP en het nieuwere DHCP voorzien hierin.

Het besturingssysteem zorgt onder meer voor het starten en beëindigen van andere programma's, het regelt de toegang tot de harde schijf, het beeldscherm, de invoer van gegevens. De andere programma's die gestart kunnen worden, heten applicaties. Zo'n applicatie maakt gebruik van het besturingssysteem door middel van een application programming interface (API). Deze API abstraheert de toegang tot de verschillende randapparatuur, zoals harde schijf, printer en beeldscherm.

Gebruikers maken van het besturingssysteem gebruik door middel van een opdrachtregel, zoals MS-DOS of de UNIX-terminal, of een grafische gebruikersomgeving zoals Microsoft Windows of het X Window-systeem.

8.2 Taken

8.2.1 Hoofdtaken

- Het opstarten van het systeem; er wordt gezorgd dat alle benodigde bestanden worden geladen.
- Het verdelen van toegang tot systeembronnen (RAM-geheugen, opslag, printer etc.) tussen actieve programma's.
- Actieve programma's de mogelijkheid bieden om een gebruikersinterface weer te geven. Vrijwel elk besturingssysteem heeft ook zelf een gebruikersinterface. Voorbeelden zijn de DOS-prompt en Windows Verkenner.
- Programma's uitvoeren. Het uit te voeren programma wordt naar het interne geheugen geschreven. De processor voert de opdracht uit.
- Communicatie met randapparatuur
  - Invoer: via randapparaten zoals het toetsenbord en de muis moet correct verwerkt worden.
  - Uitvoer: via randapparaten zoals de monitor en de printer, deze moeten de juiste instructies krijgen.
- Geheugenbeheer:
  - *Intern geheugen*: indeling en gebruik ervan door een of meer applicaties.
  - *Extern geheugen*: Organisatie voor opslag van gegevens en regeling voor het ophalen en wegschrijven van bestanden.

8.2.2 Bijkomende taken in complexere systemen

- Multitasking: bepalen welk programma op welk moment moet draaien (als het besturingssysteem het toelaat dat meer programma's tegelijkertijd draaien).
- Gebruikersbeheer bij servers en multi-useromgevingen.
- Uitvoer van achtergrondprocessen.
- Energiebeheer, voornamelijk bij laptops en computers die op batterijen werken.

8.3 Opstarten

Het is gebruikelijk om het besturingssysteem na het starten van de computer te laden vanaf een harde schijf. Deze werkwijze geeft de mogelijkheid het besturingssysteem door een meer recente versie te vervangen, of zelfs een geheel ander besturingssysteem te kiezen. Het laden van een systeem vanaf een harde schijf was vroeger minder vanzelfsprekend.

Ook kan het besturingssysteem, net als de firmware, in chips gebrand worden. Dit werkt zelfs sneller dan het starten vanaf een harde schijf en maakt de hardware compacter. Dit wordt toegepast bij veel mobiele apparaten, zoals *personal digital assistants* (pda's) en mobiele telefoons

Ook worden computers gebruikt met een ingebed systeem, vaak inclusief een toepassingsprogramma. Het gaat dan meestal om een apparaat met slechts één doel, bijvoorbeeld besturing van wasmachine, een melkmachine, slagbomen, een weegbrug enz. Diverse besturingssystemen hebben hiervoor een speciale 'embedded' versie, een uitgeklede versie van het besturingssysteem.

8.3.1 Pc

Het eerste programma dat na het inschakelen van een personal computer actief wordt, was tot 2006 het *Basic Input/Output System* (BIOS). Vanaf 2006 is dit geleidelijk vervangen door EFI, hoewel de markt het nog niet massaal als standaard aanvaardt.

Tegenwoordig verschijnt bij het aanzetten van je computer eerst het BIOS-scherm: dit is het zwarte scherm met witte letters wat altijd voorbijflitst. Waar je een besturingssysteem op een harde schijf hebt staan welke je uit de computer kunt halen, is BIOS een chip. Je kunt BIOS dus niet van je computer verwijderen. Wel is het vaak mogelijk om een andere versie op de chip te zetten (flashen).

8.4 Zie ook

- Lijst van besturingssystemen
- Monolithische kernel
- Netwerkbesturingssysteem

Hoofdstuk 9

BIOS

Een BIOS ROM IC

Het **BIOS**, wat een acroniem is voor ***B**asic **I**nput/**O**utput **S**ystem*, is een bibliotheek met een set basisinstructies voor de eerste communicatie tussen het besturingssysteem en de hardware. Tijdens het opstarten van een pc, wanneer het besturingssysteem nog niet geladen is, is dit ook de enige software die beschikbaar is.

Wanneer een computer wordt gestart, wordt eerst de *Power-On Self-Test* (POST) in het BIOS doorlopen. Als alles in orde lijkt, roept het BIOS vervolgens de *bootloader* aan (meestal door de eerste sector van een aanwezige harde schijf te lezen). Dit opstarten wordt *booten* genoemd: de *bootstrap*-routines in het BIOS zijn de eerste stap waarmee de computer zichzelf start.

9.1 Instellingen

Bij sommige BIOS-systemen van computers is weinig in te stellen. Sommige computerfabrikanten willen niet dat gebruikers iets verkeerd kunnen instellen. Wanneer een computerhobbyist zelf een computer samenstelt, dan is er ruime keuze aan moederborden met vele instelmogelijkheden van het BIOS.

De instellingen van het BIOS kunnen zijn:

1. Instellingen voor de processor (snelheid, spanning, etc.).
2. Instellingen voor de harde schijven en cd-romdrives, en de volgorde van opstarten.
3. Instellingen voor het geheugen.
4. Instellingen voor extra onderdelen op het moederbord, zoals geluid, usb, lan, seriële en parallelle poorten.

Het is eenvoudig om in het BIOS iets verkeerd in te stellen, waardoor de computer het niet goed zal doen of oververhit kan raken (bij overklokken).

9.2 BIOS-updates

Een fabrikant van computers of moederborden komt soms met nieuwere versies van het BIOS. Er kunnen fouten verholpen zijn, of nieuwe hardware wordt ondersteund. Als tijdens het vernieuwen van het BIOS de computer wordt uitgezet, dan is het mogelijk dat het BIOS maar gedeeltelijk in de computer is geschreven en zal de computer het niet meer doen. Sommige computers hebben daarom twee chips met een BIOS op het moederbord (het zogenaamde dual BIOS-systeem). Indien het vernieuwen mislukt, dan wordt een oudere reserve BIOS gebruikt om op te starten.

De merknaam in het BIOS maakt deel uit van de OEM-licentie van Microsoft Windows. Indien het BIOS wordt vervangen door een type met een andere merknaam, dan moet Windows soms opnieuw geactiveerd worden. Een BIOS van een ander merk is alleen in uitzonderlijke gevallen geschikt, bijvoorbeeld wanneer hetzelfde moederbord gebruikt is in computers van verschillende merken.

9.3 Geschiedenis

Het BIOS van een computer is opgeslagen in een aparte geïntegreerde schakeling op het moederbord. Vroeger (rond 1990) stond het BIOS gewoonlijk in een EPROM en kon niet gewijzigd worden zonder speciale apparatuur,

vanaf ca. 1995 werd steeds vaker EEPROM gebruikt, waarmee een BIOS vernieuwd kon worden zonder een chip te vervangen.

Moderne personal computers hebben doorgaans uitgebreide *setup*-mogelijkheden. Doorgaans werkt dit als volgt: bij het opstarten van een computer kan men met een speciale toets [1] (vaak *Delete*, *F10*, *F2* of nog andere toetsencombinaties) dit opstartproces onderbreken en “naar de *setup* gaan”, nog voordat het besturingssysteem geladen wordt. Via meerdere schermen kunnen dan BIOS-instellingen gewijzigd worden. Na het terugschrijven van deze instellingen naar de CMOS-Data (RAM) wordt het bootproces opnieuw gestart.

Een voorbeeld van een BIOS-instelling, is de volgorde waarin de pc informatiedragers (floppy, harde schijf/schijven, usb-stick, cd, netwerk[2]) afloopt op zoek naar een geldig besturingssysteem om te laden (de *boot sequence*): als er -volgens de genoemde volgorde- geen opstartinformatie op de floppy gevonden is zal er op de harde schijf/schijven gezocht worden en zo verder.

Intel heeft voor dit reeds meer dan 20 jaar oude systeem een vervanging gemaakt met de naam Extensible Firmware Interface (EFI). UEFI, een uitgebreide en verbeterde versie van EFI, wordt in de praktijk als EFI verkocht.

9.4 Virus

Het BIOS is in principe gevoelig voor virussen. Op sommige moederborden is een versleuteling aanwezig, waardoor het BIOS niet gewijzigd kan worden zonder een wachtwoord in te geven. Er zijn tot op heden geen grote virusaanvallen van het BIOS bekend.

9.5 Zie ook

- Extensible Firmware Interface (EFI), de voornaamste opvolger van het BIOS

Hoofdstuk 10

Bluecasting

Door middel van **bluecasting** krijgen gebruikers van een device zoals een telefoon of PDA met Bluetooth ingeschakeld automatisch content zoals clips, mini-ads etc. aangeboden, zodra zij in de buurt zijn van speciaal ontwikkeld plasmascherm of multi-mediazuil. De telefoon moet dan wel als 'waarneembaar' voor andere devices ingesteld staan.

Rockgroep Coldplay, gebruikte Bluecasting voor het lanceren van hun nieuwe album X&Y.

Bluecasting is een vorm van narrowcasting.

Hoofdstuk 11

Bluejacking

Bluejacking is het verkrijgen of versturen van informatie van een apparaat dat Bluetooth gebruikt.

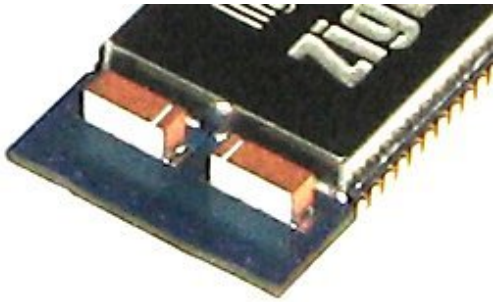
De term bluejacking is een combinatie van *bluetooth* en *jack*, jack is vergelijkbaar met het Engelse woord *prank* wat in het Nederlands 'grap' betekent, hoewel enkele bronnen aangeven dat bluejacking een samentrekking zou zijn van *Bluetooth* en *hijacking* (Engels voor kapen). [1] *Hijacking* verwijst hierbij naar het via bluetooth kunnen gebruikmaken van een mobiele telefoon, zonder toestemming van de eigenaar. Dit kan onschuldig zijn zoals het verzenden van berichtjes naar een ander willekeurige mobiele telefoon in de buurt waar bluetooth aanstaat. Maar ook het lezen van alle gegevens en bellen naar dure nummers op een mobiele telefoon (Bluesnarfing) door gebruik te maken van - inmiddels door middel van veiligheidsupdates gedichte - veiligheidslekken in bepaalde mobiele telefoons.

11.1 Externe link

- (en) bluejackQ, een website die bluejacking beschrijft

Hoofdstuk 12

Bluetooth



Chip met bluetooth-antenne

Bluetooth is een open standaard voor draadloze verbindingen tussen apparaten op korte afstand. Dankzij bluetooth kunnen bijvoorbeeld adresgegevens tussen mobiele telefoons worden uitgewisseld, kan snel vanaf een handheld computer worden geprint, of kan een mobiele telefoon worden uitgerust met een draadloze *headset*. De techniek is ontwikkeld door het Zweedse Ericsson.

12.1 Geschiedenis

Het bluetooth-logo

De geschiedenis van bluetooth begint in 1994, toen Ericsson zocht naar een goedkope manier om via een radioverbinding communicatie tot stand te brengen tussen mobiele telefoons en andere apparaten. Men had zich ten doel gesteld om allerlei kabels tussen mobiele telefoons en pc-cards, koptelefoons, desktopapparaten et cetera overbodig te maken. Naarmate het onderzoek vorderde, werd het de onderzoekers duidelijk dat de toepassingsmogelijkheden voor een dergelijke korteafstandsradioverbinding legio waren.

De techniek zelf is ontwikkeld door de Nederlander Jaap Haartsen die bij Ericsson in dienst was in Emmen. De naam *bluetooth* verwijst naar de Vikingenkoning Harald Blauwtand (Harald Blåtand) die het christendom in Scandinavië introduceerde. Het was oorspronkelijk de werknaam van het project, maar bij gebrek aan een betere naam is het ook de definitieve naam geworden.

Voor de ontwikkeling en het 'in de markt zetten' van de bluetooth-techniek is in 1998 besloten tot het oprichten van de 'Bluetooth Special Interest Group' (SIG), waarbij zich al gauw vrijwel alle grote elektronicabedrijven, software-ontwikkelaars en telecombedrijven aansloten (onder meer Palm, Ericsson, IBM, Intel, Lucent Technologies, Apple, Microsoft, Motorola, Nokia en Toshiba). Bluetooth moest vrij van royalty's worden en geheel 'open'.

Voor bluetooth is een frequentie uitgezocht die ook wereldwijd beschikbaar is. De 2,4GHz-band was met name voor Spanje, Japan en Frankrijk aanvankelijk een probleem, in Frankrijk was deze al in gebruik voor militaire toepassingen, maar sinds 1 januari 2001 staat ook daar deze frequentie voor bluetooth ter beschikking. De frequentie is vrij en wordt ook gebruikt voor babyfoons, afstandsbedieningen van garagedeuren, draadloze telefoons, magnetrons en wifi-toepassingen. Bluetooth valt onder de regeling voor Short Range Devices, waarvoor geen zendmachtiging benodigd is. De eerste versie is versie 1.0 en had nog last van "kinderziektes" (hij was storingsgevoelig), daarom kwam al snel versie 1.1 die op vele punten was verbeterd.

12.2 De techniek

Bluetooth is een radioverbinding (in de 2,4GHz-band, dit is in het frequentiegebied van UHF) voor spraak en data op korte afstand. Het werkt 'point to multipoint', hetgeen

inhoudt dat een enkele bron meer 'ontvangers' kan bedienen. Wanneer twee bluetoothapparaten een verbinding hebben opgebouwd, dan ontstaat een zogenoemd piconet. Er kunnen op dezelfde plek meerdere van dergelijke piconets naast elkaar bestaan, in wat men een scatternet noemt. Binnen een piconet ondersteunt bluetooth maximaal acht actieve verschillende apparaten, terwijl er in totaal 127 apparaten een verbinding kunnen houden (deze zijn tijdelijk 'geparkeerd').

Normaal gesproken zal het binnen een straal van 1 tot 10 meter functioneren, maar wanneer het zendvermogen wordt opgevoerd, kan de 100 meter worden gehaald. Een zogenoemde 'zichtverbinding' (elkaar kunnen zien) is niet nodig; dankzij de GHz-radioverbinding dringt het bluetoothsignaal ook door vaste materialen (zolang het geen metaal is).

De communicatie van digitale spraak behoort tot de standaardmogelijkheden van bluetooth. Bluetooth ondersteunt binnen een piconet tot drie gelijktijdige full-duplex-gesprekken.

Omdat bluetooth een vervanger is voor de (korte) kabels, kan het worden gebruikt om allerlei apparaten met elkaar te laten communiceren. De ontwerpers hebben met opzet gebruikgemaakt van een goedkope radiotechniek, zodat bluetooth zonder veel bezwaar in ieder apparaat kan worden ingebouwd. Omdat bluetooth normaal gesproken ook weinig stroom verbruikt (30 microampère in 'hold mode' en 8-30 milliampère bij een actieve verbinding), kan het ook worden toegepast in mobiele apparaten die afhankelijk zijn van batterijen.

Vanaf versie 1.2 gebruikt bluetooth frequency hopping, of Adaptive Frequency Hopping (AFH).

Bluetoothapparatuur is verdeeld in 3 verschillende klassen:

- Class 1: Ontworpen voor lange afstandsverbindingen (tot ~100m)
- Class 2: Voor normaal gebruik (tot ~10m)
- Class 3: Voor korte afstanden (10 cm - 1 m)

Er bestaan ook verschillende bluetoothversies:

- Versie 1: de datasnelheid bedraagt bruto 1 Mbit/s.
- Versie 1.2: deze vernieuwde versie maakt datasnelheid tot 2 Mbit/s mogelijk. Daarnaast verbeterde het spraakkwaliteit en audio-overdracht.
- Versie 2: eind 2004 is een nieuwe verbeterde versie van bluetoothstandaard ontwikkeld en goedgekeurd. De belangrijkste kenmerken zijn:
  - 3 keer zo hoge datasnelheid
  - lager stroomverbruik (wat de levensduur van de batterij verlengt)
  - verbeterde foutcorrectie
  - verbeterde mogelijkheid verbindingen met meerdere apparaten.
- Versie 3: op 21 april 2009 werd een nieuwe versie van bluetooth gepresenteerd. De nieuwe bluetoothversie is weer een stuk sneller en betrouwbaarder en gebruikt wifi (802.11n).
- Versie 4: op 7 juli 2010 werden de specificaties van deze standaard vastgelegd, waarbij er vooral aan de energiezuinigheid werd gewerkt. Vanaf deze versie zijn bluetoothaccessoires die werken op een knoopcel mogelijk.

12.3 Toepassingen

Belangrijke toepassingen zijn het verzenden van bestanden tussen apparaten zoals computers en mobiele telefoons, het zenden van een document of afbeelding van een computer naar een printer, het zenden van toetsaanslagen van een toetsenbord naar een computer, het zenden van een afbeelding van een scanner naar een computer, het zenden van geluid naar een draadloze koptelefoon enzovoort. Tevens wordt bluetooth gebruikt om verkeersinformatie mee in te winnen door middel van het bluetooth-meetsysteem.

12.4 Beveiliging

Omdat de radiosignalen kunnen worden opgevangen door alle ontvangers die zich in de buurt van de bluetoothapparaten bevinden, ondersteunt bluetooth in het basisprotocol authenticatie en encryptie. Authenticatie vindt plaats middels een geheime sleutel, die zich op beide apparaten moet bevinden. Het protocol staat het wel toe dat het ene apparaat het andere authenticeert. Na authenticatie is het mogelijk om de verbinding te versleutelen (encryptie).

Als het bluetoothapparaat niet voldoende beveiligd wordt, kan door middel van bluejacking informatie verzonden worden naar het apparaat. Het ongevraagd en dus illegaal lezen van de documenten via bluetooth wordt dan bluesnarfing genoemd. Verder kan een apparaat onbruikbaar worden gemaakt door middel van bluesmacking. Dit is een denial-of-service aanval middels bluetooth. Bluesniffing is het afluisteren van bluetooth-verkeer.

12.5 Bluetooth versus IrDA

Bluetooth is net als de infrarode verbinding (IrDA), een communicatiemiddel voor de korte afstand. Beide verbindingsmogelijkheden concurreren dus met elkaar. Met name bij het uitwisselen van data, zoals het 'synchroniseren' van een handheld computer met een pc, mikken

de beide technieken ook op dezelfde functionaliteit. Zij maken hiervoor zelfs gebruik van hetzelfde 'upper layer' protocol (OBEX) en beide streven ernaar om gebruik te kunnen maken van dezelfde applicatie.

Toch hebben bluetooth en IrDA specifieke eigenschappen, waardoor zij in verschillende situaties de voorkeur verdienen. In een ruimte met veel apparaten op de bluetooth-frequentie (veel mobiele telefoons, bijvoorbeeld), is het eenvoudiger om gegevens uit te wisselen via IrDA; het is dan mogelijk om beide apparaten op elkaar te 'richten', zonder dat andere tussenbeide kunnen komen. Met bluetooth is het wat lastig 'mikken' en daardoor duurt het even voordat bluetooth alle soortgenoten in de buurt heeft ontdekt. Vervolgens kan er nog tijd overheen gaan, voordat uit de naburige apparaten het juiste is geïdentificeerd, waarvoor extra informatie nodig kan zijn. Ook het beveiligingsmechanisme in bluetooth vraagt tijd.

In andere gevallen verdient bluetooth weer de voorkeur. Zo kan met mobiele apparatuur worden gecommuniceerd, zonder dat deze tevoorschijn hoeft te worden gehaald; de mobiele telefoon kan in de tas blijven tijdens het synchroniseren. Bovendien mag, in tegenstelling tot bij IrDA, een apparaat worden bewogen tijdens de communicatie, waardoor het apparaat ook klaar is om te ontvangen wanneer het 'op het lichaam' wordt gedragen. Hierdoor kan de gebruiker van een mobiele telefoon met bluetooth zijn telefoon gewoon in zijn zak laten zitten wanneer hij via een laptop een 'dial up'-verbinding met het internet maakt. De telefoon hoeft niet, zoals bij infrarood, naast de laptop te liggen. Bluetooth kan ook grotere afstanden overbruggen (ongeveer 15 tot 20 meter) terwijl IrDA (infrarood) al na enkele meters geen goede verbinding meer kan maken. Het verbinden met bluetooth is erg makkelijk omdat je bij de meeste bluetoothapparaten een lijst kan opvragen via je pda, mobiele telefoon of laptop welke andere bluetoothapparaten er in de buurt zijn, vervolgens kun je ze makkelijk koppelen. Dankzij het 'multi-point'-karakter van bluetooth is het ook mogelijk om meerdere van bluetooth voorziene apparaten, via een enkel LAN Access Point in een ruimte, toegang te geven tot een (bekabeld) netwerk. Hier kan echter wel de beperkte snelheid van bluetooth een rol spelen. Bluetooth kan maar communiceren met 1 Mb/s (bij IrDA is dat tot 4 Mb/s, respectievelijk 16 Mb/s voor modernere varianten).

Verder is bluetooth niet merkgebonden wat als voordeel heeft dat men bijvoorbeeld in een auto met een bluetooth-car-kit kan aanmelden met elke mobiele telefoon uitgerust met dit systeem. Hoewel niet elk bluetoothapparaat compatibel is met elk ander bluetoothapparaat. Zo moet het apparaat dat aan bijvoorbeeld een car-kit wordt gekoppeld beschikken over het handsfree profiel. Daarnaast hoeft dan ook niet elke functie te werken met elk toestel. De fabrikanten van de apparaten hebben hier meer informatie over.

Bluetooth concurreert niet met het draadloze LAN 802.11 (wifi). Bluetooth biedt een lager bereik en een lagere bandbreedte, maar is veel goedkoper en energiezuiniger en daardoor beter op grote schaal toe te passen in (mobiele) apparatuur.

12.6 Doordringend vermogen van microgolven

Microgolven kunnen onze huid doordringen en de cellen van inwendige weefsels bereiken. Net als bij de magnetron veroorzaakt dit in principe opwarming, maar vanwege het zeer geringe vermogen is de temperatuurverandering veroorzaakt door bluetoothapparatuur onmeetbaar klein. Hoewel de schadelijkheid van bluetoothstraling niet uitputtend onderzocht is, is het vermogen van bluetoothapparatuur zo laag dat het optreden van gezondheidseffecten uiterst onwaarschijnlijk is. Een uurtje buiten lopen op een zonnige dag is in termen van straling vele malen ongezonder dan een uur naast een bluetoothapparaat doorbrengen.

Bluetoothfrequenties zullen in de toekomst mogelijk hoger komen te liggen. Fabrikanten ijveren daar al jaren voor.

12.7 Bluetooth-profielen

- A2DP
- SIM Access Profile
- AptX

12.8 Zie ook

- IrDA
- Draadloos netwerk
- Bluecasting
- Bluejacking
- ZigBee

12.9 Externe links

- (en) Een leerprogramma over bluetooth, met informatie over architectuur, protocollen, de verbindingen, veiligheid en vergelijkingen
- (nl) Interview met de man achter bluetooth, Jaap Haartsen
- (en) Bluetooth-profielen

Hoofdstuk 13

Bootloader

Een **bootloader** is een computerprogramma dat zorgdraagt voor het starten van het besturingssysteem bij de opstart (*bootstrap*) van een computer.

Bij het starten van een computer wordt eerst programmatuur uitgevoerd die op het moederbord aanwezig is, dit is de BIOS (*Basic Input/Output System*) of tegenwoordig ook UEFI (*Unified Extensible Firmware Interface*). Deze programmatuur initialiseert en test de componenten en heeft als laatste taak het starten van het besturingssysteem. Omdat het besturingssysteem bijvoorbeeld op een harddisk staat, is het normaliter alleen bereikbaar via een bestandssysteem. Maar werken via een bestandssysteem vereist eerst een werkend besturingssysteem. Dit geldt evengoed voor het *booten* vanaf cd, of een netwerk. Deze impasse is doorbroken door de afspraak dat de eerste sectoren van een 'medium' een programma bevatten dat het besturingssysteem start. Dit programma heet de *bootloader*. Een *disk bootloader* start meestal het systeem op de eerste actieve partitie. Een netwerk-*bootloader* laadt het besturingssysteem via het netwerk vanaf een zogenaamde *bootserver*.

13.1 Bootmanager

Als de *bootloader* een wat uitgebreider programma is, dat zelf ingesteld kan worden, dan spreekt men meestal van een "*bootmanager*". Voorbeelden van *bootmanagers* zijn GRUB, Lilo en Gag.

Een bootmanager zoals 'Gag' is te groot (meer dan 440 bytes) dat het niet meer in het MBR-gedeelte van een harde schijf past. Net als hedendaagse disk-bootloaders (zoals Lilo en GRUB) is er dus onvoldoende ruimte in het bootrecord voor het hele bootloaderprogramma. Dan staat in het MBR een kleine -primaire- bootloader, die een secundaire bootloader start vanaf een diskpartitie. Deze bootloaders vragen de gebruiker - indien gewenst - door middel van een keuzemenu welk besturingssysteem er gestart dient te worden.

13.2 Zie ook

- BootX (Linux)
- BootX (Apple)
- Live-system

Hoofdstuk 14

Bootsectorvirus

Een **bootsectorvirus** is een klein computerprogramma dat zichzelf op de harde schijf of diskette schrijft, juist op die plek die tijdens het opstarten van de computer gelezen wordt om het besturingssysteem te vinden, de zogenaamde bootsector. Eenmaal geladen, probeert een dergelijk virus de bootsectoren van verdere aanwezige schijven te infecteren.

In de begintijd van de personal computer kwamen *bootsectorvirussen* regelmatig voor. De verspreiding vond vooral plaats via diskettes die per ongeluk in de diskettedrive waren achtergebleven. Een computer probeerde in die tijd doorgaans eerst van de diskette op te starten. Ook als het opstarten vanaf de diskette niet lukte, kon het virus zich in het geheugen nestelen en de harde schijf infecteren. Een virus dat op de harde schijf stond, probeerde alle diskettes te infecteren die werden gebruikt.

Door de opkomst van de cd-rom en internet zijn diskettes in onbruik geraakt en is het mechanisme van de verspreiding van *bootsectorvirussen* niet meer effectief. Ook heeft het moderne BIOS de mogelijkheid om het overschrijven van de bootsector van de harde schijf te blokkeren.

Tegenwoordig bestaan opstartbare USB-sticks, die vaker gebruikt worden dan diskettes. Omdat deze dezelfde functionaliteit hebben als de diskette zie je tegenwoordig ook computervirussen die USB-sticks en andere vormen van smart media infecteren. Moderne antivirussoftware controleert daarom ook de op deze vorm van opslag aanwezige gegevens, omdat een USB-stick ook als opstartbaar kan zijn ingesteld in het BIOS. Vóór het opstarten van de computer dient deze functie dan ook uitgeschakeld te worden, omdat het virus niet “al in het geheugen zit”.

Hoofdstuk 15

Botnet

Botnet is jargon voor een collectie van softwarerobots of bots, die automatisch en zelfstandig opereren. De term wordt vaak geassocieerd met ongewenste software of het automatisch versturen van ongewenste e-mail van computers waarop deze software is geïnstalleerd (spam) maar kan ook refereren aan een netwerk van computers die distributed-computing-software gebruiken.

15.1 Achtergrond

Hoewel de term "botnet" gebruikt kan worden voor elke groep bots, zoals IRC-bots, wordt de term vooral gebruikt voor een collectie van aan elkaar gekoppelde computers die software gebruiken die meestal is geïnstalleerd door een computerworm, Trojaans paard of achterdeurtje. De meeste computers die door deze software worden geïnfecteerd draaien onder Microsoft Windows, maar andere besturingssystemen kunnen ook worden aangetast. De geïnfecteerde computers heten ook wel zombies, het botnet heet ook wel zombienetwerk.

Een botnet heeft altijd een beheerder genaamd een "bot herder". Deze beheerder kan de groep op afstand besturen, vaak via middelen als IRC, meestal met slechte bedoelingen.

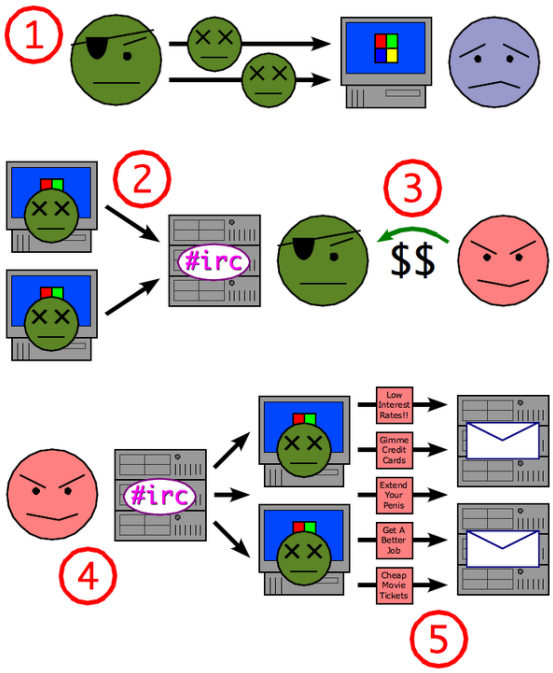
Een bot van een botnet draait op een computer meestal op de achtergrond zodat hij niet opvalt. Vaak heeft de beheerder van een botnet de beschikking over een aantal hulpmiddelen om firewalls en buffers op andere computers te omzeilen. Nieuwere bots kunnen vaak zelf zwakke punten in een computer opzoeken.

Botnets zijn een significant onderdeel geworden van het internet. Veel internetservers blokkeren botnets. Er zijn al verschillende botnets opgespoord en verwijderd. Zo vond de Nederlandse politie in Sneek een botnet opgezet door een 19-jarige hacker.[1]

15.2 Organisatie

Botnets gaan steeds vaker gebruikmaken van hun eigen servers. Deze servers staan doorgaans in verbinding met andere botnetservers, die samen gemeenschappen vormen op internet. Deze netwerken zijn vaak klein om detectie te voorkomen.

15.3 Gebruik



Hoe een botnet spam kan versturen.

Een voorbeeld van hoe een botnet wordt gebruikt voor het maken en sturen van spam:

1. Een botnetbeheerder stuurt een computervirus of computerworm het internet op, die andere computers infecteren met een bot.
2. De bot op de geïnfecteerde computer logt in op een door de beheerder bepaalde server.
3. Een spammer koopt toegang tot het botnet van de beheerder.
4. De spammer stuurt instructies naar alle besmette computers via het netwerk.

5. De besmette computers beginnen uit zichzelf spammail te sturen.

De afgelopen jaren vormen botnets een echte plaag op het internet. Niet alleen zijn botnets vaak verantwoordelijk voor een groot deel van de wereldwijde spam in mailboxen, ze worden ook steeds vaker ingezet om formulieren op internet te misbruiken. Denk maar aan het misbruiken van een gastenboek om reclame te maken voor bepaalde websites, het beïnvloeden van internetstemmingen e.d. De meeste internetformulieren worden bijgevolg beveiligd met een captcha, een automatisch gegenereerde afbeelding met een combinatie van letters en cijfers die de gebruiker moet overtypen. Op die manier wordt er gecontroleerd of er wel degelijk een mens aan het werk is of een botnet, vermits botnets het erg moeilijk hebben met het ontcijferen van die afbeeldingen.

15.4 Types

Botnets kunnen op de volgende manieren een computer aanvallen:

- Via adware en spyware.
- Klikfraude: de computer bezoekt websites zonder dat de eigenaar van die computer dat weet.
- Denial-of-Service: hierbij maken verschillende systemen autonoom contact met een internetsysteem of dienst, waardoor het systeem overbelast raakt.

15.5 Preventieve maatregelen

Als een machine een denial-of-service-aanval ontvangt van een botnet, zijn er een aantal opties. Vanwege het grote aantal machines en bijbehorende IP-adressen heeft een firewall vaak geen zin. Passive OS fingerprinting kan aanvallen die van een botnet komen identificeren, waardoor netwerkbeheerders een nieuwe firewall kunnen maken om een botnet te blokkeren.

Sommige botnets gebruiken gratis DNS-diensten voor het verspreiden van hun bots. Door een dergelijke dienst uit te schakelen kan vaak een heel botnet worden lamgelegd.

Verschillende bedrijven zoals Symantec, Trend Micro, FireEye, Simplicita en Damballa hebben aangekondigd bezig te zijn met het ontwikkelen van software om botnets tegen te gaan. Sommige, zoals Norton Anti-Bot, zijn gericht op klanten, maar de meeste zijn gericht op ondernemingen en/of ISPs.

15.6 Externe links

- ATLAS Global Botnets Summary Report - Real-time database of malicious botnet command and control servers.

Hoofdstuk 16

Browserkaper

Een **browserkaper** of in computertermen een *browser hijacker* genoemd, is een spywareprogramma dat een deel van een browser overneemt.[1] Een browserkaper zal een persoon bij zoekopdrachten omleiden naar kwaadaardige websites. Het belangrijkste doel van een browserkaper is het verkeer toe te laten nemen naar de site waar de gebruiker naar wordt omgeleid. De browserkaper installeert bijvoorbeeld vaak een zoekbalk of verandert keer op keer de thuispagina op iemands persoonlijke computer. Daarnaast zal een browserkaper zich automatisch op de achtergrond bezighouden met het verzamelen van vertrouwelijke informatie om deze vervolgens door te sturen naar een hacker.

Een browserkaper zal meestal geïnstalleerd worden zonder medeweten of toestemming van de persoon in kwestie door middel van downloads of besmette e-mails.

16.1 Voorbeelden van browserkapers

16.2 Oplossing

Een groot deel van de bestaande browserkapers kan snel en effectief verwijderd worden met een anti-spywareprogramma. Het is echter beter te voorkomen dan te genezen. Daarom wordt aangeraden om een behoorlijk antispyware-programma te installeren en kritisch te zijn in wat men aanklikt.

Hoofdstuk 17

Brute force (methode)

Brute force (Engels voor “brute kracht”) is het gebruik van rekenkracht om een probleem op te lossen met een computer zonder gebruik te maken van algoritmen of heuristieken om de berekening te versnellen. *Brute force* wordt gebruikt als er geen algoritme bekend is dat sneller of efficiënter tot een oplossing leidt. De methode bestaat uit het botweg uitproberen van alle mogelijke opties, net zo lang tot er een gevonden is die overeenkomt met de gewenste invoer.

17.1 Kraken van wachtwoorden met *brute force*

Brute force wordt vaak gebruikt voor het kraken van wachtwoorden of achterhalen van verloren gegane of vergeten wachtwoorden die versleuteld zijn met sterke encryptie. Hierbij worden alle mogelijke combinaties van beschikbare tekens geprobeerd. Dit is een zeer inefficiënte methode door de zeer lange duur, maar 100% trefzeker.

De formule voor de schatting van de maximumtijd om een wachtwoord te vinden (gebaseerd op drie miljoen wachtwoorden per seconden) is:

$$\text{seconden} = \text{karakters}^{\text{posities}}/3000000$$

Voorbeeld: We hebben de mogelijkheid om in een wachtwoord alleen cijfers en alle kleine letters van het alfabet te gebruiken (dus 26 + 10 = 36 verschillende karakters) en het wachtwoord is maximaal 6 posities lang. Dan duurt het circa $36^6/3000000 = 725{,}6$ seconden voordat dit wachtwoord is geraden. Indien men uitgaat van de 95 (alle karakters op het toetsenbord) dan duurt het reeds $95^6/3000000 = 245.030$ seconden, wat overeenkomt met 68 uur. Indien men het wachtwoord 7 karakters lang maakt in plaats van 6, duurt het inmiddels $95^7/3000000 = 23277910$ seconden, wat overeenkomt met 269 dagen. Om deze reden is het raadzaam om lange wachtwoorden te gebruiken. In de praktijk is de gemiddelde zoektijd naar een juist wachtwoord meestal binnen de helft van een doorlopen zoekruimte: de bovenstaande formule kan men het aantal $\text{karakters}^{\text{posities}}$ delen door 2 voor een benadering van de gemiddelde zoektijd.

Voor het kraken met *brute force* moeten er niet te veel mogelijke sleutels zijn. Wanneer het aantal mogelijke cryptografische sleutels extreem hoog is, moet ook extreem veel worden geïnvesteerd in rekenkracht en -tijd om een sleutel te kraken. Een RSA-sleutel bestaat uit het product van twee priemgetallen en is daarom zeer moeilijk te kraken met gebruik van *brute force*. Voor de 56 bits van een DES sleutel is dat praktisch haalbaar, voor een AES sleutel van 128 bits niet.

Vaak zal een aanval gebruikmaken van een combinatie van slimme trucs die de zoekruimte inperken en een aanval in *brute force* op datgene wat overblijft. Daarom moeten sleutels voor asymmetrische encryptie ook langer zijn dan die voor symmetrische encryptie om een vergelijkbaar veiligheidsniveau te bereiken – er is meer informatie aanwezig die structuur kan helpen achterhalen. Het is ook om deze reden, dat het aanmaken van sleutels met grote zorgvuldigheid dient te gebeuren, ofwel dat de entropie van sleutelmateriaal zo hoog mogelijk moet zijn. Als een symmetrische sleutel 112 bits inneemt, maar door interne structuur slechts voor 40 bits aan verrassing bevat, dan kan een kraker die daar weet van heeft, een veel kleinere zoekruimte aanpakken met brute kracht en daarmee de slaagkans verhogen.

De enige bestaande perfect veilige vercijfering die bestand is tegen een bruteforce-aanval of een andere cryptoanalytische aanval is Vernams one-time-pad. Dit werd bewezen in Claude Shannons verhandeling 'Communication theory of secrecy systems'. De correcte toepassing hiervan stelt de gebruiker echter voor enorme problemen op het gebied van sleutelbeheer.

17.1.1 Toepassing bij MD5-hashes

Een voorbeeld waarbij dit gebruikt wordt is om MD5-hashes te achterhalen. Stel we hebben een wachtwoord als md5-hash opgeslagen: 900150983cd24fb0d6963f7d28e17f72
Dan zal bij een bruteforce attack het kraakprogramma alle mogelijkheden afgaan:
a = 0cc175b9c0f1b6a831c399e269772661
b = 92eb5ffee6ae2fec3ad71c777531578f
...

aa = 4124bc0a9335c27f086f24ba207a4912
ab = 187ef4436122d1cc2f40dc2b92f0eba0
..
En uiteindelijk zal het bij de goede komen:
abc = 900150983cd24fb0d6963f7d28e17f72

Merk op dat Abc een andere uitkomst geeft dan abc, en dat dit dus alweer tientallen extra pogingen vereist.
Wachtwoorden zouden als het goed is altijd opgeslagen moeten staan als hash. Dit is in Windows zo, en bij de meeste webdiensten. Hierdoor is het wachtwoord nooit meer zomaar terug te halen, maar wel te resetten (de opgeslagen hash overschrijven). Dit is tegen dat als de database ooit gehackt zou worden, alle wachtwoorden zo te vinden zijn.

17.1.2 Overige toepassingen

Bruteforce-aanvallen zijn niet alleen van toepassing op MD5-hashes. Ook NTLM-hashes (gebruikt om een Windows-wachtwoord op te slaan) kunnen via deze methode gedecodeerd worden. Deze techniek heet ook wel 'reverse engineering'.

Als de aanvaller de hash niet bezit kan deze ook gewoon een script schrijven dat in een loginscherm alle mogelijkheden uitprobeert. Een hash zal normaal de voorkeur hebben aangezien die het programma niet nodig heeft, het programma zou namelijk restricties aan het aantal loginpogingen per minuut of per uur kunnen opleggen. Ook zal het programma iedere poging het scherm minimaal een keer verversen, wat ook weer tijd kost. Dit lijkt nihil, maar zelfs 3 miliseconden maken een gigantisch verschil als er bijvoorbeeld 3 miljoen pogingen vereist zijn om het wachtwoord te raden.

Via internet is nog langzamer, zeer vaak zijn er een bepaald aantal loginpogingen mogelijk voor een captcha ingevuld moet worden of men moet een aantal seconden wachten tussen de pogingen. Zelfs als deze restricties niet aanwezig zijn, duurt het vaak nog 20-200 miliseconden voor een enkele poging.

Stel we hebben een wachtwoord Za113, en we weten dat er alleen alfanumerieke karakters in het wachtwoord voorkomen, dan zal het iets minder dan 916000000 pogingen vereisen het wachtwoord te kraken. Ditmaal, in het allerbeste geval, 15 milliseconden is al een behoorlijke tijd.

MD5-hashes kunnen met de juiste software en een goede computer met een snelheid van 500 miljoen pogingen per seconde geprobeerd worden. Als deze als MD5 opgeslagen zou staan in een database, en deze database zou gehackt worden, zou het wachtwoord dus slechts 2 seconden nodig hebben om te kraken.

17.1.3 Parallellisatie

Om *brute force*-methodes te doen versnellen gebruiken programmeurs een techniek genaamd *parallellisatie*. Een parallelle machine verdeelt de taak over zo veel mogelijk afzonderlijk opererende rekencellen. In plaats van een voor een de mogelijkheden te proberen, kunnen meerdere processoren dan wel systemen meerdere mogelijkheden tegelijkertijd uitproberen. Dit kan relatief eenvoudig gedaan worden door het *probleem* in stukken op te splitsen en aan verschillende systemen/processoren toe te wijzen. Zo kan men theoretisch bij het kraken van een wachtwoord van bijvoorbeeld 7 posities met een systeem met 4 processoren (SMP-systeem) de tijd van 17 jaar terugbrengen naar iets meer dan 17/4=4,25 jaar.

De methoden daarbij kunnen verschillen – het is mogelijk het werk tussen de cellen te coördineren om dubbelwerk te voorkomen (vergelijkbaar met de aanpak van het SETI-project) of het is mogelijk om elke cel willekeurige pogingen te laten wagen (zoals in een Chinese Loterij). In het laatste geval valt de te verwachten rekenklus tweemaal zo hoog uit, maar wel zonder enige vorm van overhead in het aansturen van de rekencellen.

Door het gebruik van parallellisatie komt extra rekenkracht om de hoek kijken doordat gegevens moeten worden opgesplitst en verdeeld en er onderlinge communicatie tussen de verschillende processen (programma's dan wel threads) plaats moet vinden. De rekenkracht moet dus opwegen tegen de complexiteit dan wel duur van het te behalen resultaat.

17.1.4 Beveiliging tegen bruteforce-aanvallen

Restricties

Zorg altijd dat er restricties gesteld worden aan het aantal loginpogingen per uur en per minuut. Bijvoorbeeld hooguit 45 per minuut, met een maximum van 150 per uur.

Salt

Bij hashes (MD5, SHA1, NTLM, enzovoorts), gebruik altijd een salt. Een salt, of zout in het Nederlands, vertroebelt de hash.

Als crackers of hackers de hash kennen van een aantal veelgebruikte wachtwoorden, en ze krijgen toegang tot een lijst met hashes, dan kunnen ze heel gemakkelijk de gebruikers met die veelgebruikte wachtwoorden er uit halen. Met een salt zal men voor elke gebruiker een willekeurige salt bijhouden, en deze samenvoegen met zijn of haar wachtwoord om de hash te berekenen. Hierdoor krijgen gebruikers met eenzelfde wachtwoord toch een andere hash.

Het werkt zo:

Even ervan uitgaand dat functies zo werken: uitkomst = functie (variabele), zou een md5-functie er zo uit kunnen zien:
hash = md5 (“abc”)
De uitkomst van md5(“abc”) is dan dus 900150983cd24fb0d6963f7d28e17f72. We zouden de salt op deze manier toe kunnen passen:
variable salt = “am1MAi1mDA*1msA__”
hash = md5 (salt + “abc”)
Dit zal de complexiteitsfactor van O(26^3) verhogen naar de complexiteitsfactor O(95^{20}). Ofwel, het verschil tussen 17576 pogingen en ~358485920000000000000000000000000000000 pogingen.
Waarom het grondgetal van 26 naar 95, en de macht van 3 naar 20?
Het grondgetal stelde de 26 letters van het alfabet voor. Er komen in het wachtwoord abc geen hoofdletters, cijfers of tekens voor, dus zijn er maar 26 mogelijkheden. Maar als er ook tekens in zitten wordt het opeens 95 karakters: 26 (kleine letters) + 26 (hoofdletters) + 10 (cijfers) + ~!@#$%^&*()_+-=[]\|}{;:<>?,./"'` (inclusief de laatste spatie) = 95.
Dan de macht van 3 naar 20, dit is de lengte van de gehashte tekenreeks. Eerst berekenden we de hash van abc (3 tekens), en met de salt berekenden we de hash van am1MAi1mDA*1msA__abc (20 tekens).

Een nog sterkere hash kan bereikt worden door de hash-functie meerdere malen uit te voeren op dezelfde tekenreeks. We gaan weer uit van dezelfde functiestructuur:
variabele salt = “am1MAi1mDA*1msA__”
hash = md5 (salt + “abc”) - in de variabele hash staat nu “d39faeb254034fdf0503bd33c6f509d9” -
hash = md5 (hash) - in de variabele hash staat nu “1ee5ce0c0ee2c7efe89af6f96c1f15df”, ofwel md5(“d39faeb254034fdf0503bd33c6f509d9”) -
Hierdoor zal een kraker dus eerst de tekst achter 1ee5ce0c0ee2c7efe89af6f96c1f15df moeten achterhalen, en vervolgens de tekst achter d39faeb254034fdf0503bd33c6f509d9 om bij het originele wachtwoord te komen.

Opmerking: niet alle hash-functies zijn veilig. Soms kunnen er collisions voorkomen, dit is als twee tekenreeksen dezelfde hash-uitkomst geven. Bijvoorbeeld (fictief voorbeeld) zou het kunnen zijn dat “nads91” dezelfde md5-uitkomst geeft als “m19d00amms”. Verouderde NTLM-hashes hebben ook een zwakte met lengte, maar dit is in nieuwere versies van Windows opgelost door een dubbele hash toe te passen. De kwetsbaarheid van korte hashes is zeer verminderde maten aanwezig met SHA1, maar deze techniek is langzamer, heeft een grotere uitkomst (24bits extra, wat toch wel uitmaakt op een database van miljoenen mensen) en wordt minder ondersteund door verschillende software. Echter MD5 is simpelweg de standaard, en is met een salt ruim voldoende beveiligd zolang er geen staatsgeheimen achter bewaard moeten worden.

Overigens, als er te veel bewerkingen worden uitgevoerd met een tekenreeks is het mogelijk dat een andere tekenreeks dus eenzelfde uitkomst geeft (ofwel een collision veroorzaakt). Weer een fictief voorbeeld: abc zou dezelfde uitkomst kunnen genereren als salt+"abc"+salt. De kans is ontzettend klein, maar wel aanwezig. MD5 staat als semi-veilig bekend vanwege deze reden. Toch moet u het algoritme ook niet als onveilig zien, over het algemeen geldt de regel “de beveiliging is zo sterk als het wachtwoord”.

Key stretching

Een andere methodiek die ter bemoeilijking van *brute force*-aanvallen kan worden ingezet, is het oprekken van een wachtwoord. Het oprekken van wachtwoorden werkt door versleuteling van wachtwoorden met een sterker salt-algoritme. Deze techniek noemen we key stretching. Voor het controleren van juistheid van een opgerekt wachtwoord moeten, afhankelijk van de gebruikte salt, minimaal een paar duizend rekenkundige operaties worden uitgevoerd. Deze ingebrachte complexiteit voor het controleren van een opgerekt wachtwoord werkt als een vertragende factor tijdens een *brute force*-aanval.

Key stretching kan ook enige bescherming bieden tegen het gebruik van *brute force* tegen aanvankelijk zwak gekozen wachtwoorden, omdat het vooraf laten berekenen en vastleggen van alle mogelijke hashes van wachtwoorden in sommige gevallen haast een onmogelijke taak is (zoals het samenstellen van rainbow tables). Bij gebruik van een 512-bits-salt zijn er bijvoorbeeld 2^{512} mogelijkheden voor ieder wachtwoord.

17.2 Zie ook

- British Museum-algoritme
- Rainbow table

Hoofdstuk 18

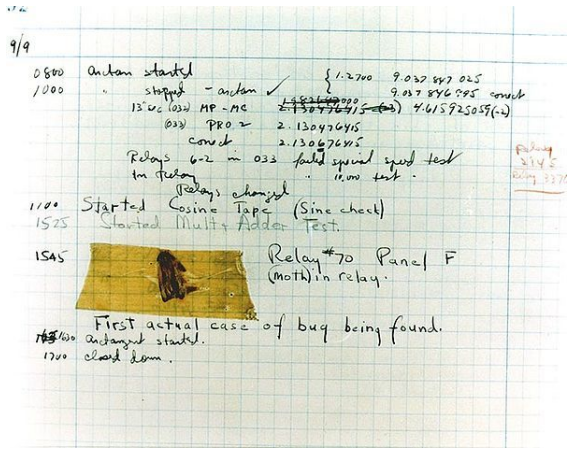
Bug (technologie)

Een **bug** is een fout in een computerprogramma of een website, waardoor het zijn functie niet (geheel) volgens specificaties vervult.

Praktisch alle programma's van enige omvang bevatten bugs, maar de meeste worden niet als storend ervaren of treden alleen onder zeldzame omstandigheden op. Een van de bekendste bugs (of eigenlijk een verzameling bugs die onder dezelfde omstandigheid tot uitdrukking kwam) was de millenniumbug. De millenniumbug is echter geen echte bug, maar een voorbeeld van slechte specificaties.

Het traceren en verwijderen van bugs wordt debuggen genoemd. Speciale software, de debugger, kan helpen bij het vinden van (de oorzaak van) een bug. Er bestaat ook hulpsoftware, vaak geïntegreerd in de ontwikkelomgeving, die verdachte constructies in de broncode kan signaleren voordat een fout in de werking van het programma tot uitdrukking komt.

18.1 De eerste bug



De "eerste bug"

De ontdekking van de eerste computerbug wordt wel (ten onrechte) toegeschreven aan Grace Murray Hopper. Zij werkte in 1947 op de Harvard University. Bij het zoeken naar de oorzaak van een storing in de *Mark II Aiken Relay Calculator* vond een van de operators een nachtvlinder in relais nummer 70 op paneel F. Dit insect werd in het logboek geplakt, met als bijschrift "first actual case of bug being found" (eerste echte vondst van ongedierte).

Volgens Grace Hopper zelf werd de term bug al gebruikt voor een storing in de radar tijdens de Tweede Wereldoorlog. In het Engels is het woord *bug* een algemene benaming voor ongedierte zoals kevers. Nadien vond men de term "debuggen" uit. Dit was het controleren of er geen ongedierte in de computer verscholen zat; later kreeg het de betekenis van het verwijderen van fouten uit programma-code.

Hawkin's New Catechism of Electricity (1896 Theo. Audel & Co.)zegt erover:

> *The term "bug" is used to a limited extent to designate any fault or trouble in the connections or working of electric apparatus.*

Zoekend naar de herkomst van de term schrijft dit boek:

> *said to have originated in quadruplex telegraphy and have been transferred to all electric apparatus.*

Thomas Edison schreef in een brief in 1878:

> *It has been just so in all of my inventions. The first step is an intuition, and comes with a burst, then difficulties arise — this thing gives out and* [it is] *then that 'Bugs' — as such little faults and difficulties are called — show themselves and months of intense watching, study and labor are requisite before commercial success or failure is certainly reached.*[1]

Het woord **bug** als term voor "fout" kan al ontstaan zijn in de 14e eeuw afgeleid van het Welsh woord *bwg* (Concise Oxford Dictionary of English Etymology).

Webster's 10th Collegiate Dictionary beschrijft het woord **bug** in de betekenis "an unexpected defect, fault, flaw, or imperfection" met bronnen teruggaand tot 1622.

18.2 In andere betekenissen gebruikt

De term bug wordt onder andere gebruikt voor semiautomatische seinsleutels sinds 1902. De fabrikant Vibroplex van seinsleutels had een kever in het logo. Ook afluistermicrofoontjes worden wel bugs genoemd.

18.3 Oorzaken

Een storing in de werking van een programma, ook wel goedmoedig “onbedoelde functionaliteit” genoemd, berust vaak op een fout van een programmeur. Zo'n fout kan uiteenlopende oorzaken hebben:

- misinterpretatie van de bedoelde werking van het te schrijven programma (-onderdeel);
- misinterpretatie van constructies of functies van de programmeertaal of -omgeving;
- misinterpretatie van de bedoelingen van een andere programmeur die eerder aan hetzelfde programma-onderdeel werkte;
- onvoldoende rekening houden met alle voorkomende (normale) invoer en omstandigheden;
- wijziging van onderdelen van een programma die gevolgen hebben voor de werking van andere delen van het programma zonder die andere delen daarop aan te passen;
- overnemen van fragmenten uit een ander (deel van hetzelfde) programma zonder de noodzakelijke aanpassingen;
- lees- en schrijffouten (verwisselen van letters die op elkaar lijken, verkeerde schrijfwijze waardoor een andere dan de bedoelde functie ontstaat);
- tikfouten (een andere toets raken dan de bedoelde).

Wanneer een programma (-onderdeel) anders wordt gebruikt dan volgens specificaties, kunnen storingen ontstaan die strikt genomen geen bugs zijn. Een spectaculair voorbeeld daarvan was de ramp met de Ariane 5-raket op 4 juni 1996, waarin software uit de (minder krachtige) Ariane 4 werd hergebruikt maar niet met alle daarvoor benodigde aanpassingen.

18.4 Trivia

- Schertsend worden bugs soms *undocumented features* (ongedocumenteerde eigenschappen) genoemd.

18.5 Zie ook

- Bufferoverloop
- Dode code

18.6 Externe links

- Effectief softwarestoringen melden

Hoofdstuk 19

Cloud computing

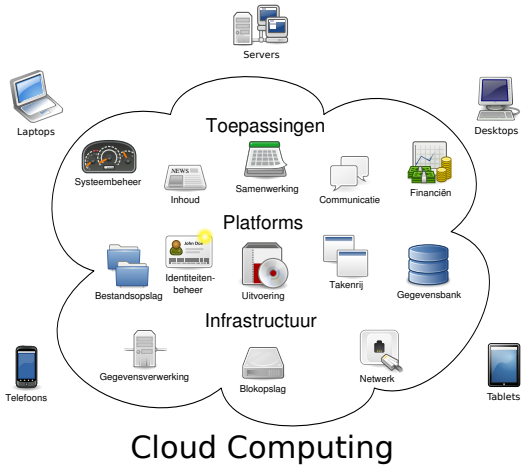


Diagram dat een globaal overzicht geeft van cloud computing.

Cloud computing is het via een netwerk – vaak het internet – op aanvraag beschikbaar stellen van hardware, software en gegevens, ongeveer zoals elektriciteit uit het lichtnet. De term is afkomstig uit de schematechnieken uit de informatica, waar een groot, decentraal netwerk (zoals het internet) met behulp van een wolk wordt aangeduid.

De *cloud* (Nederlands: wolk) staat voor een netwerk dat met al de computers die erop aangesloten zijn een soort 'wolk van computers' vormt, waarbij de eindgebruiker niet weet op hoeveel of welke computer(s) de software draait of waar die computers precies staan. De gebruiker hoeft op deze manier geen eigenaar meer te zijn van de gebruikte hard- en software en is dus ook niet verantwoordelijk voor het onderhoud. De details van de informatietechnologische infrastructuur worden aan het oog onttrokken en de gebruiker beschikt over een "eigen", in omvang en mogelijkheden schaalbare, virtuele infrastructuur. De cloud is dus een techniek waarmee schaalbare online diensten kunnen worden aangeboden. Zonder de mogelijkheid tot schalen heeft een aangeboden online dienst geen betrekking op cloud computing.

19.1 Geschiedenis

De term *cloud* is ontstaan samen met het concept van *packet switching*. Doordat de verzonden datapakketten niet meer over een vastgelegd traject gingen, wist men niet meer, en hoefde men niet meer te weten, welke weg ze volgden om aan hun eindpunt te komen. Sindsdien stelde men het netwerk voor als een wolk om aan te duiden dat men niet met zekerheid kon zeggen welke route binnen de wolk werd gevolgd. In *cloud computing* gaat het niet meer over verbindingswegen maar over infrastructuren. Sun Microsystems gaf als eerste invulling aan het concept met de slogan *"the network is the computer"* (het netwerk is de computer) en de introductie van software die het mogelijk maakte taken en gegevens over vele computers te verdelen, zoals het Network File System.

De eerste definitie werd in 1997 als volgt door Ramnath K. Chellappa geformuleerd: "Een computerparadigma waarbij de grenzen van de computer worden vastgesteld door het economische aspect eerder dan de technische limieten."[1]

Rond het jaar 2000 kwam SaaS erg sterk op. Salesforce.com bouwde technologieën van onder andere Google en Yahoo! om tot echte bedrijfstoepassingen. Microsoft breidde SaaS uit met webdiensten en Amazon moderniseerde zijn datacentra. Door deze spelers kende *cloud computing* een sterke toename.

In 2005 kwam Amazon op de markt met zijn webdiensten en in 2007 begonnen Google, IBM en enkele universiteiten met onderzoeksprojecten om informaticastudenten te trainen in de complexe techniek van *cloud computing*. Belangrijke aanjager van het succes van *cloud computing* is de mogelijkheid om de serveromgeving te virtualiseren. Het succes van *cloud computing* loopt dan ook synchroon met dat van virtualisatie, zoals geleverd door partijen als VMware, VirtualBox, Microsoft en Citrix.

In de eerste decennia van de computer werd gewerkt met mainframes (server) en terminals (clients). Men gaat met *cloud computing* terug naar dit concept met als grote verschil dat er geen centraal mainframe meer wordt gebruikt maar een gedistribueerd serverfarm.

19.2 Architectuur

De servers bieden verschillende niveaus van virtualisatie voor hun diensten. Deze zijn beschikbaar via het internet op elke computer die de clientsoftware (meestal een webbrowser) heeft.

De client is de computerhardware en/of -software van de gebruiker die verbinding maakt met de server en de gebruiker in staat stelt gebruik te maken van de dienstverlening (de software op de server).

19.3 Lagen

19.3.1 Cloudapplicaties: *software as a service (SaaS)*

Bij *software as a service* (SaaS) biedt de dienstaanbieder eindapplicaties aan “via de cloud”. Deze applicaties kunnen van allerlei soort zijn, bijvoorbeeld e-mail, klantenbeheer, personeelsbeheer, video-applicaties enz. De dienstaanbieder heeft de volledige controle over de applicaties, maar de klant of een derde partij die het beheer uitvoert voor de klant, kan in veel gevallen wel de applicatie configureren en functioneel beheren. In veel gevallen zijn de SaaS-applicaties te gebruiken via een webbrowser op een computer. Hierbij wordt er doorgaans gebruikgemaakt van moderne technologieën zoals Ajax en HTML5 om een interactieve functionaliteit te verkrijgen die vergelijkbaar is of beter is dan die van traditionele client-software. Veel SaaS-applicaties werken ook met mobiele apparaten zoals smartphones en tabletcomputers. Ook is er soms een specifiek stuk clientsoftware vereist en/of is de applicatie te gebruiken via een technische interface (API).

19.3.2 Cloudplatforms: *platform as a service* (PaaS)

De PaaS-laag biedt een aantal diensten boven op de infrastructuur die het SaaS-aanbieders mogelijk maken hun toepassingen op een gestructureerde en geïntegreerde wijze aan te bieden. Voorbeelden van diensten in deze laag zijn toegangsbeheer, identiteitenbeheer, portaalfunctionaliteiten en integratiefaciliteiten.

De klant van PaaS-diensten is een professionele, technische partij die voor het uitoefenen van zijn rol dan ook de nodige vrijheidsgraden moet hebben, binnen vastgelegde grenzen. In dit systeem wordt het framework en de infrastructuur beheerd door de dienstverlener en kan de gebruiker verder instaan voor de applicaties. Er is dikwijls ook sprake van faciliteiten voor de ontwikkeling. Hier wordt vaak gewerkt met een ontwikkelingstaal of framework zoals Python, .NET of Java waarin men functionaliteiten kan definiëren.

19.3.3 Cloud Infrastructure: *infrastructure as a service* (IaaS)

In deze laag wordt de infrastructuur aangeboden via een virtualisatie of hardware-integratie. In deze laag vindt men de servers, netwerken, opslagcapaciteit en andere infrastructuur. Dit laat de gebruiker volledige vrijheid toe over de hardware. Hier is dus ook kennis nodig over de drie lagen en het onderhoud ervan. De cloudserver kan dan ook worden bediend vanaf een externe locatie door meerdere personen.

19.4 Typen

19.4.1 Publiek

In de traditionele zin van *cloud computing* werkt men publiek of extern. De software en data staan dan volledig op de servers van de externe dienstverlener en er wordt een generieke (voor alle afnemers gelijke) functionaliteit geleverd.

19.4.2 Privaat

Met private 'cloud' werkt men op een (virtueel) private ICT-infrastructuur. In deze wolk heeft de gebruiker volledige controle over data, beveiliging en kwaliteit van de dienst. De applicaties die via de Private Cloud beschikbaar worden gemaakt, maken gebruik van gedeelde infrastructuurcomponenten die worden ingezet voor meerdere afnemers (bijvoorbeeld afdelingen van een bedrijf), maar worden zelf niet gedeeld met andere klanten. De verantwoordelijkheid voor het onderhouden van de private cloud kan worden uitbesteed aan een professionele leverancier van ICT-diensten. De fysieke locatie van de infrastructuurcomponenten kan zowel de cloudleverancier als de klant zelf zijn.

19.4.3 Gemeenschappelijk

Bij een gemeenschappelijke cloud werken afnemers uit meerdere organisaties op dezelfde infrastructuur. Als deze organisaties elkaar voldoende vertrouwen en vergelijkbare eisen stellen combineert een gemeenschappelijke cloud een gedeelte van de schaalvoordelen die een publieke cloud heeft, terwijl tegelijkerijd de vertrouwelijkheid van een private cloud wordt bereikt. Een voorbeeld van een groep organisaties die een gemeenschappelijke cloud zouden kunnen benutten is een groep overheden (gemeentes, provincies etc.), die vanwege het werken met persoonsgegevens vergelijkbare eisen aan vertrouwelijkheid hebben waaraan een publieke cloud niet kan voldoen, maar waarbij het meermaals optuigen van een private cloud tot onnodige kosten zou leiden.

19.4.4 Hybride

Als meerdere interne en/of externe clouds samen worden gebruikt wordt er gesproken van een hybride cloud.

19.5 Risico's en bezwaren

Volgens juristen en IT-kenners kleven er diverse bezwaren aan het "zomaar" uitbesteden van diensten die vertrouwelijke informatie kunnen bevatten.

19.5.1 Europese privacywetgeving

Europese regelgeving stelt diverse eisen aan de opslag van data. Het is de verantwoordelijkheid van bedrijven om ervoor te zorgen dat de data van dat bedrijf die (mogelijk) vertrouwelijke gegevens bevatten van medewerkers en klanten op een veilige manier worden opgeslagen. Een bedrijf kan aansprakelijk gesteld worden als vertrouwelijke gegevens uitlekken en het bedrijf moet dan kunnen aantonen dat het afdoende maatregelen heeft getroffen om dat te voorkomen. Zolang een bedrijf de data op zijn eigen infrastructuur in eigen datacentra opslaat is dat vrij eenvoudig te doen, maar als men gebruikmaakt van online clouddiensten heeft men zelf geen controle over de locatie en manier waarop de data worden opgeslagen. In dat geval is men afhankelijk van de aanbieder van clouddiensten.

Om in te spelen op Europese regelgeving bieden dienstenaanbieders opties aan om te garanderen dat er alleen gebruikgemaakt wordt van opslagfaciliteiten in een EU-land.[2]

19.5.2 Amerikaanse Patriot Act

De Patriot Act is Amerikaanse wetgeving gericht op het bestrijden van terrorisme. Op grond van deze wetgeving bezitten de Amerikaanse overheid en overheidsinstanties vergaande bevoegdheden, onder meer ten aanzien van forensisch onderzoek. Dat impliceert onder meer dat Amerikaanse organisaties en bedrijven verplicht zijn om toegang te verlenen op infrastructuur, zoals servers en netwerken. Ook bedrijfsonderdelen buiten het Amerikaanse grondgebied moeten medewerking verlenen aan onderzoek. Dat betekent concreet dat Amerikaanse cloudproviders niet kunnen garanderen dat gegevens in bijvoorbeeld Europa niet door Amerikaanse overheidsdiensten gecontroleerd kunnen worden[3]. Om die reden zou het voor Europese instanties verboden kunnen zijn om een Amerikaanse cloudprovider te kiezen[4].

19.5.3 Sarbanes-Oxley-wetgeving

Ook de Sarbanes-Oxley-wetgeving in Amerika kan een probleem zijn voor de implementatie van cloud-computing en *SaaS*-diensten. Er zijn gespecialiseerde bedrijven die organisaties kunnen adviseren op het gebied van deze potentiële gevaren.

Net als bij alle SaaS- en cloud-computingdiensten, zijn er mogelijke bezwaren: men moet goed beseffen dat het uit handen geven van vertrouwelijke gegevens niet zonder risico is. Diverse IT-specialisten en -juristen hebben gepubliceerd over de potentiële gevaren van deze diensten.[5]

In dit verband moet nog worden opgemerkt, dat aan de uitbesteding van de dienst, op het gebied van beveiliging en risico's, ook voordelen zijn verbonden. Doordat de betreffende gegevens niet binnen de eigen organisatie worden vastgelegd en beheerd, wordt daarmee het risico van interne manipulatie, vervreemding of misbruik verminderd. Dit moet dan worden afgewogen tegen de risico's van externe opslag.

19.6 Karakteristiek

- De betrouwbaarheid wordt wel betwist omdat de software op de servers van de dienstverlener staat. Die staat ook in voor de werking en eventuele correcties van fouten en bugs. Als er toch iets mis gaat, zijn de gebruikers echter volledig machteloos tot de dienstverlener het probleem oplost. Daar staat echter tegenover dat de serviceprovider meestal over gespecialiseerde deskundigen beschikt om eventuele verstoringen op te lossen. Vaak zal bij een dergelijke serviceprovider meer expertise aanwezig zijn dan bij de afnemer. In de praktijk kan dit betekenen, dat complexere problemen bij de serviceprovider eerder zijn opgelost dan wanneer de dienst bij de afnemer in een 'eigen' datacenter zou draaien. Om de betrouwbaarheid verder te verbeteren kan worden gekozen om de diensten in meerdere datacentra van de dienstverlener te laten draaien of door bijvoorbeeld meerdere dienstverleners in te schakelen. De belangrijkste zwakke schakel die dan nog overblijft is de (internet)verbinding.
- Men is niet gebonden aan een apparaat of locatie, aangezien de gebruiker vaak enkel een webbrowser en internetverbinding nodig heeft. Als er toch een speciale applicatie nodig is, is deze vaak van klein volume en gratis te downloaden via de dienstverlener.
- De kostprijs wordt bepaald door het abonnement of de gebruikte diensten. Dit drukt de vaak hoge aankoopkosten voor software en de hardware die de software moet kunnen gebruiken
- De infrastructuur kan zeer flexibel worden ingezet.

Vanwege het verhuurmodel en de grote hoeveelheid aanwezige capaciteit kan de infrastructuur binnen enkele minuten worden ingericht en op uurbasis worden ingezet.

- De diensten kunnen eenvoudig schaalbaar worden gemaakt, omdat cloudleveranciers over zeer veel capaciteit beschikken in zowel hardware als netwerkverbindingen. Hoe het opschalen precies werkt is afhankelijk van de cloud-leverancier. Soms moet men het opschalen zelf automatiseren, soms is het opschalen in het cloudplatform ingebouwd.
- De beveiliging wordt vaak ook geregeld door de dienstverlener en is vaak even goed of beter dan een privégebruiker zelf kan regelen.
- Als beveiligingsrisico wordt wel genoemd de *afgeleide* kwetsbaarheid bij een aanval door derden op het netwerk van de serviceprovider (DDoS-aanval). Hoewel een dergelijke aanval dus niet direct op de afnemer van de dienst is gericht, bestaat er de mogelijkheid dat de afnemer toch door een dergelijke aanval wordt getroffen. Uiteraard is het aan de serviceprovider zich voldoende tegen dergelijke aanvallen te beschermen.
- De reactiesnelheid van de software is eerder afhankelijk van de internetverbinding dan van de computer van de gebruiker.
- Juridische aspecten zijn er onder andere op het gebied van het eigendom van de data en applicaties. Veel landen hebben regels met betrekking tot waar data opgeslagen moet worden en hoelang het bewaard moet worden. Dit is nog lastig af te dwingen.

19.7 Externe links

- Inleiding tot *cloud computing*
- Concept en definitie
- Microsoft Cloud Computing
- Video's Cloud Computing

Hoofdstuk 20

Computer

Apple II, een van de eerste personal computers

Een **computer** is een apparaat waarmee gegevens volgens formele procedures (algoritmen) kunnen worden verwerkt. Meestal wordt met het woord computer een elektronisch, digitaal apparaat bedoeld, maar er bestaan ook mechanische en analoge computers. Daarnaast kan een computer in verschillende getalstelsels zoals het decimale (tientallige) of binaire (tweetallige) stelsel werken. De huidige computers werken alle in het binaire stelsel.

De genoemde procedures liggen vast in een of meer programma's, software genoemd, die door de gebruiker gewisseld kunnen worden. Zijn de programma's niet verwisselbaar, dan spreekt men niet over een computer maar over een controller of processor.

Oorspronkelijk werd het Engelse woord *computer* gebruikt om iemand mee aan te duiden die gecompliceerde berekeningen uitvoerde, met of zonder mechanische hulpmiddelen – vergelijk ook de Duitse term voor computer: *Rechner* (rekenaar), de Afrikaanse term voor computer: *rekenaar* en de niet-ingeburgerde Nederlandse variant *rekenaar*. Moderne computers worden voor veel meer gebruikt dan alleen wiskundige toepassingen. Ook veel administratieve en financiële taken worden aan de computer opgedragen, het Franse woord voor computer was eerst *calculateur* of rekenaar en evolueerde naar *ordinateur*, letterlijk iets wat ordent en regelmaat aanbrengt.

De wetenschap die tegelijk met de ontwikkeling van de computer is ontstaan, is de informatica.

Computers zijn in te delen in een aantal types. Zo zijn er supercomputers, grote computers (of mainframes), minicomputers, persoonlijke computers en spelcomputers. Dit lemma gaat hoofdzakelijk over de laatste twee types.

Sinds de grote opkomst van de computer worden zij ook gebruikt voor informatievoorziening (internet) en amusement. Bij de moderne productie worden computers geïmplementeerd om machines mee te besturen en om processen mee aan te sturen, bijvoorbeeld bij de assemblage van auto's door robots. Doorgaans wordt hiervoor een programmable logic controller gebruikt.

Door de verregaande miniaturisering en snelheidsvergroting is het steeds vaker mogelijk functionaliteit die voorheen in hardware werd aangebracht softwarematig te implementeren. Het grote voordeel van een dergelijke ontwikkeling is dat achteraf functionaliteit kan worden toegevoegd.

In 1980 introduceerde IBM zijn Personal Computer: de IBM-PC. Dit in navolging van eerdere initiatieven, zoals de Altair 8800, Tandy TRS-80, Apple II en Commodore PET-computers en de homecomputers. De IBM-compatible pc vormde echter uiteindelijk de standaard (met tegenwoordig als enige uitzondering de Mac), nadat vele fabrikanten de computer goedkoop kloonden en zodoende het ontwerp standaardiseerden. Inmiddels speelt de pc in het dagelijks leven van veel mensen een essentiële rol.

20.1 Opbouw

De opbouw van de computer is voor te stellen in lagen.

1. De elektronica waaruit de computer grotendeels bestaat wordt meestal aangeduid met hardware (dat overigens in het Engels een veel bredere betekenis heeft).

2. Om deze hardware aan te sturen wordt een computer bij het opstarten automatisch geladen met de meest basale software, die nodig is om onder andere de schijfconfiguratie te bepalen, en om te bepalen van welke schijf het besturingssysteem moet worden geladen. Deze laag wordt ook wel firmware genoemd, en staat in de pc-wereld bekend als BIOS. Op andere platforms heeft deze code een andere naam, bijvoorbeeld *microcode* in een IBM System i, MacROM op de Apple Macintosh en Open Firmware op de latere Macs. Na het laden van deze firmware is de computer gereed om een besturingssysteem te laden. En op de huidige Intelmacs wordt er gebruikgemaakt van EFI, de opvolger van de BIOS.

3. De kern van het besturingssysteem heeft als belangrijkste functies het beheren van het werkgeheugen, het verdelen van de processortijd, het beheren van het interne gegevenstransport, het uitvoeren van programma's, en het verzorgen van een of meer invoer- en uitvoermechanismen. Het besturingssysteem voorziet daarnaast de computer van een werkomgeving waarin allerlei faciliteiten ter beschikking worden gesteld. De meningen lopen uiteen over wat een besturingssysteem moet bevatten, zo vindt Microsoft dat een internetbrowser ingebakken moet zijn, vindt Sun dat een JVM onontbeerlijk is, en vindt IBM dat OS/400 een ingebouwde database moet hebben. In ieder geval bevat een besturingssysteem faciliteiten om het vaste geheugen (harddisks) te beheren, en om programma's uit te voeren.

4. De scheiding tussen functies van een besturingssysteem en de onderdelen van de applicatiesoftwarelaag is dus vaag. Onder applicatiesoftware wordt verstaan de programmatuur die wordt gemaakt of aangeschaft om de specifieke functies uit te voeren waarvoor de computer is aangeschaft. Denk hierbij aan boekhoudprogramma's, tekstverwerkers, CRM-software, salarisadministratie en verkoopsystemen, maar ook aan webservers, printerdrivers en allerlei andere hulpprogramma's.

20.2 Hardware

Onder hardware wordt verstaan "alle tastbare onderdelen in en aan de computer". Er wordt onderscheid gemaakt tussen interne en externe hardware. Interne hardware zit in de behuizing van de computer. Externe hardware (randapparatuur) wordt aangesloten op een van de poorten op de computer.

Veel hardware wordt volgens bepaalde standaarden gemaakt, vooral binnen het segment van de pc. Regelmatig wordt een standaard vervangen door een verbeterde versie, waardoor oudere apparatuur niet altijd meer uitwisselbaar is met nieuwere. Dit kan een reden zijn om een computer volledig te vervangen. De historie kent enkele voorbeelden van verouderde hardware.

- Diskette - een opslagapparaat dat bestaat uit een dunne schijf van een flexibele magnetische opslagmedium met een harde plastic hoes die de schijf beschermt van deuken.

- Iomega ZIP drive - een medium capaciteit verwisselbare schijf-opslagsysteem, geïntroduceerd door Iomega in 1994.

20.2.1 Pc

Een voorbeeld uit de praktijk van de pc: de muis werd in de jaren 80 meestal aangesloten op de seriële poort en de printer op de parallelle poort. Beide poorten konden ook gebruikt worden om te communiceren met een andere computer. De aansluiting voor de muis en het toetsenbord zijn later vervangen door de PS/2-interface. Tegen het einde van de jaren 90 werden muizen uitgerust met een USB-verbinding. Ook de printer, die de afgelopen jaren sterk verbeterd is, werkt tegenwoordig meestal via een USB-poort, hoewel sommige printers ook nog op de parallelle poort aangesloten kunnen worden. Muizen die op de seriële poort aangesloten kunnen worden, zijn tegenwoordig een zeldzaamheid. Communiceren met andere computers gebeurt tegenwoordig bijna uitsluitend in netwerken, met ook hier weer een beperkt aantal standaarden.

20.2.2 Overige architecturen

Andere architecturen dan de pc (zoals de Sun SPARC, IBM RS/6000 of SGI), hebben vaak eigen standaarden. Ook deze zijn uiteraard aan verandering onderhevig. Wel ziet men steeds vaker dat standaarden *geharmoniseerd* worden en dat apparatuur daardoor met vrijwel alle typen computers kan werken. Een voorbeeld hiervan is de USB.

Het overwicht van de Intel-architectuur betekent ook dat voor veel computermerken Intel de *de facto*-standaard wordt. Zo werd in 2006 voor het eerst een Apple Apple Macintosh op de markt gebracht met een Intel x86-gebaseerde-architectuur en is de Intel-architectuur bij SUN, HP en IBM de leiding aan het nemen.

20.3 Geschiedenis

20.3.1 Mechanische computers

De geschiedenis van de computer begint met de geschiedenis van het rekenen. Vanouds hebben mensen hulpmiddelen ontwikkeld voor berekeningen die niet gemakkelijk uit het hoofd gemaakt konden worden, zoals de kerfstok en het telraam (abacus). Toen de behoefte aan berekeningen steeds complexer werd ontwikkelde men tabellen met hulpgegevens (bijvoorbeeld logaritmetabellen als hulp bij het vermenigvuldigen). Ook de rekenliniaal was een uitvinding om het rekenen makkelijk te maken.

Als er zeer veel gerekend moest worden werden veel mensen ingezet. Deze zaal met rekenaars werd dan ook aangeduid met het woord computer. In het Verenigd Koninkrijk waren naar aanleiding van de koloniale scheepvaart veel centra met menselijke computers ontstaan. Deze maakten tabellen die voor navigatie konden worden gebruikt. Ook in andere gebieden vonden deze tabellen gretig aftrek, zoals de astronomie.

Charles Babbage, een wiskundige, vroeg zich af of de tabellen niet machinaal gegenereerd konden worden. Hiervoor bedacht hij in 1822 de "differentiemachine" (*differential engine*): een concept voor een machine die tabellen van veeltermen kon uitschrijven. De machine werkte mechanisch en de tandwieltechniek was nog niet geavanceerd genoeg om tot een goed resultaat te komen. Verder veranderde Babbage steeds het ontwerp van de machine.

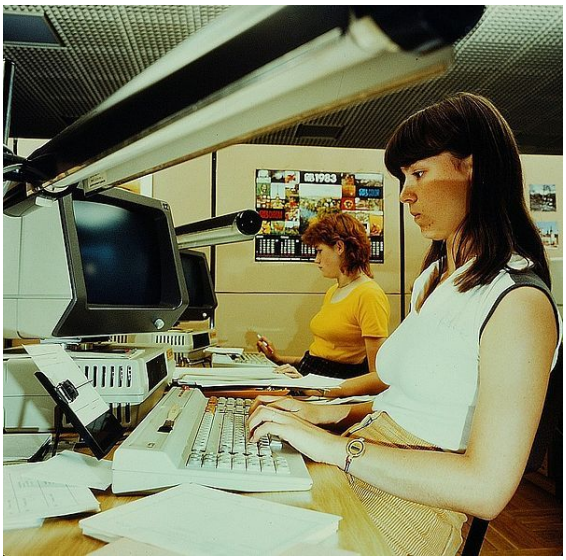
Aldus kwam hij in 1833 met de "analytische machine" (*analytical engine*). Deze machine zou met invoer vanaf ponskaarten wiskundige bewerkingen kunnen uitvoeren. Deze machine wordt algemeen gezien als het concept van de computer, maar is nooit gebouwd.

Wel zijn er (nog tot in de tweede helft van de twintigste eeuw) vele mechanische rekenmachines gebouwd en gebruikt. Een van de eerste ontwerpen (1645) was van de hand van Blaise Pascal. Omdat deze machines niet programmeerbaar waren, noemt men ze in het algemeen geen computer.

Pas in 1938 bouwde de Duitse fysicus Konrad Zuse de eerste computer, de Z1. Ook Zuses machine werkte nog mechanisch, maar Zuse had het zichzelf een stuk eenvoudiger gemaakt door van het binaire stelsel gebruik te maken. Enkele jaren later bouwde Zuse de eerste volledig functionele elektromechanische computer, de Z3.

20.3.2 Elektronische computers

Door de Tweede Wereldoorlog kreeg de ontwikkeling van computers een snelle vlucht. In het Verenigd Koninkrijk werd van de Colossus gebruikgemaakt om Duitse geheime codes te kraken, onder andere die van de Enigma-codeermachine. De Colossus was de eerste elektronische computer, gebruikmakend van elektronenbuizen. De eerste computer in de VS was de ENIAC, die enkele klaslokalen in beslag nam. De eerste computer in Nederland was de ARRA bij het Mathematisch Centrum. De eerste computer in een commerciële omgeving was de Miracle, een Ferranti Mark I bij het Shell-laboratorium in Amsterdam. In de periode dat het permanente geheugen (de harde schijf) nog niet algemeen bestond, was het invoeren van gegevens of programma's in een computer vrij moeizaam. Dit gebeurde oorspronkelijk met schakelaartjes en ponsband, nog iets later met ponskaarten, en in een nog later stadium met magneetbanden.



Vrouw gebruikt computer voor haar werk (1983)

De computers in de jaren 1950-1980 waren vooral mainframes: zeer grote computers, waar honderden tot duizenden gebruikers gelijktijdig op konden werken. Vooral banken en verzekeringsmaatschappijen gebruikten zulke mainframes op grote schaal. De mainframe was verbonden met de gebruikers via een simpele applicatie op een bureaucomputer (vroeger ook wel via een zogenaamde *domme* terminal). De mainframe is met de komst van de kleine computers nog niet volledig uitgestorven en wordt nog steeds gebruikt door professionele instellingen. De bekendste bouwer van mainframes is IBM.

20.3.3 Miniaturisatie

Met de enorme ontwikkeling van de elektronica en de halfgeleiders, toegepast in transistoren, kon de computer veel kleiner en sneller worden. Later werden de transistors geïntegreerd in een geïntegreerde schakeling. De microprocessor is zo'n geïntegreerde schakeling. Hoewel microprocessor-gebaseerde computers zoals de Commodore PET (Personal Electronic Transactor) en de Apple II al vanaf het midden van de jaren zeventig opgang deden, was de IBM PC uit 1981 het eerste systeem dat expliciet met de naam personal computer op de markt werd gebracht. De pc werd steeds goedkoper en gemakkelijker

te gebruiken waardoor steeds meer bedrijven en huisgezinnen er een kochten. De ontwikkelingen gaan voort, zakenmensen gebruiken veelal een laptop om met hun computer op stap te gaan. De steeds verdere miniaturisering leidde ertoe dat de kleine Personal Digital Assistant (pda) met steeds meer mogelijkheden in beeld kwam. Ook veel apparaten zoals wasmachines, auto's, digitale camera's en dergelijke bevatten tegenwoordig een computer om allerlei zaken te regelen, deze worden dan meestal een ingebed systeem of - in het Engels - embedded system genoemd.

20.4 Computertoepassingen

Tegenwoordig worden computers op het werk veelal aangesloten op een computernetwerk, waarbij verschillende gebruikers met een eigen pc gebruikmaken van software en data die op een centrale opslagplaats (server) zijn opgeslagen. Voor het ophalen van bestanden van internet wordt meestal een breedbandverbinding gebruikt en in een heel enkel geval nog een modeminbelverbinding. Breedbandverbindingen zijn naast goedkoper ook vele malen sneller dan inbelverbindingen. Een voorbeeld van een breedbandverbinding is: computernetwerk, een router, die is gekoppeld aan een breedbandinternetverbinding zoals DSL, kabel, E1, T1 of glasvezel. In het geval van een groot computernetwerk wordt vaak gebruikgemaakt van een proxyserver om de gegevens van het internet te "filteren".

Een toepassing van computers die nog sterk in opkomst is, is die van de kunstmatige intelligentie, welke toegepast wordt in onder andere computerspellen en de robotica.

Thuis worden computers veel gebruikt om computerspellen te spelen, informatie via internet op te zoeken en voor communicatie door middel van e-mail, chatten (een veel gebruikt programma hiervoor is Windows Live Messenger) en internetforums. Ook telefoneren via het internet is tegenwoordig in opkomst. Een veelgebruikte applicatie hiervoor is Skype. De huidige generatie computers is ook uitstekend te gebruiken om digitale foto- en videobestanden te bewerken. Veel mensen gebruiken de computer ook voor correspondentie, hun administratie of als mediacenter voor het afspelen van muziek of bekijken van foto's.

In het onderwijs wordt de computer gebruikt voor het opzoeken van informatie en tekstverwerking voor het maken van huiswerk zoals werkstukken en verslagen. Steeds meer studenten gebruiken een laptop.

20.5 Zie ook

- Personal computer
- Informatica
- Netwerk
- Lijst van computerpioniers
- Hobby Computer Club
- Computerkast
- IBM PC-compatibel

20.6 Externe link

- (en) Website met computertermen

Hoofdstuk 21

Computercriminaliteit

Computercriminaliteit, **cybercriminaliteit** of **cybercrime** is criminaliteit met ICT als middel én doelwit.[1] De meeste telefoons en bankpassen bevatten computerchips, die kunnen eveneens worden gemanipuleerd door cybercriminelen. Maar ook bedrijfssystemen, moderne auto's en chipkaarten zijn vatbaar voor cybercrime. Voor het plegen van cybercriminaliteit gebruiken criminelen speciale apparatuur en software. Daarom hanteert de politie voor de opsporing van cybercriminaliteit op haar beurt ook geavanceerde middelen en technieken.

Cybercriminaliteit betreft onder andere terrorisme, fraude en kinderporno en duikt sinds de jaren tachtig op wegens de doorbraak van de communicatie- en informatietechnologie. In 2001 ondertekenden de lidstaten van de Raad van Europa, de Verenigde Staten, Canada, Japan en Zuid-Afrika het zogenaamde cybercrimeverdrag of, in het Engels de *Convention on Cybercrime*.

21.1 Definitie

Computercriminaliteit kan zowel in brede als in enge zin gedefinieerd worden.

- Computercriminaliteit in brede zin betreft misdrijven waarbij computers of netwerken een rol spelen.
- Computercriminaliteit in enge zin betreft misdrijven die niet zonder tussenkomst of gebruik van computers of netwerken gepleegd kunnen worden.

Bij de brede definitie is de rol van computers of netwerk een onderdeel van het misdrijf. Het nadeel is het feit dat er onbedoeld allerlei 'gewone' misdrijven van toepassing zijn, doordat die toevallig met een computer gepleegd zijn. Bij het inbreken in een computernetwerk is het gebruik van ICT essentieel, dit is niet mogelijk zonder computers en netwerken. Ook het verstoren van de werking van een computer of het vernielen van elektronische gegevens wordt beschouwd als computercriminaliteit.

Computercriminaliteit wordt ook omschreven als het gebruik van cyberspace voor criminele doeleinden. Dit is echter een te beperkte omschrijving.

21.2 Voorbeelden

Computercriminaliteit kent vele vormen. Vaak worden deze vormen aangeduid met de voorvoeging van "cyber" of de letter "e", bijvoorbeeld cyberpesten of e-fraude.

Voorbeelden van computercriminaliteit zijn:

- Computervredebreuk: ongeoorloofd toegang verschaffen tot een computersysteem;
- Het kopiëren van vertrouwelijke gegevens;
- Ongeoorloofd computerdata verwijderen of aanpassen;
- Ongeoorloofd computersystemen uitschakelen of onbruikbaar maken;
- Het versturen van virussen;
- Fraude met behulp van computers en valsheid in geschrifte met betrekking tot computerdata, bijvoorbeeld door berichten te onderscheppen en te veranderen zoals met een man-in-the-middle-aanval;
- Het valselijk beschuldigen of bedreigen via een sociaal netwerk of e-mail.

21.3 Wetgeving

21.3.1 België

Het Belgisch recht wordt bepaald door de Wet van 10 april 1990 tot Regeling van de Private Veiligheid, gewijzigd door de wetten van 18 juli 1997, 9 juni 1999, 10 juni 2001 en 7 mei 2004. Vanaf de millenniumwisseling ontstond aandacht voor computercriminaliteit, met als gevolg de invoering van de Wet van 28 november 2000 inzake informaticacriminaliteit.

De wet beschrijft vier misdrijven die betrekking hebben op computercriminaliteit:

- Valsheid in informatica: Dit is het wijzigen of wissen van gegevens in een informaticasysteem of het

gebruik van die gegevens veranderen, zodat de juridische draagwijdte verandert.

- Informaticabedrog: Informaticabedrog is met bedrieglijk opzet zichzelf of iemand anders onrechtmatig verrijken via datamanipulatie. Het gaat om de manipulatie van een toestel. Bij internetfraude manipuleert men personen.
- Informaticasabotage: Informaticasabotage is te omschrijven als vandalisme in een informaticaomgeving. Het verschil met informaticabedrog is dat dit geen verrijking tot gevolg hoeft te hebben: gegevens zonder toestemming wijzigen, is op zichzelf een misdrijf. Van informaticasabotage is sprake als iemand opzettelijk een virus in omloop brengt en als iemand de klantengegevens van een concurrent vernietigt zonder er zelf financieel voordeel uit te halen. Ook het ontwikkelen en verspreiden van datasabotagetools is strafbaar. De wetgever viseert vooral virusbouwers.
- Hacking: Hacking is het ongeoorloofd binnendringen in een computersysteem.

In 2001 werd het verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (cybercrimeverdrag) ondertekend door 38 staten, waaronder België. Sinds 2001 is in het Belgische Strafwetboek een nieuw hoofdstuk van toepassing: “Boek II, Titel IXbis: misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en van de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen”.

21.3.2 Nederland

De Nederlandse wetgeving op het gebied van computercriminaliteit is tot stand gekomen vanaf de jaren 1980 en is sindsdien herhaaldelijk aangepast.

Met de Wet computercriminaliteit, in werking getreden op 1 maart 1993, is het Wetboek van Strafvordering aangevuld met bevoegdheden op het gebied van onderzoek van geautomatiseerde werken en zijn specifieke strafbepalingen, zoals computervredebreuk toegevoegd aan het Wetboek van Strafrecht.

De eerste voorstellen om de vorige wet aan te passen, dateerden al uit 1998, maar de wetswijzigingen liepen nogal wat vertraging op. In 1999 werd een wetsvoorstel Computercriminaliteit II ingediend bij de Tweede Kamer, met diverse aanpassingen en uitbreidingen. De behandeling van dit wetsvoorstel werd echter opgeschort omdat binnen de Raad van Europa het verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (cybercrimeverdrag) werd ontwikkeld, dat op 23 november 2001 door dertig landen werd ondertekend en dat op 1 juli 2004 van kracht werd voor de deelnemende landen. Het verdrag werd door Nederland op 23 november 2001 ondertekend en op 16 november 2006 geratificeerd, en voor Nederland op 1 maart 2007 in werking getreden. Tegelijk met dit wetsvoorstel was een wetsvoorstel ter implementatie van de verdragsbepalingen op 22 maart 2005 bij de Tweede Kamer ingediend, als nota van wijziging bij het wetsvoorstel Computercriminaliteit II en gebaseerd op een eerder ontwerpvoorstel Aanpassing aan het Cybercrimeverdrag uit februari 2004. De Wet computercriminaliteit II werd op 30 mei 2006 aangenomen door de Eerste Kamer en trad, met uitzondering van één artikellid, in werking op 1 september 2006.

Trb. 2002, 18 bevat op de even pagina’s de Engelse tekst en op de oneven pagina’s de Franse tekst; vervolgens in het Nederlands gegevens zoals de lidstaten die het verdrag hebben ondertekend en de vindplaatsen in het Tractatenblad van aangehaalde verdragen. Trb. 2004, 290 meldt de wijziging van de Engelstalige titel van *Convention on Cyber-Crime* in *Convention on Cybercrime*. Vervolgens bevat het de Nederlandse vertaling van het verdrag en een update van de partijgegevens, waaronder ook ratificaties en in het Engels “Verklaringen, voorbehouden en bezwaren”.

Verder is er de Rijkswet van 1 juni 2006 tot goedkeuring van het op 23 november 2001 te Boedapest tot stand gekomen Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, 18) (Stb. 299), behandeld als kamerstukdossier 30 036 (R 1784).

Trb. 2007, 10 zet de verwijzingen op een rij, en geeft weer een update van de partijgegevens.

Sindsdien is de wet ingrijpend aangescherpt. Zo is de definitie met betrekking tot hacken flink uitgebreid. Het expliciet toepassen van denial-of-service is vanaf deze datum verboden. De regels die gaan over het afluisteren en aftappen van communicatie en het kraken of hacken van beveiligde diensten (zoals betaaltelevisie) zijn ook aangescherpt. Het afluisteren van netwerkverkeer is strafbaar gesteld. Een uitzondering is het door middel van een radio-ontvanger ontvangen van radiosignalen, het ontvangen van vrije signalen uit de ether is immers een Europees grondrecht. Wordt echter “een bijzondere inspanning” geleverd, of een niet toegestane ontvanginstallatie gebruikt, dan is er toch sprake van strafbaar afluisteren.

De belangrijkste wijzigingen zijn:

- Bij computervredebreuk is elke vorm van wederrechtelijk binnendringen strafbaar, ook als daarbij geen beveiliging wordt doorbroken.
- De definitie van virussen en malware is aangescherpt: een programma moet bedoeld zijn om de definitie van schade aan te richten, maar niet per se (zoals in de oude wet) “door zichzelf te vermenigvuldigen in een geautomatiseerd werk”.
- De maximale straf voor veel delicten is verhoogd.

Hierdoor kan een verdachte in voorlopige hechtenis worden genomen. Verder zijn de meeste vormen van computercriminaliteit nu ook strafbaar in Nederland wanneer een Nederlander ze in het buitenland begaat. Dit is een gevolg van het cybercrimeverdrag.

- Uitbreiding van het delict grooming met het geval van een lokpuber.

Aanhangig is het wetsvoorstel *Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)*.[2][3] Het wetsvoorstel regelt vier onderwerpen:

- Onderzoek in een geautomatiseerd werk ingeval van verdenking van een ernstig strafbaar feit, ten behoeve van bepaalde doelen op het gebied van de opsporing. Bij communicatie met versleuteling kan dan worden afgetapt en opgenomen op het geautomatiseerde werk, voordat de gegevens worden versleuteld of nadat ze zijn ontsleuteld. In het belang van het onderzoek gebeurt een en ander heimelijk zodat de verdachte niet op de hoogte komt van het feit dat de politie in hem is geïnteresseerd. Het betreft onder meer een nieuw artikel 125ja Sv in de zevende afdeling, Doorzoeking ter vastlegging van gegevens (art. 125i t/m 125o Sv), van Titel IV, Eenige bijzondere dwangmiddelen (art. 52 t/m 126fa Sv), van het Eerste Boek, *Algemeene bepalingen* (art. 1 t/m 138d Sv).
- Herziening van de bestaande regeling van artikel 54a Sr over het ontoegankelijk maken van gegevens.
- Strafbaarstelling van het wederrechtelijk overnemen en 'helen' van gegevens.

21.3.3 Raad van Europa

1. Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (cybercrimeverdrag)

   Inwerkingtreding: 1 juli 2004

   Status: geldt voor alle landen die het verdrag hebben geratificeerd

2. Additioneel protocol

   Inwerkingtreding: 1 maart 2006

   Inhoud: strafbaarstelling van racistische en xenofobe uitingen via computersystemen

3. Aanbeveling R(89) 9, Raad van Europa

   Inhoud: aanbevelingen voor strafbaarstelling van diverse vormen van computercriminaliteit

   Status: niet-bindende aanbeveling, kan door landen worden overgenomen in eigen wetgeving

4. Aanbeveling R(95) 13, Raad van Europa

   Inhoud: aanbevelingen voor bevoegdheden voor opsporing in een digitale omgeving

   Status: niet-bindende aanbeveling, kan door landen worden overgenomen in eigen wetgeving

21.3.4 Europese Unie

1. Mededeling: Naar een algemeen beleid voor de bestrijding van cybercriminaliteit, COM(2007) 267def
2. Mededeling: betreffende de strijd tegen spam, spyware en kwaadaardige software, COM(2006) 688def
3. Kaderbesluit aanvallen op informatiesystemen (24 januari 2005, PbEG L69/67 van 16/03/2005)

   inhoud: stelt aanvallen op informatiesystemen, zoals hacken en verstikkingsaanvallen (DoS-aanvallen) strafbaar

   status: bindend, moet wel door elke lidstaat in eigen wetgeving worden geïmplementeerd

21.4 Zie ook

- Internetcriminaliteit

21.5 Externe links

- (nl) Computercriminaliteitlinks
- (en) Informatie platform over computercriminaliteit
- (nl) Meldpunt Cybercrime
- (nl) European Cybercrime Centre

Hoofdstuk 22

Computergeheugen

Een stapel insteekkaarten met geheugen-IC's

Computergeheugen stelt een computer in staat informatie op te slaan voor later gebruik. Computergeheugen kan worden onderscheiden in intern geheugen en extern geheugen of in vluchtig geheugen en niet-vluchtig (permanent) geheugen.

22.1 Soorten

Een indeling naar de manier waarop geheugen in een computer is geïmplementeerd:

- *read-only memory* (ROM) - geheugen dat alleen gelezen kan worden;
- *programmable read-only memory* (PROM) - geheugen dat slechts eenmalig beschreven kan worden en daarna alleen nog maar gelezen;
- *erasable programmable read-only memory* (EPROM) - PROM met wismogelijkheid, daardoor herprogrammeerbaar (met EPROM-programmer);
- *electrically erasable programmable read-only memory* (EEPROM) - geheugen dat elektronisch opnieuw geschreven kan worden (zonder uit de schakeling gehaald te hoeven worden);
- *random-access memory* (RAM) - geheugen dat zowel gelezen als beschreven kan worden. RAM-geheugen vormt de basis voor het werkgeheugen van de computer.

Daarnaast zijn er nog verschillende vormen van extern geheugen zoals:

- harde schijf
- diskettes
- cd-roms
- Digital Versatile Disc (dvd)
- magneetband
- SD-kaart
- USB-stick

Vluchtig geheugen verliest de opgeslagen gegevens als de computer wordt uitgeschakeld, niet-vluchtig geheugen behoudt ook dan de gegevens.

Oudere vormen van opslag die nu nauwelijks meer gebruikt worden, zijn:

- ponsband
- ponskaarten
- ringkerngeheugen
- trommelgeheugen

22.2 Hiërarchie

De soorten geheugen die een computer heeft zijn te rangschikken aflopend in snelheid en kosten per opgeslagen byte:

- registergeheugen
- processorcache
- random-access memory

- harde schijf
- secundaire opslag (cd, dvd, magneetband)

Veel componenten in een moderne personal computer (PC) bevatten zelf ook geheugen en soms een eigen processor. Veel hardeschijfcontrollers zijn voorzien van een cachegeheugen en videokaarten zijn in het algemeen voorzien van een ruime hoeveelheid videogeheugen.

22.3 Zie ook

- Holografisch geheugen

Hoofdstuk 23

Computerkraker

Een **computerkraker** is iemand die criminele activiteiten met computers uitvoert. De term 'computerkraker' (jargon **cracker** of **black hat hacker**) stamt uit de 'hacker-gemeenschap'. Het is een benaming voor een kwaadwillig iemand die zich bezighoudt met onder andere het zich wederrechtelijk toegang verschaffen tot al dan niet beveiligde computersystemen. In Nederland en België is het een vorm van computercriminaliteit en strafbaar als computervredebreuk.

Crackers zijn computer- en programmakrakers of computercriminelen die beveiligingen trachten te doorbreken en te misbruiken of verminken. Wanneer de toegang is gekraakt, spreekt men over een *crack*. Men heeft dan een *crack* gezet, bijvoorbeeld door een website te bevuilen. Middelen om specifieke programma's te kraken (*reverse engineering*), met het doel om daar onrechtmatig gebruik van te kunnen maken, worden aangeboden als *cracks*.

Programma's cracken is het vervangen van een stuk programmacode door een gewijzigde versie van die code, die de gebruikersbeperkingen tegen de zin van de auteur opheffen. Als de auteur niet meer bestaat dan is het legaal cracken van een programma met gebruikersbeperkingen een noodzaak om de volledige versie te kunnen gebruiken. Het beperken van de gebruikersfunctionaliteit wordt ook crippleware genoemd.

Over computerkrakers bestaan soms de wildste verhalen. Zo wordt wel eens het beeld geschetst dat een computerkraker zonder moeite weet binnen te komen in welke computer ook. Dit idee stamt uit de jaren tachtig. In die tijd waren computers op grote schaal aanwezig en het belang van beveiliging was ongekend. Het gevolg was dat zelfs tieners met het grootste gemak in de computers van militaire bases inbraken, door gewoon "aan de deur te rammelen" (verfilmd in *WarGames* en *Hackers*).

23.1 Hackers en crackers

De benaming *hacker* wordt vaak verward met een kraker. Een hacker is een persoon die geniet van de intellectuele uitdaging om op een creatieve en onorthodoxe manier aan technische beperkingen te ontsnappen. Maar in het dagelijkse spraakgebruik is het meestal iemand die inbreekt in computersystemen. De benaming is in de jaren negentig gebruikt om een categorie programmeurs aan te duiden die de computer kennen als hun broekzak en zich niets aantrekken van algemene softwareontwerptechnieken en dat ook niet nodig hebben voor hun producten.

Hackers zien zichzelf niet als criminelen en wensen dan ook niet met *cracken* geassocieerd te worden.[1]

23.2 Zie ook

- Hacker
- Identiteitsfraude
- Scriptkiddie

Hoofdstuk 24

Computernetwerk

Een **computernetwerk** is een systeem voor communicatie tussen twee of meer computers.[1] De communicatie verloopt via netwerkkabels of via een draadloos netwerk. In de netwerktopologie worden fysieke en logische topologieën onderscheiden. Men spreekt van een LAN in het geval van lokale plaatsgebonden bekabeling waarop computers binnen één gebouw of een campus aangesloten worden en een WAN wanneer er sprake is van verbindingen over grotere afstanden.

24.1 Het lagenmodel

Voor computernetwerken is TCP/IP het meest gebruikte communicatie protocol, met op de derde laag het internetprotocol (IP) en op de vierde laag het Transmission Control Protocol (TCP) van het OSI-model.

- Toepassingslaag: Op deze laag bevinden zich de communicatieprotocollen die rechtstreeks uitgewisseld worden met de applicatie zoals een e-mail-programma of een webbrowser,

  Voorbeeld: HTTP, FTP, ODBC, SMTP, Telnet

- Presentatielaag: Op deze laag bevinden zich onder andere compressie- en versleutelingsprotocollen.

  Voorbeeld: IPsec, IPComp, CCP

- Sessielaag: Op deze laag wordt de communicatiedialoog onderhouden tussen de twee communicatiepartners, door het opzetten en verbreken van de sessie.

  Voorbeeld: NetBIOS, NetBEUI PPTP, Apple Talk

- Transportlaag: Op deze laag wordt de volgordelijkheid van de afzonderlijke gegevenspakketten bewaakt.

  Voorbeeld: TCP, UDP, SPX

- Netwerklaag: Op deze laag wordt de route-informatie over de IT-infrastructuur afgehandeld, zodat de gegevenspakketten op de juiste wijze gerouteerd kunnen worden door zogenaamde routers.

  Voorbeeld: IP, IPX

- Datalinklaag: Op deze laag vindt Protocol multiplexing, mediumtoegang en de fysieke addressing (MAC) plaats.

  Voorbeeld Ethernet (IEEE802.3), ARCNET (IEEE802.4), Token Ring (IEEE802.5), WiFi (IEEE802.11)

- Fysieke laag: deze laag definieert de binaire transmissie en de elektrische of optische specificaties van het transportsignaal, alsmede de fysieke specificaties van het transportmedium.

  Voorbeeld: 10BASE-T, 100BASE-TX, 1000BASE-T, 10GBASE-T.

24.2 Topologieën

- **Point-to-point** - Twee computers communiceren 1:1 via een seriële- of netwerkkabel of een bluetooth-verbinding.

  Toepassing: tijdelijke 1:1 verbindingen t.b.v. overzetten van data en bediening op geringe afstand

  Voordeel: Eenvoudig te realiseren

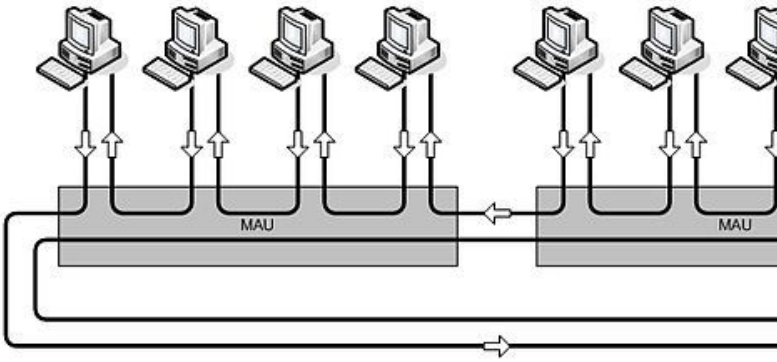
  Nadeel: Maximaal 2 computers per netwerk

- **Bus** - Alle computers op één kabel.

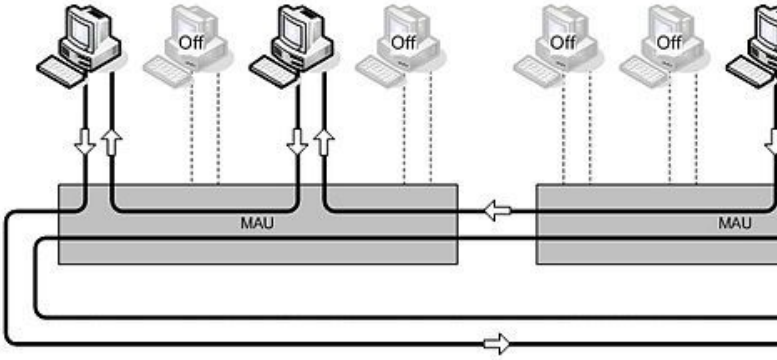
Toepassing: ethernet en ARCNET over coaxkabel (beide in onbruik geraakt)

Voordeel: Eenvoudig te realiseren en meer dan twee computers per netwerk mogelijk

Nadeel: gevoelig voor fysieke onderbrekingen, aangezien slechts twee computers tegelijkertijd met elkaar kunnen communiceren wat een relatief hoge toegangstijd tot gevolg heeft (zie ook: CSMA/CD)



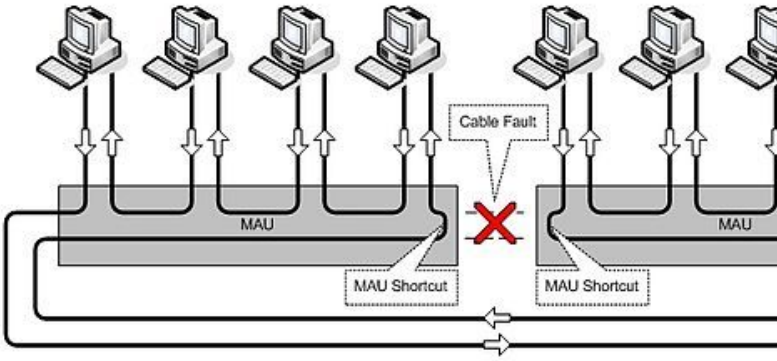
- **Ster** - Alle computers hebben een kabel naar een centraal punt.



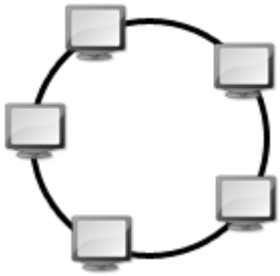
Toepassing: telefoonnetwerken en glasvezel netwerken op districtniveau

Voordeel: iedere eindpunt apparaat (computer, telefoon, etc.) heeft de volledige bandbreedte van de kabel ter beschikking

Nadeel: vereist veel bekabeling



- **Ring** - De computers zijn met elkaar verbonden en vormen samen een ring.



Toepassing: Token Ring-netwerken (populair in de jaren-1980, echter volledig in onbruik geraakt)

Voordeel: ten tijde van de introductie: robuust en snel (ten opzichte van het toenmalige 10Mbps Ethernet en het 2,5Mbps ARCNET)

Nadeel: kabeltechnisch complex, omdat de ring redundant moest zijn werd deze fysiek uitgevoerd als een stervormige dubbele ring

24.3 Zie ook

- Voor algemene info over netwerken zie netwerk (algemeen)
- Voor info over thuisnetwerken, zie thuisnetwerk en zeroconf

Hoofdstuk 25

Computervirus

Een **computervirus** (in het dagelijks taalgebruik wordt meestal kortweg over *virus* gesproken) is een vorm van schadelijke software (malware). Het is een computerprogramma dat zich in een bestand kan nestelen, bijvoorbeeld in bestanden van een besturingssysteem. Computervirussen worden als schadelijk beschouwd omdat ze schijfruimte en computertijd in beslag nemen van de besmette computers. In ernstige gevallen kunnen virussen binnenin de computer schade aanrichten, bijvoorbeeld het wissen en verspreiden van gevoelige gegevens. In zeer ernstige gevallen kan de gebruiker zelfs de totale controle over de computer verliezen.

Hoewel er veel verschillende computervirussen bekend zijn, komt er slechts een fractie daarvan "in het wild" voor. De Wildlist Organization International houdt een maandelijkse lijst bij van de virussen die in het wild zijn aangetroffen. Maandelijks worden er enkele duizenden verschillende virussen in het wild aangetroffen. Veel bestaande virussen zijn niet virulent genoeg om zich zelfstandig te verspreiden.

Het in omloop brengen van een computervirus is een misdrijf, zowel in het Nederlandse Wetboek van Strafrecht als in het Belgische Strafwetboek.

25.1 Andere soorten malware

Computervirussen die zich ongemerkt in een computersysteem nestelen en vermenigvuldigen moeten onderscheiden worden van *Trojan horses*. Trojaanse paarden zijn programma's die andere dingen doen dan ze voorgeven, bijvoorbeeld de computer gemakkelijker toegankelijk maken voor andere virussen of spam versturen. *Wormen* zijn geen virussen maar worden wel vaak zo genoemd. Het zijn zelfstandige programma's die zich direct over het netwerk verspreiden. Als de schade pas aangebracht wordt op een vooraf bepaald tijdstip, zoals bij een tijdbom of op het moment dat de software een bepaalde - vooraf vastgelegde - verandering waarneemt, spreekt men van een *logic bomb*.

25.2 Geschiedenis

In 1984 beschreef de Amerikaan Fred Cohen in zijn thesis *Computer Viruses – Theory and Experiments* een functioneel computervirus voor het Unix-besturingssysteem. In 1987 publiceerde de Duitser Ralph Burger in het boek *"Computer Viruses, a high tech disease"* de complete broncode van een werkend virus voor MS-DOS. Bijna alle computervirussen uit de periode 1987 tot circa 1991 zijn gebaseerd op de publicaties van Cohen en Burger. De Nederlander Jan Terpstra pionierde in deze periode via zijn BBS als een van de eersten met het opsporen en onschadelijk maken van computervirussen. Hij wordt gezien als één van de grondleggers van de antivirusindustrie.

Oorspronkelijk (vanaf circa 1988) verspreidden virussen zich vooral via software op diskettes en (illegale) cd-roms. Sinds e-mail een grote vlucht genomen heeft verspreiden virussen zich vooral via e-mailprogramma's en dragen zij bij aan de hoeveelheid junkmail die de doorsnee internetgebruiker ontvangt. Ze maken daarbij vaak gebruik van het adresboek dat de gebruiker in zijn e-mailprogramma heeft gemaakt. De meest gebruikte en daardoor gevoeligste e-mailprogramma's zijn Microsoft Office Outlook, Outlook Express, Windows Mail, Google Mail en Windows Live Mail. Macrovirussen verspreiden zich voornamelijk via Office-bestanden.

Uit een verslag van IBM bleek dat het aantal bekende computervirussen in 2004 met 25 procent toegenomen was tot 112438. Ongeveer 6 procent van de gescande e-mails in 2004 bevatten een virus. Het aantal geïnfecteerde e-mails ligt daarmee dubbel zo hoog als in 2003 (3 procent). In 2002 was dat slechts een half procent.

25.3 Invloed van het besturingssysteem

Virussen komen het meest op het besturingssysteem Microsoft Windows voor. Andere besturingssystemen zoals GNU/Linux en Mac OS X, worden minder vaak blootgesteld aan computervirussen. Sinds eind jaren 2000 komt hier langzaam verandering in door de stijgende po-

pulariteit van andere besturingssystemen. Deze zijn vaak niet aangepast om bescherming te bieden tegen virussen. Over de redenen dat Windows een geliefd doelwit is voor virusschrijvers kan men speculeren, maar de volgende redenen worden vaak aangegeven:

- Windows is een populair besturingssysteem, waardoor virusmakers zich sneller hierop zullen richten; ze hebben immers een grotere doelgroep.
- Veel Windows-programma's pogen zo gebruiksvriendelijk en idiotproof te zijn, dat de veiligheid hiervoor het veld heeft moeten ruimen.
- Windows was van oorsprong gericht op *personal* computers, terwijl andere besturingssystemen zoals Linux en Mac OS X, vanaf de grond af zijn opgebouwd met het oog op meerdere gebruikers en netwerkgebruik. Werking en veiligheid van Linux en OS X zijn hierdoor veel beter bestand tegen de gevaren van internet.

Dit betekent echter niet dat deze besturingssystemen niet beschermd zouden moeten worden. Ze kunnen immers "drager" zijn van virussen en wormen voor Windows-systemen. Als besmette bestanden op bijvoorbeeld een Linux-systeem staan, kan het voorkomen dat de Windows-machines virusvrij gemaakt zijn, maar dat er daarna weer een nieuwe besmetting gebeurt via die bestanden. Tegenwoordig wordt ook aangeraden antivirusprogramma's aan te schaffen voor Mac OS X.

Tegenwoordig komen virussen meer en meer voor GNU/Linux en Mac OS X (bijvoorbeeld MacShield). GNU/Linux was in 2011 een populair doelwit op dedicated servers,. Omdat dedicated servers de laatste jaren betaalbaarder zijn geworden voor particulieren en GNU/Linux een gratis besturingssysteem is, komt dit meer en meer voor.

25.4 Levensloop

Computervirussen hebben een zekere levensloop, gaande van het creëren tot het uitroeien van het virus. Het creëren gaat om de tijd die de programmeur nodig heeft om een virus te ontwikkelen. Vervolgens komt het virus tot stand en wordt het gekopieerd naar een strategische plaats zodat het zo vlug mogelijk verspreid kan worden. Daarna volgt de reproductie. Een virus vermenigvuldigt zich een aantal keren vooraleer het actief wordt. Voor bepaalde virussen vindt vervolgens een activeringsprocedure plaats. Het ogenblik waarop iemand de aanwezigheid van een virus vaststelt, wordt de ontdekking genoemd. Zodra de ontdekking is gebeurd, zullen software-ontwikkelaars trachten de aanwezigheid van het virus vast te stellen. Na deze assimilatie volgt de uiteindelijke uitroeiing.

25.5 Bestrijding

Er is een complete industrie die softwarepakketten ontwikkelt om virussen te bestrijden, zowel voor Windows als voor Mac OS X. Naast de softwarepakketten die op pc's of servers van bedrijven draaien is er nog een technologie om virussen te bestrijden, de zogenaamde *managed e-mail solutions*. Hierbij wordt de mail al op de server van de e-mailaanbieder gecontroleerd op virussen en spam. Het voordeel hiervan is dat een geïnfecteerde mail niet in het eigen systeem van de gebruiker komt en daar dus geen kwaad kan uitrichten.

25.6 Wijzen van verspreiding

Voorbeelden van manieren waarop een virus in een computer kan doordringen zijn:

- Websites
- USB-sticks
- diskette
- geheugenkaarten
- cd-rom, dvd ...
- modem (niet via internet, bijvoorbeeld BBS)
- e-mail
- bestanddeling (bijvoorbeeld Kazaa, LimeWire en andere p2p-systemen)
- misbruik van bugs (vulnerabilities) in software
- door het aankoppelen van een besmette harddisk
- Infectie door in BIOS genestelde code. Alleen het wissen of het verwijderen van de harde schijf heeft dan geen zin.
- Infectie door in de batterijchip van een laptop genestelde code. Dit is een nieuw onderzoeksgebied en komt nog heel zelden voor.
- Infectie via de draadloosnetwerkkaart. Hiervoor zijn hardware specifieke instructies nodig. Via een bufferoverflow zou hiermee toegang verschaft kunnen worden tot de computer zelf.
- Open netwerkpoorten en het niet gebruiken van een wachtwoord, een makkelijk te kraken of een makkelijk te achterhalen wachtwoord (bijvoorbeeld omdat hetzelfde wachtwoord overal gebruikt wordt door iemand). Hierdoor kan er externe code verstuurd worden naar deze computer.

- Windows Update (en mogelijk ook andere authentieke updatemethoden). Deze verspreidingsmethode is voor het eerst gesignaleerd in Flame. Het was mogelijk gemaakt door een Man-In-The-Middle en het gebruik van valse certificaten, die gegeneerd konden worden door zwakheden in het md5-algoritme.

25.6.1 Verspreiding per e-mail

De e-mails die een virus bevatten proberen meestal de indruk te wekken dat ze een belangrijke boodschap bevatten en afkomstig zijn van een bekende afzender die men kan vertrouwen. Vaak is de schijnbare afzender iemand waarin de persoon in kwestie in het verleden al contact mee heeft gehad. Dit komt doordat de e-mailadressen in het adresboek vaak gebruikt worden voor de verzending van zulke berichten. Valse virusberichten worden hoaxes genoemd.

Ook een bekende truc is het misbruiken van de naam van een firma zoals de virusmail *MS Update Announcement*. Deze e-mail lijkt bedrieglijk echt en er wordt in gesuggereerd dat door uitvoer van het bijgevoegde programma de computer wordt beveiligd tegen de nieuwste virussen. De afzender is echter niet Microsoft en de bijlage is een virus.

Verder zijn e-mails met virussen die de indruk wekken afkomstig te zijn van een mailserver of internetprovider ook populair. Dat zijn berichten zoals “Mail Delivery failure” of “Internet Provider Abuse” of iets gelijkwaardigs. Sommige virussen zijn in staat om de e-mails af te stemmen op het e-mailadres van de geadresseerde, zo kan iemand met bijvoorbeeld een @yahoo.com-adres een e-mail krijgen die schijnbaar van de helpdesk van Yahoo afkomstig is maar in werkelijkheid van iemand anders.

Door het inlassen van een valse melding dat het bericht virusvrij is trachten sommige virussen de kans op infectie te verhogen. Toch zijn er ook nog steeds veel 'domme' virussen die zich beperken tot gewoon een “Hi” of “see attached file”.

Bij verspreiding via e-mail is het virus meestal bijgesloten in bijlage. De bestandsnaam kan vast zijn maar ook op basis van het e-mailadres van de ontvanger of volstrekt willekeurig. Meestal is er een poging gedaan om te verbergen dat het een uitvoerbaar bestand is. Een constructie zoals *data.txt.pif* is gebruikelijk (deze truc werkt echter alleen op computers met het Microsoft Windows-systeem). Men maakt hier handig gebruik van de optie die sommige e-mailclients hebben om de bestandsextensie te verbergen. Hierdoor is het schijnbaar een onschuldig tekstbestand. Ongelukkig genoeg is deze optie standaard ingeschakeld op de meeste versies van Microsoft Outlook, Outlook Express.

De bestandsextensie van het virus kan verschillen. Macrovirussen kunnen aanwezig zijn in documenten die een macrotaal ondersteunen die programma’s kan opstarten zoals het geval is bij Microsoft Word, Microsoft Powerpoint, Microsoft Excel of Microsoft Access.

De recentere virussen maken gebruik van de spoofeigenschap: het sturen onder een e-mailadres van iemand anders.

25.7 Soorten virussen

Vroeger waren er allerlei typen virussen die op hun eigen manier schade aanrichtten.

Zo waren er bestandsvirussen die viruscode aan programma’s toevoegden die de extensie EXE of COM hebben. Als er zo'n programma wordt gestart, wordt het virus geactiveerd. Dan kan het virus zich naar andere bestanden kopiëren.

Bootsectorvirussen voegden gegevens toe aan het opstarten van een besturingssysteem.

Macrovirussen werden verspreid in bestanden met een macro erin, zoals Word-documenten.

Zoals reeds gezegd zijn computerwormen en Trojaanse paarden geen virussen, maar wel andere vormen van malware.

25.7.1 Mailvirussen

Dit zijn de 'ouderwetse' virussen die zichzelf als bijlage verspreiden via e-mail. Tijdens een besmetting kan er een mailserver automatisch geïnstalleerd worden, zodat er geen gebruik hoeft te maken van een e-mailprogramma op de geïnfecteerde computer. Ook de mailserver van de internetprovider waar de besmette computer mee is verbonden, hoeft niet te worden gebruikt. Internetproviders controleren streng op dit soort virussen dus de kans is groot dat de berichten er direct zouden worden uitgefilterd als ze via de provider verstuurd zouden worden.

Door een goede virusscanner te installeren en die altijd up-to-date te houden kan men zich wapenen tegen deze virussen. De meeste internetproviders filteren de geïnfecteerde mail er al uit. Bij sommige providers moet er daarvoor extra betaald worden.

25.7.2 Mobiele virussen

Ook voor mobiele telefoons bestaan er tegenwoordig virussen. Een echte doorbraak blijft echter uit, ondanks het feit dat mobiele telefoons en smartphones aan het uitgroeien zijn tot volwaardige computers.

Uit een studie van een groep netwerkdeskundigen onder leiding van hoogleraar Albert-László Barabási (Northeastern University, Boston, Verenigde Staten) blijkt dat we hiervoor vooral moeten kijken naar de besturingssystemen van de mobiele telefoons. Er zijn namelijk heel veel

verschillende besturingssystemen, zoals dat ook het geval is bij pc's. Virussen kunnen enkel worden overgedragen tussen twee apparaten met hetzelfde besturingssysteem.

De onderzoekers rekenden uit dat minstens 10% van alle mobiele telefoons hetzelfde besturingssysteem moet hebben alvorens een epidemie mogelijk is. Om tot dat resultaat te komen bekeken ze gedurende een maand de telefoongegevens van zes miljoen mobiele abonnees. Met die gegevens stelden ze een simulatie op met mobiele telefoongebruikers waarin ze ongeremd virussen konden loslaten.

Na een heleboel virusuitbraken kwamen ze dus tot de conclusie dat of een epidemie uitbreekt afhankelijk is van de populariteit van een welbepaalde telefoon. Een populaire telefoon zal immers meer kans hebben om een andere telefoon tegen te komen met hetzelfde besturingssysteem waarop het virus kan worden overgedragen.

De overdracht

De overdracht van mobiele virussen kan op drie manieren: via bluetooth, via mms of via het internet.

Hoe een besmetting gebeurt via internet ligt voor de hand. De gebruiker van de telefoon downloadt het virus rechtstreeks van het internet en besmet zo zijn telefoon. Deze methode is de minst efficiënte van de drie omdat de overdacht niet gebeurt van telefoon naar telefoon en kan zo ook aangezien worden als een buitenbeentje.

De bluetooth-methode is heel wat efficiënter. De reeds besmette telefoon zoekt contact met andere telefoons binnen zijn bereik en eens hij een vatbaar slachtoffer heeft gevonden kopieert het virus zichzelf naar de andere telefoon. De bluetooth-methode is een goede manier om een virus snel te verspreiden over korte afstand, maar heeft als nadeel dat verspreiding over grotere afstand niet mogelijk is.

De laatste methode is veruit de efficiëntste. Een telefoon stuurt automatisch een mms naar iedereen uit zijn netwerk met in de bijlage geen foto of filmpje, maar wel een virus. Als de ontvanger de mms dan opent en instemt om het 'filmpje' te bekijken, heeft het virus vrij spel en kan het zich verder verspreiden.

25.7.3 Andere

- *Bootsectorvirus*. Dit virus voegt gegevens toe aan het opstartgedeelte van een computer die het besturingssysteem moet starten (de bootsector).
- *Macrovirus*. Dit virus wordt verspreid door bestanden met een macro erin. Voorbeelden zijn Word-documenten.
- *Tijdbomvirus*. Dit virus wordt pas actief op een bepaalde datum of tijd (1 april en vrijdag de dertiende zijn daarbij populair). Hierbij kan elk soort virus worden geactiveerd.
- *Logic bomb*. Dit virus activeert als er een bepaalde, voorgeprogrammeerde, verandering optreedt in de computer. Hierbij kan elk soort virus worden geactiveerd.

25.8 Zie ook

- Lijst van malware
- Phishing
- Spam
- Social engineering
- Trojan horse
- Computerworm

25.9 Referenties

- Backer, J. 2009. Mobiele epidemie, Quest, oktober 2009, p. 108-110
- Ministerie van economische zaken. April 2000. Gids voor internetgebruikers, p. 47-48
- Wokke, A. 24 april 2009. Mobiele virussen gaan zicht verspreiden via mms (http://tweakers.net/nieuws/59787/mobiele-virussen-gaan-zich-verspreiden-via-mms.html), (accessed 30 november 2009)
- Wang, P. , González, M. , Hidalgo, C. , Barabási, A. 2009. From human mobility pattern to mobile virus's spreading (http://puwang.barabasilab.com/Talks/Venice_PPT.pdf), (accessed 30 november 2009)
- Pruyn, R. 28 september 2007. Mobiele virussen lopen twintig jaar achter, (http://www.itprofessional.be/news.cfm?id=73682]), (accessed 30 november 2009)
- Metheringham, N. 13 december 2010. Exim Exploit In The Wild Advisory (http://packetstormsecurity.org/files/96667/Exim-Exploit-In-The-Wild-Advisory.html), (accessed 12 juni 2011)

Hoofdstuk 26

Computervredebreuk

Computervredebreuk is de juridische omschrijving voor het inbreken in een computersysteem, ook wel hacken of kraken genoemd. De term is gevormd naar analogie met het woord huisvredebreuk.

26.1 Nederland

Computervredebreuk is in Nederland strafbaar gesteld in artikel 138ab van het Wetboek van Strafrecht en artikel 144a van het Wetboek van Strafrecht BES. Het wetboek omschrijft computervredebreuk als "opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk of in een deel daarvan". Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:

> a. door het doorbreken van een beveiliging,
>
> b. door een technische ingreep,
>
> c. met behulp van valse signalen of een valse sleutel, of
>
> d. door het aannemen van een valse hoedanigheid.

De maximale straf voor computervredebreuk is 1 jaar gevangenisstraf of een geldboete van de vierde categorie (in 2012: 19.500 euro of 14.000 dollar). Echter indien de inbreker:

1. gegevens uit de computer vastlegt (voor zichzelf of anderen), of
2. de verwerkingscapaciteit van de computer aanwendt voor zichzelf, of
3. de ingebroken computer gebruikt als startpunt voor een verdere inbraakpoging in een andere computer

dan neemt de maximumstraf toe tot vier jaren of een geldboete van de vierde categorie (zie Boete).

Door de wettelijke omschrijving van computervredebreuk zijn activiteiten als "cracking", het overnemen van andermans computers (zombies) en het installeren van spyware (zie Spyware) in Nederland verboden en strafbaar.

26.1.1 Wetsgeschiedenis

Op 1 maart 1993 werd de Wet computercriminaliteit ingevoerd om computercriminaliteit, waaronder computervredebreuk, strafrechtelijk te kunnen vervolgen.[1]

26.2 Zie ook

- Computerkraker
- Intrusion detection system
- GPD-affaire

26.3 Externe link

- Artikel 138ab, Wetboek van strafrecht (Nederland)

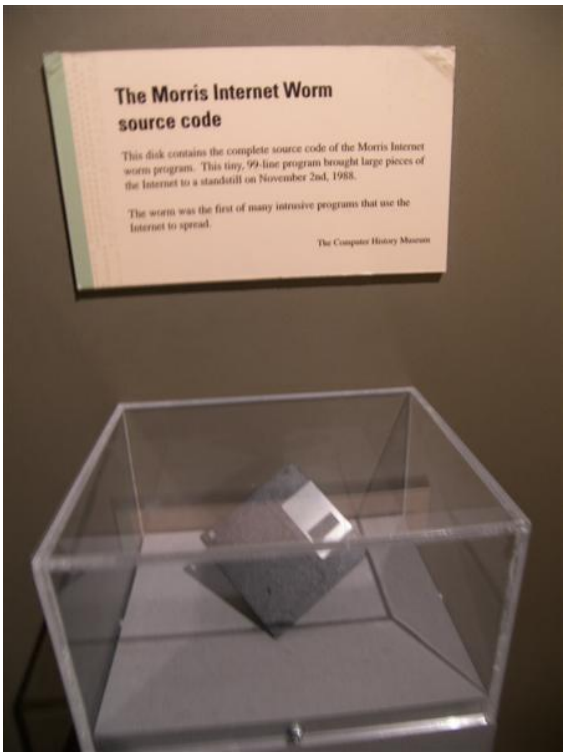
26.4 Noten

[1] Opgepakte hacker ging hoppend door de systemen, *NRC Handelsblad*, 23 maart 1993

Hoofdstuk 27

Computerworm

Een **computerworm** (of kortweg **worm**) is een zichzelf vermenigvuldigend computerprogramma. Via een netwerk worden kopieën van deze worm doorgestuurd zonder een tussenkomst van een tussengebruiker. Een worm is geen computervirus want hij heeft geen computerprogramma nodig om zich aan vast te hechten. Men kan stellen dat een worm schade toebrengt aan een netwerk, waar een virus een gerichte aanval op een computer doet.



De broncode van de Morris-worm in het Computer History Museum.

27.1 Verspreiding

Het verschil met een computervirus is dat een worm zichzelf verspreidt over het net, terwijl een virus dit op zichzelf niet kan. Een computervirus heeft een host nodig zoals een bestand of e-mail. Dit is in het voordeel van een computerworm. Hij probeert op alle open poorten van een computer een geïnfecteerde code naar binnen te loodsen. Zo heeft een lek in Windows Explorer al veel voor de verspreiding van wormen op het net gezorgd. Een koppeling met het internet is dan genoeg om besmet te raken.

27.2 Soorten

27.2.1 Payloads

Er bestaan wormen die gemaakt zijn om enkel zichzelf te verspreiden en deze proberen de tussenliggende systemen niet te wijzigen. Netwerkverkeer wordt wel keer op keer vertraagd en valse toegangen kunnen in je configuratie sluipen. Voorbeelden van dit soort wormen zijn de Morris-worm en Mydoom.

De payload is de lading, het doel waarvoor de worm is geschreven en is meestal alleen nuttig voor de maker. Bijvoorbeeld de ExploreZip-worm zal bepaalde bestanden verwijderen, andere versleutelen ze via een cryptologische aanval of versturen documenten via mail. De meest voorkomende payload is het installeren van een achterdeur op een computer om bijvoorbeeld ongewenste e-mail te versturen. Deze achterdeuren kunnen ook gebruikt worden voor andere payloads. Een voorbeeld hiervan is Doomjuice die via de achterdeur van een Mydoomworm in een systeem sluipt.

27.2.2 XSS-wormen

Cross site scripting (XSS)-wormen zijn geschreven voor een website om bezoekers te infecteren. Deze wormen komen voor op bekende sociale sites als MySpace, Hyves, Facebook en Yahoo!. Het grote doel hiervan is persoonlijke informatie van de gebruiker te stelen.

27.2.3 Nuttige wormen

Sommige wormen zijn geschreven om een systeem gebruiksvriendelijker te maken. Xerox PARC en de Nachiworm proberen patches van de Microsoftwebsite te

downloaden en te installeren. Het nadeel is ook hier dat andere wormen hiervan profiteren. Sommige personen vinden dit nuttig maar het is tijdrovend en het neemt de keuze af van de eigenaar of gebruiker.

27.2.4 Logic bomb

Als een worm pas schade aanricht op een vooraf bepaald tijdstip (net als bij een tijdbom) of op het moment dat de software een bepaalde verandering waarneemt, wordt gesproken van een *logic bomb*.

27.3 Bescherming

Een computergebruiker kan zich beschermen door het computersysteem up-to-date te houden door middel van het installeren van updates en patches en door het systeem te voorzien van een up-to-date antivirussoftware.

27.4 Zie ook

- Computervirus
- Trojaans paard (computers)

27.5 Externe links

- (en) The Wildlist - Lijst van virussen en wormen “in het wild” (regelmatig gevonden door anti-virus-bedrijven)

Hoofdstuk 28

Contentmanagementsysteem

Een **content-beheersysteem** of **contentmanagementsysteem** is een softwaretoepassing, meestal een webapplicatie, die het mogelijk maakt dat mensen eenvoudig, zonder veel technische kennis, documenten en gegevens op internet kunnen publiceren (contentmanagement). Als afkorting wordt ook wel *CMS* gebruikt, naar het Engelse *content management system* (inhoudbeheersysteem). Een functionaliteit van een CMS is dat gegevens zonder lay-out (als platte tekst) kunnen worden ingevoerd, terwijl de gegevens worden gepresenteerd aan bezoekers met een lay-out door toepassing van sjablonen. Een CMS is vooral van belang voor websites waarvan de inhoud regelmatig aanpassing behoeft, en de inhoud in een vaste lay-out wordt gepresenteerd aan bezoekers. De meeste grote bedrijven gebruiken voor hun website tegenwoordig een CMS. Een bekende variatie op het CMS is bijvoorbeeld de weblog.

Naast bovenstaande betekenis van content management (ook wel web content management) wordt de term ook gebruikt voor de bredere variant, Enterprise Content Management (ECM).

Een webmanager kan voor de invulling van een CMS-website zorgen.

28.1 Onderdelen

Een CMS bestaat ten minste uit de volgende onderdelen:

- een (bijna altijd afgeschermde) administratiemodule, waar gegevens kunnen worden ingevoerd, verwijderd of aangepast.
- een database of een andere vorm van opslag van de gegevens.
- een presentatiemodule, waar de ingevoerde gegevens door bezoekers kunnen worden bekeken.

Daarnaast kunnen er andere onderdelen zijn:

- een zoekmodule
- een inlogmodule voor bezoekers, als het niet gewenst is dat anonieme bezoekers toegang hebben tot de inhoud
- een beheersmodule voor de gegevens van geautoriseerde bezoekers (en beheerders)
- een beheersmodule voor de presentatiesjablonen
- een module om persoonlijke informatie aan de bezoeker te tonen (personalisaties)
- een module om centraal artikelen aan te kunnen maken die op verschillende pagina's getoond kunnen worden

Een CMS kan worden gebouwd voor een specifieke toepassing, maar er zijn ook generieke CMS'en beschikbaar. Een aantal daarvan is onder een opensourcelicentie gepubliceerd. Deze open source-oplossingen zijn volgens onderzoek voor 77% een goed alternatief[1] voor closed source-oplossing.

28.2 Contentmanagementsystemen

Enkele contentmanagementsystemen zijn:

- Apache Lenya
- CMS Made Simple
- Contao
- Daisy CMS
- DotNetNuke
- Drupal
- E107
- Enterprise Content Management
- ImpressCMS
- Joomla!
- Mambo

- MMBase
- Movable Type
- Net Toolbox
- Nuke
- PHP-Fusion
- PHP-Nuke
- Plone
- PostNuke
- RenovatioCMS
- Spip CMS
- Textpattern
- TYPO3
- Umbraco
- WebGUI
- Website Baker
- WordPress
- XOOPS
- Zikula

28.3 Zie ook

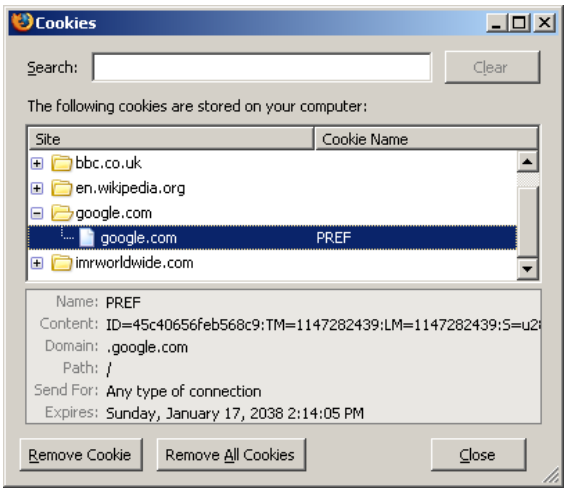
- Enterprise Content Management System

28.4 Referenties

[1] Brian Mort, Marktonderzoek Ingres: Forrester: Managing 21st Century Business Information, nieuwsbericht bij "CMSmatrix", 24 september 2007

Hoofdstuk 29

Cookie (internet)



Cookies beheren met Firefox

Een **cookie** of **magic cookie** is een hoeveelheid data die een server naar de browser stuurt met de bedoeling dat deze opgeslagen wordt en bij een volgend bezoek weer naar de server teruggestuurd wordt. Zo kan de server de browser opnieuw herkennen en bijhouden wat de gebruiker, c.q. de webbrowser, in het verleden heeft gedaan. Een dergelijk historie is bijvoorbeeld voor marketingdoeleinden interessant. Vanwege de privacyaspecten is het gebruik van cookies, dat zich veelal aan het oog van de internetgebruiker onttrekt, in deze situaties omstreden.

29.1 Achtergrond

Het gebruik van cookies is vooral bekend op het world wide web. Het Hypertext Transfer Protocol, dat het ophalen van informatie uit het web beschrijft, is namelijk als eenrichtingsverkeerssysteem ontworpen. De browser vraagt informatie en de server levert die, waarna de server het contact met de vrager weer kan vergeten. Verdere vragen worden dan weer precies zo behandeld als de eerste. Voor veel moderne internettoepassingen is het echter nodig dat de server een specifieke gebruiker kan herkennen en de illusie van een vaste verbinding met de klant kan wekken.

29.2 Gebruik van cookies

Cookies kunnen gebruikt worden voor:

- het onthouden van loginnaam of instellingen
- het vergaren van surfinformatie (profiling)
- het koppelen van een browser aan tijdelijke variabelen op de server (session cookie)

Een cookie hoeft niet veel data te bevatten. Als het cookie een unieke sleutel bevat, dan kan de server onder die sleutel alle verdere gegevens over de betreffende gebruiker c.q. webbrowser zelf bewaren en oproepen wanneer het cookie in een volgende sessie verschijnt.

29.3 Geschiedenis

Cookies zijn voor het eerst in Netscape 1.0 geïntroduceerd. Internet Explorer ondersteunde cookies pas vanaf versie 2.0.

Cookies werden pas zichtbaar voor internetgebruikers toen de Amerikaanse computerprogrammeur Lou Montulli in Netscape 3 een optie had laten inbouwen, die gebruikers in staat stelde om gewaarschuwd te worden wanneer er geprobeerd werd een cookie te plaatsen. Adverteerbureaus ontdekten het cookie ook en gebruikten het voor profiling.

In 1997 kwam er een voorstel dat browsermakers aanmoedigde om het gebruik van cookies inzichtelijker te maken voor de gebruiker. Het gevolg hiervan was dat de gebruiker vanaf toen kon instellen in welke mate cookies geaccepteerd mogen worden en of aan de gebruiker gevraagd moet worden of een cookie geaccepteerd mag worden. Dit was om het eerder genoemde profiling tegen te gaan want als gebruikers de cookies van een internetadvertentiebureau niet accepteren kan een internetadvertentiebureau geen profile samenstellen.

Cookies kwamen pas echt in opspraak toen DoubleClick, een internetadvertentiebureau, een bedrijf overnam met een grote klantendatabase. DoubleClick wilde de naamsgegevens koppelen aan de profiles van surfers en was van

plan deze gegevens te verkopen. Deze combinatie van naamsgegevens en profile is heel aantrekkelijk voor marketingbedrijven, want zij kunnen hiermee advertenties gericht naar iemand sturen, waardoor er meer geld voor een advertentie gevraagd kan worden. Onder druk van verschillende privacy-organisaties heeft DoubleClick de gegevens niet verkocht.

In 2002 is de eerste P3P recommendation gepubliceerd door het W3C. Browsers die zich aan deze specificatie houden, accepteren standaard veel minder cookies. De gebruiker kan desgewenst de instellingen van de browser aanpassen. Bijvoorbeeld cookies in een frame van een ander domein worden niet meer automatisch geaccepteerd door zo'n browser, tenzij de server een statement opstuurt dat de cookies niet gebruikt worden om privacygevoelige informatie op te slaan.

29.4 Tracking cookies

Het doel van een bepaald soort cookies, genaamd **tracking cookies**, is het verzamelen van informatie over websurfers.

Dit gaat als volgt:[1]

- Men bezoekt een website (laten we deze website A noemen) die reclame in de pagina heeft. Deze reclame is meestal afkomstig van de website van een advertentiebureau en deze website kan ook cookies opslaan.
- Later komt men op een andere website (website B), die van ditzelfde advertentiebureau gebruikmaakt om reclame weer te geven, dus kan de advertentiewebsite het eerder geplaatste cookie opvragen.
- Hierdoor kan men dan te weten komen dat de gebruiker ook naar website A geweest is en de inhoud van de reclame daaraan aanpassen. Als het aantal sites waar dit advertentiebureau actief is groot genoeg is kunnen er gebruikersprofielen gemaakt worden.

Niet enkel websites, maar ook flash-applicaties kunnen tracking cookies achterlaten. Deze worden meestal niet verwijderd door antivirussoftware omdat het in een andere vorm wordt opgeslagen, maar men kan ze wel zelf verwijderen[2].

Men zou als privacy-maatregel cookies kunnen uitschakelen, maar dit zal vaak meer problemen opleveren dan het zal voorkomen (sommige sites kunnen geen normale werking aanbieden zonder cookies). Tracking cookies zijn echter minder gevaarlijk dan sommige antivirussoftware voorspiegelen.[3] Ze kunnen bijvoorbeeld geen virus op een computer plaatsen. Het grootste probleem is de inbreuk op de privacy en anonimiteit.

29.5 Nederlandse cookiewetgeving

Artikel 11.7a van de Telecommunicatiewet[4] (in de volksmond “Cookiewet”) is sinds juni 2012 van kracht. Deze wet vereist van elke website die bezoekers vanuit Nederland trekt dat de bezoeker wordt geïnformeerd over welke cookies er worden geplaatst op zijn of haar computer en waar deze voor dienen. Dit kan via een privacystatementpagina. Daarnaast moet elke bezoeker vanuit Nederland vooraf eenmalig expliciet toestemming geven voor het plaatsen van deze cookies. Toestemming vragen kan via een pop-up of een balk bovenaan de website met een knop “Ik geef toestemming” (ev. de optie “Ik geef geen toestemming”). Het verwijzen naar hoe cookies achteraf te blokkeren zijn via de browser is niet voldoende.

Voor technisch noodzakelijke cookies, zoals een winkelmandje of een inlogformulier, is geen toestemming vereist. Voorbeelden waarvoor wel toestemming is vereist zijn: Google Analytics, Google Maps, YouTube, Facebook, Twitter enz. Zonder toestemming mogen er geen cookies worden geplaatst en is het aan de eigenaar van de website om die functionaliteiten te blokkeren, of de gehele website te blokkeren.

Er was een internetconsultatie gaande over een wetswijziging.[5] Na de wijziging zouden de melding en de vraag om toestemming niet meer in alle gevallen nodig zijn. De status van de wijziging is “gesloten”.

Hoofdstuk 30

Cyberoorlog

Cyberoorlog of **informatieoorlogvoering** is een soort oorlogvoering waarbij hackers uit politieke motieven natiestaten aanvallen met computer- of netwerksabotage en spionage.[1][2][3]

De eerste cyberoorlog werd gevoerd op 27 april 2007 in Estland. Aanleiding was de omstreden verplaatsing van de Bronzen Soldaat van Tallinn, een monument met oorlogsgraven uit het Sovjettijdperk.[4][5] De meeste aanvallen kwamen van servers van de Russische overheid en waren van het DDoS-type. Ze werden uitgevoerd door individuen en richtten zich tegen het Estse Parlement, ministeries, banken en media in Estland.[6][7][8][5] Wie achter de aanvallen zat is onduidelijk. Sergei Markov, lid van de Russische Doema, beweerde dat zijn assistent de aanval had uitgevoerd.[9] Ook Konstantin Goloskokov, een "commissaris" van de door het Kremlin gesteunde jeugdgroep Nashi eiste de verantwoordelijkheid op.[10] Experts zijn kritisch ten aanzien van deze aanspraken.[11] De aanvallen zetten militaire organisaties aan om hun netwerkbeveiliging te herzien. Op 14 juni 2007 kwamen de ministers van Defensie van de NAVO hier voor samen in het NAVO-hoofdkwartier Brussel.[12]

30.1 Aanvalsmethoden

Een cyberoorlog levert verschillende soorten dreigingen voor een land op:[13]

30.1.1 Spionage en veiligheidslekken in de nationale veiligheid

Cyberspionage is de illegale praktijk voor het verkrijgen van geheimen (gevoelige, eigendoms- of gerubriceerde gegevens) van particulieren, concurrenten, groepen, overheden of vijanden om er militair, politiek of economisch voordeel uit te halen. Onveilig behandelde informatie kan worden onderschept en zelfs gewijzigd, waardoor spionage en desinformatie mogelijk wordt vanaf de andere kant van de wereld. Specifieke aanvallen op de Verenigde Staten kregen codenamen zoals *Titan Rain* en *Moonlight Maze*. Volgens Generaal Keith B. Alexander heeft het onlangs opgerichte Cyber Command als doel om vast te stellen of activiteiten zoals commerciële spionage of diefstal van intellectueel eigendom criminele activiteiten zijn of daadwerkelijke "inbreuken op de nationale veiligheid".[14]

30.1.2 Sabotage

Militaire activiteiten die computers en satellieten gebruiken voor coördinatie lopen het risico van materiaalstoringen. Bevelen en communicatie kunnen worden onderschept of veranderd. Elektriciteit, water, brandstof, communicatie en transportinfrastructuur kunnen alle kwetsbaar zijn voor verstoring. Volgens Richard A. Clarke is de civiele wereld in gevaar, omdat de inbreuken op de beveiliging reeds verder gaan dan gestolen creditkaartnummers, en dat potentiële doelwitten ook het elektriciteitsnet, treinen, of de aandelenmarkt kunnen behelzen.[14]

Medio juli 2010 hebben beveiligingsexperts een kwaadaardig stuk software genaamd Stuxnet ontdekt. Het had fabriekscomputers geïnfiltreerd en had zich voortgeplant over de hele wereld. Het wordt beschouwd als "de eerste aanval op kritieke industriële infrastructuur die de basis vormen van de moderne economie", merkt The New York Times op.[15]

Elektriciteitsnet

De federale regering van de Verenigde Staten geeft toe dat het elektriciteitsnet gevoelig is voor cyberoorlog.[16][17] Het Amerikaanse ministerie van Homeland Security werkt samen met het bedrijfsleven om kwetsbaarheden te identificeren. Om het bedrijfsleven te helpen met het verbeteren van de beveiliging van systeemnetwerken, zorgt de federale regering er ook voor dat er veiligheid is ingebouwd als de volgende generatie van "smart grid"-netwerken worden ontwikkeld.[18] In april 2009 doken, volgens huidige en voormalige nationale veiligheidsambtenaren, meldingen op dat China en Rusland het Amerikaanse elektriciteitsnet hadden geïnfiltreerd en computerprogramma's hadden achtergelaten die kunnen worden gebruikt om het systeem te verstoren.[19][20] De North American Electric Reliability Corporation (NERC) heeft verklaard dat het

elektriciteitsnet niet voldoende beschermd is tegen een cyberaanval.[21] China ontkent dat het binnengedrongen is in het elektriciteitsnet van de Verenigde Staten.[22][23] Eén tegenmaatregel zou zijn om het elektriciteitsnet los te koppelen van het internet en het elektriciteitsnet enkel op *droop speed control* te laten lopen.[24][25] Massieve stroomuitval veroorzaakt door een cyberaanval zou de economie kunnen verstoren, afleiden van een gelijktijdige militaire aanval, of een nationaal trauma kunnen veroorzaken.

Howard Schmidt, Cyber-Security Coördinator van de Verenigde Staten, zegt over deze mogelijkheden:[26]

> Het is mogelijk dat hackers toegang hebben gekregen tot administratieve computersystemen van nutsbedrijven, maar deze zijn niet gekoppeld aan de apparatuur die het net regelen, althans niet in de ontwikkelde landen. [Schmidt] heeft nog nooit gehoord dat het net zelf is gehackt.

30.2 Motivaties

30.2.1 Militaire motivaties

In de VS deelde generaal Keith B. Alexander, hoofd van het recent gevormde USCYBERCOM, aan het Senate Armed Services Committee mede dat oorlogsvoering over computernetwerken zo snel evolueert dat er een "wanverhouding ontstaat tussen onze technische mogelijkheden om operaties uit te voeren en het huidige beleid en de wetgeving. Cyber Command is de nieuwste wereldwijde soldaat en zijn enige domein is cyberspace, buiten de traditionele slagvelden van land, zee, lucht en ruimte". Het zal proberen cyberaanvallen te vinden en, indien nodig, te neutraliseren en de militaire computernetwerken te verdedigen.[27]

Alexander schetste het brede slagveld waarop computeroorlog zich afspeelt, met de vele doelwitten die mogelijk moeten worden aangevallen, met inbegrip van het "traditionele slagveld buiten: command- en control-systemen op militaire hoofdkwartieren, luchtverdedigingsnetwerken en wapensystemen die computers vereisen om ze te bedienen."[27]

Cyber ShockWave, een scenario voor cyberoorlog, werd als spel op kabinetsniveau gespeeld door oud-ambtenaren en bracht vele kwesties aan het licht, van de National Guard via het elektriciteitsnet tot de grenzen van het wettelijke gezag.[28][29][30][31]

De uiteenlopende aard van aanvallen op internet betekent dat het moeilijk is om het doel en de aanvallende partij te bepalen, zodat het onduidelijk is wanneer een bepaalde handeling moet worden beschouwd als een oorlogsdaad.[32]

30.2.2 Burgerlijke motivatie

Mogelijke doelen van internetsabotage zijn alle aspecten van het internet, van de ruggengraat van het web, tot de internet service providers, tot de uiteenlopende vormen van datacommunicatie en netwerkapparatuur. Dit behelst onder meer webservers, bedrijfsinformatiesystemen, client-serversystemen, communicatieverbindingen, netwerkapparatuur, en desktops en laptops in bedrijven en woningen. Elektriciteitsnetten en telecommunicatiesystemen worden ook kwetsbaar geacht, vooral als gevolg van de huidige trends in de automatisering.

30.2.3 Privésector

Computerhacking is een moderne vorm van industriële spionage en doet zich naar men aanneemt op grote schaal voor. Dit soort van criminaliteit wordt ondanks de grootschaligheid weinig gerapporteerd. Volgens George Kurtz van McAfee moeten bedrijven over de hele wereld miljoenen cyberaanvallen per dag het hoofd bieden. "De meeste van deze aanvallen krijgen geen aandacht in de media en leiden ook niet tot uitgesproken politieke verklaringen van de slachtoffers."[33] Dit soort van criminaliteit is meestal financieel gemotiveerd.

30.3 Cyberoorlogsvoering internationaal

Het internet beveiligingsbedrijf McAfee vermeldt in zijn jaarverslag over 2007 dat ongeveer 120 landen het internet gebruiken als een wapen om financiële markten en overheidscomputersystemen te viseren.[34]

30.3.1 Cyberoorlogsvoering in Europa

Cooperative Cyber Defence Centre of Excellence (CCD CoE)

In het kielzog van de cyberoorlog van 2007 tegen Estland, heeft de NAVO het Cooperative Cyber Defence Centre of Excellence (CCD CoE) opgericht in Tallinn, Estland, om de cyberdefensie van de organisatie te verbeteren. Het centrum is opgericht op 14 mei 2008, kreeg de volledige erkenning van de NAVO en bereikte de status van de Internationale Militaire Organisatie op 28 oktober 2008.[35]

Estland had een dergelijk centrum reeds in 2003 voorgesteld. Het is dus niet direct terug te voeren op de spectaculaire aanvallen op Estland in 2007. Deze aanvallen hebben mogelijk de doorslag hebben gegeven die tot de beslissing leidde. Behalve door het gastland wordt de internationale militaire organisatie momenteel door Litouwen, Letland, Italië, Spanje, Slovakije en Duitsland ondersteund. De Verenigde Staten en Turkije hebben aan-

gekondigd om tot het CCD CoE, dat enkel toegankelijk is voor NAVO-leden, binnenkort te willen toetreden. Er werken 30 personen (april 2009). Het "Coöperatiecentrum voor Cyberverdediging" duidt zijn prioriteiten als inzichten, bijstand en vakkennis van diverse aspecten van het thema en die aan de NAVO ter beschikking te stellen. Daar hoort bij conceptualisering, training en oefeningen, publicatie van onderzoeksresultaten maar ook het ontwikkelen van een juridisch kader voor de, zoals het bij het CCD CoE heet, nog "onrijpe discipline" cyberverdediging.[36] Directeur van het CCD CoE is sinds februari 2008 luitenant-kolonel Ilmar Tamm.[37]

Tijdens de NAVO-top in Boekarest in april 2008[38] werd de bereidwilligheid van de alliantie om het "vermogen om alliantieleden op verzoek bij de afweer van een cyberaanval te ondersteunen" onderstreept. De eerste "CCD COE Conference on Cyber Warfare"[39] onder leiding van Kenneth Geers vond plaats van 17 tot 19 juni 2009.[40] Het CCD CoE wil zo snel mogelijk eveneens een lexicon betreffende *Cyber Warfare* creëren: "De definitie en de concepten zijn uiterst uitdagend in Cyberspace", aldus Geers bij de opening van de conferentie in Tallinn: "En ze zullen sterk gerichte aandacht vereisen."[41] Van 9 tot 11 september 2009 vond eveneens in Tallinn de *Cyber Conflict Legal & Policy Conference 2009* plaats, georganiseerd in samenwerking met het *George Mason University Center for Infrastructure Protection*[42] en het CCD CoE.[43]

Suleyman Anil, die bij de NAVO het centrum voor Computer Incident Response Capability(NCIRC TC[44]) voorzit, verklaarde in het voorjaar 2008 ter gelegenheid van een congres betreffende internetcriminaliteit in London: "Cyberverdediging wordt nu in de hoogste rangen in één adem met rakettenafweer en energiebeveiliging genoemd. We hebben een toename van dergelijke aanvallen vastgesteld en we geloven niet dat dit probleem in afzienbare termijn zal verdwijnen. Zolang er geen wereldwijd ondersteunde maatregelen genomen worden kan dit een globaal probleem worden." Alhoewel sommige stemmen sinds de jaren 1980 voor dergelijke gevaren gewaarschuwd zouden hebben, is deze aangelegenheid slechts sinds enkele jaren op de radar van de regeringen gekomen. De kosten van Hi-Tech-Aanvallen zijn gedaald terwijl de omvang van de schade die zij kunnen aanrichten stijgt, aldus Anil.[45]

In het SHAPE-hoofdkwartier van de NAVO in het Belgische Casteau heeft de alliantie haar *Incident Management Section*.[46]

Aangezien Estland internationale inspanningen om cybercrime te bestrijden heeft verlangt, zegt het Federal Bureau of Investigation dat het in 2009 permanent een deskundige op het gebied van computercriminaliteit in Estland zal plaatsen om te helpen bij de internationale strijd tegen de bedreiging van computersystemen.[47]

België

De verantwoordelijkheid voor cyberverdeding is in de Belgische regering verspreid over verschillende departementen en er is geen centrale nationale autoriteit ter zake. Het Belgische Netwerk voor Informatiebeveiliging, een overlegplatform waar verschillende regeringsinstanties aan deelnemen, adviseert de regering over cyberdreigingen en de bescherming van kritische infrastructuur.[48] Het Strategisch Plan 2000-2015 van Defensie noemt "verhoogde gecomputeriseerde acties" als een van de vier redenen voor het oprichten van een verenigde generale staf.[49] België heeft met Nederland en Luxemburg een memorandum van overeenstemming getekend voor een samenwerking bij cyberbeveiliging, met inbegrip van het delen van informatie en expertise, en samenwerking bij best practices en het ontwikkelen van publiek-private samenwerking.[50]

Nederland

In Nederland is het Nationaal Cyber Security Centrum opgericht voor de coördinatie van onderzoek en afhandeling van incidenten onder de verantwoordelijkheid van de Nationaal Coördinator Terrorismebestrijding en Veiligheid. Op Inlichtingengebied hebben de AIVD en MIVD samen de Joint Sigint Cyber Unit opgericht. Het Nederlandse Ministerie van Defensie heeft het Defensie Cyber Commando (DCC) opgericht, waarmee cyberoperaties onderdeel gemaakt kunnen worden van militaire inzet.[51]

30.3.2 Cyberoorlogsvoering in de United States

Cyberwarfare in the United States is de militaire strategie van de Verenigde Staten voor proactieve cyberverdediging en het gebruik van cyberoorlog als een platform voor de aanval.[52] De nieuwe Amerikaanse militaire strategie maakt expliciet dat een cyberaanval *casus belli* is voor een traditionele oorlogsdaad.[53]

In augustus 2010 waarschuwde de VS voor het eerst publiekelijk dat het Chinese leger gebruikmaakt van civiele computerexperts voor clandestiene cyberaanvallen die gericht zijn op Amerikaanse bedrijven en overheidsinstellingen. Het Pentagon verwees ook naar een vermeend Chinees spionagenetwerk genaamd GhostNet, dat werd onthuld in een onderzoeksrapport vorig jaar.[54] Het Pentagon verklaarde:

> "De People's Liberation Army gebruikt "informatie-oorlogsvoeringeenheden" om virussen te ontwikkelen om vijandelijke computersystemen en -netwerken aan te vallen, en die eenheden bevatten civiele computerprofessionals. Commandant Bob Mehal zal de opbouw van de cyberoorlogsmogelijkheden

> van het PLA opvolgen en zal capaciteiten blijven ontwikkelen om potentiële bedreigingen tegen te gaan."[55]

Het Amerikaanse ministerie van Defensie ziet het gebruik van computers en het internet voor oorlogsvoering in cyberspace als een bedreiging voor de nationale veiligheid.[1] Het United States Joint Forces Command beschrijft een aantal van zijn attributen:

> Cyberspace-technologie is in opkomst als een "instrument van de macht" in de samenleving, en wordt steeds meer beschikbaar om de tegenstanders van een land, die kunnen het gebruiken om aan te vallen, af te breken, en verstoren de communicatie en de stroom van informatie. De lage toetredingsdrempels, in combinatie met het anonieme karakter van de activiteiten in cyberspace, de lijst van potentiële tegenstanders is breed. Bovendien zal de hele wereld verspreid overaanbod van cyberspace en zijn minachting voor landsgrenzen uitdaging rechtsstelsels en bemoeilijken een land in staat is om bedreigingen af te schrikken en te reageren op onvoorziene gebeurtenissen.[56]

In februari 2010, bracht het Joint Forces Command van de Verenigde Staten een studie waarin een overzicht van de gevaren van het internet vermeldt stond:[56]

> Met zeer weinig investeringen, en gehuld in een sluier van anonimiteit, zullen onze tegenstanders onvermijdelijk pogen om onze nationale belangen te schaden. Cyberspace is een van de belangrijkste fronten in zowel conventionele en niet-conventionele conflicten aan het worden. Vijanden in cyberspace zullen zowel staten en niet-staten zijn en zullen variëren van de onervaren amateur tot de hoog opgeleide professionele hackers. Via cyberspace, zullen vijanden zich op de industrie, de academische wereld, de overheid, maar ook het leger in de lucht, over land, zee en ruimte richten. In vrijwel dezelfde manier dat de luchtmacht het slagveld van de Tweede Wereldoorlog veranderde, heeft cyberspace gebroken met de fysieke barrières die een natie beschermen tegen aanvallen op de handel en communicatie. Inderdaad hebben tegenstanders al gebruikgemaakt van computernetwerken en de kracht van informatietechnologie, niet alleen om terroristische daden te plannen en uit te voeren, maar ook om direct invloed op de perceptie en de wil van de Amerikaanse regering en de Amerikaanse bevolking uit te oefenen.

Amerikaanse "kill switch bill"

Op 19 juni 2010 presenteerde senator Joe Lieberman (I-CT) het wetsvoorstel "Protecting Cyberspace as a National Asset Act of 2010" (Bescherming van Cyberspace als een Nationaal Bezit Wet van 2010),[57] die hij samen met senators Susan Collins (R-ME) en Thomas Carper (D-DE) schreef. Als dit controversiële wetsvoorstel, dat in de Amerikaanse media ook wel de *kill switch bill* wordt genoemd, wordt goedgekeurd, verleent het de president noodbevoegdheden over delen van het internet. De drie coauteurs verklaarden echter dat het wetsvoorstel integendeel "de bestaande brede presidentiële autoriteit om de telecommunicatienetwerken over te nemen [versmalt]".[58]

30.3.3 Cyberoorlogsvoering in China

Diplomatieke telegrammen benadrukken Amerikaanse zorgen dat China de toegang tot Microsofts broncode gebruikt en dat 'het de talenten oogst van zijn privésector' om zijn offensieve en defensieve capaciteiten te versterken.[59]

30.4 Cybercontra-intelligentie

Cybercontra-inlichtingen zijn maatregelen om buitenlandse activiteiten, die cybermiddelen gebruiken als primaire spionagetechniek, te identificeren, binnen te dringen of te neutraliseren, evenals de verzameling inspanningen van buitenlandse inlichtingendienst die de traditionele methoden gebruiken om cybercapaciteiten en intenties van het eigen land te peilen.[60]

- Op 7 april 2009 kondigde Het Pentagon aan dat ze al meer dan $ 100 miljoen hebben uitgegeven in de afgelopen zes maanden om te reageren op en om schade als gevolg van cyberaanvallen en andere computernetwerk problemen te herstellen.[61]
- Op 1 april 2009 hebben de Amerikaanse wetgevers aangedrongen op de benoeming van een cybersecurity-"tsaar" van het Witte Huis om de Amerikaanse defensie tegen cyberaanvallen dramatisch te escaleren, door voorstellen uit te werken die de overheid in staat zou stellen om voor de eerste keer veiligheidsnormen voor de particuliere sector te bepalen en af te dwingen.[62]
- Op 9 februari 2009 heeft het Witte Huis aangekondigd dat het een inspectie zal uitvoeren van de cyberveiligheid van de natie om ervoor te zorgen dat de cybersecurity-initiatieven van de federale regering van de Verenigde Staten op passende wijze worden geïntegreerd, middelen ter beschikking krijgen en gecoördineerd worden met het Congres van de Verenigde Staten en de privésector.[63]

30.5 Controverse over de terminologie

Er is discussie over de vraag of de term “cyberoorlog” juist is. In oktober 2011 bijvoorbeeld publiceerde het *Journal of Strategic Studies* een artikel door Thomas Rid, “Cyber War zal niet voorkomen”. Een daad van cyberoorlog zou potentieel dodelijk, instrumenteel en politiek moeten zijn. Geen enkele geregistreerde cyberovertreding is een daad van oorlog op zichzelf. In plaats daarvan, zijn alle politiek gemotiveerde cyberaanvallen, argumenteerde Rid, slechts geavanceerde vormen van drie activiteiten die net zo oud zijn als de oorlog zelf: sabotage, spionage en ondermijning.[64]
Howard Schmidt, een Amerikaanse beveiligingsexpert, betoogde in maart 2010

> *Er is geen cyberoorlog ... Ik denk dat het een beroerde vergelijking is en ik denk dat het een beroerd begrip is. Er zijn geen winnaars op dit gebied*

Andere experts zijn echter van mening dat dit soort activiteiten reeds een oorlog vormen.[26] De vergelijking met oorlog wordt vaak gezien als misleiding om een militaristisch antwoord te motiveren wanneer dat niet per se nodig is. Ron Deibert, van Canada’s Citizen Lab, heeft gewaarschuwd voor een 'militarisering van cyberspace'.[65]

30.6 Incidenten

30.6.1 2013

- Op 19 februari 2013 maakte internetbeveiligingsbedrijf Mandiant bekend dat de Volksrepubliek China hoogstwaarschijnlijk achter het hacken van verschillende Amerikaanse bedrijven zit. De spil in het netwerk zou de geheime Eenheid 61398 zijn.[66]

30.6.2 2012

- Op 5 juni 2012 werd LinkedIn door Russische cybercriminelen gehackt. Voor het eerst werd een sociaal netwerk gehackt. Ongeveer 6,5 miljoen wachtwoorden van accounts werden gestolen [67].
- Op 27 februari verschenen er interne e-mails van het Amerikaanse particulier onderzoeksbedrijf Stratfor op de klokkenluiderswebsite WikiLeaks. In totaal publiceerde Wikileaks 5 miljoen e-mails. Vooral controversieel was de publicatie waarin stond dat de Pakistaanse inlichtingendienst ISI frequent contact had met Osama Bin Laden. Daarnaast wisten mogelijk twaalf medewerkers van de ISI waar Osama Bin Ladens zich bevond[68].

30.6.3 2011

- Op 24 december 2011 werd het Amerikaanse particulier onderzoeksbedrijf Stratfor door hackersgroep Anonymous gehackt. Er werden vooral interne e-mails gestolen, die drie maanden later op WikiLeaks gepubliceerd werden. Daarnaast stal Anonymous creditcardgegevens om vervolgens voor één miljoen dollar aan donaties voor liefdadigheid af te schrijven[69].
- Op 21 november 2011 werd er in de Amerikaanse media breed besproken dat een hacker een waterpomp had vernield in het Curran-Gardner Township Public Water District in Illinois.[70] Later bleek echter dat deze informatie niet enkel vals was, maar ook ten onrechte was gelekt door het Terrorisme en Intelligence Center van de staat Illinois.[71]
- Op 6 oktober 2011 werd aangekondigd dat de gegevensstroom van het commando en controle van de Drone en Predator van Creech AFB was gekeylogged. Alle pogingen om de daad ongedaan te maken stuitten op hevig verzet gedurende de afgelopen twee weken.[72] De luchtmacht heeft een verklaring afgelegd dat het virus “geen bedreiging heeft gevormd voor onze operationele missie”.[73]
- In juli 2011 werd het Zuid-Koreaanse bedrijf SK Communications gehackt. Dat resulteerde in de diefstal van de persoonlijke gegevens (inclusief namen, telefoonnummers, huis en e-mailadressen en rijksregisternummers) van 35 miljoen mensen. Een “getrojaande” software-update werd gebruikt om de toegang tot het SK Communications-netwerk te verkrijgen. Er bestaan banden tussen deze hack en andere kwaadaardige activiteiten en het wordt verondersteld om onderdeel uit te maken van een bredere, gecoördineerde hackingcampagne.[74]
- Operation Shady RAT is een doorlopende reeks cyberaanvallen die begonnen medio 2006, en gerapporteerd werden door internetsecuritybedrijf McAfee in augustus 2011. De aanvallen hebben ten minste 72 organisaties geraakt, waaronder overheden en defensie aannemers.[75]

30.6.4 2010

- Op 4 december 2010 hackte een groep, die zichzelf het Pakistaanse Cyber Leger noemt, de website van opsporingsagentuur van India, het Central Bureau of Investigation (CBI). Het National Informatics Center (NIC) is begonnen met een onderzoek.[76]
- Op 26 november 2010 hackte een groep die zichzelf het Indiase Cyber Leger noemt de websites van het Pakistaanse leger en andere behorende tot verschillende ministeries, waaronder het ministerie van

Buitenlandse Zaken, Ministerie van Onderwijs, Ministerie van Financiën, Pakistan Computer Bureau, Council of Islamic Ideology etc. De aanval werd uitgevoerd als een wraak voor de terroristische aanslag in Mumbai, die de betrokkenheid van Pakistaanse terroristen had bevestigd.[77]

- In oktober 2010 zei Iain Lobban, de directeur van het Government Communications Headquarters (GCHQ), dat Groot-Brittannië geconfronteerd wordt met een "echte en geloofwaardige" dreiging van cyberaanvallen door vijandige staten en criminelen en overheidssystemen worden 1000 keer per maand aangevallen. Dergelijke aanvallen bedreigen de economische toekomst van Groot-Brittannië. En sommige landen gebruiken reeds cyberaanvallen om druk uit te oefenen op andere naties.[78]

- In september 2010 werd Iran aangevallen door de worm Stuxnet Vermoed wordt dat het specifiek gericht zou zijn op de Natanz nucleaire verrijkingsfabriek. De worm wordt gezien als het meest geavanceerde stukje malware ooit ontdekt en verhoogt aanzienlijk het profiel van cyberoorlog.[79][80]

- In mei 2010 werden, als reactie op het *defacen* van Pakistaanse websites door de Indian Cyber Army, meer dan 1000 Indische websites beschadigd door PakHaxors, TeaMp0isoN, UrduHack & ZCompany Hacking Crew. Onder hen waren de Indische CID-website, de lokale overheid van Kerala, Box Office van de Indiase, Brahmos missile-website, Indische HP-helpdesk, Indian Institute of Science, en het Indische directoraat-generaal of Shipping.

30.6.5 2009

- In juli 2009 waren er een reeks gecoördineerde denial-of-service-aanvallen tegen grote overheids-, media- en financiële websites in Zuid-Korea en de Verenigde Staten .[81] Terwijl velen dachten dat de aanval werd geleid door Noord-Korea, kon een onderzoeker de aanvallen traceren naar het Verenigd Koninkrijk.[82]

30.6.6 2008

- Russische, Zuid-Ossetische, Georgische en Azerbeidzjaanse sites werden aangevallen door hackers tijdens de oorlog in Zuid-Ossetië in 2008.[83]

30.6.7 2007

- In 2007 werd de website van de Kirgizische centrale kiescommissie gedefaced tijdens de verkiezingen. De boodschap die op de website achtergelaten werd: "Deze site is gehackt door Dream of Estonian organization". Tijdens de verkiezingscampagnes en de rellen voorafgaand aan de verkiezingen, waren er gevallen van denial-of-service-aanvallen tegen de Kirgizische ISP's .[84]

- In september 2007 voerde Israël een luchtaanval uit op Syrië genaamd Operatie Orchard. De Amerikaanse industrie en militaire bronnen speculeerden dat de Israëli's cyberoorlogsvoering hebben gebruikt om hun vliegtuigen ongezien door de Syrische radar te krijgen.[85][86]

30.6.8 2006

- In de oorlog van 2006 tegen de Hezbollah betoogde Israël dat cyberoorlogsvoering deel uitmaakte van het conflict, waarbij de inlichtingendienst Israel Defense Force (IDF) schatte dat verschillende landen in het Midden-Oosten Russische hackers en wetenschappers gebruikten om in hun naam te werken. Als gevolg hiervan verhoogde Israël toenemend gewicht aan cybertactieken, en werden de VS, Frankrijk en een paar andere landen betrokken bij cyberoorlogplanning. Vele internationale hightechbedrijven verplaatsten hun onderzoeks- en ontwikkelingsactiviteiten naar Israël, waar de lokale werknemers vaak veteranen zijn van de elite van de computereenheden van het IDF.[87]

30.7 Inspanningen tot verbod

De Shanghai Cooperation Organisation (leden zijn onder andere China en Rusland) bepaalt dat er in de definiëring van cyberoorlog het verspreiden van informatie "die schadelijk zijn voor de spirituele, morele en culturele sferen van andere staten" dient te worden opgenomen. In tegenstelling richt de aanpak van de Verenigde Staten zich op fysieke en economische schade en letsel, waardoor het politieke belangen onder de vrijheid van meningsuiting plaatst. Dit meningsverschil heeft geleid tot terughoudendheid in het Westen om mondiale cyber-wapensbeheersingsovereenkomsten na te streven.[88] De Amerikaanse Generaal Keith B. Alexander, echter, ondersteunde gesprekken met Rusland over een voorstel om militaire aanvallen in cyberspace te beperken.[89] Een Oekraïense hoogleraar Internationaal Recht, Alexander Merezhko, heeft een project ontwikkeld genaamd het Internationaal Verdrag inzake het verbod op Cyberwar op Internet. Volgens dit project is cyberoorlog gedefinieerd als het gebruik van internet en de daarmee samenhangende technologische middelen door de ene staat tegen de politieke, economische, technologische en informatieve soevereiniteit en de onafhankelijkheid van een andere staat. Professor Merezhko's project doet vermoeden dat het internet zou moeten vrij blijven van oorlogsvoeringtactieken en behandeld worden als een internationale mijlpaal.

Hij stelt dat het internet (cyberspace) een “gemeenschappelijk erfgoed van de mensheid” is.[90]

In 2009 verklaarde president Barack Obama dat de digitale infrastructuur van Amerika een “strategische nationale asset” is en in mei 2010 richtte het Pentagon haar nieuw U.S. Cyber Command (USCYBERCOM), onder leiding van generaal Keith B. Alexander, directeur van de National Security Agency (NSA), op om de Amerikaanse militaire netwerken te verdedigen en om systemen van andere landen aan te vallen. Het Verenigd Koninkrijk heeft ook een cyber-security en 'operationeel centrum' opgezet. Het is gevestigd in het Government Communications Headquarters (GCHQ), het Britse equivalent van de NSA. In de VS echter, is Cyber Command alleen opgezet om het leger te beschermen, terwijl de overheids- en bedrijfsinfrastructuur primair de verantwoordelijkheid is van respectievelijk het Department of Homeland Security en private bedrijven.[91]

In februari 2010 waarschuwden hooggeplaatste Amerikaanse wetgevers dat de “dreiging van een verlammende aanval op telecommunicatie- en computernetwerken sterk in de lift was”.[92] Volgens The Lipman Report zijn een groot aantal belangrijke sectoren van de Amerikaanse economie, samen met die van andere landen, in gevaar, met inbegrip van cyberbedreigingen op openbare en private voorzieningen, bankwezen en financiën, transport, productie, medische diensten, onderwijs en overheid. Deze zijn nu allemaal afhankelijk van computers voor de dagelijkse operaties.[92] In 2009 heeft president Obama gezegd dat “cyberindringers onze elektrische netten hebben gepeild.”[93]

The Economist schrijft dat China plannen heeft om “tegen het midden van de 21e eeuw geïnformatiseerde oorlogen te winnen”. Zij merken op dat andere landen ook organiseren voor cyberoorlogen, onder hen Rusland, Israël en Noord-Korea. Iran beroemt zich erop 's werelds tweede grootste cyberleger te hebben.[91] James Gosler, een cybersecurityspecialist van de regering, is bezorgd dat de VS een ernstig tekort aan computerbeveiliging specialisten heeft. Hij schat dat er slechts ongeveer 1000 gekwalificeerde mensen zijn in het land vandaag, maar men heeft een behoefte aan een strijdmacht van 20.000 tot 30.000 bekwame experts.[94] Op de Black Hat-computerbeveiligingsconferentie in juli 2010 daagde Michael Hayden, voormalig adjunct-directeur van de National Intelligence, duizenden bezoekers uit om te helpen om manieren te ontwikkelen “om de internetbeveiligingsarchitectuur te hervormen”, verklarend: “Jullie laten de cyberwereld uitzien als de Noord-Duitse laagvlakte.”[95]

30.8 Zie ook

- Elektronische oorlogvoering
- Cyberterrorisme
- Distributed denial-of-service
- Hacker
- Stuxnet

30.9 Literatuur

- Andress, Jason en Winterfeld, Steve (2011), *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Syngress. ISBN 1597496375
- Benschop, Albert (2013), *Cyberoorlog - Internet als slagveld* Tilburg: De Wereld. ISBN 9789079051069
- Brenner, S. (2009), *Cyber Threats: The Emerging Fault Lines of the Nation State*. Oxford University Press. ISBN 0195385012
- Carr, Jeffrey (2010), *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reilly. ISBN 9780596802158
- Cordesman, Anthony H. en Cordesman, Justin G. *Cyber-threats, Information Warfare, and Critical Infrastructure Protection*, Greenwood Publ. (2002)
- Janczewski, Lech en Colarik, Andrew M. Cyber Warfare and Cyber Terrorism IGI Global (2008)
- Pérez, Nathalie (2013) De cyberoorlog is begonnen en ook uw computer doet mee Scientes.nl (9.3.2013)
- Rid, Thomas (2011) “Cyber War Will Not Take Place,”, *Journal of Strategic Studies*, DOI:10.1080/01402390.2011.608939
- Ventre, D. (2007), *La guerre de l'information*. Hermes-Lavoisier. 300 pages
- Ventre, D. (2009), *Information Warfare*. Wiley – ISTE. ISBN 9781848210943
- Ventre, D. (Edit.) (2010), *Cyberguerre et guerre de l'information. Stratégies, règles, enjeux*. Hermes-Lavoisier. ISBN 978-2-7462-3004-0
- Ventre, D. (2011), *Cyberespace et acteurs du cyberconflit*. Hermes-Lavoisier. 288 pages
- Ventre, D. (Ed.) (2011), *Cyberwar and Information Warfare*. Wiley. 460 pages
- Ventre, D. (2011), *Cyberattaque et Cyberdéfense*. Hermes-Lavoisier. 336 pages

Hoofdstuk 31

Cyberpesten

Cyberpesten, **digitaal pesten** of **digipesten** is het pesten op internet. Dit gedrag komt zowel tussen kinderen en tieners thuis en op school als tussen volwassenen als collega's op het werk voor.

31.1 Definitie

Iemand kan op verschillende manieren cyberpesten. Het gaat om kwetsende of bedreigende teksten bijvoorbeeld via chatprogramma's als WhatsApp of Facebook. Ook kunnen beledigende foto's, video's of persoonlijke gegevens van het slachtoffer op internet worden gebruikt om deze op sociaalnetwerksites te plaatsen (cyberbaiting) zoals Facebook en Twitter. Dan is er sprake van cyberstalking, waarbij een of meer daders doelbewust een slachtoffer lastig blijft vallen en er kan op fora en vrij bewerkbare pagina's, bijvoorbeeld Wikipedia, beledigende of bedreigende informatie geplaatst worden.

31.2 Kenmerken

- Cyberpesten gebeurt vaak anoniem. De daders voelen zich veilig, onbereikbaar en onherkenbaar, waardoor ze weinig terughoudend zijn.
- Niet enkel fysiek of sociaal dominante personen doen aan cyberpesten. Door zijn kennis van internet voelt de dader zich vaak machtiger dan het slachtoffer en denkt dan 'veilig achter de computer' zijn slag te kunnen slaan.
- Cyberpesten is niet terug te draaien – vaak blijven de gegevens op internet bestaan, zodat het slachtoffer er jaren nadien nog mee geconfronteerd kan worden.

31.3 Incidentie

Uit Belgisch onderzoek is gebleken dat één op de tien jongeren gepest wordt via internet. Volgens een onderzoek in Nederland waarin vijfhonderd tieners ondervraagd werden, komt het voor op vier van de tien scholen. Ook via bedrijfsservers worden werknemers slachtoffer van pestgedrag door collega's. Het venijnige hiervan is dat cyberpesten anoniem gebeurt, waardoor het harder is dan gewoon pesten en bedreigender is voor het slachtoffer, terwijl de dader geheim en buiten schot blijft. Ook weten ouders, leerkrachten en werkgevers niet wat er aan de hand is.

31.4 Preventie op school

Ouders en leerkrachten spelen bij het tegengaan van cyberpesten een belangrijke rol. De kinderen kunnen beter op de hoogte worden gebracht door het kind te begeleiden bij het surfen op internet en er voor te zorgen dat zij/hij het meldt als er zaken gebeuren die niet integer zijn. Ook voorlichtingen over hoe om te gaan met wachtwoorden, persoonlijke gegevens en het plaatsen van informatie is belangrijk. Leerkrachten hebben in hun lessen een voorlichtende functie over wat internet is en wat de gevaren hierop kunnen zijn. Bij geconstateerd wangedrag kan via de schoolservers de vandaal opgespoord worden en via een internetprotocol kunnen regels gegeven worden. Er zijn pestprogramma's die onder meer ook over cyberpesten gaan.

31.5 Preventie op de werkplek

Een bedrijf kan via pestprotocollen en met behulp van de bedrijfsvertrouwenspersoon handelen volgens richtlijnen. Hierbij is voorlichting essentieel. Er is een verschil tussen *practical jokes* en het stelselmatig blijven belagen via internet van een medewerker. Bedrijven kunnen leren van de manier waarop scholen omgaan met het probleem. Een pestende werknemer is te vergelijken met een pestende scholier. Een bedrijf dient zich ervan bewust te zijn dat een pester een negatieve invloed heeft op de bedrijfscultuur en -resultaten en dat cyberpesten extra bedreigend is voor mensen.

31.6 Zie ook

- Bezemen
- Centrum voor Algemeen Welzijnswerk

Hoofdstuk 32

Cyberspace

Hoewel er bij de term **cyberspace** niet echt te spreken is over een objectieve definitie, wordt het vaak gebruikt om een elektronisch medium van computernetwerken aan te geven waarin communicatie plaatsvindt. Oftewel “de virtuele wereld van computers”.

32.1 Historie van de term

De term *cyberspace* is een combinatie van cybernetica en space (ruimte). Het werd voor het eerst gebruikt door William Gibson, een schrijver uit het cyberpunkgenre, in zijn verhaal *Burning Chrome* (1982) in het Amerikaanse magazine Omni[1]. Dankzij het gebruik van de term in zijn latere boek *Neuromancer* (1984) kreeg de term bekendheid om vervolgens in de jaren 90 uit te groeien tot een synoniem voor het World Wide Web, vooral in de academische kringen.

32.2 Zie ook

- Virtuele gemeenschap
- Cyberoorlog

32.3 Referenties

Hoofdstuk 33

Dialer

Een **dialer** is een computerprogramma dat een modemverbinding laat maken met een duur telefoonnummer. Dit kan legaal, maar vaak ook illegaal gebeuren. Zonder enige waarschuwing wordt verbinding gemaakt met een duur 0909- of 0906-nummer. Hierdoor wordt de eigenaar van de computer op kosten gejaagd.

Voorboden van een dialer die op de computer aanwezig is:

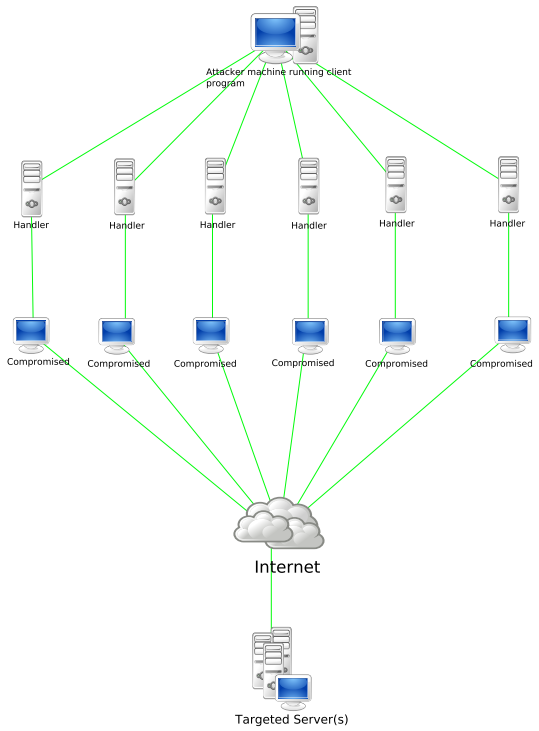
- uit de modem komt het geluid van de kiestoon
- de internetverbinding wordt duidelijk trager

Een onverwacht hoge telefoonrekening kan veroorzaakt zijn door een dialer. Dit is een computerprogramma dat inbelt naar dure betaal- of buitenlandse nummers tijdens het internetten. Dialers komen voornamelijk voor bij spelletjes-, ringtone- en erotische websites. Als bij een dergelijke website op OK of Ja wordt geklikt, bestaat de kans dat een dialer op de computer wordt geïnstalleerd.

Dialers werken alleen via een analoge modem (of ISDN-adapter). Breedbandgebruikers lopen dus geen gevaar, tenzij nog een analoge modem en een telefoonlijn zijn aangesloten.

Hoofdstuk 34

Distributed denial-of-service



Een distributed denial-of-service aanval

Denial-of-service-aanvallen (**dos-aanvallen**) en ***distributed denial-of-service*-aanvallen** (**DDoS-aanvallen**) zijn pogingen om een computer, computernetwerk of dienst onbeschikbaar te maken voor de bedoelde gebruiker.[1] Het verschil tussen een 'gewone' dos-aanval en een distributed dos-aanval is dat meerdere computers tegelijk de aanval uitvoeren naar hun doelwit.

34.1 Werking

Voor DDoS wordt vaak een botnet gebruikt,[2] maar het kan ook gaan om meerdere personen die hun acties coördineren, iets wat bijvoorbeeld gebeurt bij aanvallen van de zogenaamde *Anonymous*-beweging of de Syrian Electronic Army.[3] In reactie hierop werd het publiek-private Nationaal Cyber Security Centrum[4] opgericht, Europol startte het European Cybercrime Centre[5] en het Team High Tech Crime van de nationale recherche werd uitgebreid van 30 naar bijna 120 mensen en het Ministerie van Defensie deed een oproep in 2013 voor 150 white hats als cyberreservisten.[6][7] De AIVD en MIVD startten in 2014 met de Joint SIGINT Cyber Unit, een aftap- en cybercommando onder de codenaam Symbolon met 350 mensen.[8] en hebben voor 17 miljoen euro niet toegestane systemen om grootschalig telefoon- en internetverkeer op te kunnen vangen en verwerken besteld.[9] Voor 2013 werden er op ruim vijf miljoen .nl-domeinen[10] 39 DDoS-aanvallen gemeld in Nederland[11], inclusief vermeende aanvallen die enkel een storing betroffen.[12]

Ook al kunnen de methode, het motief en het doelwit verschillen, toch blijft het hoofddoel een website, internetdienst of server ervan te weerhouden aanvragen van reguliere gebruikers te behandelen.[13] Vaak zijn de doelen prominente websites of diensten, zoals die van banken of creditkaartservices. De term wordt gebruikt in verband met computernetwerken, maar is niet beperkt tot dit gebied; hij wordt bijvoorbeeld ook gebruikt met betrekking tot CPU resource management.

Een veel voorkomende vorm van aanvallen is doelbewust overbelasten van het doelsysteem met externe communicatieverzoeken, zodat het niet kan reageren op legitieme verzoeken, of zodat het zo traag wordt, dat het niet meer effectief te gebruiken valt. Dergelijke aanvallen leiden doorgaans tot een overbelasting van de server. Programma's die specifiek zijn ontworpen om dergelijke aanvallen uit te voeren, heten flooders. Meestal zijn dos-aanvallen bedoeld om te bewerkstelligen dat het doelwit zijn computer moet resetten of andere zaken moet doen, waardoor het doelwit zijn beoogde diensten niet meer kan aanbieden. Denial-of-service-aanvallen zijn in strijd met de regels van gebruik van vrijwel alle internetproviders. Daarnaast zijn ze in strijd met allerhande landeigen wetgevingen. Wanneer een dos-aanvaller een grote hoeveelheid informatiebestanden tracht te versturen naar een netwerkgebruiker, dan ervaren alle gebruikers van dat netwerk mogelijk storingen en/of vertragingen.

34.2 Symptomen en verschijningsvormen

Het Amerikaanse Computer emergency response team (US-CERT) noemt de volgende symptomen van een DDoS-aanval:[14]

- ongebruikelijke traagheid van het netwerk,
- het niet beschikbaar zijn van een bepaalde website,
- het onvermogen om een website te bezoeken,
- een drastische toename van het aantal spam e-mails (deze vorm van dos-aanval noemt men een e-mailbom of mailbom).

Denial-of-service-aanvallen kunnen ook leiden tot problemen bij andere computers of netwerken die verbonden zijn met het doelwit. Bij een grootschalige aanval kunnen gehele geografische gebieden getroffen worden, ook al is dit niet de intentie van de aanvaller.

34.3 Soorten aanvallen

Een denial-of-service-aanval wordt gekenmerkt door een expliciete poging van de cybercriminelen om de legitieme gebruikers van een service de toegang tot die service te ontnemen. Er zijn twee algemene vormen van dos-aanvallen: de crashaanvallen en de floodaanvallen. Er zijn verschillende manieren of soorten van dos-aanvallen, maar ook verschillende vormen van aanvallen. De vijf basisvormen zijn:

- verbruik van computergerelateerde middelen, zoals bandbreedte of schijfruimte,
- verstoring van configuratie-informatie,
- verstoring van de staat van het apparaat, zoals het ongevraagd resetten,
- verstoring van netwerkcomponenten,
- obstructie van communicatiemiddelen tussen de beoogde gebruikers en het doelwit, zodat ze niet meer adequaat kunnen communiceren.

34.3.1 ICMP-aanvallen

Er zijn dos-aanvallen die gebruikmaken van het Internet Control Message Protocol. Voorbeelden van programma's die dergelijke aanvallen inzetten, zogenaamde flooders, zijn Crazy Pinger en Some Trouble.

Zo worden er bij een smurfaanval *echo requests* (pings) met een vervalst IP-bronadres naar een broadcastadres binnen een netwerk gestuurd. Daardoor gaat het netwerk zelf dienen als een versterker van de smurfaanval. Bij een dergelijke aanval sturen de daders grote aantallen netwerkpakketten met een vervalst bronadres naar het slachtoffer. De bandbreedte van het netwerk van het slachtoffer wordt zo opgebruikt, waardoor legitieme zaken niet meer kunnen plaatsvinden. Om een smurfaanval te voorkomen, kunnen internetproviders verkeerd ingestelde netwerken opsporen.

Bij een ping flood zal men, uitgaande van een grotere bandbreedte, een aantal ping-pakketten naar het slachtoffer verzenden. Dit is eenvoudig, maar het hoofdvereiste blijft dat de bandbreedte van de aanvaller groter is dan die van het slachtoffer.

Bij de zogenaamde *ping-of-death* worden pakketten groter dan 65535 bytes verstuurd, dat mag niet volgens het protocol en daarom zal alles worden opgesplitst in meerdere, kleinere pakketten. Deze pakketten worden bij de server weer in elkaar gezet wat een crash in het besturingssysteem veroorzaakt. Hierdoor wordt de website onbereikbaar.

34.3.2 SYN flood

Bij een SYN flood stuurt de aanvaller TCP/SYN-pakketten, vaak met een vervalst bronadres. Elk van deze pakketten is een verzoek tot verbinding van de zender aan de ontvanger, waardoor er een halfopen verbinding bij de server wordt geopend. Deze halfopen verbindingen verzadigen het aantal verbindingen dat de ontvanger aankan. Daardoor krijgen legitieme gebruikers geen toegang meer tot het netwerk.

34.3.3 Teardropaanval

Een teardropaanval is het verzenden van vervormde IP-fragmenten met grote ladingen naar de doelcomputer. Hierdoor kan het besturingssysteem crashen. Verschillende besturingssystemen blijken hiervoor vatbaar.

34.3.4 Permanente denial-of-service-aanvallen

Een permanente dos (BOB's), ook bekend als phlashing, is een aanval die een systeem zo zwaar beschadigt, dat het vervangen of opnieuw geïnstalleerd moet worden. In tegenstelling tot de ddos-aanvallen maakt de BOB gebruik van veiligheidsproblemen op een computer, die het mogelijk maken om extern de computer te beheren. Wanneer het systeem extern beheerd wordt, kan de hacker het van binnenuit kapotmaken, waardoor het niet meer bruikbaar is. De BOB is een pure hardwaregerichte aanval die sneller is dan een DDoS-aanval, waarbij botnetwerken gebruikt moeten worden. Omdat deze manier van dos makkelijker is, zijn er al allerhande Super-BOB-middelen op de markt gebracht, zoals PhlashDance.

34.3.5 Distributed aanvallen

Een distributed-denial-of-service-aanval (DDoS) treedt op wanneer meerdere systemen vanuit meerdere webservers een flood van de bandbreedte van een ander systeem veroorzaken. Bij DDoS-aanvallen maakt men vaak gebruik van botnetwerken. Deze botnetwerken bestaan uit computers die allemaal extern aangestuurd kunnen worden. De externe bestuurder kan de computer van zijn slachtoffer laten crashen door alle computers in zijn botnetwerk tegelijkertijd bestanden te laten verzenden naar het slachtoffer. De bestanden die verstuurd worden, kunnen verschillen, zoals e-mails of verbindingsaanvragen. Er zijn tools beschikbaar die maken dat de eigenaar een botnetwerk kan besturen, zoals met een Trojaans paard.

LOIC

LOIC of Low Orbit Ion Cannon is een van de mogelijke opensourceprogramma's waar een DoS-aanval mee uitgevoerd kan worden. Het programma is gemakkelijk te bemachtigen en is beschikbaar op Windows, Linux en Mac OS X. Het was ooit bedoeld om over IRC grote aanvallen te doen, waarbij duizenden netwerken op een doelwit gezet werden.

DNS amplification attacks

Een DNS amplification attack is een vorm van DDoS-aanval waarbij het DNS-systeem wordt gebruikt. Bij een DNS amplification attack stuurt een server DNS queries van een gespooft IP (het IP dat hij wil aanvallen) en in deze query vraagt hij data op. Deze query is dan bijvoorbeeld 30 bytes, maar het DNS-netwerk zal een antwoord van bijvoorbeeld 30000 bytes naar het gespoofte IP-adres sturen. Deze vorm van DDoS werd gebruikt door cyberbunker tegen spamhaus.[15] Voorbeelden hiervan zijn bijvoorbeeld NTP amplification, hierbij wordt het NTP protocol misbruikt om gespoofte packets te sturen.

34.4 Preventiemethodes

De preventie van dos-aanvallen wordt meestal gedaan door speciale software die een aanval kan detecteren. Deze software begint het verkeer te herkennen en classificeren. Wanneer niet-legitiem verkeer toegang zoekt tot de computer, wordt dit geblokkeerd. Een aantal mogelijke preventie- en bestrijdingsmethoden:[14]

- Firewall: een firewall is een systeem dat de middelen van een netwerk of computer kan beschermen tegen misbruik van buitenaf.
- Switches: switches veroorzaken een vertraging in verkeer, zodat het makkelijker wordt om het verkeer te identificeren en classificeren.
- Routers: deze hebben eenzelfde functie als firewalls. Ze hebben ook als eigenschap het verkeer te vertragen.
- Clean pipes: al het verkeer wordt door een "clean pipe" gestuurd. Deze controleert het verkeer op zijn legitimiteit. Het laat alleen goedgekeurd verkeer doorgaan naar de server.
- Scrubbing center: al het verkeer wordt gestuurd naar een anti-DDOS center, zodra nodig, waar verschillende methoden en geavanceerde monitoring wordt toegepast om legitiem te scheiden van ongewenst verkeer. Verschil met een Clean pipe is dat het alleen wordt omgeleid tijdens een aanval.

34.5 Booters

Tegenwoordig zijn er verscheidene "booters" online, dit zijn web-applicaties die meestal gebruikmaken van (gehackte) servers, hierop staat dan een script dat veel packets verstuurt, of zoals een amplification attack uitvoert. 90% van alle booters zijn slecht geschreven, illegaal. Dit terwijl het eigenlijk bedoeld was voor stress-testing.

34.6 DDoS met maatschappelijke impact

34.6.1 20 oktober 2016

Op Donderdag 20 oktober 2016 vonden twee DDoS aanvallen plaats op een uitbater van een DNS systeem die ervoor zorgden dat Twitter, Spotify, en Paypal onbereikbaar werden. Opmerkelijk was hierbij dat de aanval mee uitgevoerd werd door aan het internet gekoppelde toestellen.[16]

34.7 Zie ook

- Black hat

Hoofdstuk 35

Domain Name System

Het **Domain Name System (DNS)** is het systeem en netwerkprotocol dat op het Internet gebruikt wordt om namen van computers naar numerieke adressen (IP-adressen) te vertalen en omgekeerd. Hoewel dit "vertalen" genoemd wordt gaat het gewoon om opzoeken in tabellen, waarin namen aan nummers gekoppeld zijn.

DNS is een client-serversysteem: een opvrager (*client*) gebruikt het DNS-protocol om aan een aanbieder (DNS-*server*) een naam of adres op te vragen, waarop de server een antwoord terugstuurt. Het opzoeken van een nummer bij een naam wordt *lookup* genoemd; het opzoeken van een naam bij een nummer *reverse lookup*.

De naamgeving is hiërarchisch opgezet: namen bevatten punten, en organisatorische eenheden corresponderen met onderdelen van de naam. Zo'n eenheid wordt een *domein* genoemd, en een naam een *domeinnaam'*. Zo is bijvoorbeeld de Nederlandstalige Wikipedia te vinden op de domeinnaam nl.wikipedia.org, die (op het moment van schrijven) correspondeert met het IP-adres 91.198.174.192. Deze naam is onderdeel van het domein wikipedia.org, waarvan de domeinnamen door de organisatie van Wikipedia worden beheerd.

DNS wordt ook gebruikt in het SMTP-protocol om de mailservers voor een domein op te zoeken, de computers die de e-mail ontvangen die aan de desbetreffende organisatie geadresseerd is. Daarnaast is er een protocol, het Sender Policy Framework (SPF), waarmee van een e-mail versturende computer via DNS kan worden opgezocht of die daartoe volgens zijn organisatie het recht heeft. Dit is één van de instrumenten die zijn ingezet ter bestrijding van wereldwijde spam.

35.1 Geschiedenis

Elke computer die met het internet verbonden is moet een IP-adres hebben om van op afstand bereikbaar te zijn; zo'n computer wordt een *host* genoemd omdat hij fungeert als gastheer voor de gebruiker die er op afstand gebruik van maakt. Omdat zulke nummers voor mensen moeilijk te onthouden zijn, kreeg daarnaast elke computer een naam toegekend, en werd in de software die internetverbindingen maakt ingebouwd dat zulke namen gebruikt konden worden door hun nummer op te zoeken in een tabel.

Deze tabel was aanvankelijk een bestand, /etc/hosts (soms hosts.txt genoemd), dat op elke aan Internetverkeer deelnemende computer aanwezig moest zijn.

Naarmate het aantal en de omvang van de deelnemende netwerken groeide werd het actueel houden van dat bestand op elke deelnemende computer ondoenlijk. Daarom werd het DNS-protocol ontworpen, zodat deze informatie zelf over het Internet kon worden opgevraagd. Daardoor kan een organisatie de toewijzing van nummers aan namen altijd aanpassen zonder dat voor het doorvoeren van die wijziging bij anderen expliciete acties nodig zijn.

Alle software die Internetverbindingen gebruikt ondersteunt DNS, maar ook nog steeds het hosts-bestand. Soms wordt dit laatste bestand nog gebruikt om -bijvoorbeeld- lokale computers een makkelijke naam te geven of om tijdelijk voor een specifieke host het DNS systeem te negeren - soms handig bij het testen van een nieuwe website die nu nog een andere URL heeft of lokaal draait. Een 2e toepassing is het opnemen van een lijst van domeinnamen die als ongewenst zijn geklasseerd en in het hosts bestand een verwijzing naar een ander adres (dan een DNS-server) heeft, zoals naar 127.0.0.1. Antimisbruikproducten zoals Spybot Search & Destroy maken hier ook gebruik van.

35.2 Basistechniek

DNS in praktische implementaties bestaat uit drie onderdelen:

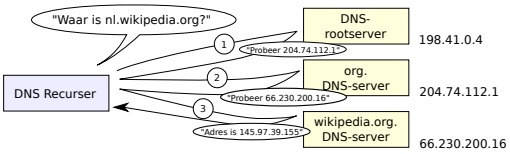
- De *stub resolver*
- De *caching/recursing resolver* (ook wel *recursor* genoemd)
- De *authoritative nameserver*

Het opzoeken van data met behulp van DNS wordt in de regel een *lookup* genoemd. Software, zoals een webbrowser, die een lookup wil doen vraagt dit aan de

stub resolver. Dit is relatief simpele software die, afhankelijk van de configuratie, de vraag kan stellen aan een *recursor* of eerst kan kijken in een bestand (zoals het o.a. Unix-afgeleiden bekende /etc/hosts).

De *stub resolver* stelt een DNS-pakket samen en stuurt dit naar de *recursor*. Vaak levert de internetprovider een recursor en wordt deze gebruikt, alhoewel bij netwerken ook regelmatig een interne recursor wordt opgezet. De recursor is geavanceerder dan de stub resolver en zal in eerste instantie beginnen met het stellen van de vraag aan een DNS-rootserver. Deze kan dan doorverwijzen naar andere servers, vanaf waar weer doorverwezen kan worden naar andere servers, etc., totdat uiteindelijk een server bereikt is die het antwoord weet of weet dat de lookup niet mogelijk is. Van dit laatste kan sprake zijn indien de naam niet bestaat of de servers niet reageren. Het proces van het langslopen van verschillende authoritative servers heet recursie.

Bij het opzoeken van een domein wordt begonnen op het hoogste niveau (*root* genaamd) en daarna wordt steeds specifieker gezocht. Bij het zoeken naar een domein wordt meteen aan de DNS-rootserver gevraagd voor bijvoorbeeld nl.wikipedia.org. Er is geen tussenstap waarbij alleen om org gevraagd wordt. Het is immers theoretisch mogelijk dat de rootserver zelf al het antwoord voor nl.wikipedia.org weet. Zo weten rootservers bijvoorbeeld wel het antwoord voor a.root-servers.net. In de regel zal door de DNS-rootserver echter wel verwezen worden naar de nameservers voor org. Deze zou in het geval van nl.wikipedia.org dan verwijzen naar de nameservers voor wikipedia.org die vervolgens het antwoord weten.



Vereenvoudigde weergave van recursie bij het resolven van nl.wikipedia.org

Deze servers waar de recursor vragen aan kan stellen zijn de *authoritative nameservers*. Deze zijn ook relatief dom en geven simpele antwoorden. Deze antwoorden zijn vaak in bestanden of in een database opgeslagen. Een authoritative nameserver kan een antwoord geven, wat zowel een verwijzing naar een andere server of een direct antwoord op de vraag kan zijn.

Zowel de recursor als de authoritative nameserver worden vaak DNS-server genoemd. Het is mogelijk om deze beide functies te combineren in één programma. Dit wordt bijvoorbeeld gedaan in BIND, een van de bekendste en meest gebruikte DNS-servers. Er bestaan ook programma's die slechts een van beide functies vervullen. NSD is een voorbeeld van een puur authoritative nameserver. Bij programma's die beide functies combineren, is het vaak mogelijk om een van beide uit te schakelen of alleen open te stellen voor het interne netwerk.

35.3 Caching

Om te voorkomen dat recursors zeer regelmatig overbodige query's doen (DNS-data verandert relatief weinig) hoort een recursor *caching* te implementeren. Dit wil zeggen dat een eenmaal ontvangen antwoord enige tijd bewaard wordt. Deze tijd kan de beheerder per record aanpassen en wordt Time to live (TTL) genoemd. In de regel ligt deze tussen enkele minuten en enkele dagen.

35.4 Redundantie

In de regel zijn er meerdere authoritative servers voor dezelfde data. Dit om de mogelijke gevolgen van het uitvallen van een server te beperken.

In principe moet een recursor, als geconstateerd wordt dat een bepaalde authoritative server niet werkt, alle andere proberen. Uiteindelijk zal er een gevonden worden die wel werkt, of kan de recursor concluderen dat het niet mogelijk is om de naam te vertalen.

35.5 DNSSEC

Het DNS-protocol is kwetsbaar voor misbruik. Onder meer door middel van zogenaamde 'DNS cache pollution'-aanvallen (zoals de 'Kaminsky Aanval'), is het DNS om de tuin te leiden. Als gevolg hiervan kunnen argeloze gebruikers bijvoorbeeld naar een valse, malafide website worden gestuurd. In antwoord op deze bedreiging is een uitbreiding op het DNS protocol ontwikkeld: de 'Domain Name System Security Extensions', kortweg DNSSEC. Met behulp van deze internet-standaard zijn DNS-antwoorden cryptografisch te beveiligen, zodat ze niet meer kunnen worden vervalst. Dit gebeurt op basis van zogenaamde digitale handtekeningen, die met een private sleutel worden gegenereerd en met behulp van een publieke sleutel kunnen worden gevalideerd. Van DNS-antwoorden is zodoende de integriteit en authenticiteit gegarandeerd (ook als dit een ontkennend, of leeg antwoord is). Het is echter een misverstand om te veronderstellen dat DNSSEC het DNS-verkeer ook beschermt tegen afluisteren.

35.6 Resource records

Data in DNS wordt opgeslagen in een *Resource Record*. Een resource record bevat een type, een TTL, een naam en data. De data kan bijvoorbeeld een IP-adres zijn of

een andere naam. Dit is afhankelijk van het type van het resource record.

Veel voorkomende types zijn:

- SOA Start-Of-Authority, met instellingen voor het (sub)domein, zoals TTL (Time-To-Live), serienummer, primaire server, responsible person
- A voor het bepalen van het IPv4-adres bij een naam
- AAAA voor het bepalen van het IPv6-adres bij een naam
- CNAME Canonical name voor het configureren van alias van een A of AAAA record
- PTR voor het bepalen van een naam bij een IPv4- of IPv6-adres (zie verder bij *Omgekeerde lookups*)
- MX voor het bepalen van de mailservers voor een domein, waarbij elke mailserver een eigen prioriteit toegewezen krijgt
- NS voor het aangeven welke nameservers de authoritative nameservers zijn (ook gebruikt voor het verwijzen naar andere nameservers)
- TXT aanvankelijk gebruikt voor ieder door de gebruiker gewenst commentaar. Nu mede in gebruik door het SPF anti-spam initiatief.
- SRV een relatief nieuw record dat gebruikt wordt om services aan te duiden.
- DKIM een relatief nieuw record dat wordt gebruikt om de authenticiteit van e-mail te kunnen valideren. Grote partijen zoals Gmail maken inmiddels van deze 'DomainKeys Identified Mail (DKIM)' gebruik.

35.7 Omgekeerde lookups

Omgekeerde of “reverse” lookups kunnen dienen om te weten te komen welke naam bij een IP-adres hoort. Voor het bepalen van de naam bij een IPv4- of IPv6-adres heeft DNS een op het eerste gezicht ingewikkelde constructie. Voor het bepalen van een naam bij een IPv4-adres, moet men de juiste naam opvragen die zich bevindt onder in-addr.arpa.

Voorbeeld: 1.2.3.4 wordt vertaald naar 4.3.2.1.in-addr.arpa. En 52.61.63.53 wordt vertaald naar 53.63.61.52.in-addr.arpa. Voor deze naam (deze naam is vanuit DNS-perspectief niet veel anders dan een naam als wikipedia.org) wordt het PTR-record opgevraagd. Hieruit komt vervolgens de naam behorend bij het IP-adres.

Voor IPv6 is dit vergelijkbaar, maar veel langer en de records bevinden zich in ip6.arpa. De reverse van bijvoorbeeld 2001:200:0:8000::42 kan worden verkregen door het opvragen van het PTR-record voor 2.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.0.0.0.0.0.0.0.2.0.1.0.0.2.ip6.arpa.

35.8 Nameserver tools

Voor het effectief beheer van een nameserver zijn verschillende diagnostische *tools* beschikbaar. De zogeheten BIND-tools zijn de bekendste. Hieronder vallen bijvoorbeeld *nslookup*, *host* en *dig*.

35.9 Zie ook

- Second-level-domein en subdomein

35.10 Externe links

Enkele DNS-RFC's (er zijn er nog vele andere met aanpassingen en toevoegingen)

- RFC1034: Domain names - concepts and facilities
- RFC1035: Domain names - implementation and specification
- RFC1912: Common DNS Operational and Configuration Errors
- RFC2182: Selection and Operation of Secondary DNS Servers
- RFC4033: DNS Security Introduction and Requirements
- RFC4044: Resource Records for the DNS Security Extensions

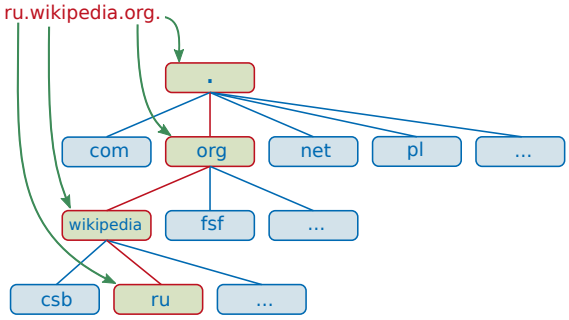
Overige links

- Sender Policy Framework

Hoofdstuk 36

Domeinnaam

Een **domeinnaam** (of, afgekort, 'domein') is een naam in het *Domain Name System* (DNS), het naamgevingssysteem (op internet) waarmee computers zoals webservers en mailservers alsmede bepaalde diensten en toepassingen kunnen worden geïdentificeerd. De domeinnaam verwijst doorgaans naar een IP-adres dat uit nummers bestaat, maar kan ook andere technische verwijzingen omvatten. Het DNS functioneert zodoende als het ware als een telefoongids (van het internet). Een goede domeinnaam is treffend en eenvoudig te onthouden. Zowel bedrijven als particulieren maken er daarom intensief gebruik van, zowel om te vinden als om gevonden te worden op internet.



De niveaus topleveldomein, secondleveldomein, subdomein van de Russische Wikipedia

36.1 Naamgeving

De verschillende delen van een domein(naam), labels genoemd, worden van elkaar gescheiden door punten. Een voorbeeld van een domein(naam) is wikipedia.org. Een label kan nooit langer zijn dan 63 tekens. Het totaal van labels en tussenliggende punten, mag niet langer zijn dan 255 tekens. De combinatie mag bestaan uit de letters a tot en met z, eventueel aangevuld met cijfers 0 tot en met 9 of een streepje −.

Sinds 2003 kunnen domeinnamen ogenschijnlijk ook diakritische en andere tekens bevatten. Hierbij gaat het echter om door middel van punycode-gecodeerde tekens die uiteindelijk toch uitsluitend uit een reeks van bovengenoemde tekens bestaan. Een voorbeeld hiervan is: bücher.de, wat in het DNS als xn--bcher-kva.de wordt opgenomen. [1]

36.1.1 Niveaus

Een domeinnaam kan in verschillende niveaus worden opgesplitst. Zo bestaat er hoofdniveau (*Top Level Domain*), middelniveau en onderniveau (subdomein). De verschillende niveaus worden gescheiden door punten in de domeinnaam. Het niveau is zichtbaar door de verschillende delen van de domeinnaam van rechts naar links te lezen.

In het voorbeeld (zie afbeelding rechts) ru.wikipedia.org is org het topleveldomein, wikipedia is het secondleveldomein en ru het subdomein. Wikipedia koos ervoor, hier de ISO-taalcode te gebruiken.

Het is aan de server op het hogere niveau om te bepalen welke onderniveaus bestaan. Voor niet-gedefinieerde subniveaus kan de server naar een ander domein omleiden. Het laagste niveau maakt van de naam een zogenaamde hostnaam. De hostnaam 'www.wikipedia.org' kan dus verwijzen naar een (web)server van 'wikipedia.org'. Maar het is ook mogelijk die verwijzing direct onder 'wikipedia.org' (de zogenaamde apex) te maken, iets wat tegenwoordig vaak voor komt. Webbrowsers zijn dikwijls zo ingesteld dat ze tikfouten of luiheid van de gebruiker automatisch herstellen wanneer de gevraagde website niet (meer) bestaat, bijvoorbeeld naar het hoofdniveaudomein ".com" of het onderniveau "www.".

36.2 TLD

Het achterste gedeelte in het bovenstaande voorbeeld is .org. Dit is een *generic top level domain* (gTLD). Een gTLD is, naast een ccTLD, een van de twee soorten TLD's. TLD's geven meestal het type of het land van de website weer.

- Generic TLD's zijn naast .org (voor non-profitorganisaties), ook .info, .net, .com (voor websites met voornamelijk commerciële doeleinden) en .int (voor internationale organisaties).

Aan deze lijst worden regelmatig nieuwe TLD's toegevoegd. Sinds 2014 zijn ook langere TLD's toegevoegd, zoals .bike, .guru of .agency.

- ccTLD's (Country Code - landcode) zijn de codes van het land waar de website zijn basis heeft, bijvoorbeeld .be voor België en .nl voor Nederland.

De meeste TLD-operators stellen tegenwoordig geen eisen aan het type organisatie dat een domein registreert. Het is dus bijvoorbeeld mogelijk dat een commercieel bedrijf een .org-domeinnaam registreert.

Alle TLD's zijn vastgelegd in de DNS-rootservers. De lijst van TLD's wordt beheerd door Internet Corporation for Assigned Names and Numbers (ICANN). De TLD's afzonderlijk worden beheerd door registries, voluit: *domain name registry*. De registry van .nl is de Stichting Internet Domeinregistratie Nederland (SIDN); voor .be is dit DNS Belgium. Registry's kunnen verschillende voorwaarden stellen aan domeinnamen. Zo mag een .nl-domeinnaam niet korter zijn dan twee tekens, gevolgd door .nl, terwijl technisch gezien een domeinnaam als a.nl ook zou werken. Onder .nl zijn ook geen diakritische tekens mogelijk.

Sinds eind 2005 is gefaseerd de nieuwe domeinnaam .eu voor registratie ter beschikking gesteld. Deze heeft de status van een ccTLD (en dus gelijkgesteld worden met een landcode-domeinnaam). De TLD .eu wordt beheerd door EurID. Tevens bestaat .asia.[2]

Sommige TLD-operators kiezen ervoor om hun domein onder te verdelen in second-level-domeinen (SLD's). Een voorbeeld is .uk, dat onder meer co.uk (voor bedrijven) en org.uk (voor non-profitorganisaties) aanbiedt.

36.3 Registratie

Zowel particuliere personen als bedrijven mogen een domeinnaam als combinatie van een naam met een TLD registreren.

De meeste TLD's maken gebruik van een *registry-registrar-registrant*-model (RRR). De TLD-operator (registry) verleent hierbij de mogelijkheid aan diverse bedrijven (de registrars) om wijzigingen in het TLD aan te maken. Een registrar kan nieuwe domeinnamen aanvragen en de Whois-informatie en nameservers van de domeinnamen bepalen. Deze opzet heeft het voordeel dat de domeinhouders (vaak miljoenen bij bekende TLD's) niet direct zaken hoeven te doen met de TLD-operators. Een registrar betaalt voor het recht om domeinnamen te registreren meestal een vast periodiek bedrag plus een bedrag per domeinnaam.

Het aanvragen van een domeinnaam doe je bij een registrar naar keuze. De registrar is een agent bij DNS Belgium in het geval van een .be-domein en heette bij de SIDN in het verleden 'deelnemer'. Meestal kost een registratie jaarlijks een vast bedrag, waarvan de hoogte mag worden bepaald door de registrar. Soms komen daar ook nog startkosten bij. Niet zelden zitten er tussen de domeinnaam houder ('registrant') nog een of meerdere resellers. Deze zijn niet aangesloten bij de registry, maar opereren via de registrar.

Voor het registreren van een .nl-domein is het lang een voorwaarde geweest een inwoner van of bedrijf in Nederland te zijn. Dit is voor een .be-domein nooit zo geweest, wat maakt dat zo'n 18% van de Belgische domeinnamen in handen van Nederlandse particulieren of bedrijven is. Dit geldt ook voor de mailserver van de Nederlandstalige Wikipedia.

36.4 Technische werking

Een domeinnaam verwijst naar een IP-adres zoals een naam in een telefoonboek naar een telefoonnummer. In de gegevenspakketten die via het computernetwerk verstuurd worden, wordt alleen het IP-adres gebruikt. Omdat domeinnamen veel eenvoudiger te onthouden zijn dan IP-adressen, worden IP-adressen door de meeste mensen niet direct gebruikt.

Per niveau in de domeinnaam kan een andere lijst (DNS-server) geraadpleegd worden om het betreffende nummer op te zoeken. Door deze hiërarchische opbouw kunnen lagere niveaus door de eigenaar van het hogere adres zelf bepaald worden. Dus nadat bijvoorbeeld Wikipedia bij een registrar van de org-registry de domeinnaam wikipedia.org heeft verkregen, kan Wikipedia zelf IP-adressen met als naam www.wikipedia.org, mail.wikipedia.org of 123.wikipedia.org aanmaken. Iedere computer kan die adressen vinden, doordat ze door de DNS-server van .org naar de DNS server van wikipedia.org verwezen worden voor alle subdomeinen die eindigen op .wikipedia.org.

36.5 Statistieken

Eind 1995 waren er in Nederland nog slechts 10.000 .nl-domeinnamen uitgegeven; sinds 2013 meer dan 5 miljoen. In België kan pas sinds 11 december 2000 iedereen .be-domeinnamen registreren. Na deze vrijgave steeg het aantal .be-domeinnamen dan ook van 40.000 eind 2000, een half miljoen medio 2005 tot iets meer dan 1,1 miljoen eind 2010[3]. In 1995 waren er in de VS al 100.000 .com-domeinnamen geregistreerd, in 1997 een forse 1,6 miljoen, tegenwoordig staan er ruim 100 miljoen .com-domeinnamen te boek (het aantal .com-domeinnamen is weer wat gezakt, onder andere door vervallen domeinnamen). Het totaal aantal domeinnamen bedroeg op 1 december 2009 130.473.977.

Nevenstaande tabel toont de resultaten uit een onderzoek naar het aantal domeinen in enkele topleveldomeinen per maart 2013.[4]

36.6 Zie ook

- Domeinkaper
- Domeinnaamrecht
- Internetprovider
- Lijst van topleveldomeinen op het internet
- Webhosting

36.7 Externe links

- https://www.ietf.org/rfc/rfc1035.txt RFC1035
- http://www.sidn.nl/
- http://www.dnsbelgium.be/
- http://www.eurid.eu/nl
- http://whois.domaintools.com/ Whois-service voor alle domeinextensies.
- http://www.iusmentis.com/merken/domeinnamen/jurisprudentie/ domeinnaam-jurisprudentie

Hoofdstuk 37

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (**DHCP**) is een computerprotocol dat beschrijft hoe een computer dynamisch zijn netwerkinstelling van een DHCP-server kan verkrijgen. Het DHCP-protocol is gebaseerd op het Internet Protocol IP en werkt met UDP-pakketten.

37.1 Introductie

Bij DHCP is het principe dat toestellen in een IP-netwerk geen vast geconfigureerd IP-adres hebben, maar hun IP-adres dynamisch verkrijgen van een centraal beheerde DHCP-server. De server, die zelf een vast IP-adres heeft, beheert hiertoe een "pool" van beschikbare IP-adressen. Na opstarten van de DHCP-server zijn die adressen vrij en kunnen ze aangevraagd worden door de toestellen op het netwerk. Door de aanvragen worden de IP-adressen toebedeeld, uiteraard in aantal beperkt tot de grootte van de pool.

Toestellen die op het netwerk komen, kunnen via een aanvraagsequentie een IP-adres verkrijgen dat beperkt geldig is, voor de ingestelde geldigheidsduur, de "lease time". Toestellen die het netwerk verlaten, dienen hun adres vrij te geven. Dit gebeurt uiteraard niet in alle gevallen. Het adres komt echter uiteindelijk toch weer vrij door het verlopen van de geldigheidsduur.

DHCP-servers kunnen voor bepaalde toestellen een vast uit te reiken IP-adres geconfigureerd hebben. Zo kan het bv. zijn dat binnen een bedrijf alle netwerkprinters een vast IP-adres krijgen, dit terwijl andere toestellen een willekeurig adres uit de pool toebedeeld krijgen.

37.2 Oorsprong en classificatie

DHCP vindt zijn oorsprong in het BootP-protocol, dat oorspronkelijk ontworpen was om computers hun besturingssysteem vanaf het netwerk te laten laden. Tegenwoordig bevindt BootP zich net als DHCP in de TCP/IP-suite, om precies te zijn in de internet-laag. Men kan deze laag vergelijken met de netwerklaag in het OSI-model, ofwel laag 3.

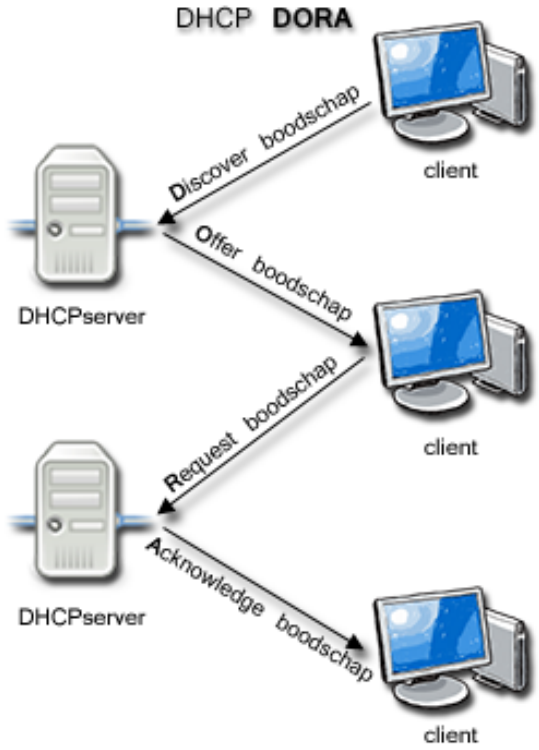
37.3 Voordelen

Gebruik van DHCP heeft belangrijke voordelen voor het netwerkbeheer:

- Men hoeft niet op elk toestel afzonderlijk een IP-configuratie te maken, maar kan de configuratie voor alle toestellen centraal beheren.
- Bij wijzigingen van de netwerkconfiguratie, bv. het gebruiken van andere subnetten, hoeft men alleen centraal een aanpassing te doen.
- Bij verplaatsing van een toestel, bv. naar een andere afdeling met een ander subnet, hoeft men op het toestel geen wijzigingen door te voeren.
- Met DHCP kan men bepaalde regels, "policies", realiseren, bv. door een toestel slechts gedurende een bepaalde tijd een IP-adres te geven. Ook kan men het toegewezen adres regelmatig wijzigen, om de veiligheid te bevorderen. Hier staat echter wel tegenover dat er geen vaste één-op-éénrelatie meer bestaat tussen MAC-adres en IP-adres, wat de traceerbaarheid en daardoor de veiligheid dan weer negatief kan beïnvloeden.
- Men kan efficiënter omgaan met IP-adressen. Stel dat er in een afdeling 1000 mobiele toestellen zijn, maar er maximaal slechts 200 tegelijk aanwezig kunnen zijn. Bij statische allocatie zou men 1000 adressen moeten gebruiken. Bij dynamische allocatie kan men daarentegen gebruikmaken van een "pool" van 200 adressen. Met name voor dienstenaanbieders die publieke IP-adressen aan gebruikers moeten geven, is dit traditioneel zeer belangrijk. Wel neemt het belang in zekere zin af doordat veel toestellen continu of quasi-continu verbonden zijn. Aan de andere kant is het aantal IP-adressen waarover een aanbieder beschikt beperkt en zijn er ook kosten aan verbonden, waardoor het van groot belang blijft hier efficiënt mee om te gaan.

37.4 Protocol

Een toestel dat een IP-adres wenst te verkrijgen, dient daartoe een sequentie van aanvraag te starten. Bij een correcte configuratie van het netwerk zal ten minste één DHCP-server op de aanvraag moeten reageren. Het aanvragende toestel kan vervolgens de finale aanvraag doen, waarop de aanbiedende server normaal bevestigend zal antwoorden. Vanaf dat moment maakt het aanvragende toestel deel uit van het netwerk ook op de internetlaag en kan het op IP-pakketten gebaseerde communicatie uitvoeren. Het is mogelijk dat er zich meer dan één DHCP-server op het netwerk bevindt, voor verschillende subnetten.



DHCP DORA (D)iscover (O)ffer (R)equest (A)ck proces

Het volledige proces ter verkrijging van de netwerkinstellingen bestaat uit een sequentie van vier aanvragen en reacties. Dit proces staat bekend onder de afkorting **DORA**. (**D**)iscover (**O**)ffer (**R**)equest (**A**)cknowledge.

Hieronder het verloop van een succesvolle aanvraag, met vermelding van de naam van de boodschap binnen het DHCP-protocol tussen haakjes:

- DHCP discovery (DHCPDISCOVER): het aanvragende toestel, de client, stuurt een netwerkpakket gericht aan alle computers binnen het eigen Ethernet-segment door het gebruik van broadcast. Hiervoor gebruikt de aanvrager ofwel het globale broadcastadres 255.255.255.255, dan wel het broadcastadres van het netwerksegment waarop het zich bevindt. Alle toestellen in het betreffende netwerksegment ontvangen dit DHCPDISCOVER-pakket.
- DHCP offer (DHCPOFFER): uitsluitend de DHCP-server of eventueel DHCP-servers in het netwerk behoort/behoren te reageren op het DHCPDISCOVER-pakket. Elke DHCP-server die wenst te antwoorden reserveert een nog vrij IP-adres en stuurt een DHCPOFFER pakket terug naar het MAC-adres van de aanvrager, met vermelding van het aangeboden IP-adres.
- DHCP request (DHCPREQUEST): het aanvragende toestel weet nu van welke server of servers deze het IP-adres kan verkrijgen. Het toestel gebruikt DHCPREQUEST om daadwerkelijk de aanvraag te doen bij de eerst reagerende DHCP-server en mogelijke overige DHCP-servers te laten weten dat het een IP-adres heeft verkregen via een andere DHCP-server. Dit gebeurt dientengevolge net als bij DHCPDISCOVER met een broadcast-pakket, dat door alle DHCP-servers wordt ontvangen.
- DHCP acknowledgement (DHCPACK): de DHCP-server bevestigt hiermee de aanvraag. Het verzonden DHCPACK-pakket bevat nog eens alle informatie met de netwerkinstellingen. Het toestel dat het nieuwe IP-adres heeft ontvangen, zou op dit punt een test moeten uitvoeren om zeker te stellen dat er toch geen andere toestellen hetzelfde IP-adres in bezit hebben.

De client gebruikt dus de gegevens van de eerste DHCP-server waarvan hij antwoord krijgt en gebruikt deze gegevens om zijn netwerkverbinding in te stellen. De betreffende computer heeft nu een uniek IP-adres en kan derhalve vervolgens communiceren met andere toestellen.

Uiteraard is het ook mogelijk dat de aanvraag niet slaagt, door een fout of een reeds bestaande allocatie. Hiertoe dienen de volgende DHCP-berichten:

- DHCP negative acknowledgement (DHCPNAK): bij een fout zal de DHCP-server antwoorden met een DHCP-NAK-pakket.
- DHCP decline (DHCPDECLINE): het clienttoestel rapporteert terug naar de DHCP-server dat het netwerkadres reeds in gebruik is.

Een clienttoestel kan het in gebruik zijnde IP-adres ook weer vrijgeven:

- DHCP release (DHCPRELEASE): het clienttoestel rapporteert terug naar de DHCP-server dat het netwerkadres vrijgegeven mag worden en annuleert hierdoor de huidige *leasetime*.

Gegevens die onder meer (kunnen) worden doorgestuurd zijn:

- Een uniek netwerknummer (IP-adres);
- Welk(e) adres(sen) in het netwerk een gateway is/zijn, waarmee er verbinding is met een ander netwerk, zoals het internet (niet noodzakelijk);
- Wat de naamserver(s) (DNS-servers) is/zijn (niet noodzakelijk);
- Hoe groot het netwerk is, dus onder welke omstandigheden de doelcomputer binnen het netwerk ligt of via de gateway benaderd moet worden. Dit wordt de netmask genoemd.
- De geldigheidsduur (*leasetime* of looptijd)

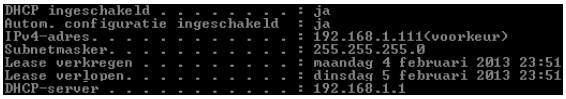
37.5 Handmatig

Het is niet noodzakelijk om DHCP te gebruiken. Een computer kan ook handmatig van de correcte instellingen worden voorzien. In de praktijk echter vinden veel systeembeheerders DHCP eenvoudiger, omdat zij dan niet zelf alle computers in het netwerk handmatig hoeven te configureren. Ook als er zich wijzigingen in het netwerk voordoen, hoeft alleen de DHCP-server van de nieuwe instellingen te worden voorzien.

In veel grote netwerken wordt juist wél gewerkt met vaste IP-nummers (en dus geen DHCP), om op die wijze voor tienduizenden PC's de instellingen eenmalig handmatig te verrichten. Daarmee kunnen ook eenvoudiger routes van het ene netwerkapparaat (PC) naar het andere (een printer bijvoorbeeld) worden opgegeven, op basis van het IP-adres. Eén van de grootste netwerken in Nederland (Defensie MULAN) is op deze wijze ingericht. Bijkomend voordeel op gebied van beveiliging is dat IP-pakketten van onbekende MAC-adressen meteen kunnen worden gedetecteerd.

37.5.1 ISP's

Internet Service Providers maakten ook graag gebruik van DHCP. Zo konden ze het aantal benodigde IP-adressen beperken, omdat niet al hun abonnees tegelijkertijd verbinding maken. Dit aantal was dan gelimiteerd aan het aantal modems dat bij deze ISP aanwezig was (door landelijke uitrol ADSL en kabelinternet achterhaald). Omdat veel computers met ADSL of kabelinternet continu op het internet aangesloten zijn (als het modem thuis aan blijft staan), is tegenwoordig (2009) elke abonnee voorzien van een eigen IP-adres. Een paar aanbieders schermen nog met 'dynamisch IP-adres' maar dit is met name om geen garantie te geven dat men altijd hetzelfde IP-adres blijft houden.



Voorbeeld van DHCP lease, waarbij de DHCP-server (192.168.1.1) een client het adres 192.168.1.111 heeft gegeven met een lease *van 86400 seconden (1 dag).*

37.6 Looptijd

Aan de DHCP-gegevens is een bepaalde *leasetime* of looptijd gekoppeld, variërend van enkele minuten tot enkele weken. In die tijd is het IP-adres voor deze specifieke computer gereserveerd. Voordat de leasetijd verlopen is moet de computer opnieuw een aanvraag indienen, en krijgt dan eventueel een ander IP-adres (maar meestal hetzelfde IP-adres). Als een computer, of netwerkverbinding, herstart tijdens de looptijd van een *lease* voorziet het protocol in een voortzetting van het reeds verkregen IP-nummer zodat de eerste stap (initiële aanvraag) overgeslagen wordt en een verlenging gebruikt wordt. Voor het opnieuw uitgeven van IP-adressen gebruikt de DHCP-server een groep adressen ('pool'). Deze pool is bij thuisgebruik vaak 50 adressen, bijvoorbeeld van 192.168.1.100 - 192.168.1.149.

37.7 Breedband

In het geval van breedband-internetverbindingen, zoals kabelinternet en ADSL, wordt vaak ook met DHCP gewerkt, hoewel een aantal providers ook vaste adressen uitdeelt. Mensen met een dynamisch IP-adres zullen iets meer moeite moeten doen als zij een server willen draaien. Hoewel hun IP-adres over het algemeen hetzelfde zal blijven (toegewezen op basis van hun MAC-adres), kan het zijn dat het toch verandert. Dit gebeurt bijvoorbeeld als de host langere tijd offline is geweest (en het IP-adres is vrijgegeven of zelfs al toegewezen aan iemand anders), of als er bijvoorbeeld een andere netwerkkaart wordt geplaatst. De ISP herkent dan het MAC-adres van de host niet meer. Eventuele DNS-instellingen moeten dan worden aangepast. Dit kan handmatig of automatisch door middel van een script (zoals DynDNS) gebeuren.

37.8 Problemen bij DHCP

Wanneer de computer niet als zodanig is ingesteld dat deze zelf aan de DHCP-server verlenging van de looptijd vraagt, of er is langere tijd geen DHCP-server beschikbaar, wordt de verbinding met een regelmaat van een half uur tot een dag tijdelijk verbroken. Dit kan bij applicaties als IRC hinderlijk zijn. Ook het onjuist instellen van de DHCP-server en/of de overige netwerkapparatuur kan problemen geven: indien een netwerkgebruiker een IP-adres gebruikt dat binnen de pool van de DHCP-server

ligt, dan zijn er op een gegeven moment twee netwerkapparaten met hetzelfde IP-adres. Hierdoor ontstaan op ethernetverbindingen veel collisions en haperende apparatuur. Het reserveren van adresgebieden is van groot belang.

37.9 DHCP Authentication

Om DHCP veiliger te maken werd in juni 2001 authenticatie voor DHCP-berichten bedacht. DHCP Authentication is beschreven in RFC 3118[1] en is een verbetering in de beveiliging die de normale DHCP-berichten met geverifieerde servers/clients vervangt. Clients en servers controleren de afkomst van de bron met verificatie-informatie en berichten. Indien ongeldig zal de bron geweigerd worden. Een DHCP Authentication-server kan tevens overweg met clients die alleen het standaard DHCP-protocol ondersteunen.

37.10 DHCP Relay Agent

In grotere, typisch hiërarchisch georganiseerde netwerkomgevingen met vele subnetten en verschillende IP-reeksen is het niet efficiënt om één DHCP-server per LAN/subnet op te zetten en te onderhouden. Voor dergelijke netwerken zal men er daarom de voorkeur aan geven om te werken met een of meer centrale DHCP-servers die IP-adressen kunnen toewijzen voor verschillende LANs/subnetten. Dit betekent echter dat DHCP-verkeer tussen de verschillende LANs en de DHCP-server mogelijk moet zijn, waarbij er toestellen op hogere lagen dan de datalinklaag, zoals routers, moeten worden gepasseerd. Om dit toe te laten kan men werken met *DHCP-relay-agents*.

Een DHCP-relay-agent communiceert met een DHCP-server in een ander IP-netwerk (segment) en fungeert als een proxy voor DHCP-broadcastberichten die moeten worden gerouteerd naar dat andere IP-netwerk. Hierdoor verloopt het DHCP-verkeer, in verschillende netwerken, transparanter.

Om de DHCP-relay-agent goed DHCP-verkeer te laten uitwisselen is het essentieel om zowel een DHCP-server als een DHCP-relay-agent te hebben in de andere IP-netwerken. De DHCP-relay-agent wordt geïnstalleerd op een geschikt apparaat (router, modem of server) dat het protocol ondersteunt.

Het gebruik van een DHCP-relay-agent compliceert op zich de opzet en is daardoor doorgaans alleen geëigend voor grote, complexe netwerkomgevingen met vele subnetten, waar centralisatie meer voordelen biedt dan het behouden van eenvoud op het niveau van de individuele netwerksegmenten.

37.11 DHCP MAC Binding

DHCP wijst een willekeurig IP-adres toe aan elk apparaat in het netwerk. Om te voorkomen dat een apparaat steeds een ander IP-adres krijgt bestaat er MAC-binding (Bind IP to MAC). In feite doet MAC-binding niets anders dan dit: Een MAC-adres met een vast IP-adres reserveren in het netwerk met een leasetime die nooit verloopt. Het grote voordeel hiervan is dat er een betere controle is op de apparaten binnen een netwerk en het beheer met DHCP doeltreffender is. MAC-binding kent twee mogelijkheden:

- Normal mode: Het apparaat met MAC-adres krijgt steeds hetzelfde IP-adres en zal niet verlopen.
- Strict mode: Het apparaat met MAC-adres krijgt steeds hetzelfde IP-adres en zal niet verlopen. Niet geautoriseerde apparaten krijgen wel een tijdelijk IP-adres maar kunnen niet de router/server bereiken waarop MAC Binding werkt. Toegang tot internet wordt tevens geblokkeerd.

37.12 Voorbeeld bij ADSL

Een mogelijke instelling zoals bij ADSL gebruikt kan worden: 10.0.0.0

10.0.0.1 standaard gateway (ADSL-modem)

10.0.0.150 - 10.0.0.200 pool van uit te geven IP-adressen

10.0.0.255 broadcastadres (bericht aan alle netwerkstations in dit segment)

Apparatuur die via DHCP werkt, krijgt van de DHCP-server op aanvraag een adres uit de adressen-pool. Overige apparatuur op het netwerk dat niet met DHCP werkt (dus handmatig of fabrieksmatig is ingesteld) moeten buiten dit adressen-gebied blijven. Een mogelijke indeling zou kunnen zijn:

10.0.0.10 - 10.0.0.50 netwerkopslagapparatuur (NAS) en netwerkprinters

10.0.0.51 - 10.0.0.100 PC's op vaste adressen

37.13 Zie ook

- DHCP-snooping
- Voor algemene info over computernetwerken zie computernetwerk
- Voor info over huisnetwerken, zie huisnetwerk

37.14 Externe link

- (en) RFC 2131 Dynamic Host Configuration Protocol

Hoofdstuk 38

E-mail

E-mail is de naam van digitaal, elektronisch postverkeer. Zowel het individuele bericht als het onderliggende systeem kunnen met e-mail worden bedoeld. Als synoniemen worden gebruikt: mail, e-post, e-brief, elektronische post en elektronische brief.

38.1 Algemeen

De eerste e-mail over een computernetwerk werd in 1971 door Ray Tomlinson verzonden. Rond 1995 werd het populair bij het grote publiek toen het internet meer algemeen toegankelijk werd. E-mail kan echter ook met andere technieken dan het internet verstuurd worden.

Recentelijk heeft communicatie per e-mail in Nederland en België dezelfde wettelijke status gekregen als die per brief. De e-mails moeten dan wel aan een aantal voorwaarden voldoen. De authenticiteit moet zijn gewaarborgd; er moet zekerheid bestaan over de afzender, en er moet niet achteraf aan kunnen worden geknoeid. De zogenaamde "elektronische handtekening" biedt hier uitkomst.

De lage kosten van het verzenden van e-mail hebben al vroeg geleid tot het verschijnsel spam: ongevraagde reclame via e-mail die doorgaans weinig doelgericht wordt verstuurd aan grote aantallen ontvangers.

Voorgangers van e-mail zijn de brief, het telegram, de telex, de telefax en binnen Nederland het op Datanet gebaseerde Memocom 400 dat echter nooit succesvol werd. In de context van e-mail wordt de veel tragere briefpost wel *snail mail*, Engels voor slakkenpost, genoemd.

In tegenstelling tot briefpost heeft e-mail een informeler karakter. Veelal besteedt de schrijver minder aandacht aan opmaak en zinsbouw. Hoewel de e-mail primair tekst bevat, ontstonden al snel mogelijkheden om andere data mee te sturen die daartoe als letters in een afzonderlijk tekstblok gecodeerd werden. Tegenwoordig wordt hiervoor doorgaans de MIME standaard gebruikt. De andere data wordt “bijlage” of in het Engels “attachment” genoemd.

38.2 E-mail via mobiel internet

E-mail via mobiel internet is een van de vormen van mobiele communicatie van teksten en andere bestanden, naast sms, mms, WhatsApp, enz.

38.3 Etymologie

De Engelse term *mail* is afgeleid van het woord voor reistas (1205), verwant met Oudfrans *male* (beurs), < Frankisch **malha*, Indo-Europees **molko-* “huis, tas”. Via de brieventas heeft het begrip zich ontwikkeld tot de drager van de poststukken (1654) en uiteindelijk tot het bericht zelf. De Oxford dictionary legt het e- voorvoegsel als volgt uit: “Het gebruik van elektronische dataverzending, vooral via internet”.[1].

38.3.1 Schrijfwijze

Internationaal is *email* de meest gebruikte versie. De officiële Nederlandse spelling is *e-mail*, dus met streepje, omdat het een samenstelling is met een letter.[2]

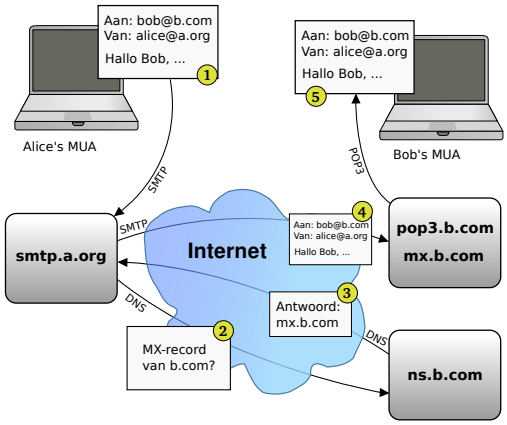
38.4 Techniek

Technisch wordt e-mail beschreven in RFC 561 en RFC 861 In hoofdzaak zijn twee typen functies benodigd:

1. de zogenaamde MUA (Mail user agent), het softwareprogramma dat de gebruiker van de e-mail ziet en gebruikt om e-mail te lezen en schrijven.

2. de zogenaamde MTA (Mail transfer agent), het softwareprogramma dat de e-mail van de MUA aanneemt en verder verstuurt naar een volgende MTA of naar een MUA.

De MTA is vergelijkbaar met de postbode en de keten van postkantoren in het traditionele briefverkeer.



38.4.1 Routering en infrastructuur

Over het algemeen wordt een e-mail niet direct naar de ontvanger gestuurd, maar verloopt de verzending via een of meer tussenschakels.

Elke e-mail wordt door de MUA voorzien van een koptekst (Engels: header) die van de door de gebruiker geschreven tekst gescheiden is met twee regelovergangen. In deze header staan onder meer de gegevens die de MTA benodigd bij het doorsturen van de e-mail. Een e-mail kan naar meerdere adressen doorgestuurd worden afhankelijk van de adressering.

Als de geadresseerde en alle tussenstation online zijn, kan een e-mail in seconden op de plaats van bestemming zijn. Het protocol garandeert dit echter niet. Wat wel door het protocol gegarandeerd wordt, is dat de e-mail door de MTA na een instelbare tijd als “onbestelbaar” wordt teruggestuurd naar de afzender. Traditioneel zal de MTA ingesteld zijn om na enkele uren ter informatie een waarschuwing aan de afzender te sturen; na vijf dagen geeft de MTA het op en stuurt de e-mail retour.

Bounce

Het terugsturen van de e-mail lukt om uiteenlopende reden niet altijd. Dan is er sprake van een zogenaamde “bounce” (ping-pong). De MTA probeert zo'n situatie te herkennen en geeft dan alle pogingen voor deze e-mail op.

Ontvangstbevestiging

Sommige MUA's bieden aan om een ontvangstbevestiging te vragen bij de ontvanger. Daar dit niet in het oorspronkelijke e-mailprotocol was opgenomen, is er geen garantie dat dat werkt. Dat is dan mede afhankelijk van de MUA die de ontvanger gebruikt.

Voor de MTA is een ontvangstbevestiging een onafhankelijke e-mail die op zijn beurt al dan niet succesvol ergens moet worden afgeleverd.

38.4.2 SMTP en Internet

Voor het doorsturen van e-mail wordt gebruikgemaakt van een aantal andere internetdiensten, met name DNS. Een e-mailgebruiker gebruikt een bepaald e-mailaccount, bijvoorbeeld bij een Internet Service Provider of een andere aanbieder van e-maildiensten zoals Gmail, Yahoo!, Hotmail of Windows Live Mail.

Aan een e-mailaccount is een e-mailadres gekoppeld, dat nodig is om e-mail te kunnen ontvangen. Dit adres is opgebouwd uit een aantal delen: een gebruikersnaam, het @-teken, server- of ISP-naam, en het top-level domain, bijvoorbeeld .nl.

Voorbeeld: jan.jansen@provider.nl

Hier is:

- “jan.jansen” de gebruikersnaam
- “provider” de domeinnaam (kan de ISP-naam zijn)
- ".nl” de top-level-domain-aanduiding

38.4.3 SMTP

Het Simple Mail Transfer Protocol is de de facto standaard voor het verzenden van e-mail via het internet.

38.4.4 UUCP

Vooral in de begintijd van het e-mailverkeer en voordat het internet als zodanig algemeen toegankelijk was, werd e-mail veelal met het UUCP-protocol verstuurd. De adressering ziet er daarbij anders uit: een reeks van adressen van tussenstations, gescheiden door uitroeptekens. Doordat alle tussenstations in het adres zijn opgenomen, is er geen centrale database zoals DNS nodig om de e-mail door te sturen.

38.4.5 Websites als MUA

Een andere manier om e-mail te versturen is via een website. Daarbij wordt aan de gebruiker bijvoorbeeld formulier gepresenteerd. Bedrijven maken graag van deze mogelijkheid gebruik om de inhoud van de e-mail (deels) te standaardiseren door bijvoorbeeld keuzelijsten aan te bieden met productgroepen of de gebruiker te verplichten bepaalde adresgegevens te versturen. Het bedrijf hoeft daarbij zijn e-mailadres niet te publiceren en ontvangt daardoor minder spam.

Nadelen

De gebruiker is minder vrij in het schrijven van de e-mail, de interface biedt gewoonlijk minder functies als het eigen bekende e-mailprogramma en doorgaans is het niet mogelijk, bijlages te versturen langs deze weg.

38.4.6 Brievenbus voor e-mail

E-mail kan, net als gewone briefpost, onderweg in een brievenbus landen. Deze brievenbus kan door een MUA direct worden gelezen of via een Post Office Protocol of Internet Message Access Protocol. De functie en werking van deze systemen is in de betreffende artikelen beschreven.

38.5 Misbruik

In de bijlage kunnen virussen en andere schadelijk software verstuurd worden. Als de MUA deze zonder meer uitvoert, is dat voor de ontvanger een probleem.

Spam is niet alleen een ergernis voor de ontvanger. Meer dan 90% van het e-mail verkeer is ongevraagde reclame en zodoende een last voor de verbindingscapaciteit en voor de verwerkingscapaciteit van computers en gebruikers.

Net als bij briefpost is er geen garantie dat het afzenderadres correct is. Door dit hiaat kan iedereen een e-mail versturen met een vals afzendadres. Hierdoor krijgen internetgebruikers e-mails in hun postvak die zich voordoen als belangrijke berichten en de gebruiker oproepen actie te ondernemen waardoor ze persoonlijke gegevens zouden meedelen via een nagemaakte website. Deze vorm van misbruik wordt phishing genoemd. Bij phishing wordt onder valse voorwendselen een ongevraagde e-mail verstuurd, waarbij de ontvanger gevraagd wordt om bepaalde informatie, zoals een wachtwoord of een pincode.

38.6 Nevenwerking van e-mailverkeer

De laagdrempeligheid van het schrijven van een e-mail heeft invloed op de onderlinge communicatie en brengt ook gevaren met zich mee.

Onderzoek wees uit dat e-mailverkeer op de werkplek persoonlijk contact tussen collega's onder druk zet en zorgt voor een minder prettige werksfeer. De helft van de collega's e-mailt of belt elkaar terwijl men net zo makkelijk even langs kan lopen.[3] Vanwege dit spontane contactverlies *face to face*, bande het ICT-bedrijf Atos het dikwijls onnodige e-mailen zo veel mogelijk onder zijn personeel.[4]

Vaak worden in professionele elektronische correspondentie grote groepen personen ingekopieerd die slechts zijdelings bij het werk betrokken zijn. Vaak worden ook korte boodschappen die slechts voor een enkele persoon relevant zijn ('OK', 'Bedankt', 'Zal ik doen', 'Ja', 'Nee') op deze manier met iedereen gedeeld. Het lezen van onbenullige e-mails blijkt ook nefast te zijn voor de concentratie op de werkplek. Zo blijkt het 64 seconden te duren om terug in gang te schieten na het lezen van zo'n e-mail.

Een ander nadeel van (zakelijke) e-mail is dat fouten en onzorgvuldigheden sneller kunnen voorkomen en soms met grote gevolgen, nou juist omdat het medium zo laagdrempelig is en omdat men zo makkelijk met vele mensen tegelijk kan communiceren. Vaak wordt het met de etiquette, tekstindeling, aanhef en taalgebruik minder nauw genomen. Ook boze of schadelijke inhoud is zo verstuurd. In een brief schiet men minder snel uit de slof doordat men het stuk eerst moet typen of printen, en vervolgens in een envelop stoppen, posten en frankeren. Deze handelingen bouwen een zekere bedenktijd in. Een e-mail is zo (aan iedereen) verstuurd. Onzorgvuldig e-mailverkeer heeft in een aantal gevallen zeer nadelige gevolgen voor personen gehad.

38.7 Nederland

38.7.1 E-mailgedragslijn voor overheden

Sinds december 2005 geldt/gold in Nederland een *E-mailgedragslijn voor overheden*. Deze gedragslijn van *burger@overheid*, een adviesorgaan dat tot 2007 bestond, geeft / gaf aan hoe de overheden moeten handelen bij ontvangst, beantwoording en archivering van e-mail en gaat ook in op het hanteren van richtlijnen en het monitoren van prestaties.

Deze gedragslijn omvat de volgende punten:

- A. *Bereikbaarheid*

Elke overheidsinstantie is bereikbaar per e-mail. Een instantie die niet bereikbaar is per e-mail, maakt de reden van dit besluit bekend op de website.

- B. *Ontvangstbevestiging*

Bij binnenkomst van een e-mail wordt per omgaande een *ontvangstbevestiging* gestuurd, tenzij de betreffende e-mail direct wordt afgehandeld. De ontvangstbevestiging geeft aan binnen hoeveel dagen na ontvangst van de e-mail een eerste reactie kan worden verwacht.

Zolang een burger geen eigen dossier bij het overheidsorgaan in kwestie heeft waarmee hij zijn contacten kan beheren, adviseert *burger@overheid* een referentienummer toe te kennen waarnaar de aanvrager kan verwijzen.

- C. *Afhandeling*

Bij de afhandeling van e-mail wordt onderscheid gemaakt naar eenvoudige en complexe vragen. Eenvoudige vragen hebben betrekking op bekende feiten of procedures, zoals openingstijden, parkeerregels, vergunningprocedures etc. Dit soort vragen dient binnen twee werkdagen te worden afgehandeld. Complexe vragen of verzoeken kunnen meer tijd in beslag nemen. In ieder geval wordt de afzender binnen 10 werkdagen geïnformeerd over de verwachte afhandelingstermijn. Wanneer een overheidsinstantie voorziet dat een toegezegde afhandelingstermijn niet kan worden nagekomen, stelt zij de afzender hiervan direct op de hoogte en geeft een nieuwe termijn af.

- D. *Archivering*

E-mail wordt op een goede en veilige manier gearchiveerd, volgens dezelfde regels die gelden voor brieven.

- E. *Richtlijnen*

Elke overheidsinstantie hanteert heldere richtlijnen voor de afhandeling van e-mail. Burgers kunnen hier kennis van nemen via de website van de betreffende instantie. Ook worden burgers geïnformeerd over de wijze waarop klachten over de behandeling van e-mail kunnen worden ingediend.

- F. *Openbaar maken van prestaties*

Elke overheidsinstantie meet regelmatig haar prestaties met betrekking tot de afhandeling van e-mail en maakt deze openbaar, bijvoorbeeld via publicatie op haar website of in haar jaarverslag.

38.7.2 Juridische waardering

Op 24 maart 2009 werd door de rechtbank Zwolle, in een bestuursrechtelijke zaak tegen het UWV met betrekking tot een weigering van een WW-uitkering na een vrijwillig overeengekomen beëindiging van een arbeidsovereenkomst, uitgesproken dat, gelet op de ontwikkelingen in de moderne communicatie, ook correspondentie per of vastlegging in e-mail in beginsel kan worden aangemerkt als *"schriftelijk"*[5] .'

Om een overeenkomst te sluiten tussen twee partijen moet één partij een aanbod doen dat door de andere wordt geaccepteerd. De wijze waarop is in principe vrij. Het kan dus ook per e-mail, en geldt dan als *"koop of afstand"*[6][7] .

Ook als de overeenkomst schriftelijk moet worden gesloten, kan dat volgens het Burgerlijk Wetboek onder voorwaarden per e-mail (BW Boek 6, artikel 227a[8]):

1. Indien uit de wet voortvloeit dat een overeenkomst slechts in schriftelijke vorm geldig of onaantastbaar tot stand komt, is aan deze eis tevens voldaan indien de overeenkomst langs elektronische weg is tot stand gekomen en

a. raadpleegbaar door partijen is;

b. de authenticiteit van de overeenkomst in voldoende mate gewaarborgd is;

c. het moment van totstandkoming van de overeenkomst met voldoende zekerheid kan worden vastgesteld; en

d. de identiteit van de partijen met voldoende zekerheid kan worden vastgesteld.

Als een overeenkomst via e-mail is gesloten, kan die overeenkomst ook weer via e-mail worden ontbonden. (BW Boek 6, artikel 267[9])

38.8 Zie ook

- IMAP, het Internet Message Access Protocol gebruikt om e-mail te ontvangen.
- POP3, het Post Office Protocol gebruikt om e-mail te ontvangen.
- SMTP, het Simple Mail Transfer Protocol gebruikt om e-mail te versturen.
- Webmail
- Gmail, gratis service van Google om e-mailberichten te ontvangen en te verzenden.
- Windows Live Hotmail, gratis e-mailservice van Microsoft
- Autoresponder, antwoordapparaat voor e-mail
- Push e-mail, e-mail die real-time gedownload wordt
- Private message
- Webbaken, een afbeelding die gebruikt wordt voor tracking

38.9 Externe link

- (en) Richard Griffiths. History of Electronic Mail Geraadpleegd op 30 oktober 2010

W

Hoofdstuk 39

Emoticon

Emoticons zijn weergaven van emoties door middel van een afbeelding, een teken of een combinatie van lees- en lettertekens. De volgende tekenreeks is een emoticon die een lachend gezicht (een *smiley*) voorstelt:

:-)

Het emoticon begon als een korte tekenreeks die een gezichtsuitdrukking uitbeeldt en waarmee de schrijver van een tekst een gevoel wil uitdrukken. Vooral bij toepassingen als e-mail, sms en chatten, waar vaak korte berichten uitgewisseld worden, helpt het emoticon om de bedoeling van de schrijver toe te lichten.

39.1 Interpretatie

Om deze emoticons goed te kunnen lezen, moet het hoofd een kwartslag naar links worden gedraaid. Op deze manier zijn de uitdrukkingen beter te herkennen. Niet alle emoticons zijn even herkenbaar of accuraat. De dubbele punt stelt meestal de ogen voor, het minteken de neus, en het openings- of sluitingshaakje de mond. De neus wordt vaak weggelaten om typ-economische redenen omdat deze in vrijwel elk volledig emoticon hetzelfde is.

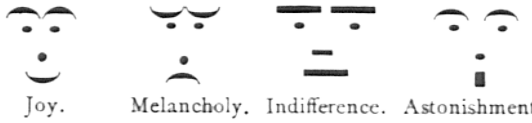
De emoticons die het meest gebruikt worden, en ook door de meeste lezers wel herkend worden, zijn wel de :-) en de :-(- een blij en een droevig gezicht. Voor sommigen is het emoticon een cultsymbool geworden, waarmee zij zich van de grote massa kunnen onderscheiden.

Enkele bekende emoticons:

39.2 Geschiedenis

Op 11 juni 1841 publiceerde de lithograaf en uitvinder Marcellin Jobard een artikel waarin hij gebruikmaakt van het ironieteken. In het verslag *Les lacunes de la typographie* (De tekortkomingen van de typografie)[1] uit 1842 beschrijft hij het gebruik van tekens om emoties in teksten over te brengen.

Verticale typografische tekens werden al op 30 maart 1881 gepubliceerd in een artikel in het Amerikaanse satirisch blad *Puck*.



Rechtopstaande "emoticons" afgedrukt in de Puck *van 30 maart 1881*

Op 19 september 1982 typte Scott Fahlman, computerwetenschapper aan de Carnegie Mellon University, de eerste :-). Dit wordt gezien als de geboorte van het emoticon. Hij gebruikte de emoticons voor het eerst op het interne bulletinboard van de universiteit. Nadat een studentengrap over een besmetting aan de universiteit voor onrust had gezorgd, was er een debat ontstaan over de grenzen van de humor binnen de instelling. Fahlman stelde een symbooltje voor om aan te geven welke boodschappen niet helemaal serieus bedoeld zijn. [2]

Het bericht zag er als volgt uit:

De smiley werd een succes. Vandaag de dag zijn er allerlei varianten in gebruik. Er bestaat inmiddels een groot aantal Unicode-tekens voor smileys (0x2639: ☹ 0x263a: ☺ en 0x263b: ☻) en andere emoticons. Het originele bericht was jaren onvindbaar. Pas in 2002 zijn, na uitgebreid onderzoek, de opgeslagen back-uptapes teruggevonden. Fahlman ziet zijn bedenksel als 'zijn cadeautje aan de wereld'. Hij heeft er nooit geld mee verdiend.

39.3 Grafische emoticons

In 1997 zag de Fransman Nicolas Loufrani hoe het gebruik van ASCII-emoticons binnen de mobiele technologie toenam, en hij begon te experimenteren met bewegende smileys.[3][4] Hij wilde zo een kleurige, verbeterde versie van de uit leestekens bestaande ASCII-emoticons creëren voor meer interactief digitaal gebruik. Hierna maakte Loufrani een online lijst met emoticons.[5] De emoticons waren onderverdeeld in categorieën: klassiekers, humeur, vlaggen, feest, grappig, sport, weer, dieren, eten, landen, beroepen, planeten, sterrenbeelden en baby's. De

ontwerpen werden in 1997 geregistreerd bij het United States Copyright Office en in 1998 als gif-bestanden op het internet geplaatst - de allereerste grafische emoticons in de geschiedenis.[6]

39.4 Bekend citaat

> «*The English language, complete with irony, satire, and sarcasm, has survived for centuries without smileys. Only the new crop of modern computer geeks finds it impossible to detect a joke that is not Clearly Labelled as such.*»
>
> Ray Shea, op de nieuwsgroep rec.music.misc, Link

39.5 Gebruik van emoticons

Emoticons worden voornamelijk gebruikt bij het chatten of bij het versturen van e-mail. Door de opkomst van nieuwe communicatiekanalen wordt het emoticon ook gebruikt in weblogs en sms.

Tegenwoordig is het gangbaar de emoticons weer te geven als (bewegende) afbeeldingen (animated gif). Deze trend is voornamelijk afkomstig van bulletinboards en *instant messaging*-programma's. Hierdoor is het onderscheid tussen emoticon en geanimeerde afbeelding voor sommige gebruikers enigszins vervaagd. In de regel zijn emoticons klein en dienen zij als aanvulling op de tekst.

Op internet zijn vele emoticons te vinden die kunnen worden geïnstalleerd ter vervanging van de afbeeldingen in een *instant messaging*-programma, een mobiele telefoon of een bulletinboard. Er zijn ook websites die geld vragen voor het downloaden van emoticons.

39.6 Overzicht emoticons

39.7 Overige emoticons

39.8 Japanse emoticons

In Japan gebruikt men ook emoticons, misschien nog wel meer dan in westerse landen. Deze zijn anders dan de emoticons die hier bekend zijn. Je hoeft je hoofd geen kwartslag te draaien, de bovenkant is gewoon boven en de onderkant onder. Een bekend voorbeeld is (^_^), een glimlachende smiley. Door de haakjes wordt vaak de rand van het hoofd getekend. Soms worden de haakjes in het emoticon weggelaten of zelfs ook de streep in het midden. Dan krijg je ^_^ of ^^. Dat zijn alleen nog de ogen (en de mond).

Japanners zijn heel inventief met emoticons en Japanse emoticons zijn vaak een stuk complexer dan westerse. Zo kun je zichtbaar maken waar het emoticon heen kijkt door een spatie toe te voegen. Op deze manier: (^_^) kijkt hij naar (voor de kijker) rechts.

Ook worden Japanse tekens gebruikt: \(^∀^)□(^∀^)□ (dit emoticon stelt vriendschap voor). De armen in het midden zijn hier een Japans karakter.

Het Japanse katakana-teken □ wordt ook wel eens gebruikt om blijdschap uit te drukken.

39.9 Zie ook

- Emoji
- Jiong / □

Hoofdstuk 40

Encryptie

Binnen de cryptografie staat **encryptie** voor het coderen (versleutelen) van gegevens op basis van een bepaald algoritme. Deze versleutelde gegevens kunnen nadien weer gedecrypteerd (ontcijferd of gedecodeerd) worden zodat men de originele informatie weer terugkrijgt. Dit proces wordt **decryptie** genoemd.

Eén van de bedoelingen van cryptografie is dat gegevens veilig uitgewisseld kunnen worden tussen twee personen over een onveilig communicatiekanaal, dat wil zeggen een communicatiekanaal waar ook derden toegang toe kunnen hebben, zoals het internet. De versleuteling zorgt er dan voor dat deze derden de gegevens niet kunnen lezen. Dit gebeurt meestal door het gebruik van sleutels. Wat precies een sleutel vormt verschilt per algoritme, maar meestal is een sleutel een reeks van tientallen of honderden cijfers en letters. Het doel van het cryptografische algoritme is dan om er voor te zorgen dat alleen de personen met de juiste sleutel de versleutelde gegevens weer kunnen ontcijferen.

Bij de meeste cryptografische algoritmen is het in principe wel mogelijk om zonder de juiste sleutels de versleutelde gegevens te decoderen, maar dit decoderen kost dan zo veel rekenwerk en tijd dat het praktisch onmogelijk is. Het decoderen van gegevens zonder de juiste sleutel kan op de snelste computers van nu miljarden jaren rekentijd kosten, door alle mogelijke sleutels uit te proberen, totdat er een sleutel wordt gevonden die werkt. Als de sleutel een groot genoeg getal is, zijn zelfs de snelste computers niet in staat om alle mogelijke sleutels in afzienbare tijd uit te proberen. Aangezien computers door de jaren heen steeds sneller worden is het wel nodig om in de loop van de tijd grotere getallen als sleutel te gebruiken.

Er zijn grofweg twee vormen van cryptografie: symmetrische en asymmetrische.

40.1 Symmetrisch

Bij symmetrische cryptografie gebruiken zender en ontvanger dezelfde sleutel. Die sleutel moet van tevoren uitgewisseld worden via een veilig kanaal (waarbij zender en ontvanger elkaars identiteit kunnen controleren en onderschepping van de sleutel door derden niet mogelijk is).

Het gebruik van dezelfde sleutel wil niet altijd zeggen dat het coderen en het decoderen identiek zijn. Bij de sleutel Rot13, die bij e-mail veel wordt gebruikt, is dat wel het geval. Wie een gecodeerd bericht opnieuw met ROT13 decodeert, ziet weer het oorspronkelijke bericht. Bij een code als A→B, B→C enz. is dat niet het geval, maar de decodeersleutel kan eenvoudig worden afgeleid uit de codeersleutel. Beide gelden als symmetrische cryptografie.

40.2 Asymmetrisch

Moderner is de asymmetrische cryptografie, ook wel *public key encryption* genoemd. Hierbij hebben zender en ontvanger elk een eigen set van twee sleutels, waarvan er één publiek is en één niet. Het is in theorie mogelijk, maar niet praktisch haalbaar, om de geheime sleutel uit de publieke sleutel af te leiden.

Berichten die met een publieke sleutel worden versleuteld, kunnen alleen met de geheime sleutel worden ontcijferd. Met andere woorden: onbevoegden kunnen het bericht niet lezen.

Andersom geldt dit ook: informatie die is vercijferd met de geheime sleutel van iemand, kan alleen met de bijbehorende publieke sleutel worden ontcijferd. Dit laatste wordt gebruikt bij het digitaal ondertekenen van berichten: men heeft de zekerheid dat het bericht afkomstig is van degene die zich de afzender noemt.

De publieke sleutel mag aan iedereen bekend zijn en kan dus uitgewisseld worden over een onveilig kanaal zoals internet. Om een bericht te coderen en digitaal te ondertekenen, heeft de zender zijn eigen geheime sleutel nodig én de publieke sleutel van de ontvanger. Om het ontvangen bericht te decoderen en te verifiëren of de handtekening wel van de zender is, heeft de ontvanger zijn eigen geheime sleutel nodig én de publieke sleutel van de zender.

Het grote voordeel van asymmetrische cryptografie is dat uitwisseling van de benodigde sleutels kan plaatsvinden via een onveilig kanaal. Afluisteren van de uitgewisselde informatie - inclusief publieke sleutels - vormt geen enkel probleem. Een onderscheppingsrisico bestaat wel: wanneer zender en ontvanger nalaten te controleren of de

gebruikte publieke sleutel inderdaad hoort bij de (beoogde) ander is het voor een derde mogelijk om zich voor te doen als één van de twee partijen. Iedereen kan immers zeggen: “mijn naam is zus-en-zo en hier is mijn publieke sleutel, stuur me nu uw gegevens maar”. Zender en ontvanger dienen dus langs een betrouwbaar kanaal elkaars identiteit vast te stellen en publieke sleutels te bevestigen.

Een nadeel van asymmetrische cryptografie is dat grote sleutellengtes nodig zijn (bijvoorbeeld 4096 bytes), waardoor coderen en decoderen veel rekenkracht vergt. De sleutels moeten groot zijn, omdat het anders mogelijk wordt met een snelle computer de geheime sleutel te vinden.

Vaak wordt een combinatie van asymmetrische en symmetrische cryptografie gebruikt: eerst wordt door middel van asymmetrische cryptografie een geheim tussen zender en ontvanger uitgewisseld, die de sleutel vormt voor de snellere symmetrische cryptografie van grote blokken data.

Bij de versleuteling van e-mail wordt wel asymmetrische cryptografie toegepast, door PGP, GPG of S/MIME.

40.3 Hashing

Cryptografische hashing is in strikte zin geen versleuteling, omdat bij hashing uit de verkregen hash code de oorspronkelijke gegevens niet meer terug kunnen worden gehaald. Wel wordt bij hashing gebruikgemaakt van dezelfde technieken als bij versleuteling en vormt hashing ook vaak een onderdeel van versleutelingsprotocollen. Het verschil tussen hashing en encryptie is dus dat hashing maar 1 kant op kan (alleen hashen) en dat er bij encryptie twee kanten op gewerkt kan worden (coderen en decoderen).

Bij hashing wordt door middel van een hash algoritme een hashcode berekend van een blok gegevens. Uit deze hashcode is dan niet meer af te leiden wat de oorspronkelijke gegevens waren, maar iemand die de gegevens heeft kan wel opnieuw daarvan de hashcode berekenen en controleren of de berekende hash code overeenkomt met een eerder verkregen hash code. Aangezien de hash code vaak veel kleiner is dan het oorspronkelijke blok gegevens is het op deze manier mogelijk om bij te houden of een bepaald document al eerder is gezien, zonder dat het hele document hoeft te worden opgeslagen. Ook kan iemand door de hashcode van een document te publiceren bewijzen dat hij beschikt over een document, zonder dat document zelf publiek te maken. Als hij dan op een later moment het document alsnog publiek beschikbaar maakt kan iedereen controleren dat de persoon op het moment dat hij de hash code publiceerde al in het bezit van dat document moet zijn geweest, omdat er geen andere manier is om dezelfde hashcode te berekenen.

Voor een veilige hashcode gelden de eigenschappen dat het gegeven de hashcode niet mogelijk is om te achterhalen van welk blok gegevens de hashcode is afgeleid, en verder moet het onmogelijk zijn om twee verschillende blokken gegevens te maken die dezelfde hashcode hebben. Hierdoor heeft een hashcode de eigenschappen van een digitale vingerafdruk.

40.3.1 Hashing van wachtwoorden

Voor de aanmelding bij een computer zijn vaak een naam en een wachtwoord nodig. Deze wachtwoorden worden vaak versleuteld opgeslagen, zodat de wachtwoorden niet bekend worden als het bestand met wachtwoorden door een onbevoegde gelezen wordt. Dit gebeurt door middel van een hashing-algoritme, dat het onmogelijk maakt de versleutelde gegevens te decoderen. Dat is ook niet nodig, aangezien het voldoende is te controleren of de gebruiker het juiste wachtwoord heeft opgegeven.

Bij het versleutelen van wachtwoorden is het echter onveilig om gebruik te maken van algemene hash-algoritmen, en dient gebruik te worden gemaakt van speciale hash-algoritmen voor wachwoorden zoals bcrypt, scrypt, of PBKDF. De reden is dat normale hash-algoritmen zijn ontworpen om zo snel mogelijk berekend te kunnen worden. Bij het hashen van wachtwoorden is dat onwenselijk, omdat het daardoor mogelijk wordt dat iemand die de hashcodes van de wachtwoorden in bezit heeft gekregen achterhaalt welke hashcode van welk wachtwoord is afgeleid.

De lengte en complexiteit van wachtwoorden die mensen in de praktijk gebruiken is beperkt, terwijl computers steeds sneller worden. Daardoor wordt het voor iemand die probeert hashcodes voor wachtwoorden te kraken steeds makkelijker om een computer allerlei mogelijkheden te laten uitproberen. Hash-algoritmen voor wachtwoorden blokkeren deze methode doordat voor deze algoritmen in te stellen is hoeveel rekentijd ze moeten kosten. De algoritmen worden dan zo ingesteld dat het uitrekenen ervan bijvoorbeeld één milliseconde kost, terwijl het berekenen van een hashcode met een gewoon hash-algoritme minder dan een microseconde kan kosten. Bij het controleren van een wachtwoord is het meestal geen probleem als dit een milliseconde in plaats van een microseconde kost, terwijl iemand die wil proberen de hashcodes te kraken meer dan duizend keer zo veel rekenwerk moet doen, en dus meer dan duizend keer langer bezig is.

40.4 Decryptiebevel

Er is in Nederland een internetconsultatie geweest betreffende het concept-wetsvoorstel computercriminaliteit III met onder meer een wettelijke regeling waarbij aan een verdachte een decryptiebevel kan worden gegeven, in afwijking van het beginsel van nemo tenetur.[1][2][3][4] Dit onderdeel is uit het wetsvoorstel geschrapt.[5]

Hoofdstuk 41

Faker

Een **faker** is een persoon die zich op het internet anders voordoet dan hij of zij in werkelijkheid is. Fakers zijn actief in chatrooms, of maken profielen aan op datingsites waarbij ze foto's van anderen gebruiken als profielfoto. De reden is meestal omdat men bepaald gedrag probeert uit te lokken.

Vaak gaat het dan om oudere volwassenen die in een chatroom claimen adolescenten te zijn. Een andere zeer bekende categorie zijn oplichters, die op een of andere manier de ander proberen aan te zetten tot het overmaken van geld of waardevolle zaken. Andere motieven zijn ook mogelijk.

Hoewel fakers een aan het internet verbonden fenomeen zijn, is het misbruik maken van communicatie op afstand niet nieuw. In de jaren 80 hanteerden een aantal gedetineerden in de Angola-gevangenis een oplichterspraktijk gebaseerd op nepadvertenties in homobladen, en in de jaren 40 lichtte de Zweed Gustaf Raskenstam zoveel vrouwen via contactadvertenties op dat de tekst van zijn advertenties (Sol-och-vår, 'zon en lente') in het Zweeds synoniem is voor romantische oplichterij.

41.1 Seksuele motieven

Het bekendst zijn fakers met seksuele motieven. Zo kan worden geprobeerd om de ander aan te zetten tot het hebben van cyberseks, het toesturen van erotische foto's, of (uiteindelijk) het maken van een afspraakje met seks. Wanneer dit gebeurt door pedoseksuelen met het doel seksueel contact tot stand te brengen met een seksueel minderjarige, spreekt men ook van grooming. Internet heeft de mogelijkheid hiertoe enorm vergroot, omdat men makkelijker anoniem en snel kan opereren.

In juni 2005 kwam de chatsite van het Jeugdjournaal negatief in het nieuws vanwege seksuele benadering van (jonge) chatters. Het Jeugdjournaal, TMF, MSN en een aantal andere eigenaars van chatsites hebben besloten cyberseks niet meer toe te staan door het gebruik van moderators en zeer strenge registratie-eisen. In sommige gevallen zijn chatboxen zelfs om deze reden offline gehaald.

In februari 2006 werd een 20-jarige man veroordeeld tot 12 maanden cel vanwege het laten plegen van cyberseks door meisjes van 16 jaar oud.[1] In november 2007 werd een 49-jarige man tot vier jaar cel veroordeeld nadat hij twee minderjarige meisjes via internet had benaderd. Hij beweerde eveneens minderjarig te zijn en had hen vervolgens tot seks gedwongen.[2]

41.2 Oplichting

Oplichting is eveneens een veelvoorkomend motief. Hier probeert de faker romantische belangstelling te veinzen. Er ontstaat meestal een e-mailcorrespondentie of men ontmoet elkaar vaker op chatsites of via instant messengers zoals Yahoo Messenger of Skype. Wanneer het slachtoffer eenmaal tot over zijn of haar oren verliefd is, zal hij hem of haar proberen aan te zetten tot het overmaken van geld.

In veel gevallen doet de oplichter zich voor als een buitenlandse uit bijvoorbeeld Thailand, Rusland of de Filipijnen. Wanneer er eenmaal contact is gelegd, zal hij het slachtoffer om geld vragen voor een vliegticket om haar te kunnen bezoeken. Wanneer dit geld is overgemaakt blijken er toch opnieuw kosten te zijn die betaald moeten worden, bijvoorbeeld voor een visum. Ook worden vaak tranentrekkende verhalen aangevoerd zoals een huurschuld waardoor men op straat dreigt te komen of het niet kunnen afmaken van de opleiding omdat het lesgeld (deels) niet betaald is. Zo gaat het door tot het slachtoffer afhaakt. In essentie is dit een vorm van Nigeriaanse oplichting.

In sommige gevallen komt het tot een ontmoeting en een liefdesrelatie, maar zal de faker na verloop van tijd eveneens om geld beginnen te vragen, bijvoorbeeld ter aflossing van een schuld veroorzaakt door een zakelijke tegenvaller. Een dergelijke werkwijze doet denken aan een loverboy. Veel van dit soort oplichters hebben dan ook 'relaties' met meerdere personen.

41.3 Andere motieven

Andere denkbare motieven zijn:

- Sommige fakers proberen chatters naar (hun eigen) betaalde datingsites of telefoonlijnen lokken onder het motief 'dat iedereen maar op een open chatsite in kan loggen en hij/zij er zeker van wil zijn dat de ander serieus is'.
- Een enkele keer komt het voor dat een faker een ontmoeting met zijn slachtoffer arrangeert om hem of haar te beroven of te mishandelen.
- Commerciële motieven: de faker begint wanneer contact is gelegd reclame te maken voor een product of dienst dat hij hoopt te verkopen. Een variant hierop zijn camgirls en -boys wanneer zij chatters onder valse voorwendselen op hun website willen laten inschrijven.
- Chantage: als het slachtoffer een reputatie te verliezen heeft, is hij of zij kwetsbaar voor chantage. Seksuele geaardheid en/of voorkeuren kunnen, evenals (met een webcam opgenomen) cyberseks hiervoor gebruikt worden. Soms eist de chanteur geld (voornamelijk bij oudere welgestelde slachtoffers), maar vaak ook seks (voornamelijk bij minderjarige slachtoffers).
- Een grap uithalen met het slachtoffer, bijvoorbeeld door hem of haar voor niets op een afspraakje laten komen. Er is een geval bekend waarbij een faker met zijn slachtoffer een correspondentie opzette om na enkele maanden te beweren dat hij niet is wie hij is, niet uit was op een relatie, en het slachtoffer op deze manier wilde 'waarschuwen' voor fakers met kwade(re) bedoelingen.
- Gebrek aan zelfvertrouwen kan een reden zijn waarom iemand zich een ander alias aanmeet. Het gaat dan meer om het flirten en de aandacht. Dit soort fakers gaat een ontmoeting altijd uit de weg.
- Hieraan verwant is het verschijnsel waarbij iemand om aandacht en sympathie te krijgen zich online ziektes en kwalen voorwendt. Dit verschijnsel is verwant aan het Münchhausensyndroom en Münchhausen by proxy, en werd door de psychiater Marc Feldman in 2000 Münchausen by Internet genoemd.
- Politie/justitie/journalisten en bijvoorbeeld pedojagers kunnen ten behoeve van opsporing/aan de kaak stellen een identiteit faken.
- Cyberpesten: de faker zoekt onder een valse naam contact met de persoon die hij of zij pest, om zo persoonlijke informatie los te kunnen krijgen die later wordt gebruikt voor verdere (cyber)pesterijen.

41.4 Herkenning

Herkenning van fakers is vaak moeilijk, maar toch zijn er een aantal tekenen die erop kunnen wijzen dat een faker aan het werk is.

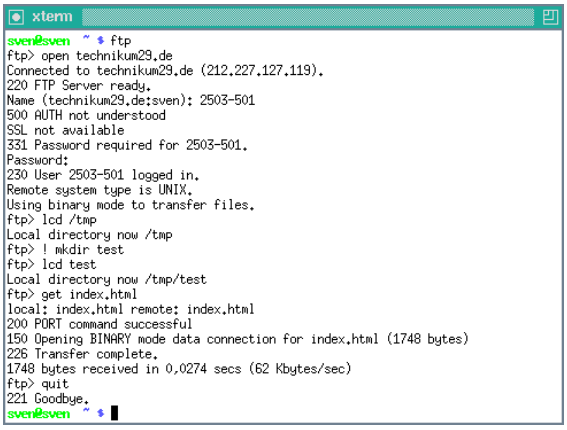
- Het Engels of Nederlands is slecht.
- De schrijver bedient zich van taalgebruik dat niet bij de leeftijd past.
- De schrijver geeft in chats en in e-mail weinig informatie over zichzelf maar vraagt voortdurend om persoonlijke (en vaak ook financiële) informatie over de ander.
- De tekst maakt een standaard indruk, omdat hij zo is geschreven dat de faker hem telkens weer opnieuw kan gebruiken, aangezien hij met zeer veel personen correspondeert. Soms leidt dezelfde vraag tot exact hetzelfde antwoord omdat de faker de tekst letterlijk kopieert en aanpast.
- De schrijver gaat vrij snel over op romantisch tot seksueel taalgebruik, terwijl bonafide daters voorzichtiger zijn. Ook het sturen van naaktfoto's kan een aanwijzing zijn.
- De schrijver is opdringerig en begint bij het tweede of derde mailtje al over een ontmoeting, een seksdate, een relatie of zelfs een huwelijk.
- De foto's maken een zeer professionele indruk. Dit komt doordat veel fakers foto's uit (erotische) tijdschriften en websites gebruiken. Dit hoeft echter niet altijd het geval te zijn daar online ook veel (erotische en niet-erotische) amateurfoto's te vinden zijn.
- Bedelmailtjes of zielige verhalen waarin om geld wordt gevraagd zijn vrijwel altijd een sterke aanwijzing dat er een faker aan het werk is.
- 100% waterdicht liegen is vrijwel onmogelijk. Tegenstrijdigheden in iemands verhaal kunnen een aanwijzing zijn.

41.5 Externe link

- Mijn puber op Hyves - *Mijnkindonline.nl*

Hoofdstuk 42

File Transfer Protocol



Een FTP-sessie in een Linux-terminal.

File Transfer Protocol (**FTP**) is een protocol dat uitwisseling van bestanden tussen computers vergemakkelijkt. Het standaardiseert een aantal handelingen die tussen besturingssystemen vaak verschillen.

Een FTP-client (zoals FileZilla) start een verbinding met een FTP-server standaard via TCP-poort 21.

De huidige versie is gedefinieerd in RFC-nummer 959 (RFC 959). Aanvullingen zijn te vinden in RFC 2228, RFC 2640 en RFC 2773.

42.1 Geschiedenis

FTP ontstond in 1971 en groeide zeer snel uit tot een wereldstandaard. Sinds die tijd maakt FTP het mogelijk bestanden te verzenden of te ontvangen van elke computer ter wereld, voor zover deze is aangesloten op internet, en zolang een eventuele proxy of firewall FTP-verkeer toelaat.

42.2 Techniek

Het concept van een FTP is gebaseerd op het cliënt-servermodel dat ook andere delen van het internet kenmerkt. De clientsoftware maakt een verbinding met de opgegeven FTP-server aan de andere kant van de 'lijn'. Deze antwoordt aan de cliënt, waarna de cliënt de gegevens aan de gebruiker toont. FTP-servers kunnen anonieme gebruikers toelaten of juist een geldige gebruikersnaam/wachtwoord combinatie vereisen alvorens toegang tot de achterliggende bestanden te geven.

42.3 Veiligheid

Standaard FTP-verbindingen zijn niet voorzien van encryptie, waardoor de verstuurde gegevens gemakkelijk kunnen worden uitgelezen door hackers. Door gebruik te maken van een encryptie-laag kan dit, voor zover mogelijk, worden voorkomen.

42.4 Bekende client- of serversoftware

Bekende FTP-clients voor Windows zijn CuteFTP, FileZilla, WinSCP en WS FTP. Voor Mac OS X is (naast FileZilla) Cyberduck een bekende opensourceclient. Ook is Transmit verkrijgbaar, een shareware-alternatief. Voor Linux is er o.a. ProFTPd en vsFTPd. De meeste webbrowsers hebben (beperkte) FTP-functionaliteit. Voor Firefox is er een plug-in beschikbaar onder de naam FireFTP die van Firefox een volwaardige FTP-client maakt.

42.5 Zie ook

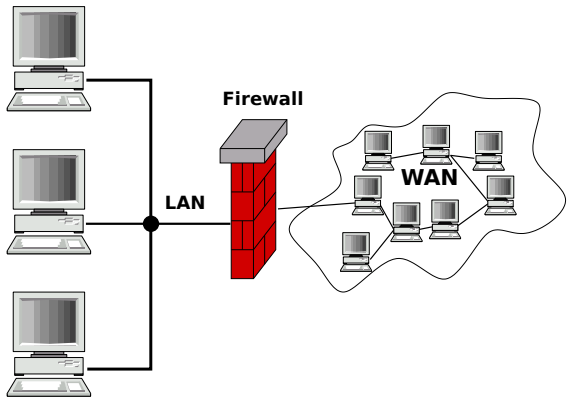
- TFTP
- Simple File Transfer Protocol
- FTP over SSL
- Lijst van FTP-serversoftware

Hoofdstuk 43

Firewall

Een **firewall** is een systeem dat de middelen van een netwerk of computer kan beschermen tegen misbruik van buitenaf.

Het beschermde netwerk is vaak een intranet of intern netwerk en dit wordt beschermd tegen het internet. Het ongewenste verkeer bestaat bijvoorbeeld uit aanvallen van hackers en computerkrakers, inbraken en/of uitbraken van computervirussen, spyware, spam en *denial of service attacks*.



Netwerktopologie met firewall

43.1 Types

Hoewel er geen eenduidige categorisering bestaat, kunnen firewalls worden ingedeeld op basis van de volgende criteria:

- of het verkeer wordt gescreend in de netwerklaag (*packet filtering firewall*), of in de applicatielaag (*application layer firewall*);
- of de firewall de status van een connectie bewaart (*stateful firewall*), of niet (*stateless firewall*);
- of de firewall één computer moet beveiligen tegen een persoon (*personal firewall*), of een netwerk (*network firewall*).

43.1.1 Packet filtering firewall

Een *packet filtering firewall* grijpt in op de netwerklaag van de TCP/IP-protocol-stack. Aan de hand van een aantal regels bepaalt de firewall of een IP-pakket wordt doorgelaten of tegengehouden. De aspecten van een pakket die hierbij in beschouwing worden genomen zijn bijvoorbeeld de poort waarvoor het pakket bedoeld is (destination port) of het IP-adres waar het pakket vandaan komt. Deze regels worden opgesteld door de beheerder of de producent van de firewall.

Een *packet filtering firewall* houdt enkel rekening met de IP-header van het datapakket. Dit type firewall werkt eenvoudig en snel, maar biedt een minder goede bescherming tegen virussen, spam e.d.

Gebruikers van computers die zich achter packet filtering firewalls bevinden merken weinig of niets van hun aanwezigheid, zolang de poortnummers van de protocollen die zij gebruiken niet door deze firewalls worden geblokkeerd.

Een *packet filtering firewall* kan bijvoorbeeld al het verkeer naar de telnetpoort verbieden. De firewall verbiedt echter niet dat het protocol van telnet op een andere poort gebruikt wordt.

43.1.2 Application layer firewall

Een *application layer firewall* grijpt in op de applicatielaag van de TCP/IP-protocolstack. Voor elk ondersteund protocol bepaalt een stukje software of pakketjes worden tegengehouden of doorgelaten. Dit stukje software kan uit veel meer bestaan dan een aantal simpele regels.

Een *application layer firewall* kan beter dan een *packet filtering firewall* beschermen tegen virussen e.d., maar is complexer, omdat elk protocol apart moet worden behandeld. Bovendien kost het bepalen of een pakketje door mag of niet meer resources.

Een voorbeeld van een *application layer firewall* is een mailserver die op de SMTP-poort luistert, en alle spam filtert.

Application layer firewalls worden meestal geïmplementeerd met behulp van proxy's.

43.1.3 Stateless firewall

Een *stateless firewall* behandelt elk pakketje op zichzelf, de firewall slaat tussentijds geen informatie op van de connecties die over de firewall lopen. Aangezien dit vrij grote beperkingen met zich meebrengt, zijn de meeste firewalls tegenwoordig stateful.

43.1.4 Stateful firewall

Een *stateful firewall* houdt wel tussentijdse informatie bij van connecties die over de firewall lopen. Hierdoor is de firewall beter in staat onderscheid te maken tussen pakketjes die wel toegestaan en niet toegestaan mogen worden.

Een voorbeeld: het FTP-protocol is zo opgezet dat soms verbindingen op willekeurige poorten nodig zijn. Als een *stateless firewall* FTP moet toestaan, dan zal daartoe verkeer op alle poorten moeten worden toegestaan. Een *stateful firewall* kan volstaan met het tijdelijk openen van de poort waarover de FTP-sessie plaatsvindt.

Tegenwoordige *packet filtering firewalls* zijn stateful.

43.2 Personal firewall

Een *personal-firewall* is een firewall die enkel de computer beschermt waarop deze geïnstalleerd is. De personal-firewall kan gebruikmaken van verschillende technieken om regels op te bouwen, maar een geavanceerde personal-firewall beschikt over een extra mogelijkheid: men kan regels definiëren op basis van processen.

Zo is het mogelijk een regel te maken dat enkel het programma E-MAILPROGRAMMA.EXE toegang geeft om via poort 25 een e-mail te versturen. Zulke regels kunnen voorkomen dat bijvoorbeeld spywareprogramma's ongewenst mails versturen vanuit de betreffende computer.

43.3 Network firewall

Een *network firewall* bestaat uit een aparte computer die twee of meer netwerken scheidt. Soms is er nog sprake van een 'niemandsland' (DMZ), waarin zich computers bevinden die bereikbaar moeten zijn vanuit het internet of een ander netwerk. Zulke computers hebben dan meestal specifieke regels nodig. Webservers zullen bijvoorbeeld vaak in een DMZ aangetroffen worden.

In grote netwerken en organisaties is het beheer van een firewall een complete dagtaak voor specialisten.

43.4 Managed firewall

Een *managed firewall* (een beheerde firewall) wordt steeds vaker toegepast in bedrijven die zelf niet genoeg kennis hebben van beveiliging van netwerken. Een *managed firewall* is een service die bestaat uit het fysiek installeren van een firewall in een netwerk met daarnaast het geheel aan onderhoud en configuratie van de firewall volledig op afstand door een bedrijf dat daarin gespecialiseerd is.

43.5 Zie ook

- Brandmuur
- *Intrusion detection systeem*

Hoofdstuk 44

Gebruikersaccountbeheer

Gebruikersaccountbeheer of **UAC** (Engels: *User Account Control*) is een beveiligingstechniek die wordt toegepast op computers die Windows Vista, Windows 7, Windows 8 of Windows 10 draaien. Als er een programma wordt geopend dat wijzigingen wil toebrengen buiten het eigen gebruikersgebied of gegevens van andere gebruikers wil lezen, zal UAC een waarschuwing geven. Het systeem is hierdoor beter beveiligd.

44.1 Voor- en nadelen

Enkele voordelen zijn:

- Betere beveiliging
- Computervirussen worden beter tegenhouden
- Strengheid van UAC is regelbaar in Windows 7 en hoger

Enkele nadelen zijn:

- Strengheid van UAC is niet regelbaar in Windows Vista SP 1 en lager.
- Sommige gebruikers vinden het nogal storend.[1]

44.2 Windows Vista

Toen gebruikers voor het eerst kennis maakten met UAC kwam er veel kritiek los. Telkens wanneer gebruikers een bestandsbewerking deden, een eigenschap aanpasten of een programma installeerden, verscheen gebruikersaccountbeheer. Velen weten echter niet dat dit hulpmiddel voor een betere beveiliging zorgt. Uit onderzoek blijkt overigens wel dat 86% van de gebruikers UAC gewoon aan laat staan.

44.3 Windows 7

In Windows 7 kan de gebruiker de strengheid van UAC regelen. Standaard is de strengheid ingesteld op het op één na hoogste niveau. Overigens bleek dat er een zwaar beveiligingslek zat in UAC. In de RC van Windows 7 werd dit probleem verholpen.[2]

44.4 Taken die leiden tot een UAC-melding

1. Wijzigingen in systeeminstellingen of bestanden in %SystemRoot% of %ProgramFiles%
2. Installeren en verwijderen van toepassingen
3. Het installeren van stuurprogramma's
4. Installeren van ActiveX-besturingselementen
5. Het wijzigen van instellingen voor Windows Firewall
6. Veranderen van UAC-instellingen
7. Configureren van Windows Update
8. Het toevoegen of verwijderen van gebruikers
9. De rechten van een gebruiker veranderen
10. De instellingen van Family Safety (Ouderlijk Toezicht) wijzigen
11. Systeemback-up terugzetten (systeembestanden terugzetten)
12. Een map van een andere gebruiker bekijken of wijzigen.

De meeste taken die als “normaal” worden beschouwd, hebben geen toestemming van UAC nodig. Een voorbeeld is: de tijdzone wijzigen. Een aantal taken, zoals het installeren van updates, vereist administratorrechten. Overigens kan de gebruiker elk programma ook uitvoeren als beheerder, zodat de gebruiker voor dat programma geen UAC-meldingen meer krijgt.

44.5 Externe links

- (en) Understanding and Configuring User Account Control in Windows Vista
- (en) Blog van het User Account Control-team
- (en) UAC – The Good and The Bad
- (en) Security Features vs. Convenience

Hoofdstuk 45

Geldezel

Een **geldezel** is een katvanger die zijn of haar bankrekening tegen beloning laat misbruiken voor criminele activiteiten. De geldezel sluist hierbij (on)bewust frauduleus verkregen geld door naar criminelen.

Door gebruik te maken van het rekeningnummer, de inloggegevens of de pinpas van een *tussenpersoon* fungeert de geldezel als katvanger waardoor de identiteit van de crimineel voor opsporingsinstanties moeilijker te achterhalen is. Door middel van een babbeltruc, door phishing of tegen een bescheiden beloning kan een oplichter de bankgegevens, pinpas en pincode van de geldezel bemachtigen waarna hij snel zijn slag kan slaan. De personen die van deze truc het slachtoffer worden zijn vaak dezelfde categorieën als reguliere katvangers: jongere onervaren mensen die tuk zijn op een bijverdienste, en personen die weinig te verliezen hebben.

In het geval van internetfraude kan de diefstal van kleine tot zeer grote bedragen binnen het tijdsbestek van enkele tientallen minuten tot een dagdeel plaatsvinden. Meestal wordt de geldezel pas met de gevolgen van de oplichting geconfronteerd wanneer hij of zij in een opsporingsonderzoek wordt betrokken. Geldezels worden doorgaans strafrechtelijk vervolgd voor medeplichtigheid aan de oplichting. De pakkans is doorgaans vrijwel 100%; de bankrekening is immers op naam.

In juni 2011 zijn de banken en de brancheorganisatie Nederlandse Vereniging van Banken een campagne gericht op jongeren gestart onder de noemer *Pas op je Pas, word geen geldezel*.

45.1 Externe links

- Pas op je Pas, word geen geldezel
- veiligbankieren.nl

Hoofdstuk 46

Grooming (pedofilie)

Grooming is het winnen van het vertrouwen van een kind met het oogmerk om tot seksueel contact te komen.[1] Wanneer grooming plaatsvindt binnen een digitale omgeving wordt het ook wel **digitaal kinderlokken** genoemd.[2]

46.1 Definitie

Er bestaan verschillende definities.

Veel kinderlokkers gebruiken het internet om in contact te komen met kinderen. Volwassenen benaderen minderjarigen online, met als doel ze seksueel te misbruiken. Deze activiteiten noemen we grooming. Daarnaast wordt grooming ook omschreven als 'het door pedofielen actief benaderen van minderjarigen, bijvoorbeeld via internet, met als doel seksueel contact'. Als laatste kunnen we zeggen dat grooming het benaderen is van en contact leggen met kinderen door een pedofiel met als uiteindelijke doel het mogelijk maken van seksueel contact door de seksuele drempels en remmingen van het kind te verlagen.

Grooming wordt soms als volgt omschreven: “Grooming is het benaderen van kinderen en jongeren en het opbouwen van een vertrouwensrelatie met hen met als uiteindelijk doel het mogelijk maken van seksueel misbruik door de seksuele of andere drempels en remmingen van het kind of de jongere weg te werken of te verlagen. Seksueel misbruik, en zeker langdurig seksueel misbruik, is doorgaans niet het onverwachte gevolg van een reeks toevallige factoren, maar wel het resultaat van een dergelijk weloverwogen proces van grooming door de dader.”[3].

46.2 Kenmerken van grooming

- Het winnen van vertrouwen bij het kind.
- Het bevoorrechten van het kind.
- Het afschermen van het kind.
- Het stapsgewijs verder leggen van de grenzen.
- Het proces gebeurt geheim.[4]

46.3 Grooming in de wet

46.3.1 Strafbaar

Grooming is in Nederland strafbaar sinds 1 januari 2010, zie artikel 248e Sr.

Grooming is ook in België strafbaar. In de wet staat dat het uit twee constitutieve bestanddelen bestaat, nl. een materieel en moreel element. Het materieel element bestaat uit vier verschillende zaken. Ten eerste moet het door een meerderjarige aan een min-zestienjarige gebeuren. Daarnaast moet het gebeuren via informatie- en communicatietechnologie. Als derde moet er een voorstel tot ontmoeting plaatsvinden van de meerderjarige aan de minderjarige gericht. Dit wordt dan gevolgd door materiële handelingen die tot een dergelijke ontmoeting zouden kunnen leiden Daarnaast wordt er in de wet ook gesproken over een moreel element. Dit verwijst naar het voorstellen van een ontmoeting aan een min-zestienjarige met het bijzonder motief (bijzonder opzet) om aldus een aanranding van de eerbaarheid, een verkrachting of een vorm van aanzetten tot ontucht of prostitutie of van openbare zedenschennis op of met de min-zestienjarige te kunnen plegen.

Grooming kan als verzwarende omstandigheid gezien worden, als aan volgende zaken voldaan is per constitutief bestanddeel. Bij het materieel element spreken we hiervan wanneer de dader een seksueel misdrijf op of met een min-zestienjarige pleegde en dit misdrijf die voorafgegaan werd door een benadering van deze minderjarige door de dader met het oogmerk op een later tijdstip het seksuele misdrijf op of met de min-zestienjarige te plegen. Bij het moreel element is er sprake van verzwarende omstandigheden als de dader het oogmerk heeft om op een later tijdstip een seksueel misdrijf te plegen. Effect op strafmaat hiervan is verdubbeling van de minimumstraf in geval van een gevangenisstraf en verhoging met twee jaar in geval van opsluiting.

46.3.2 Poging tot grooming

Poging tot grooming is niet strafbaar. Het is al een voorbereidingsdelict. Poging tot het voorbereiden van

grooming kan daardoor nooit strafbaar zijn. Voor een veroordeling voor grooming is het nodig dat er een seksafspraak wordt gemaakt. Het is niet zo dat een gewone ontmoeting al strafbaar is, er moet echt sprake zijn van een oogmerk seksuele handelingen te plegen (hetgeen uit de inhoud van chats, e-mail e.d. kan blijken). Daarnaast moet voor de ontmoeting een uitvoeringshandeling zijn uitgevoerd door de verdachte op de ontmoeting, zoals het zich naar de afgesproken plaats begeven of aan het kind geld overmaken voor bijvoorbeeld een treinticket. Dit volgt o.a. uit een uitspraak van de rechtbank Oost-Brabant van 24 juli 2015.[4]

Hoofdstuk 47

Hacker

Een **hacker**, ook wel **kraker** of **cracker** genoemd, is een persoon die zonder toestemming een computernetwerk binnendringt door de beveiliging te kraken. Niet altijd met de bedoeling om illegaal informatie toe te eigenen, maar veelal om aan te tonen dat het netwerk onvoldoende beveiligd is. Er zijn wel hackers met criminele bedoelingen, echter, voor velen is het een sport om beveiligde netwerken te kraken. [1]

47.1 Omschrijving

In bepaalde technisch georiënteerde subculturen is een hacker een persoon die geniet van de intellectuele uitdaging om op een creatieve en onorthodoxe manier aan technische beperkingen te ontsnappen; bijvoorbeeld een goede programmeur. Een hacker hoeft niet per se iets met computers te doen. In deze subculturen wordt het gebruik van de woorden *hacker* en *hacken* door en voor computerinbrekers als misbruik van de term gezien; zij worden *crackers*, krakers of script kiddies genoemd. Script kiddies worden veelal gezien als nephackers, omdat zij de code van internet af kopiëren.

In het bijzonder wordt het woord hacker gebruikt in volgende betekenissen:

- Iemand die een programmeertaal of -omgeving zo goed kent dat hij/zij zonder zichtbare moeite een programma kan schrijven.
- Iemand die onconventionele maar adequate oplossingen bedenkt tegen lekken, fouten en problemen van andere aard met behulp van beschikbare middelen.
- Iemand die tracht om via illegale wegen een computersysteem binnen te dringen teneinde een beveiligingsprobleem te kunnen aantonen en indien mogelijk te verhelpen.

In deze laatste betekenis hebben hackers vaak een negatieve bijklank. Sommige hackers houden zich niet aan de hackersethiek, hebben geen respect voor andere mensen en hacken met de intentie informatie bloot te leggen. Daarmee beïnvloeden ze de publieke opinie om aanhangers te winnen voor bepaalde opvattingen of standpunten. Een voorbeeld hiervan is het hacken van webcams: stiekem meegluren, beeldmateriaal verzamelen en verspreiden. Er wordt door sommigen zelfs van "terrorisme" gesproken. Er zijn inderdaad crackers die in de binnengedrongen systemen schade aanrichten, zich toegang verschaffen tot vertrouwelijke informatie of gekraakte systemen gebruiken voor illegale software en/of media. Een hacker zal de eigenaar van het systeem adviseren het systeem veiliger te maken en meestal wordt ook meteen aangegeven op welke manieren dat zou kunnen, zodat het systeem beter beschermd is tegen crackers. Ook proberen hackers crackers actief te stoppen.

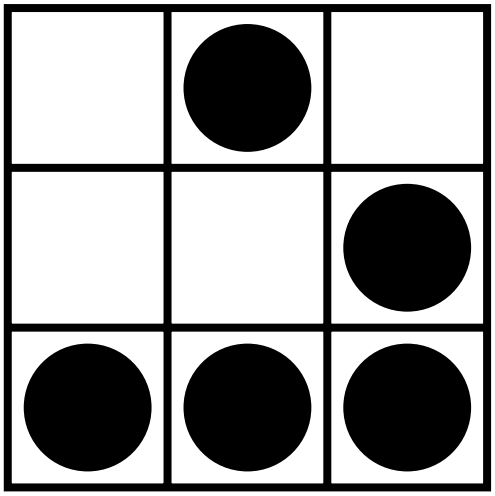
Onder (vooral academische) computerprogrammeurs kan een hacker ook een programmeur zijn die met werkende maar onelegante oplossingen voor programmeerproblemen komt. In deze zin is het woord hacker in eerste instantie afkeurend bedoeld. Het werkwoord hacken wordt ook wel gebruikt voor het “handwerk” van het programmeren, bijvoorbeeld het optimaliseren (*tweaken*) van een programma, dit in tegenstelling tot het “hoofdwerk”, het ontwerpen van het programma.

Ook autoriteiten kunnen hacken.[2][3]

47.2 Verschil tussen hackers en crackers

Binnen de hackersgemeenschap wordt wel onderscheid gemaakt tussen hackers en crackers. Een veelgenoemd verschil tussen hackers en crackers is dat hackers hun handelingen vaak verrichten als uiting van constructieve creativiteit (“voor de kunst van het bouwen”) of als goedbedoelde handelingen (zoeken naar veiligheidslekken om deze later te kunnen dichten). Soms huren bedrijven hackers in om de beveiliging van hun systemen te testen. Crackers handelen uit crimineel, ideologisch of vernielzuchtig oogpunt.

Hackers zelf noemen degenen die uit criminele oogmerken een systeem “kraken” ook wel *black-hat hackers*. Zelf noemen ze zich *white-hat hackers*, analoog aan cowboyfilms waarin de “kwaden” zwarte hoeden droegen



De glider, het symbool voor hacker

en de “goeden” witte hoeden. Ook zijn er *grey-hat hackers*, een kruising tussen crackers en hackers. Het komt voor dat crackers hun activiteiten proberen te verbergen door zich als hacker voor te doen.

Hackers hebben ook normen, de zogenaamde hackersethiek. Deze is terug te vinden in de indeling “black-hat/grey-hat/white-hat hackers”. Ook is het zo dat een hacker in de wereld van de hackers status kan verwerven door zijn of haar kennis te delen met anderen. Dit doet men door opensourcesoftware te schrijven en hun kennis te delen.

Woordenboeken maken geen onderscheid tussen 'goede' en 'kwade' hackers. Zo omschrijft de Van Dale een hacker als: “iemand die inbreekt in een computer om gegevens te achterhalen of te wijzigen, meestal met het doel de zwakke plekken aan te tonen”. Het Amerikaanse woordenboek Merriam-Webster definieert de term als: *a person who illegally gains access to and sometimes tampers with information in a computer system*.

47.3 Zie ook

- Computerkraker
- Hackerspace
- Hacken

47.4 Externe link

- Leidraad responsible disclosure op ncsc.nl

47.5 Bronnen

- (en) Eric S. Raymonds hacker-howto, versie 2006

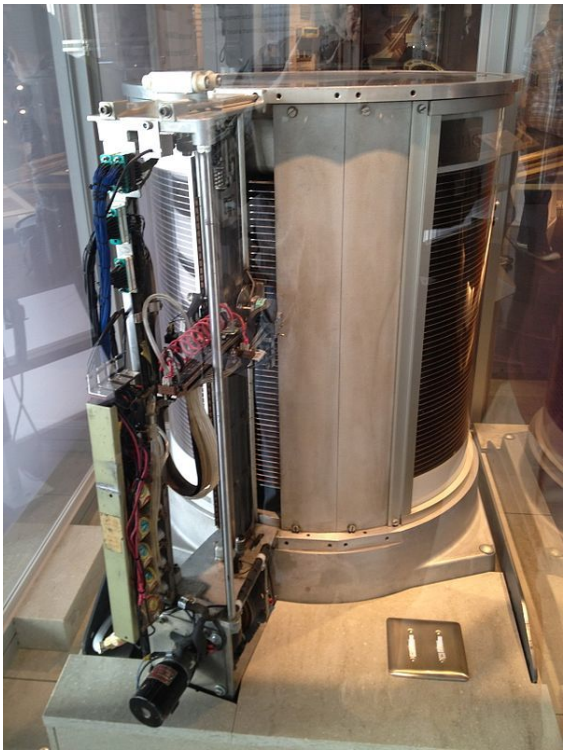
Hoofdstuk 48

Harde schijf

Een **harde schijf**, van het Engelse *hard disk drive* of HDD, is een vorm van extern geheugen, een elektromechanisch computeronderdeel waarop gegevens bewaard kunnen worden. Met de aanduiding harde schijf kan men de eigenlijke schijf bedoelen waarop in de vorm van magnetische polarisatie de gegevens zijn geschreven, maar meestal bedoelt men het hele apparaat met schijven, lees- en schrijfkoppen en besturingselektronica, samen in een behuizing. In IT-documentatie wordt de term *vaste schijf* gebruikt, omdat de schijf vast in de computer gemonteerd wordt. De gegevens zijn permanent, in tegenstelling tot het vluchtig *Random-access memory* (RAM) en blijven ook bewaard als de computer uit staat. Een harde schijf is tegenwoordig altijd voorzien van een besturingseenheid, de *controller*. Dit is een elektronische schakeling die de toegang tot de data op de schijf regelt.

Harde schijf van 512 MB van Quantum

48.1 Geschiedenis



De RAMAC buiten zijn behuizing, was de eerste harde schijf, door IBM geproduceerd.

Aanvankelijk werden magnetische tapes gebruikt als permanent opslagmedium voor data. Op 13 september 1956 introduceerde IBM de eerste harde schijf: Random Access Method of Accounting and Control. De *RAMAC* bestond uit 50 gestapelde magnetische schijven met een diameter van 61 cm (24 inch). Er waren twee speelkoppen. De totale capaciteit van deze schijf was 5 MB.

Sinds de introductie van de RAMAC groeide elk jaar de opslagcapaciteit van harde schijven, terwijl de omvang steeds kleiner werd.

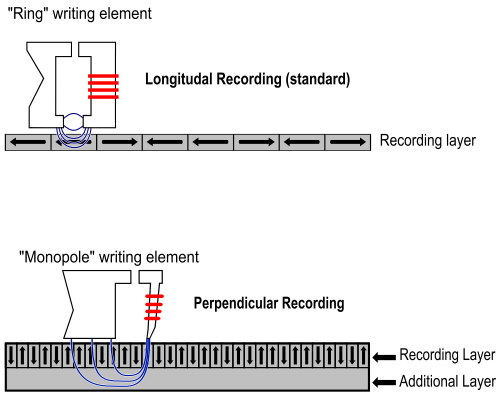
De prijs van harde schijven is door de loop der jaren drastisch gedaald. Ter illustratie, een advies van het Nederlandse Ministerie van OCW aan de Bibliotheekraad uit 1980 over automatisering van de gegevensopslag noemt

een prijs van rond de 200 gulden (ongeveer 90 euro) per megabyte.[1] Eind 2013 kostte een harde schijf van 2 terabyte (2.000.000 megabyte) ongeveer 90 euro.[2]

48.2 Toepassingen

Meestal worden op de harde schijf van een computer het besturingssysteem, de programma's en de gegevens van de gebruiker bewaard. Daarnaast kan een computer de harde schijf tijdelijk als geheugen gebruiken wanneer er geen RAM meer over is. Linux doet dit door middel van een speciale swap-partitie, terwijl Windows de "pagefile" op de systeemschijf zet (of op een door de gebruiker gedefinieerde partitie). In Windows bestaat eveneens een zogeheten hibernate/hibernation-bestand, dat wordt gebruikt wanneer het systeem in slaapstand gaat. Daarin worden de gegevens opgeslagen die weer gebruikt worden om het systeem snel uit de slaapstand te halen.

48.3 Constructie en interface



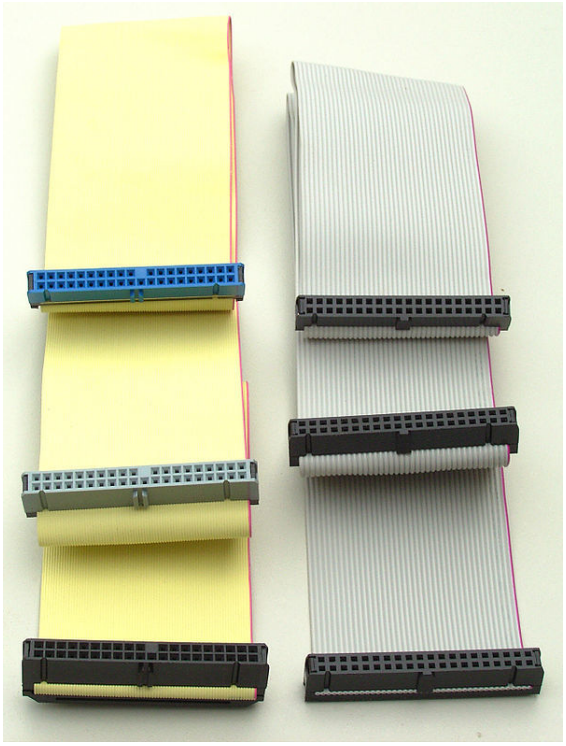
Perpendiculaire (loodrechte) opname.

De harde schijf heet *hard* omdat hij bestaat uit één of meer niet-flexibele ronde platen, in tegenstelling tot de flexibele floppy's die bij de oudste minicomputers het enige opslagmedium waren. De platen zijn gecoat met een microndunne magnetiseerbare laag. Deze platen worden *platters* genoemd. Op een beweegbare arm (actuator) zitten de lees- en schrijfkoppen. Die arm heeft een spoel die beweegt tussen sterke magneten. Door de spoel van meer en minder spanning (Positief - Negatief) te voorzien kan de arm zeer precies worden gestuurd. De informatie wordt dus met koppen op de schijf gezet en weer teruggelezen. Omdat hiervoor de kop moet worden verplaatst en soms moet worden gewacht tot het juiste gedeelte van de schijf onder de kop doordraait is de harde schijf een aantal ordes van grootte trager dan geheugen in geïntegreerde schakelingen. De opslagcapaciteit van harde schijven is de laatste decennia enorm toegenomen.

Vanwege de geringe omvang van de magnetische gebieden, ontstaat in moderne schijven het gevaar dat de magnetische toestand kan worden verloren als gevolg van thermische effecten. Dit is een thermisch geïnduceerde magnetische instabiliteit die bekendstaat als superparamagnetisme. Om dit tegen te gaan, worden de platters bedekt met twee parallelle magnetische lagen, gescheiden door een drieatoomlaag van het niet-magnetische element ruthenium. Daarnaast worden de twee lagen in tegengestelde richting magnetisch gemaakt, zodat een versterkend effect optreedt.[3] Een andere technologie die wordt gebruikt om thermische effecten tegen te gaan, en een hogere opslagdichtheid te krijgen, is perpendiculaire (loodrechte) opname. Deze techniek werd vanaf 2007 in veel harde schijven gebruikt.

In 2004 werd een nieuw concept geïntroduceerd om de opslagdichtheid verder te verhogen. Hiervoor wordt opnamemateriaal gebruikt wat bestaat uit een combinatie van harde en zachte magnetische lagen.[4]

48.4 Aansluitmethoden



IDE-kabel

In de meeste moderne computers is een harde schijf vast ingebouwd. Deze kan op verschillende manieren worden aangesloten.

De meest gebruikte manieren om een harde schijf in een computer aan te sluiten zijn:

- ST-506, interface in de IBM PC XT en AT, hiervoor is een aparte harddiskcontrollerkaart nodig.

Serial ATA-kabel

Tot midden jaren 1990 in gebruik.

- Integrated Drive Electronics (IDE) of Parallel ATA (PATA). Dit is een verouderde standaard die tot 2004 werd gebruikt.
- Serial ATA (SATA). Vanaf 2004 wordt voornamelijk SATA gebruikt.
- SCSI. Dit is een verouderde standaard voor servers.
- Serial Attached SCSI (SAS). Dit wordt vanaf 2006 gebruikt in servers en is een verbeterde SCSI.

Harde schijven kunnen ook extern op de computer worden aangesloten. De gebruikte verbindingen zijn:

- Universal Serial Bus (USB).
- FireWire-poort (ook wel IEEE 1394 genoemd).
- iLink. Dit is een propriëtaire interface van Sony en lijkt op Firewire maar is niet compatibel.
- eSATA (external Serial ATA). Dit is officieel niet precies hetzelfde als de gewone SATA, maar vaak wordt een gewone interne SATA-poort ook als externe SATA-poort gebruikt. Bij korte kabels geeft dat geen problemen.
- Network-attached storage (NAS). Een harde schijf (of ook vaak meerdere) in een netwerk. Dat kan ook draadloze NAS zijn, waarbij de harde schijf via wifi benaderd wordt.
- Storage area network (SAN) wordt bij grotere systemen toegepast.

Solid state drives (SSD) kunnen ook SATA- en SAS-aansluitingen hebben, maar sinds 2009 worden voor SSD's steeds meer andere aansluitingen ontwikkeld.

48.4.1 Geschiedenis van aansluitmethoden

De oorspronkelijke pc heeft geen aansluitingen voor harde schijven. Een ISA-insteekkaart kan worden gebruikt, met daarop de elektronica om de harde schijf te besturen. Die insteekkaart of controller hoort bij een bepaald type harde schijf zoals ST506 of ESDI. Hierbij worden twee flatkabels gebruikt; een brede voor de besturing van de harddisk en een smalle voor de data-overdracht.

Korte tijd bestonden er ISA-insteekkaarten met daarop een kleine harde schijf gemonteerd. De zogenoemde harde kaart.

Als vervolg op de ST506 kwam de IDE-aansluiting. De IDE-aansluiting maakt een einde aan de onduidelijkheden en was lange tijd de standaard. Een enkele flatcable werd gebruikt voor de gegevensoverdracht, en een stekker met +5 V en +12 V zorgde voor de voeding. Bij een IDE-aansluiting kunnen op de brede kabel twee schijven worden aangesloten, een met het besturingsprogramma (*Master*), en een als *Slave*. Jumpers, kleine doorverbinders aan de achterzijde van de harddisk, geven aan of de schijf dienstdoet als alleen Master, Master met slave present, Single of Master en Cable select.

Omdat de IDE-verbinding voor servers traag was, werd in servers vaak SCSI gebruikt als verbinding.

Om de snelheid van data-overdracht te vergroten, werd SATA ontwikkeld. Bij de SATA-aansluiting hoeft geen Master of Slave ingesteld te worden. Toch kan in het BIOS een harde schijf soms nog steeds als Master of Slave gezet worden, om compatibel te zijn met de software. Sommige desktop-computers hebben een slede voor een harde schijf. De verbinding is dan vaak een SATA-verbinding. Het voordeel daarvan is, dat gebruikers gemakkelijk van harde schijf kunnen wisselen zonder de computerkast te hoeven openen.

In servers werd niet overgestapt naar SATA, maar werd de oude SCSI verbeterd en ook serieel gemaakt. Zo ontstond SAS. Er zijn wel uitzonderingen: Dell heeft servers die wel SATA ondersteunen. Hierbij is bijvoorbeeld te denken aan de Dell PowerEdge-servers (zoals de R200-serie).

Voor servers bestaan er verschillende systemen om meerdere harde schijven in rekken te plaatsen.

In 2009 zijn er al harde schijven met een optische interface via een glasvezel, maar het is niet duidelijk of dat een standaard zal worden.

48.5 Memory in Chip

Fabrikanten van harde schijven slaan vaak gegevens over mechanische problemen van de harde schijf op in een *Electronically Erasable Programmable Read Only Memory* (EEPROM) in de controller. Om dergelijke gegevens op te vragen is een standaard ontwikkeld die S.M.A.R.T. (Self Monitoring Analysis and Reporting Technology) heet. Als gegevens nog leesbaar zijn, maar minder betrouwbaar, dan kan via S.M.A.R.T. een waarschuwing gegeven worden dat de harde schijf binnenkort stuk zou kunnen gaan.

Ook kunnen gegevens zijn opgeslagen zoals de maximale temperatuur die de schijf ooit heeft gehad.

48.6 Indeling op harddisk

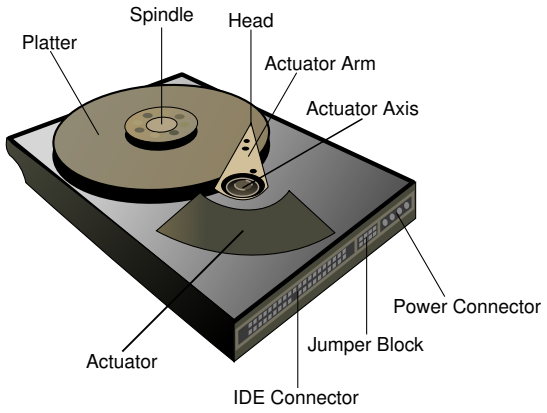


Diagram van een harde schijf.

Een harde schijf is in de fabriek geformatteerd (het zogenoemde *low-level format*) en is verdeeld in cilinders of tracks en sectoren. De gebruikersgegevens worden opgeslagen als een lange rij bits. De mappenstructuur van de schijf wordt bepaald door het bestandssysteem dat de conversie tussen mappen en bestanden enerzijds en bits anderzijds verzorgt.

De formattering op laag niveau verdeelt de schijf in sectoren, de kleinste eenheid die in één bewerking door een lees/schrijfkop kan verwerkt worden. Elke sector krijgt een uniek nummer zodat de diskcontroller (het stuurorgaan van de harde schijf) straks weet hoe de koppen moeten worden gepositioneerd.

Recentere schijven hebben echter een complexe structuur, waarbij de buitenste sporen meer sectoren hebben dan de binnenste sporen. Bij deze schijven kan de low-levelformattering uitsluitend door de fabrikant worden uitgevoerd.

De low-levelformattering wordt gewoonlijk door de producent gedaan met formatteringsroutines die specifiek voor de betrokken harde schijf geschreven zijn. Indien je andere routines gebruikt, bijvoorbeeld Calibrate of Spinrite die op BIOS-niveau werken, kan de schijf hierdoor definitief onbruikbaar worden.

Het kan zijn dat er tijdens het formatteren slechte plekken op de schijf of diskette worden gevonden. Dit noemt men beschadigde sectoren (bad blocks of bad sectors).

Veel moderne harddisks constateren de slechte blokken automatisch en proberen ze door een speciaal gereserveerd blok te herstellen. Voor het besturingssysteem is dit niet zichtbaar.

48.7 Maatvoeringen

De oorspronkelijke afmetingen van harde schijven waren gerelateerd aan de maten van floppy disk drives (FDD). Lengte en breedte kwamen overeen, de hoogte werd gevarieerd. De namen waaronder deze bekendstaan (de “form factor”), zoals 3,5” en 2,5”, zijn nominaal, ze komen slechts bij benadering overeen met de werkelijke maten. Beide maten worden hieronder genoemd.

- Nominaal 5¼", dat is 133,35 mm, feitelijk 146,1 mm (lengte) × 41,4 mm (dikte) × 203 mm (breedte).

  Deze maat, voor het eerst gebruikt door Seagate in 1980, was oorspronkelijk even hoog als een volledige hoogte van een toenmalige floppydrive met 5¼" diameter, namelijk 82,55 mm. Dit is bijna twee keer zo hoog als tegenwoordig wordt gebruikt voor cd- en dvd-drives: 41,4 mm (“halve hoogte”) en al snel hadden ook harde schijven dit formaat. De Quantum Bigfoot-HDD was de laatste met deze lengte en breedte maar dan met “low-profile” (~25 mm) en “ultra-low-profile” (~20 mm) hoge versies.

- Nominaal 3½", dat is 88,9 mm, feitelijk 146 mm × 25,4 mm × 101,6 mm.

  Deze kleinere maat was oorspronkelijk 4,14 cm hoog maar is tegenwoordig vervangen door de variant van 2,54 cm en wordt gebruikt in de huidige desktop-computers.

- Nominaal 2½", dat is 63,5 mm, feitelijk 69,85 mm × 9,5 mm × 100 mm.

  Deze kleinere maat is geïntroduceerd door PrairieTek in 1988; er is geen corresponderende FDD. Het is de meest gebruikte maat in mobiele apparaten, met name laptops. Ook wordt dit formaat steeds meer in (rack-mounted) servers gebruikt. In een 1u-server passen meestal maar twee 3,5"-schijven, tegenover

vier 2,5"-schijven. Vandaag de dag is de meest voorkomende hoogte 9,5 mm, maar er bestaan ook varianten van 19 mm, 17 mm, 12,5 mm, 7 mm en 5 mm.

- Nominaal 1,8", dat is 45,72 mm, feitelijk 71 mm × 8 mm × 54 mm.

  Deze maat is oorspronkelijk geïntroduceerd door Integral Peripherals in 1993. Hij wordt gebruikt in digitale audiospelers en subnotebooks. Dit formaat is populair in iPods en andere mp3-spelers met een harde schijf.

- Nominaal 1", dat is 25,4 mm, feitelijk 42,8 mm × 5 mm × 36,4 mm.

  Deze maat is geïntroduceerd in 1999 als IBM's Microdrive en past in een CF Type II slot. Samsung noemt dezelfde maat "1,3"" in hun productliteratuur.

- Nominaal 0,85", dat is 21,59 mm, feitelijk 32 mm × 5 mm × 24 mm.

  Toshiba kondigde deze vormfactor aan in januari 2004 voor gebruik in mobiele telefoons en soortgelijke apparaten, inclusief met SD/MMC-slot-compatibele HDD's geoptimaliseerd voor videoopslag op 4G-apparaten. Toshiba verkocht versies van 4 GB (MK4001MTD) en 8 GB (MK8003MTD) en heeft het Guinness World Record voor de kleinste harde schijf.

De kleinere maten 1" en 0,85" zijn bezig te verdwijnen vanwege de komst van solid-state disks (flash-disks).

In 1999 werd door IBM de Microdrive op de markt gebracht, een zeer kleine (42 × 36 mm) en platte (5 mm) harde schijf van 170 en 340 megabyte, die als CompactFlash-kaart in een laptop, pda of digitale camera gestoken konden worden. Deze harde schijven zijn net als de andere schijfformaten gestaag in capaciteit gegroeid, 4 en 6 gigabyte-varianten worden (in 2005) gebruikt in mp3-spelers, zoals de iPod.

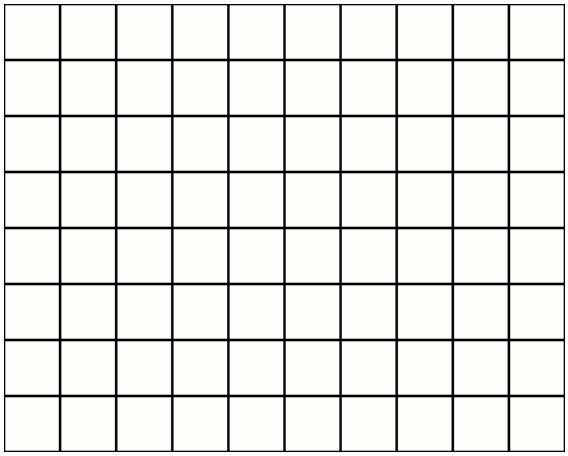
48.8 Partitioneren

Harddisks kunnen worden opgedeeld in meerdere partities. Daarvoor kunnen diverse redenen zijn:

- Gegevens zoals documenten kunnen zo worden gescheiden van het besturingssysteem, zodat het besturingssysteem makkelijker te vervangen is zonder gegevensverlies;
- Partities zijn meestal nodig om meerdere besturingssystemen op één harddisk te installeren;
- Partities zijn nodig als men meerdere bestandssystemen, zoals FAT en NTFS, naast elkaar wil gebruiken.
- Sommige fabrikanten gebruiken een herstelpartitie, zodat het apparaat terug te brengen is zoals het apparaat werd gekocht.

Er zijn diverse programma's om harddisks te partitioneren. Bij het partitioneren kunnen de gegevens op de harddisk verloren gaan. Het is daarom zeer raadzaam om voor het partitioneren eerst een back-up te maken.

48.9 Fragmentatie



Een schematische voorstelling van een bestandssysteem dat gedefragmenteerd wordt.

Omdat bestanden meestal groter zijn dan een sector en de vrije sectoren in de loop van de gebruikstijd verspreid over de schijf komen te liggen, zal fragmentatie optreden. Bij fragmentatie zal een bestand niet in aaneengesloten sectoren worden opgeslagen, maar het bestand zal worden verdeeld over de vrije ruimtes. Dit heeft tot gevolg dat de leeskop vaker naar een track en/of sector moet zoeken en de benodigde tijd voor lezen en schrijven toeneemt. Verschillende bestandssystemen zijn meer of minder gevoelig voor fragmentatie. Het proces van bestanden weer aaneengesloten op een harde schijf plaatsen, heet defragmentatie.

Sommige database-systemen maken geen gebruik van een bestandssysteem en schrijven de data als bits weg op de juiste plaats op de harde schijf. Dit verbetert de prestaties die met een RAID-configuratie nog verhogen.

48.10 Adressering

Een computerprogramma dat een schijf leest of beschrijft, zal meestal werken met bestanden. Het besturingssysteem bepaalt waar het bestand zich bevindt. Uiteindelijk wordt er een sector van de schijf gelezen of beschreven.

Het BIOS bevat routines om een sector van de schijf te lezen of te beschrijven. Ze kunnen worden aangeroepen met INT 0x13.

48.10.1 Cilinder, kop, sector

De oudste schijven kunnen geadresseerd worden met drie bytes, namelijk voor cilinder, kop en sector. In INT 0x13 (functie 0x02 en 0x03) geeft men dan op:

Dit biedt ruimte voor een schijf met 256 koppen, wat erg veel is, en 256 cilinders, wat spoedig erg weinig bleek te zijn. Daarom werd besloten bits van het cilindernummer bij de kop en de sector op te nemen:

48.10.2 LBA

Ook dit was spoedig onvoldoende. De volgende generatie schijven werd uitgerust met LBA (logical block addressing). De schijf presenteert zich als een schijf met 1024 cilinders, 32 koppen en 63 sectoren en de controller van de schijf rekent deze waarden om naar de werkelijke waarden: meer cilinders en minder koppen. Bovendien heeft de schijf wellicht meer sectoren langs de rand van de schijf, zodat er geen vast aantal sectoren meer is. De controller zorgt daarvoor.

48.10.3 Doorlopend volgnummer

De adressering van de vorige paragraaf biedt ruimte voor maximaal 2 GiB. Moderne schijven zijn veel groter. Om eens en voor altijd een oplossing te geven, werd besloten de sectoren sequentieel te nummeren. De programmering wordt daardoor vereenvoudigd: men hoeft niet meer een volgnummer op te delen in cilinder, kop en sector. De sectoren kregen een volgnummer van 64 bits.

Er waren nu nieuwe functies (0x42 en 0x43) nodig in INT 0x13. De functies 0x02 en 0x03 zijn dus verouderd. Aan de functies wordt een volgnummer van 64 bits meegegeven, wat ruimte biedt voor schijven die bijna tien miljard keer zo groot zijn als de huidige schijven van 1 TiB.

Een probleem is echter nog de standaard in de partitietabellen (zie MBR) waarin schijven van maximaal 4 TiB worden ondersteund.

48.11 Betrouwbaarheid

Gegevens die op de harde schijf zijn opgeslagen, blijven over het algemeen minstens 10 jaar intact.

De betrouwbaarheid wordt voor een deel bepaald door het merk en de serie. Sommige series harde schijven blijken in de praktijk veel meer uit te vallen dan andere. Dit heeft in het verleden geleid tot de ondergang van enkele merken van harde schijven.

Vroeger had de temperatuur van de harde schijf grote invloed op de levensduur. Toen gold de vuistregel dat de levensduur zou halveren bij iedere 10 graden meer. Tegenwoordig zijn harde schijven voor desktop-computers echter geoptimaliseerd om te werken tussen 30 en 40 graden. Harde schijven voor in een laptop zijn soms geschikt tot 60 graden, en kunnen jarenlang op 50 graden blijven werken.
Om harde schijven in een desktop-computer niet te warm laten worden zijn er speciale behuizingen en ventilatoren om harde schijven te koelen. Voor laptops zijn er koelers met ventilatoren die onder de laptop geplaatst worden.

De mechanische constructie is tegenwoordig ook veel beter dan bij harde schijven van voor 1995. Maar vooral mechanische schokken tijdens gebruik kunnen nadelig zijn. Tegenwoordig is, met name in harde schijven van laptops, een valbeveiliging ingebouwd die de koppen onmiddellijk parkeert bij versnelling of schokken.

Om gegevensverlies bij een falende schijf te beperken kunnen meerdere schijven in een *redundant array of independent disks* (RAID) configuratie gebruikt worden.

48.12 Geluid

Een harde schijf produceert de volgende geluiden:[5]

- Een laagfrequente trilling door het ronddraaien van de schijven. Deze is meestal niet hoorbaar, maar wel te voelen als een aangesloten harde schijf los in de hand wordt gehouden.
- Geruis door het ronddraaien van de schijven. Dit geluid is vooral bij oude harde schijven goed hoorbaar, maar is meestal niet hinderlijk. Sinds 2002 hebben vrijwel alle harde schijven vloeistoflagers, waardoor dit geluid sterk is verminderd.
- Een hoge toon door het ronddraaien van de schijven en door de trilling die de motor veroorzaakt. Deze hoge toon wordt meestal luider als er onbalans is, bijvoorbeeld wanneer de harde schijf gevallen is. Ook wordt deze toon luider in de loop van de jaren. Wanneer deze toon plotseling toeneemt en in de loop van weken of maanden nog sterker wordt, kan dit duiden op onbalans van de schijven en kan de harde schijf minder betrouwbaar worden. De kast van de computer kan dit geluid versterken.

- Een grommend/reutelend geluid van de arm waarop de lees/schrijf-kop zich bevindt. Dit is alleen te horen als de harde schijf gegevens moet verwerken. Dit geluid kan soms versterkt worden door de computerkast, vooral als die van dun metaal gemaakt is. Sinds 2000 hebben de meeste harde schijven mogelijkheden om dit geluid te verminderen. De arm met de lees/schrijf-kop wordt dan minder snel heen en weer bewogen. Het nadeel hiervan is dat de data minder snel opgevraagd kunnen worden. Dit komt simpelweg omdat de arm met de lees/schrijf-kop minder snel bij de plaats van bestemming is.

Er bestaan verschillende manieren om de geluiden te verminderen, bijvoorbeeld door de harde schijf niet tegen het metaal van de computer aan te schroeven, maar dat via rubbertjes te doen.

48.13 De harde schijf afdanken of repareren

Bij meerdere onderzoeken bleek in 2005 dat harde schijven die tweedehands worden aangeboden in meer dan de helft van de gevallen nog persoonlijke gegevens bevatten. Dat kan gaan om e-mailgegevens, maar ook om creditcardnummers of andere vertrouwelijke gegevens.

Het wordt dan ook dringend aangeraden gegevens grondig te verwijderen voordat men een schijf afdankt. Zonder meer verwijderen van bestanden is onvoldoende, want daarmee worden alleen de indexen (of zelfs alleen de partitietabel) verwijderd zodat veel gegevens nog teruggehaald kunnen worden. Volledig wissen (alle sectoren wissen) is veiliger, maar volgens sommigen zijn ook dan de gegevens met gespecialiseerde apparatuur nog te herstellen.

Het kan een probleem zijn als een schijf voor reparatie ingestuurd moet worden, aangezien een defecte schijf niet zelf gewist kan worden. Erger: vaak wordt de schijf niet direct gerepareerd maar omgeruild, en na reparatie wordt de schijf (als 'refurbished') aan een andere klant gegeven. Nu valt te verwachten dat een fabrikant wel iets beters te doen heeft dan een ingestuurde schijf te onderzoeken op achtergebleven gegevens, en bovendien zal een scrupuleuze fabrikant de schijf grondig wissen voordat hij opnieuw in omloop wordt gebracht. Bevat een schijf echter zeer vertrouwelijke gegevens, dan kan men beter van reparatie afzien.

48.13.1 Gegevens wissen van de harde schijf

Op een FAT-schijf onder DOS en versies van Microsoft Windows tot en met 3.11 wordt als 'verwijderd'-markering de eerste letter van de naam van het bestand vervangen door een teken (hexadecimaal E5), en de gegevensblokken die het bestand bezette worden als “vrij” gemarkeerd. De gegevens van het bestand staan echter nog steeds op de harde schijf en zijn met speciale (data recovery-)programma’s terug te vinden, zolang ze maar niet overschreven worden.

Een harde schijf bevat in tegenstelling tot een bandrecorder geen wiskop. De oude magnetische gegevens worden dus niet eerst gewist, maar de nieuwe informatie wordt eroverheen geschreven. Daardoor wordt de nieuwe magnetische informatie nog enigszins beïnvloed door de vorige informatie. Dit is normaal gesproken geen enkel probleem, omdat de elektronica van de harde schijf het altijd naar de correcte bit (een “1” of een “0”) vertaalt. Volgens het Amerikaanse NIST, Special Publication 800-88, en ook het Duitse BSI, kunnen harde schijven effectief 'geschoond' worden door de gegevens een maal te overschrijven. Diverse studies hebben dat aangetoond. Volgens de studie, Overwriting Hard Drive Data: The Great Wiping Controversy is de kans dat een byte (één karakter) juist wordt geïnterpreteerd, middels MFM (Magnetic Force Microscopy) 0,97% voor een in gebruik zijnde harde schijf. Het zou een forensisch expert circa 3,8 miljoen jaar kosten om een harde schijf van 100 GB volledig te beoordelen. Een andere wijze van datavernietiging is het mechanisch versnipperen of doorboren van de harde schijf. Dit heeft echter tot gevolg dat er een afvalstroom ontstaat en de computer waar de harde schijf uit is verwijderd veelal nagenoeg geen restwaarde meer heeft. Met de wetenschap dat een eenmalige overschrijving van de harde schijf veilig is, kunnen organisaties zowel economisch als maatschappelijk verantwoorde beslissingen nemen over de juiste wijze van datavernietiging.

48.14 Andere opslagmedia met roterende schijven

Naast de harde schijf bestaan er ook andere ronddraaiende opslagmedia waarop informatie kan worden gelezen en/of geschreven: bijvoorbeeld diskettes, cd-roms, dvd's, zipdisks, jazdisks, bernouillidrives, hd-dvd's blu-raydisks enzovoort. De prijs per gigabyte kan erg verschillen doordat sommige zojuist genoemde producten nieuw/nieuwer zijn dan de andere producten.

48.15 Toekomst

Sinds 2009 is het mogelijk om de harde schijf te vervangen door een solid-state drive (SSD), die ongeveer 10 keer sneller is met lezen en schrijven dan een conventionele harde schijf. Tegenwoordig hebben SSD’s een toegangstijd van amper 0,1 milliseconde. Een SSD heeft echter een hogere prijs per gigabyte dan de conventionele harde schijf, hoewel de prijzen al drastisch zijn ge-

daald. Kleine netbooks hebben vaak geen harde schijf meer, maar een vorm van flashgeheugen. Het flashgeheugen kan in de vorm van een SSD zijn, maar het geheugen kan ook direct in de netbook gesoldeerd zijn.

Voor grote hoeveelheden gegevensopslag is de harde schijf nog onmisbaar, aangezien de SSD's met grotere capaciteiten nog steeds erg duur zijn. Pas als de SSD's van grotere capaciteit betaalbaar worden, of als er nieuwe goedkopere technieken worden uitgevonden om nog meer gegevens op te kunnen slaan voor een lagere prijs dan de SSD, zal de harde schijf wellicht verdwijnen.

48.16 Trivia

- Op 13 september 2006 bestond de harddisk vijftig jaar. De eerste schijf van dit type (de RAMAC van IBM) had een capaciteit van 5 MB en woog ongeveer 1000 kg. Omgerekend betekent dit een gemiddelde volumetoename van ongeveer 47 procent per jaar.
- In augustus 2006 kondigde Hitachi aan datzelfde jaar harde schijven van 3,5 inch met een capaciteit van 1 terabyte te gaan produceren.
- Begin april 2007 werd de eerste harde schijf met een capaciteit van 1 terabyte gespot in een winkel in Japan. De schijf bestaat uit vijf schijven van 200 GB, draait met 7200 toeren per minuut en heeft 32 MB cachegeheugen aan boord. Medio 2007 zijn schijven van 1 terabyte verkrijgbaar in de computerwinkels. Sinds begin februari 2009 zijn er ook de eerste schijven van 2 TB (2000 GB) verkrijgbaar, die bestaan uit 4 schijven van 500 GB. Sinds maart 2011 worden ook schijven van 3 TB aangeboden.
- Eind oktober 2011 zijn de prijzen van harde schijven fors gestegen door tekorten op de markt die zijn ontstaan door de zware overstromingen in Thailand, een van de grootste exporteurs van harde schijven. Dit had tot gevolg dat de prijzen hoog bleven tot medio derde kwartaal 2012.
- In het laatste kwartaal van 2012 was de eerste harde schijf van 4 TB (4000 GB) verkrijgbaar in de computerwinkels.
- Sinds juni 2014 zijn er harde schijven van 6 TB (6000 GB) te koop in Europa, sedert begin maart/april 2015 van 8 TB (8000 GB).

Hoofdstuk 49

Hashfunctie

Een **hashfunctie** of **klutsfunctie** is een functie in de informatica die invoer uit een breed domein van waarden omzet in een (meestal) kleiner bereik, meestal een deelverzameling van de gehele getallen. Het is een vorm van pseudonimiseren. Het woord *hash* komt uit het Engels en betekent hier *hakken*.

Hashfuncties worden gebruikt in hashtabellen, cryptografie en dataverwerking. Een goede hashfunctie is er een die weinig botsingen veroorzaakt in het domein waarmee ze werkt, dit wil zeggen dat er weinig kans is dat twee verschillende invoerwaarden dezelfde uitvoer geven.

Formeel betekent dit dat een goede hashfunctie H de eigenschap heeft dat uit H(x) = H(y) volgt dat het zeer waarschijnlijk is dat x = y.

Een voorbeeld hiervan zijn de SHA-familie van functies.

49.1 Cryptografische hash

Voor een cryptografische hashfunctie geldt niet alleen dat het voor twee toevallige waarden x en y zeer onwaarschijnlijk is dat H(x) = H(y), maar ook dat iemand die bewust op zoek gaat naar zulke waarden ze niet zal kunnen vinden. Een cryptografisch veilige hashcode heeft de eigenschappen dat het niet mogelijk is om te achterhalen van welk blok gegevens de bepaalde code is afgeleid en dat het onmogelijk is om twee verschillende blokken gegevens te maken die dezelfde hashcode hebben. Hierdoor heeft een cryptografisch veilige hashcode de eigenschappen van een digitale 'vingerafdruk'.

Voorbeelden van cryptografische hashalgoritmen zijn MD5 en de SHA-familie van hashfuncties. MD5 wordt echter tegenwoordig niet meer als cryptografisch veilig beschouwd.

49.2 Hashing van wachtwoorden

Voor de aanmelding bij een computer zijn vaak een naam en een wachtwoord nodig. Deze wachtwoorden worden vaak versleuteld opgeslagen, zodat de wachtwoorden niet bekend worden als het bestand met wachtwoorden door een onbevoegde gelezen wordt. Dit gebeurt door middel van een hashing-algoritme, dat het onmogelijk maakt de versleutelde gegevens te decoderen. Dat is ook niet nodig, aangezien het voldoende is te controleren of de gebruiker het juiste wachtwoord heeft opgegeven.

Bij het versleutelen van wachtwoorden is het echter onveilig om gebruik te maken van algemene hash-algoritmen, en dient gebruik te worden gemaakt van speciale hash-algoritmen voor wachtwoorden zoals bcrypt, scrypt, of PBKDF. De reden is dat normale hash-algoritmen zijn ontworpen om zo snel mogelijk berekend te kunnen worden. Bij het hashen van wachtwoorden is dat onwenselijk, omdat het daardoor mogelijk wordt dat iemand die de hashcodes van de wachtwoorden in bezit heeft gekregen achterhaalt welke hashcode van welk wachtwoord is afgeleid.

De lengte en complexiteit van wachtwoorden die mensen in de praktijk gebruiken is beperkt, terwijl computers steeds sneller worden. Daardoor wordt het voor iemand die probeert hashcodes voor wachtwoorden te kraken steeds makkelijker om een computer allerlei mogelijkheden te laten uitproberen. Hash-algoritmen voor wachtwoorden blokkeren deze methode doordat voor deze algoritmen in te stellen is hoeveel rekentijd ze moeten kosten. De algoritmen worden dan zo ingesteld dat het uitrekenen ervan bijvoorbeeld één milliseconde kost, terwijl het berekenen van een hashcode met een gewoon hash-algoritme minder dan een microseconde kan kosten. Bij het controleren van een wachtwoord is het meestal geen probleem als dit een milliseconde in plaats van een microseconde kost, terwijl iemand die wil proberen de hashcodes te kraken meer dan duizend keer zo veel rekenwerk moet doen, en dus meer dan duizend keer langer bezig is.

49.3 Zie ook

- Cryptografie
- SHA-familie
- MD5
- Pseudonimiseren

Hoofdstuk 50

Honeypot (informatica)

Een **honeypot** is in de informatica een computersysteem dat zich bewust kwetsbaar opstelt voor (worm)virussen en andere aanvallen. Door de vergaarde informatie te analyseren, kan de verspreiding van de virussen mede worden tegengegaan. Daarnaast worden honeypots ingezet om post-admission control in quarantainenetwerken te realiseren. Soms wordt een honeypot gebruikt om de gegevens van de hacker zelf te achterhalen. Zo kunnen ze de hacker aanhouden en desnoods berechten. De gegevens die door honeypot zijn achterhaald, dienen dan als bewijs. Een honeypot zal over gegevens beschikken die een hacker interessant vindt, zoals wachtwoordgegevens.

De herkomst van de term *honeypot (nl: honingpot)* wordt vaak verbonden aan de beer Winnie de Poeh, die in allerhande situaties belandde door zijn grote voorliefde voor potten honing.

50.1 Zie ook

- Damn Vulnerable Linux, een Linuxdistributie die zich moedwillig zwak opstelt

Hoofdstuk 51

Hyperlink

Typische weergave van een hyperlink: een gekleurde, onderstreepte tekst met een veranderende muisaanwijzer

Een **hyperlink** (of kortweg **link**) – met een Nederlands woord *verbinding* of *koppeling* – is een computer- en internetterm die duidt op een verwijzing (referentie) in een hypertekst (bijvoorbeeld een website) die de gebruiker kan volgen.

Het activeerbare element van de hyperlink wordt het **anker** genoemd; meestal is dit een stukje tekst, maar het kan ook bijvoorbeeld een knop, invulbaar veld of plek (hot spot) in een afbeelding (image map) zijn.

Het volgen van een hyperlink (bijvoorbeeld door erop te klikken) roept een andere plek in de hypertekst op, meestal een andere pagina. In interactieve naslagwerken en hulpsystemen, bijvoorbeeld, zijn de ankers veelal termen waarover de opgeroepen pagina's nadere uitleg geven.

Veel hypertekst is te verdelen in onafhankelijk onderhouden verzamelingen "hyperdocumenten"; het wereldwijde web bestaat bijvoorbeeld uit websites. Deze documenten hebben meestal een algemene voorpagina (de hoofdpagina van een website). Het maken van hyperlinks naar andere pagina's dan de beginpagina wordt dieplinken genoemd.

51.1 Voorbeelden

Op het wereldwijde web worden als hyperlinks zogenaamde URL's gebruikt (*Uniform Resource Locator*s, oftewel uniforme adresseringen van een informatiebron. Een URL zoals *https://nl.wikipedia.org/wiki/Wikipedia* is als volgt opgebouwd:

1. **https**:// geeft het communicatieprotocol aan: de techniek waarmee de browser met de server moet communiceren, in dit geval HTTP. Het protocol wordt afgesloten met *://*. Er staat bijvoorbeeld *ftp*:// als FTP moet worden gebruikt.
2. **nl.wikipedia.org** is de naam van de server op het internet waar de browser contact mee moet leggen. Dit stukje tekst, vaak tot de slash (/) geeft aan van welke website we de informatie willen hebben. Dat klopt dus ook, want we gaan informatie opvragen bij *nl.wikipedia.org* en nergens anders.
3. **wiki/Wikipedia** geeft een specifieke informatiebron aan binnen de website van *nl.wikipedia.org*; dit is vaak een bestand op de harde schijf, maar dat hoeft niet. Als het een bestand is, is **wiki/Wikipedia/** meestal de naam van een map op de harde schijf waar het bestand te vinden is. Submappen worden door website beheerders/ontwerpers aangemaakt om de inhoud te organiseren en te categoriseren. In dit geval wordt dus de map *wiki* geopend en daarna de map *Wikipedia*. Meestal surfen we naar de hoofdmap van een website, zoals *https://nl.wikipedia.org* en worden we daar ontvangen.

Hoofdstuk 52

Identiteitsfraude

The Prisoner of Zenda *(1894), een voorbeeld van identiteitsfraude*

Identiteitsfraude wil zeggen dat iemand op een slinkse manier persoonlijke gegevens verwerft van iemand anders (identiteitsdiefstal) om zich dan geloofwaardig voor te doen als deze persoon. Met deze valse identiteit is hij in staat slachtoffers op te lichten. Daarnaast kan hij ook toegang verwerven tot computersystemen, vormen van elektronische dienstverlening en betaal- en creditcardrekeningen.

52.1 Methodes

Het verwerven van een identiteit of persoonlijke gegevens kan langs tal van wegen:

- Bij inbraak van de woning of auto;
- Het stelen van post uit brievenbussen of via het onderscheppen van post;
- Door het kopiëren van kaartgegevens bij kaartgebruik in winkel of geldautomaat. Het kopiëren van kaartgegevens heet Skimmen, deze identiteitsfraude gebeurt met gebruikmaking van iemands pinpas of creditcard. Met de gekopieerde pinpas kunnen kwaadwillenden betalingen doen uit jouw naam.
- Door het kopiëren van bestanden met persoonsgegevens van klanten (door medewerkers van bedrijven);
- Door het hacken van computersystemen, pharming;[1]
- Door middel van informatie in afval- en prullenbakken (dumpsterdiving);
- Door met een valse identiteit persoonlijke informatie op te vragen via internet (phishing). Met phishing proberen kwaadwillenden iemand naar een 'verkeerde' website te sturen zonder dat de persoon het merkt om hiermee de gebruikersnaam en wachtwoord van de echte website te ontfutselen.
- Het plaatsen van een valse vacature om zodoende c.v.'s en eventueel andere documenten van geïnteresseerden te 'oogsten'.
- Social engineering, dit doet men door telefonisch of op een andere manier proberen te achterhalen wat de gebruikersnaam en het wachtwoord van deze persoon is. Vervolgens kan men met de verworven gebruikersnaam en wachtwoord binnen het systeem komen.
- Het zoeken in registers. Neem bijvoorbeeld Google, als men goed zoekt kan door middel van Google al veel te weten gekomen worden over een persoon. Bij sollicitatiegesprekken kan er bijvoorbeeld gezocht worden op kandidaten om te kijken of er iets bekend is van deze persoon op internet.

52.2 De gevolgen

- Oplichting: Het gevolg van identiteitsdiefstal is meestal oplichting op grote schaal. De oplichter kan met de informatie bankrekeningen plunderen of persoonlijke informatie van anderen bemachtigen. Ook voor bedrijven kan identiteitsdiefstal gevaarlijk zijn. Bedrijfsgeheimen zijn vaak veel waard.

- Cyberpesten: Door de opkomst van sociale netwerken is het relatief eenvoudig een account aan te maken met een andere identiteit dan die van zichzelf. Dit heeft als voordeel dat men volledig anoniem mensen kan pesten op het internet. Men spreekt hier van cyberpesten. Door die valse identiteit kunnen oplichters zelfs de schuld in de schoenen van iemand anders schuiven.

52.3 Voorbeelden

52.3.1 Identiteitsfraude Ron Kowsoleea

In Nederland is het bekendste geval van identiteitsfraude de zaak van Ron Kowsoleea. Zijn naam werd in de periode 1994 tot en met 2002 stelselmatig misbruikt door Imro C., een crimineel die een oude bekende van hem was. Bij iedere aanhouding gaf Imro C. zich voor Kowsoleea uit. Nadat Imro C. in 2002 in de gevangenis terecht was gekomen, ondervond Kowsoleea hier nog tot 2009 problemen door. Hij werd in die periode bijvoorbeeld herhaaldelijk aangehouden en in 2003 kreeg hij te maken met een inval door de Fiscale Inlichtingen- en Opsporingsdienst (FIOD). Hoewel de identiteitsfraude reeds bij de eerste rechtszaak in 1994 duidelijk was, werden zijn strafdossiers niet opgeschoond, waardoor misverstanden bleven ontstaan. Door de strafrechtelijke onderzoeken verloor hij steeds meer zakenpartners en kwamen zijn bedrijven in surseance van betaling.

Eind 2008 bracht de Nationale ombudsman een rapport over de zaak uit met een vernietigende conclusie over de gang van zaken. Zijn zaak was in 2008 en 2009 veelvuldig in het nieuws. In 2008 en 2009 besteedde het actualiteitenprogramma *EenVandaag* viermaal aandacht aan Kowsoleea en identiteitsfraude. In dat jaar bood toenmalig minister van Justitie Hirsch Ballin uiteindelijk verontschuldigingen aan en werd een vergoeding voor de geleden schade betaald.[2][3][4][5][6][7][8][9][10]

52.4 Noten

[1] Bescherm je financiën: wat is pharming

[2] BN De Stem - Diefstal identiteit maakt leven zakenman tot hel

[3] NRC.nl 19 maart 2009 - Rechter negeert ombudsman, geschil blijft

[4] NRC.nl 25 september 2009 Justitie zegt slachtoffer van identiteitsfraude tegemoet te willen komen

[5] NRC.nl 24 september 2010 Ombudsman stelt slachtoffer identiteitsfraude opnieuw in gelijk

[6] VPRO Thema - Wat nou privacy

[7] EenVandaag 23 oktober 2008 - Tientallen slachtoffers identiteitsfraude

[8] EenVandaag 2 maart 2009 - Vijftien jaar lang onterecht strafblad

[9] EenVandaag 16 april 2009 - De verdwenen identiteit van Ron Kowsoleea

[10] EenVandaag 24 september 2009 - Hirsch Ballin: 'Excuus voor Ron Kowsoleea'

Hoofdstuk 53

Internet der dingen

Het **internet der dingen** (Engels: *Internet of things*) refereert aan de situatie dat door mensen bediende computers (desktops, tablets, smartphones) in de minderheid zullen zijn op het internet. De meerderheid van de internetgebruikers zal in deze visie bestaan uit semi-intelligente apparaten, zogenaamde embedded systems. Alledaagse voorwerpen worden hierdoor een entiteit op het internet, die kunnen communiceren met personen en met andere objecten, en die op grond hiervan autonome beslissingen kunnen nemen.

Internet der dingen

53.1 Verouderde betekenis van de term

Kevin Ashton, toenmalig hoofd van het 'Auto-ID Center' van het MIT, gebruikte in 1999 de term *Internet der dingen*,[1] maar de discussie hierover dateert op zijn minst van 1991.[2] Destijds werd echter vooral gedacht aan toepassingen met RFID. Door alle objecten, inclusief mensen, van identifiers te voorzien zou de echte wereld geïnventariseerd en gemanaged kunnen worden door computers. Te denken valt bijvoorbeeld ook aan het volgen van het transport van pakketjes.

53.2 Moderne visie op internet der dingen

Een hedendaagse definitie van het internet der dingen is: *Een voorgestelde ontwikkeling van het internet, waarbij alledaagse voorwerpen zijn verbonden met het netwerk en gegevens kunnen uitwisselen.*[3]

Als het belangrijkste aspect van het Internet der dingen wordt genoemd: de mogelijkheden die ontstaan wanneer fysieke objecten en de virtuele wereld samenkomen.[4]

In de huidige visie spelen 'slimme' objecten een sleutelrol in het internet der dingen. Dit omdat ingebedde informatie- en communicatie-technologie het potentieel heeft om de bruikbaarheid van objecten revolutionair te doen toenemen. Met gebruik van sensors kunnen deze hun omgeving in zich opnemen, en via ingebedde netwerktechnologie kunnen ze met elkaar communiceren, internetdiensten gebruiken en met mensen interageren.[5] In de huidige betekenis refereert de term internet der dingen dus aan 'dingen' die zelf computers zijn, en via internet zaken monitoren en regelen.

De verwachtingen rond het internet der dingen zijn dat er vanuit diverse gezichtspunten[6] voordelen zullen zijn:

- *commercieel*: efficiëntere processen, minder kosten voor logistiek/opslag, verkoop meer toegespitst op klanten;[7]
- *sociaal en politiek*: duidelijkere informatie voor klanten en burgers, betere zorg, betere veiligheid (bijvoorbeeld in het verkeer);
- *persoonlijk*: nieuwe diensten die het leven aangenamer en veiliger maken.

53.3 Basistechnologie van het internet der dingen

Het internet der dingen wordt mogelijk gemaakt door een aantal basistechnologieën. Dat betekent dat de meeste toepassingen op een groot aantal van de onderstaande technologieën gebaseerd zullen zijn.[8]

Communicatie en samenwerking Apparaten (objecten) kunnen communiceren met het internet, of zelfs met elkaar. Ze kunnen gebruikmaken van internetdata en -services, en dan hun eigenschappen veranderen (bijvoorbeeld van stilstaand naar rijdend). Hierbij zijn ontwikkelingen in draadloze communicatie zoals UMTS en wifi cruciaal.

Adresseerbaarheid Als adres van het object heeft een IP-adres het voordeel dat dit goed gestandaardiseerd is, en dus goed samenwerkt met het netwerk.[9] Door het internet der dingen neemt het aantal benodigde IP-adressen naar verwachting explosief toe. Een vereiste is immers dat elk object een eigen 'adres' heeft. Door de nu al plaatsvindende overgang van IPv4 naar IPv6 wordt voorzien in de behoefte aan (zeer) grote aantallen IP-adressen.[9][10]

Identificatie De apparaten (objecten) moeten uniek identificeerbaar zijn. Voor passieve objecten (d.i. objecten zonder energiebron) kan identificatie via RFID of barcodes plaatsvinden. Hierbij kan een RFID-lezer of mobiele telefoon als medium fungeren. Hierdoor kan een object (bv. een tandwiel met barcode) gelinkt worden aan informatie die elders daarover opgeslagen is (niet zozeer over *wat voor* tandwiel het is, maar over *welk* tandwiel het is; bijvoorbeeld dat het tandwiel in jaar x aan fabriek y verkocht is en onderdeel is van machinenummer 123456).

Sensors Met een sensor verzamelen apparaten data over hun omgeving. Ze leggen deze vast of sturen ze door of reageren er direct op. Sensors zetten een analoog signaal (bijvoorbeeld temperatuur of lichtintensiteit) om in een digitaal signaal (enen en nullen), zie analoog-digitaalomzetter.

Actuatoren Via een actuator beïnvloeden de apparaten de fysieke wereld. Een actuator zet een signaal om in een actie, bijvoorbeeld een beweging.

Ingebedde informatieverwerking Slimme apparaten hebben een microcontroller en opslagcapaciteit voor informatie, zie embedded system.

Lokalisatie In het internet der dingen moeten de objecten gevonden kunnen worden, dat wil zeggen: gelokaliseerd en herkend via opzoekdiensten. Denk hierbij aan hoe mobiele telefoons gevonden en gelokaliseerd worden.
Apparaten zijn zich 'bewust' van hun fysieke locatie. Dit gebeurt door deze zelf vast te stellen, dan wel doordat deze bepaling voor hen gedaan wordt. gps en mobiele-communicatietechnologie maken dit mogelijk. In Groot-Brittannië is men inmiddels begonnen het frequentiespectrum anders in te richten vanwege het internet der dingen.[11]

Gebruikersinterface Slimme objecten moeten met mensen kunnen communiceren, dit gebeurt direct dan wel indirect (via smartphone). Hierbij zijn vooral technologieën als spraakherkenning, beeldherkenning en geluidsherkenning van belang.

53.4 Eisen opgelegd aan de technologie

Om het internet der dingen praktisch haalbaar te doen zijn, zal de onderliggende technologie aan diverse eisen moeten voldoen.[12] Deze eisen liggen op de volgende gebieden:

- schaalbaarheid: zowel lokaal gebruik als gebruik op grote schaal
- mobiele 'dingen' moeten in staat zijn om spontaan en zelfstandig zich te configureren en verbindingen op te zetten
- interoperabiliteit, bijvoorbeeld via (waar nodig) standaardisatie
- vindbaarheid: een gebruiker zal via een 'zoekmachine' willen achterhalen waar een 'ding' zich bevindt en in welke toestand het verkeert
- software
- managen van grote datavolumes
- correcte en nauwkeurige interpretatie van de door sensoren vergaarde gegevens
- veiligheid en privacy: bij 'dingen' zullen er extra regels komen die aangeven wat (en wanneer) zij wel of niet mogen; ook zal gewaarborgd moeten zijn dat 'dingen' niet kunnen worden gehackt
- fouttolerantie door redundantie en het kunnen aanpassen aan gewijzigde omstandigheden
- energie: vanwege praktische bezwaren van batterijen (grootte en gewicht) zullen creatieve oplossingen nodig zijn voor de energievoorziening van bijvoorbeeld sensoren
- draadloze communicatie over zo kort mogelijke afstanden (enkele centimeters) maakt meer oplossingen mogelijk (bv. inductie)
- draadloze communicatie algemeen; vanwege de energieconsumptie zijn GSM, UMTS, wifi en bluetooth minder geschikt; nieuwere technieken zijn weliswaar smalbandiger maar ze gebruiken ook minder energie

53.5 Anno 2016 met het internet verbonden apparaten

Er zijn anno 2016 al heel veel embedded systemen permanent, of tijdelijk met het internet verbonden. Zo zijn er onder meer moderne fototoestellen, kopieerapparaten, wasmachines, robots, auto's. Van de overgrote meerderheid hiervan kan echter niet gezegd worden dat ze hun omgeving in zich opnemen, of met wie dan ook een communicatie starten. De apparaten zijn misschien wel in de meerderheid op het internet, maar er is nog geen sprake van een internet der Dingen.

53.6 Toepassingen en projecten

Domotica-systemen kunnen een toepassing zijn van het internet der dingen.

In Australië planten biologen jaarlijks door het hele land circa een miljoen graanplantjes om te zien onder welke condities welke soorten het beste groeien. Met een klein team moeten nu zowel de omgevingsomstandigheden als de groeisnelheid van het graan worden gemonitord. Dit wordt opgelost via een draadloos netwerk met sensoren.[13]

In de sport worden al sensoren ingezet om gegevens over workouts te verzamelen. De gegevens worden zonder menselijke tussenkomst verstuurd naar een centraal punt en daar verwerkt. Sporters of hun trainers kunnen inloggen op een website om de voortgang te analyseren.[13]

Er wordt gewerkt aan een tandenborstel die verbinding kan maken met een smartphone om zo tijdens het poetsen te vertellen hoelang en in welke mondhoeken er moet worden gepoetst.[14]

Het Dyconetproject[15], uitgevoerd bij het Fraunhofer-Institut für Materialfluss und Logistic (IML) in Dortmund, heeft betrekking op intelligente luchtvrachtcontainers. Het betreft containers die hun omgeving volgen via sensors, enige intelligentie hebben en zelf communicatie initiëren, ook met andere containers.

In oktober 2014 werd door de Europese Commissie een subsidie toegekend voor het 'Triangulum'-project, dat beoogt van Eindhoven (Nederland), Stavanger (Noorwegen) en Manchester (Groot-Brittannië) 'smart cities' te maken.[16][17] Sensornetwerken en geïntegreerde ICT-systemen zijn onderdeel van het project.

53.7 Open Internet Consortium

In juli 2014 werd door vijf technologiebedrijven het Open Internet Consortium opgericht, dat als doel heeft de ontwikkeling van standaarden voor het internet der dingen. Uitgangspunten zijn diverse reeds bestaande connectiviteitsoplossingen. Als eerste resultaat wordt opensourcecode verwacht voor specifieke smart-home- en office-oplossingen.

53.8 Kritiek en controverses

Sommigen beschouwen het internet der dingen als een technische stap vooruit, anderen tonen terughoudendheid.

Peter-Paul Verbeek, hoogleraar techniekfilosofie aan de Universiteit van Twente, schrijft dat technologie nu al onze morele besluitvorming beïnvloedt, wat weer gevolgen heeft voor privacy en autonomie.[18] Hij waarschuwt tegen het beschouwen van technologie als slechts een 'werktuig' en vindt dat we het moeten zien als een actieve entiteit.

Een ander punt van kritiek is dat het internet der dingen snel wordt ontwikkeld zonder goed rekening te houden met veiligheid en met aanpassingen in regelgeving die noodzakelijk zullen zijn.[19] In het bijzonder zullen, bij verdere verspreiding van het internet der dingen, cyberaanvallen een meer fysiek karakter krijgen in plaats van zich slechts af te spelen in de virtuele wereld.[20] In Forbes, in januari 2014, noemde cybersecurity columnist, Joseph Steinberg, diverse met het internet verbonden applicaties die nu al "mensen in hun eigen huis kunnen bespieden", waaronder televisies, keukenapparatuur, camera's, en thermostaten.[21]

In een rapport van het Amerikaanse National Intelligence Council staat dat het moeilijk zal zijn om "toegang tot netwerken bestaande uit sensoren en op afstand bestuurde objecten te ontzeggen aan vijanden van de VS en criminelen. Een open markt voor geaggregeerde sensorgegevens zal naast het bevorderen van commercie en veiligheid ook criminelen en spionnen helpen bij het in kaart brengen van kwetsbare doelen. Het op grote schaal combineren van sensorgegevens kan de maatschappelijke cohesie ondermijnen als het niet te verenigen blijkt te zijn met garanties uit het Fourth-Amendment tegen onredelijke zoekacties."[22] In het algemeen kan worden vastgesteld dat de *intelligence*-sector het internet der dingen beschouwt als een rijke gegevensbron.[23]

Er is brede erkenning voor het feit dat ontwerp en beheer van het internet der dingen via evolutie zich verder zullen ontwikkelen. De ontwerpen van toekomstvaste en veilige oplossingen zullen daarom moeten uitgaan van "anarchistische schaalbaarheid".[24] Toepassing van dit concept kan worden uitgebreid naar fysieke systemen (beheerde objecten in de reële wereld), mits bij het ontwerp daarvan rekening is gehouden met onzekerheid in de beheereigenschappen. De mogelijkheden van het internet der dingen kunnen dus in de toekomst geheel worden benut als de fysieke systemen kunnen werken met alle mogelijke beheersystemen zonder risico op uitval.

Justin Brookman, van het Center for Democracy and

Technology, maakt zich zorgen over de gevolgen die het internet der dingen zal hebben op de privacy van de consument. Zijn uitspraak is: “Er zijn binnen de commercie mensen die zeggen ‘Oh, big data — prima, we slaan alles op, gooien nooit iets weg, en later huren we iemand in om na te denken over security.’ De vraag is of we afspraken wensen te maken om hier beperkingen aan op te leggen.”[25]

De American Civil Liberties Union (ACLU) ziet het probleem dat het internet der dingen ten koste kan gaan van de controle die burgers hebben over hun eigen leven. De ACLU schreef “Het is simpelweg niet mogelijk om te voorspellen hoe deze enorme krachten -- die vooral terechtkomen bij bedrijven die zoeken naar financieel gewin en regeringen die zoeken naar steeds meer controle -- zullen worden aangewend. Het is goed denkbaar dat 'Big Data' en het internet der dingen het voor ons moeilijker zullen maken onze eigen levens in eigen hand te hebben, terwijl we steeds meer afhankelijk worden van machtige bedrijven en overheidsorganen die voor ons steeds ondoorzichtiger worden.”[26]

Een aspect dat vaak wordt vergeten heeft te maken met de gevolgen voor het milieu van het fabriceren, gebruiken en uiteindelijk als afval verwerken van apparatuur met veel halfgeleiders. Moderne elektronica bevat een grote diversiteit aan zware metalen en zeldzame metalen, en daarnaast zwaar giftige chemische bestanddelen. Dit maakt recyclen bijzonder lastig. Elektronische componenten worden vaak simpelweg gedumpt, en vervuilen vervolgens de bodem, grondwater, oppervlaktewater en lucht. Dit kan uiteindelijk leiden tot chronische ziektes bij mensen. Daarnaast neemt de milieuschade die samenhangt met het winnen van de voor moderne elektronische componenten noodzakelijke zeldzame metalen, steeds meer toe. Hoewel op wereldschaal de productie van elektronische apparatuur groeit, worden slechts weinig van de metalen (van niet meer gebruikte apparatuur) verzameld voor hergebruik. De gevolgen voor het milieu zullen hierdoor toenemen.

Bij het internet der dingen zal vaker dan voorheen sprake zijn van het inbouwen van elektronica in alledaagse objecten, zoals lichtschakelaars. Daarnaast is bekend dat de belangrijkste aanleiding voor het vervangen van elektronische componenten vaker het voortschrijden van de techniek is, dan het daadwerkelijk niet meer functioneren van de component. Het is dus te verwachten dat in de toekomst ook alledaagse objecten vaker zullen worden vervangen dan we gewend waren. Dit zal ook weer leiden tot (veel) meer afval.

In de marketing rondom het internet der dingen zal soms de nadruk worden gelegd op de realiseerbare energiebesparing. Vaak kan hetzelfde voordeel worden behaald door het hebben van een goed lopende huishouding.

53.9 Toekomst

Volgens het adviesbureau Gartner zullen in 2020 26 miljard apparaten aan het internet der dingen verbonden zijn.

53.10 Zie ook

- Slimme stad

53.11 Externe link

- “From the Internet of Computers to the Internet of Things” (F. Mattern & C. Floerkemeier)

Hoofdstuk 54

Internet protocol spoofing

Internet Protocol Spoofing of **IP spoofing** is een techniek om ongeautoriseerde toegang te verkrijgen tot een computer via diens IP stack. De techniek is gebaseerd op het vervalsen van de identiteit van een andere computer en is bijzonder effectief als de gefingeerde identiteit die is van een entiteit die door de aangevallen computer wordt vertrouwd.

54.1 De basis

IP-spoofing maakt gebruik van twee dingen om een succesvolle aanval op te zetten:

1. Een aangevallen computer herkent de herkomst van TCP/IP-pakketten enkel en alleen aan het IP-adres dat in de IP-header vermeld staat; deze header kan simpelweg aangepast worden.
2. Wanneer een bericht in stukken verzonden wordt over een Internetverbinding, wordt de volgorde van de stukken bijgehouden in een teller in de TCP-header van ieder pakket. De manier waarop de teller voor ieder pakket en voor iedere boodschap wordt verhoogd, maakt dat het volgende nummer dat een computer in een pakket verwacht te ontvangen met een zekere nauwkeurigheid voorspelbaar is.

Bij een IP-spoofing-aanval maakt de aanvaller van deze twee zaken gebruik om te proberen zijn slachtoffer te laten geloven dat hij een andere (vertrouwde) computer is dan hij eigenlijk is.

54.2 Het idee

Computers in een Internetverbinding maken gebruik van het TCP/IP-protocol om berichten te versturen. Deze berichten bestaan uit data die verstuurd worden van een zender Z naar een ontvanger O.

Omdat Internet een onbetrouwbaar medium is, wordt een aantal technieken toegepast om voor de eindgebruikers van Z en O een betrouwbare communicatie te simuleren. Het bericht wordt niet ineens verzonden, maar wordt verdeeld in kleine pakketten die makkelijk opnieuw kunnen worden verzonden. Daarbij wordt ieder pakket verzonden in een “enveloppe” met administratieve informatie, zoals zender, ontvanger, afgelegde route en volgorde van het pakket binnen het bericht.

Om een langdurige verbinding aan te kunnen bieden aan de eindgebruikers, maakt het TCP/IP-protocol gebruik van meerdere lagen. De IP-laag is verantwoordelijk voor het zenden en ontvangen van pakketten. De TCP-laag is verantwoordelijk (onder meer) voor het aan elkaar knopen van pakketten tot zogeheten transmissie-sessies. Een transmissie-sessie bestaat eruit dat de TCP-lagen van Z en O onderling een aantal controle-berichten uitwisselen (“elkaar de hand schudden”) om een sessie te openen, dan wederzijds datapakketten overdragen en ten slotte controleberichten uitwisselen om de sessie af te sluiten.

Wanneer Z een sessie wil openen met O, is het aan O om te beslissen of dat mag en hoe de berichten van Z behandeld worden. Wanneer O beslist dat Z een sessie mag openen en bepaalde handelingen op O uit mag voeren, dan zeggen we dat Z vertrouwd wordt door O.

Stel nu dat een aanvaller A een sessie wil openen met O. A zou dit kunnen doen door O ervan te overtuigen dat hij eigenlijk Z is.

54.3 De aanval

Het is voor A niet zo vreselijk moeilijk om te beweren dat hij Z is: als hij het IP-adres van Z weet (en dat moet, want anders kan hij niet beweren dat hij Z is) kan hij TCP/IP-pakketten gaan versturen met het IP-adres van Z als afzender-adres (dat wordt verder nergens nagekeken of verboden).

Het probleem voor A is dat hij, om een sessie te openen met O, niet alleen moet beweren dat hij Z is maar dat hij ook handen moet schudden. Dat wil zeggen, hij moet pakketten uitwisselen. En dat laatste is minder makkelijk want A kan wel pakketten sturen naar O maar O’s

antwoorden gaan naar Z en niet naar A (want Z was zogenaamd de afzender). Dit heeft voor A twee nadelen:

1. A kan niet zien wat O doet. Hij kan dus de volgorde van de pakketten verprutsen, of iets anders doen waardoor O de verbinding weigert.
2. O ontvangt van Z (eigenlijk A) een verzoek om handen te schudden en een sessie te starten. Daarop zegt O tegen Z (de echte Z): "Dat is prima". Hierop reageert Z uiteraard met de mededeling "Ik weet niet waar je het over hebt" (in TCP-terminologie, een reset-bericht). Waarop O de verbinding verbreekt.

De eerste stap in de aanval van A moet dus zijn om op de een of andere manier Z uit de lucht te halen, zodat deze geen reset-bericht kan sturen. Hiervoor wordt vaak een Denial of Service aanval gebruikt, bijvoorbeeld middels SYN-flooding (het opsturen van zoveel SYN-berichten dat de TCP/IP-stack van Z eraan onderdoor gaat).

Daarna kan A beginnen aan een handenschud-procedure met O. Hierbij wordt A gehinderd door het feit dat O denkt dat het handenschudden door Z is begonnen en dus al zijn antwoorden naar Z stuurt. A ziet dus niet hoe O reageert op A's poging tot handen schudden.

Wat de IP-stack betreft, maakt dit niet uit. Maar de TCP-stack van O kijkt naar de volgorde van berichten en bepaalt bij welk nummer de teller van de pakketten in het bericht begint te lopen. Binnen een bericht moeten de pakketten over en weer oplopende, opvolgende nummers hebben. Maar het nummer van het eerste pakket kan in principe overal liggen in het 32-bit gebied, dus tussen 0 en 4.294.967.295.

Op dit punt maken de meeste spoofing-aanvallen gebruik van het feit dat de nummertoewijzing van TCP-stacks meestal toch niet op toeval berust maar redelijk voorspelbaar is. Als A zijn aanval begint door onder zijn eigen adres een paar pakketten te sturen naar O, dan krijgt A van O vaak een aantal reset-berichten (met een TCP cijfer). Uit een enkel bericht weet A zo'n beetje waar de teller van O is. Met meerdere berichten kan A kijken hoeveel tijd pakketten nodig hebben om de reis van A naar O en terug te maken en hoe snel de teller van O bijgewerkt wordt. Hiermee kan A vaak redelijk schatten hoe de teller van O van waarde verandert.

Met deze informatie kan A proberen om handen te schudden met O. Hierbij stuurt A een aanvraag voor een sessie naar O (en beweert daarbij Z te zijn). Dan schat A in hoelang O nodig heeft om een reactie naar Z te sturen en welk nummer die reactie zal hebben. Daarna stuurt A op zijn beurt weer de benodigde reactie (weer zogenaamd van Z), met het juiste cijfer.

Er zijn op dit moment een aantal mogelijkheden:

- Als A te laag ingeschat heeft, ontvangt O een pakket met een cijfer dat al langsgekomen is. O neemt dan aan dat het een herhaald pakket is en gooit het weg. Op dat moment faalt de aanval (maar A kan natuurlijk gokken waar het verkeerd is gegaan en nog eens proberen).
- Als A goed heeft gegokt, heeft A een sessie met O. Dan kan A proberen om O een paar commando's te sturen.
- Als A te hoog heeft gegokt, zijn er weer twee mogelijkheden:
  - A heeft te hoog gegokt maar wel in mogelijke gebied van nummers (er is een limiet aan hoever de nummers vooruit mogen lopen op het volgende, verwachte nummer). In dat geval neemt de TCP-stack aan dat er nog pakketten moeten komen en wordt het aanvallende pakket opgeslagen tot de ontbrekende pakketten aankomen. Als gevolg hiervan kan de aanval alsnog slagen en een andere communicatie falen.
  - A heeft te hoog gegokt en veel te hoog gegokt. De TCP-stack van O gooit het pakket weg. Maar de TCP-stack stuurt wel een bericht naar Z met daarin het volgende getal dat verwacht werd. Als A nu weer een reset-bericht laat genereren door O, kan A uit de "sprong" in cijfers wellicht gokken wat er verkeerd gegaan is bij zijn aanval.

54.4 Het nut

Een spoofing-aanval is meestal een voorbereiding op iets groters. Een sessie is nooit een groot geheel, vooral omdat het niet opgemerkt mag worden door de beheerder van het aangevallen systeem en omdat A door zijn blindheid te gelimiteerd is om echt grote dingen te kunnen doen. De meeste spoof-aanvallen dienen om een achterdeur in het doelsysteem in te bouwen waardoor A later makkelijk in kan loggen op het doelsysteem – bij voorkeur als beheerder. Dan kan A het doelsysteem volledig overnemen.

54.5 Tegenmaatregelen

Er zijn verscheidene tegenmaatregelen tegen de verschillende variaties op spoofing-aanvallen. De meeste verdedigingen zijn gebaseerd op pakket-filtering door firewalls. Te denken valt dan aan analyse van pakketten door het aangevallen systeem om te herkennen dat een pakket niet mogelijk kan komen van het systeem dat in het pakket beweerd wordt. Bijvoorbeeld: een pakket dat van het open internet komt, kan niet van binnen het interne netwerk komen.

Van heel andere orde is de verdediging van het systeem dat door een aanvaller nagebootst wordt. De aanvaller moet dit systeem uitschakelen. Als dit systeem gewapend is tegen de bekendere DOS-aanvallen (zoals SYN-floods), dan is dat ook een verdediging tegen spoofing.

Hoofdstuk 55

Internetbankieren

Internetbankieren en aanmelden met de Access Key.

Internetbankieren is het giraal betalen en sparen via internet en internetapplicaties. De communicatie tussen de klant en de bank gaat over het internet. Een klant kan een rekening bij een bank met de computer beheren en transacties met internet aan de bank opgeven. De klant heeft op de computer inzicht in de financiële overzichten die horen bij het rekeningnummer. Alle grote banken in Nederland en België bieden hun klanten een vorm van internetbankieren aan. Voordeel voor de bank is onder andere het niet zelf hoeven invoeren van de mutaties en de afname van het aantal afschriften dat moet worden verstuurd. Voordeel voor de klant is de mogelijkheid om 24 uur per dag de bankzaken te regelen of te bekijken. Dit betekent niet dat de transacties door de bank per direct worden gedaan.

Bij veel spaarrekeningen en spaardeposito's kan de klant het saldo inzien en storten en opnemen via internet. Als dit de enige mogelijkheid is, wordt vaak een hogere rente geboden. Verder kunnen effecten via een internetrekening worden aangehouden, gekocht en verkocht, waarbij lagere kosten in rekening worden gebracht.

Een nieuw betalingssysteem voor bijvoorbeeld facturen en acceptgiro's in Nederland is de FiNBOX. Eind 2005 is in Nederland een nieuwe, door ING Bank, ABN AMRO, Rabobank en Postbank ontwikkelde, betaalstandaard voor directe betalingen op het internet geïntroduceerd, iDEAL.

55.1 Internetbanken

Een **internetbank** is een bank die geen fysieke filialen heeft maar waarbij bankzaken uitsluitend via het internet kunnen worden afgehandeld. Een dergelijke bank heeft vaak wel een fysiek kantoor waar medewerkers werken, maar dit is niet voor klanten beschikbaar voor bankzaken. Op een dergelijke manier kan een bank veel kosten van bankfilialen uitsparen. Soms is een internetbank een apart label van een 'fysieke' bank.

55.2 Beveiliging

De toegang tot de eigen bankzaken via het internet verschilt per bank. Bij een spaarrekening waarbij geld alleen kan worden overgeboekt naar een eigen tegenrekening hoeft de beveiliging minder uitgebreid te zijn.

55.2.1 Nederland

e.dentifier, Accesskey en Random Reader van ABN AMRO, BNP Paribas Fortis en Rabobank.

- De ABN AMRO gebruikt de e.dentifier kaartlezer om veilig aan te melden.
- Bij ING moet de klant ter bevestiging van een opdracht een TAN-code invoeren, die ING op hetzelfde moment via een gratis sms verstuurt of die op een lijst met TAN-codes te vinden is.

- De SNS Bank gebruikt een Digipass om veilig aan te melden.
- De Rabobank gebruikt een Rabo Scanner. Dit apparaat vervangt vanaf 2015 geleidelijk de Random Reader.

Aanvankelijk verliep het aanmelden met de kaartlezer door met de hand een code in te voeren. Steeds vaker gaat de aanmelding via een USB-aansluiting met de computer. Zowel de e.dentifier, de digipass als de random reader werken op dezelfde manier. Door sommige banken worden kosten in rekening gebracht voor vervanging van het apparaat (bijvoorbeeld als de batterijen leeg zijn). Deze kosten kunnen oplopen tot ruim 15 euro. Bij andere banken is deze vervanging gratis.

Bij mobiel internetbankieren op een smartphone is volgens de ING het gebruik van haar app veiliger dan het op de smartphone gebruiken van de internetsite met een browser.

55.2.2 België en Duitsland

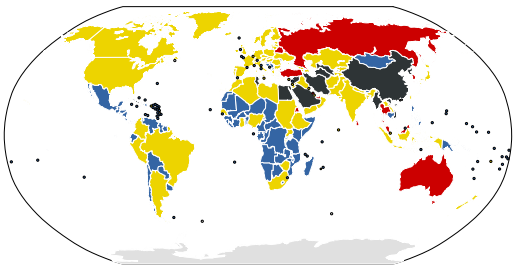
- Kaartlezers worden gebruikt door KBC, Belfius, Argenta, AXA en VDK Spaarbank
- Digipass wordt gebruikt door Crelan, Beobank, Europabank en Rabobank
- Beide gecombineerd worden gebruikt door ING, BNP Paribas Fortis, Deutsche Bank, Record Bank en Fintro

55.3 Zie ook

- Online betalen

Hoofdstuk 56

Internetcensuur



Internetcensuur wereldwijd[1][2]

Geen censuur
Beperkte censuur
Land staat onder toezicht van Verslaggevers Zonder Grenzen
Zware censuur
Het censuurniveau van Tunesië is veranderd sinds de overhead van Zine El Abidine Ben Ali ten val kwam op 14 januari 2011.

Internetcensuur is controle of onderdrukking van de toegang tot en het plaatsen van informatie op het internet. In die zin is het vergelijkbaar met offline censuur.

Internetcensuur kan worden toegepast door overheden om te voorkomen dat de bevolking toegang krijgt tot bepaalde informatie. Op internet kan informatie die in het ene land verboden is, alsnog terug worden gevonden op een website die gemaakt is in een land waar deze informatie niet verboden is. Overheden die geen controle hebben over deze websites kunnen desondanks toch proberen de site ontoegankelijk te maken, bijvoorbeeld via een zwarte lijst of een internetfilter.

56.1 Methodes

Omdat in de meeste landen (uitgezonderd Noord-Korea) de overheid geen totale controle heeft over alle computers die op het internet zijn aangesloten, is internetcensuur vaak lastig toe te passen. Datahavens als Freenet maken het mogelijk informatie online te zetten die niet kan worden verwijderd, en waarvan de plaatser niet te traceren is naar een specifieke digitale identiteit of organisatie.

De meest effectieve methode van internetcensuur, is de toegang tot internet geheel onmogelijk maken. Dit kan door alle routers af te snijden, alle hardware uit te schakelen.

Een specifiekere methode is het gebruik van internetfilters, zoals SmartFilter. Deze kunnen worden gekoppeld aan alle routers waardoor bepaalde sites niet meer toegankelijk zijn voor computers die via deze router op internet zitten. Dit soort filters worden onder andere toegepast door Saoedi-Arabië, Tunesië en Soedan. Filters kunnen filteren op IP-adressen, het Domain Name System, en URL's. Deze filters zijn echter niet altijd even waterdicht, en kunnen soms met (weinig) moeite worden omzeild.

Internetcensuur kan ook in het geheim plaatsvinden, bijvoorbeeld door de router in te stellen dat er een valse foutmelding in beeld komt indien men een specifieke website wil bezoeken, waardoor het lijkt alsof de site zelf uit de lucht ligt.

56.2 Omzeilen

Er bestaan verschillende manieren om internetcensuur door middel van filters te omzeilen. Een voorbeeld is het gebruik van proxyservers. Deze sites worden zelf vaak niet geblokkeerd door het filter, maar kunnen wel informatie van wel geblokkeerde sites weergeven.

Ook een Virtueel Particulier Netwerk kan gebruikt worden om een blokkade te omzeilen. De gebruiker kan via een VPN geblokkeerde websites bezoeken via een server in een ander land.

Psiphon is software waarmee gebande sites kunnen worden bezocht. Hiervoor moet de software eerst worden geïnstalleerd op een computer die wel vrij toegang tot de gewenste site heeft, zodat deze als proxy kan dienen voor andere computers.

56.3 Landen die internetcensuur toepassen

56.3.1 Wereldwijd

De organisatie Verslaggevers Zonder Grenzen houdt zich wereldwijd bezig met het aankaarten van internetcensuur. In 2006 begon de organisatie met het bijhouden van een lijst van zogenaamde “vijanden van het internet”.[3] Tevens bestaat er een lijst van landen die door de organisatie sterk in de gaten worden gehouden. Beide lijsten worden jaarlijks bijgewerkt.[4]

Vijanden van het internet:[2]

- Myanmar
- China
- Cuba
- Iran
- Noord-Korea
- Saoedi-Arabië
- Syrië
- Turkmenistan
- Oezbekistan
- Vietnam

Landen onder toezicht[2]

- Australië
- Bahrein
- Wit-Rusland
- Egypte
- Eritrea
- Frankrijk
- Libië
- Maleisië
- Rusland
- Zuid-Korea
- Sri Lanka
- Thailand
- Tunesië
- Turkije
- Verenigde Arabische Emiraten
- Venezuela

56.3.2 Europa

Veertien Europese landen, waaronder Nederland en België, nemen sinds 2004 deel aan het Cospol Internet Related Child Abusive Material Project (CIRCAMP) tegen kinderpornografie. Politiediensten van deze landen verzorgen een gezamenlijke zwarte lijst in samenwerking met Interpol. Domeinnamen op deze Interpol “Worst of"-List (IWOL) worden door de nationale politiediensten meegedeeld aan de Internetaanbieders, die op vrijwillige basis kunnen beslissen de toegang te ontzeggen.[5] Bezoekers worden dan omgeleid naar een stoppagina.

Deze werkwijze is later veralgemeend tot de hele Europese Unie.[6]

56.3.3 België

Belgische internetproviders kunnen van het parket het bevel krijgen om de toegang tot binnenlandse of buitenlandse websites te blokkeren. De vordering van de Procureur des Konings wordt gecommuniceerd via de Federal Computer Crime Unit of de Kansspelcommissie. Bezoekers krijgen dan de stoppagina van de Belgische overheid te zien, gehost door Fedict. Voor dit “ontoegankelijk maken van in een informaticasysteem opgeslagen gegevens” moet een dubbele voorwaarde vervuld zijn:[7]

- de gegevens vormen het voorwerp van een misdrijf of zijn eruit voortgekomen; en
- de gegevens zijn strijdig met de openbare orde of de goede zeden of leveren een gevaar op voor de integriteit van informaticasystemen.

Vooral sinds 2009 is dit ruime instrument ook in de praktijk toegepast. De getroffen websites werden onder meer verdacht van: het organiseren van kansspelen zonder vergunning, privacyschendingen door “pedojagers”, inbreuken op het auteursrecht (bv. het Belgische luik van de Amerikaanse operatie In our sites), verkoop van illegale medicijnen zoals anabole steroïden... In juni 2013 waren er in totaal 83 websites geblokkeerd.[8] In 2014 was dit opgelopen tot 127, alleen al voor de buitenlandse websites.[9] Daaronder waren ook racistische, extremistische, discriminerende en lasterlijke websites.

Via het meldpunt van e-cops kunnen burgers illegale websites aangeven en hun blokkering vragen. Als het Belgische gerecht een website viseert die onder het beheer valt van DNS Belgium of Eurid, kan het deze wereldwijd offline halen. De procedure tot vrijgave kent geen onafhankelijk toezicht en moet per fax worden ingesteld. Ze verloopt via een zogenaamd strafrechtelijk kortgeding, met verzoekschrift bij de procureur des Konings en een beroepsmogelijkheid bij de kamer van inbeschuldigingstelling.[10]

Er bestaat ook een burgerrechtelijke procedure die DNS-blocking toelaat.[11] Ze werd gebruikt tegen The Pirate

Bay, maar bleek weinig effectief. Het Hof van Beroep te Antwerpen ging bij arrest van 26 september 2011 weliswaar in op de eis van B.A.F., maar het blokkeren van elf domeinnamen bleek niet afdoende.

Volgens sommige academici is met dit alles in België sprake van een echte overheidscensuur, die de essentie van het internet als een neutraal doorgiftemechanisme aantast.[12]

56.4 Vaak getroffen websites

Websites die het vaakst worden geweerd via internetcensuur zijn:

- Pornografische sites.
- Aan pedofilie gerelateerde sites
- Sites voor het delen van media, zoals Flickr en YouTube.[13]
- Sociale netwerksites zoals Facebook en Twitter.
- Wikipedia (vrije neutrale kennis)
- Wikileaks[14]
- Politieke blogs[15]
- Nazi en soortgelijke sites — met name in Frankrijk en Duitsland.[16]
- Religieuze websites
- Filesharing en P2P-related websites
- Google – vooral in China en Cuba[17]
- Sites voor en over het omzeilen van censuur.
- Buitenlandse websites
- 4chan

56.5 Zie ook

- Netneutraliteit

56.6 Externe links

- (en) Wikia Censorship op Wikia
- (en) Internet censorship wiki op cship.org
- (en) Index on Censorship
- (en) WebCensor - Gratis censuur plugin voor webbrowsers.

Hoofdstuk 57

Internetfraude

Internetfraude is oplichting via het internet, waarbij gegevens en goederen van nietsvermoedende gebruikers afhandig gemaakt worden. Typerend hierbij is dat in een beperkte tijd en met weinig financiële middelen een groot aantal slachtoffers kan gemaakt worden. [1]

Hoewel internet een relatief nieuw fenomeen is, zijn de trucs internetvarianten van al oudere oplichtingstrucs, waarbij uiteraard de anonimiteit en verbeterde communicatiemogelijkheden van het internet de fraudeur in de kaart spelen.

Het kan gaan om valse advertenties voor producten die nooit geleverd, maar wel betaald worden. Ook zijn er fraudegevallen bekend met internetbankieren. In artikelen over phishing en pharming wordt uitgelegd hoe fraudeurs te werk gaan bij het oplichten en misleiden. Computerbeveiliging is een belangrijk aandachtspunt om internetfraude zo veel mogelijk te voorkomen.

57.1 Veelvoorkomende trucs

Internetfraude is een zeer breed begrip en kan dan ook op zeer veel manieren gepleegd worden. Hieronder volgt een kleine greep:

Pharming Een DNS-server wordt aangevallen en het internetadres van een bepaalde domeinnaam wordt gewijzigd. De nietsvermoedende surfer typt het bekende webadres in, maar komt op een nagebootste site terecht. Indien dit bijvoorbeeld de site van een bank is, dan kan een hacker vervolgens gevoelige gegevens van de gebruiker ontfutselen.

Phishing Een op pharming lijkend proces waarbij de slachtoffers met e-mail naar de nagebootste website worden gelokt. Er wordt bijvoorbeeld een mailtje gestuurd, zogenaamd afkomstig van de bank, met het verzoek gegevens te bevestigen op de website, omdat anders de bank de rekening blokkeert in verband met een 'poging tot fraude'. Uiteraard dient ook deze site om gevoelige gegevens van de gebruiker te ontfutselen, waarmee de hacker vervolgens bijvoorbeeld de bankrekening kan gaan plunderen.

Fraude met online advertenties De fraudeur plaatst een advertentie voor de verkoop van goederen en laat zich wel betalen zonder te leveren. Het kan ook andersom: de fraudeur reageert op een advertentie en laat goederen leveren zonder te betalen.

Spyware De fraudeur verspreidt spyware, programma's die computer- en surfgedrag en andere op de computer aanwezige gegevens registreren en doorsturen. Men denke ook hier aan wachtwoorden voor internetbankieren, bedrijfsinformatie, etc. De spyware wordt vaak op zo'n manier verspreid dat gebruikers dit onwetend installeren, bijvoorbeeld samen met computerspelletjes of pornografie die gebruikers downloaden.

Acquisitiefraude De fraudeur koopt een domeinnaam en maakt een website aan die advertenties of bedrijvenregisters bevatten. Vervolgens laat hij ondernemers betalen voor een vermelding op deze website, soms via ongevraagde facturen en soms door hen onder valse voorwendselen een 'offerte' te laten tekenen. De website dient hier om de schijn op te houden dat de fraudeur een bonafide onderneming runt en inderdaad advertenties plaatst of een bedrijvenregister bijhoudt. Deze websites zijn te herkennen aan het feit dat alle informatie die ze geven afkomstig is uit weblinks naar andere sites (een zoekopdracht in het bedrijvenregister leidt bijvoorbeeld automatisch naar de website van de Kamer van Koophandel, en wanneer men op de link 'aandelenkoersen' klikt wordt men automatisch doorgelinkt naar de website van de effectenbeurs).

Nep-virusscanners De fraudeur creëert een programma dat een pop-up doet verschijnen bij gebruikers met de mededeling dat hun computer besmet is met een computervirus, dat slechts met de via een bepaalde link te downloaden virusscanner bestreden kan worden. De virusscanner (waarvoor betaald moet worden) is waardeloos, schadelijk, of bevat spyware.

Ransomware De fraudeur circuleert virussen die ervoor zorgen dat de besmette computer na het opstarten slechts een scherm vertoont met de mededeling dat de computer geblokkeerd is en pas gedeblokkeerd wordt (bijvoorbeeld door verstrekking van een

code die het virus deactiveert) wanneer een bedrag wordt overgemaakt. De computer wordt zodoende door de fraudeur 'gegijzeld'. Het virus doet zich vaak voor als software van de politie. De gebruiker krijgt dan vergezeld van indrukwekkende logo's en citering van wetsartikelen de tekst in beeld dat de computer geblokkeerd is wegens het downloaden en/of verspreiden van IP-beschermde muziek of films, of van kinderporno. Omdat het echter zogenaamd de eerste keer is, kan worden volstaan met betaling van een bedrag aan de zogenaamde politie, waarna de gebruiker de code ontvangt waarmee het virus gedeactiveerd wordt. Veel gebruikers schrikken hier dusdanig van dat ze uit angst voor een slepende strafvervolging of strafblad betalen om er snel vanaf te zijn. Bovendien durven ze hierdoor niet de politie of een reparateur in te schakelen. Meestal wordt bij toegave het geld van de slachtoffers verloren en de blokkade verdwijnt niet.

Faker De fraudeur logt in op een chat- of datingsite en doet zich voor als een chatter of dater om op deze manier mensen op te lichten (romantische fraude) of gevoelige informatie van hen te verkrijgen.

Nigeriaanse oplichting Hoewel Nigeriaanse oplichting ouder is dan internet, wordt internet dankbaar gebruikt door bendes die zich hiermee bezighouden. Ze kunnen immers op deze manier makkelijker veel mensen tegelijk benaderen, wat voor hen cruciaal is vanwege het feit dat de respons laag is. Ook voor andere soorten oplichtingen gebruiken de oplichters vaak bulkmail.

Zakenkansen De fraudeur benadert mensen met een aanbieding tot het doen van thuiswerk of deelname aan een Multi Level Marketing organisatie. De slachtoffers moeten wel eerst betalen voor bijvoorbeeld cursusmateriaal of toetreding. Ook worden op een vergelijkbare wijze via chatsites onervaren jonge meisjes benaderd voor een kans om als model te werken. Ook hier wordt vooraf een bijdrage gevraagd voor bijvoorbeeld de fotoshoot of zelfs een reis naar bijvoorbeeld New York of Milaan. In alle gevallen laat de oplichter na betaling niets meer van zich horen of geeft hij een reden waarom de droombaan niet doorgaat maar het geld niet terugbetaald kan worden. Het geld was bijvoorbeeld leges voor een werkvergunning die uiteindelijk geweigerd was, 'er waren nu eenmaal geen belangstellenden' voor de betaalde fotoshoot van het meisje, of de fraudeur verzint een ander verhaal waarmee hij zich op overmacht beroept.

Koersmanipulatie De fraudeurs verspreiden via e-mail, chatboxen etc. geruchten over een bedrijf die de aandelenkoersen beïnvloeden. Vervolgens speculeren ze op de koerswijziging. Ze kunnen bijvoorbeeld geruchten verspreiden dat een onderneming voor een hoge prijs gaat worden overgenomen, waardoor de koers stijgt. Hier maken ze gebruik van door goedkoop in te kopen en duur te verkopen. Wanneer het gerucht ontzenuwd wordt daalt de koers weer en blijven de kopers met koersverliezen achter.

PayPal De fraudeur koopt iets via een website die het gebruik van PayPal toestaat, betaalt via PayPal, haalt de zaak in persoon op, maar eist vervolgens zijn geld terug onder het mom dat hij de zaak niet ontvangen heeft. PayPal honoreert deze actie wanneer er geen nummer of leveringsbewijs overhandigd kan worden, waardoor oplichters ironischerwijs het systeem kunnen misbruiken via een regel die oplichting beoogt te bestrijden.

Spoofing De oplichter manipuleert e-mail, websites of een IP-adres om zich zo als een ander voor te kunnen doen.

Klikfraude Klikfraude is het verschijnsel waarbij derden moedwillig klikken op tekstadvertenties op internet met een pay per click-model (PPC) om zodoende de adverteerder armer en zichzelf rijker te maken. Dit kan eventueel met speciale programmaatjes die de klikken automatisch genereren.

Misbruik van advertenties De oplichter plaatst een advertentie en laat zich wel betalen zonder te leveren. Andersom is ook mogelijk: de oplichter reageert op een online advertentie en laat zich beleveren zonder te betalen.

Misbruik van netwerksites De oplichter hackt of verschaft zich op andere wijze onrechtmatig toegang tot iemands account of een netwerksite als Facebook of LinkedIn. Vervolgens doet hij zich als de eigenaar van het account voor om gelinkte vrienden geld af te troggelen met allerlei voorwendselen, bijvoorbeeld dat de persoon gestrand is in een ver land en geld nodig heeft voor een vliegticket naar huis.

Misbruik van vacaturesites De oplichter gaat via een vacaturesite op zoek naar werkzoekenden met een uitnodiging om 'op gesprek' te komen. Dit soort oplichterij is te herkennen aan flitsende 'hippe' termen die echter weinig of niets over het werk zelf zeggen. Ook wordt het slachtoffer voorgehouden dat de oprichters inmiddels miljonair zijn en dat voor hem ook weggelegd is, dat hij veel mooie zakenreisjes zal maken, en dat hij een visionair kan zijn die niet afhankelijk is van de grillen van de baas. Uiteindelijk blijkt het niet om een betaalde baan maar om Multi-Level Marketing of franchising te gaan, waarbij de werkzaamheden colportagewerk betreffen. Het is zelfs mogelijk dat de site op deze wijze wordt misbruikt voor werving voor piramidespelen, of dat de werkzaamheden witwaspraktijken inhouden. Soms wordt een frauduleuze vacature aangemaakt om persoonsgegevens te kunnen verzamelen

(cv, naam, adres, foto, paspoortkopie), waarna deze worden misbruikt voor identiteitsfraude bij andere oplichtingstrucs.

Erotische contactadvertentiesites De oplichter zet een contactsite op waarop men profielen kan aanmaken. Vaak is de inschrijving zelf gratis, maar moet men betalen om daadwerkelijk contact te kunnen maken. Wie zich gratis inschrijft, merkt al snel dat hij allerlei reacties krijgt vanuit profielen met foto's mooie dames, waar hij of zij niet op kan reageren. Veel mannen schrijven zich dan als betalend lid in. De meeste profielen zijn echter computerprogramma's (bots), die automatisch verleidelijke correspondentie sturen om de slachtoffers (zo lang mogelijk) betalend lid te maken. Hiervoor worden ook wel (uitzend)krachten ingehuurd. Tot een afspraak komt het uiteraard nooit. Na verloop van tijd haakt het slachtoffer af. Uit schaamte doen de meeste slachtoffers geen aangifte. Ook is het mogelijk dat de 'mooie dame' het slachtoffer aanzet tot het sturen van een sms. Hiermee abonneert hij zich op een betaalde en dure sms-dienst.

57.2 Wetgeving

57.2.1 België

Volgens het Strafwetboek artikel 496 is oplichting in België strafbaar. Ook wanneer men opgelicht wordt met elektronische communicatiemiddelen zoals internet is het strafbaar.

57.2.2 Nederland

In Nederland is deze vorm van fraude strafbaar onder het artikel 326 van het strafwetboek. In dit artikel staat het volgende: "Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, hetzij door het aannemen van een valse naam of van een valse hoedanigheid, hetzij door listige kunstgrepen, hetzij door een samenweefsel van verdichtsels, iemand beweegt tot de afgifte van enig goed, tot het ter beschikking stellen van gegevens met geldswaarde in het handelsverkeer, tot het aangaan van een schuld of tot het tenietdoen van een inschuld, wordt, als schuldig aan oplichting, gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie." [2]

57.3 Zie ook

- Nederlands Nationaal Meldpunt Cybercriminaliteit
- man-in-the-middle-aanval
- Nigeriaanse oplichting

57.4 Externe links

- Veilig internetten
- Veilig internetbankieren
- Fraudehelpdesk

57.5 Bibliografie

- http://www.polfed-fedpol.be/crim/crim_fccu_internet00_nl.php
- http://www.wetboek-online.nl/wet/Sr/326.html

Hoofdstuk 58

Internetprovider

Een **internetprovider** of **internetaanbieder** (Engels: ***internet service provider*** of **ISP**) is een organisatie of persoon die diensten levert op of via het internet. Dit kan zowel de verbinding van een gebruiker aan het internet zijn, alsook diensten die de gebruiker via het internet kan gebruiken. De verschillende diensten die een internetprovider aanbiedt zijn hieronder uitgewerkt.

58.1 Aanbod

58.1.1 Internet access provider

Een *(Internet) Access Provider* of **IAP** is een organisatie of persoon die aan particulieren en/of bedrijven faciliteiten biedt om een vaste computer of een mobiel apparaat verbinding te laten maken met het Internet. Dit kan op verschillende manieren: bijvoorbeeld via inbellen of ADSL (beide via het telefonienetwerk), kabelinternet (via het kabeltelevisienetwerk) of via mobiel internet of wifi.

58.1.2 Internet service provider

Een *Internet Service Provider* of **ISP** is een bedrijf dat internetdiensten aan klanten aanbiedt. De meeste ISP's bieden internettelevisie en internettelefonie aan en ze leveren netwerkapparatuur voor huisnetwerken. Traditioneel bieden ISP's eigen e-mailadressen aan, de mogelijkheid een eigen site op het world wide web te maken en vaak bieden ze de mogelijkheid om gegevens via FTP toegankelijk te maken. Vaak biedt een ISP ook een nieuwsserver voor Usenet.

In de volksmond wordt vaak ISP gezegd als de *access provider* wordt bedoeld. Meestal bieden *access providers* ook allerlei diensten aan die hen tot ISP maken. Steeds vaker worden de genoemde diensten op het internet door grote bedrijven als Microsoft, Google en Yahoo! gratis aangeboden.

58.1.3 Internet hosting provider

Een *internethostingprovider* of een **IHP** is een ISP die diensten levert voor het toegankelijk maken van een internet domeinnaam en webhosting (het maken van een eigen website).

58.2 Nederland

58.2.1 Ontwikkeling

In 1991 waren de eerste particulieren met een aansluiting op internet de leden van een groepje binnen de HCC in het kader van het EUnet-project HobbyNet. In 1993 was XS4ALL samen met EuroNet Internet een van de eerste commerciële providers. Deze twee providers kregen al snel meer klanten. Aanvankelijk konden klanten verbinding maken met internet door met een modem via de telefoonlijn te bellen naar een inbelnummer van de internetprovider; eerst meestal via een interlokaal telefoonnummer, maar omdat de tarieven voor interlokale netnummers hoger waren dan tarieven voor lokale netnummers gingen de providers hun inbelpunten uitbreiden tot landelijke dekking. Voor verbinding met internet moest immers per minuut (de kosten van het telefoongesprek) betaald worden.

Vanaf 1995 maakten kabelmodems het mogelijk om het kabeltelevisienetwerk niet alleen voor radio- en televisiesignalen te gebruiken, maar ook voor internetverkeer. Daardoor konden ook de kabelmaatschappijen zich als internetproviders gaan opstellen. Daarmee was voor het eerst een internetverbinding mogelijk die niet per minuut, maar per maand betaald werd en bovendien was voor het eerst breedbandinternet mogelijk: internet via het kabeltelevisienetwerk was veel sneller dan via een inbelmodem. Twee jaar later kreeg het kabeltelevisienetwerk een concurrent: ADSL via de telefoonkabel. Door de goede kwaliteit van ADSL stapten veel ontevreden klanten van het kabeltelevisienetwerk over naar de providers die ADSL-abonnementen aanboden. De grote investeringen die nodig waren voor een breedbandnetwerk met landelijke dekking konden niet door alle providers worden opgebracht, waardoor het aantal providers door overnames

en faillissementen flink afnam.

In Nederland heeft KPN het complete telefoonnet naar alle huizen in beheer. Om te zorgen dat er toch een concurrerende markt mogelijk is moet KPN van de Autoriteit Consument en Markt (ACM) ook aan andere internetproviders de mogelijkheid aanbieden van deze kabels gebruik te maken om internet over de telefoonlijn aan te bieden. De providers mogen daarvoor in de centrales van KPN apparatuur neerzetten voor het maken van internetverbindingen over de telefoonlijnen die van daaruit naar de huizen gaan. Daarnaast biedt KPN ook zelf internettoegang aan via dochterbedrijven (met de merken XS4ALL, KPNInternet en Telfort). Omgekeerd bieden nu kabelproviders ook telefonie aan. Tiscali Wholesale (voorheen BaByXL), BBned (InterNLnet, BIT internetprovider, Alice, Pilmo en Bbeyond), Unet, Versatel, EasyNet (voorheen NovaXess) en T-Mobile Online zijn een uitzondering omdat zij een eigen infrastructuur hebben om ADSL aan te bieden, en hierbij als enige ADSL-providers dus niet afhankelijk zijn van het ADSL-product van KPN.

Op de markt voor de kabeltelevisie zijn meerdere bedrijven actief, die allemaal ook actief zijn als internetprovider. Hoewel het hier om meer spelers gaat, kan dit nog steeds als een monopolie worden gezien: elk huis heeft immers slechts een verbinding met een enkele coaxkabel, en heeft daarin geen keuze. Het internet via het kabeltelevisienetwerk is niet zo gereguleerd als ADSL.

58.2.2 Provideraansprakelijkheid

Omdat internetproviders vaak servers beheren waarop niet zijzelf, maar hun klanten informatie kunnen plaatsen, was in het verleden onduidelijk wie nu verantwoordelijk was voor onrechtmatige informatie op een bepaalde website: de beheerder van de webserver of degene die de informatie op de website beheert. Dit is kort uitgelegd het vraagstuk van de provideraansprakelijkheid.

Artikel 54a van het Nederlandse Wetboek van Strafrecht luidt:

Een tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn, wordt als zodanig niet vervolgd indien hij voldoet aan een bevel van de officier van justitie, na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris, om alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om de gegevens ontoegankelijk te maken.

Dit betekent dat een internetprovider in beginsel niet verantwoordelijk is voor de informatie die haar klanten online plaatsen, mits de provider informatie ontoegankelijk maakt wanneer de officier van justitie of de rechter-commissaris dit bevelen.

Dat klinkt redelijk, maar is in de praktijk niet zo eenvoudig: Wanneer het informatie betreft op een webserver van een provider, dan kan die provider de informatie simpelweg verwijderen. Maar wanneer het informatie betreft op een server die eigendom is van de klant, en waar de internetprovider dus alleen zorg draagt voor de internetverbinding, dan ligt dat minder eenvoudig. In zo'n geval kan de provider de informatie niet van de server verwijderen: de enige maatregel die de provider zou kunnen nemen, is de internetverbinding verbreken. Maar daarmee zou ook alle andere informatie op de betreffende server, ontoegankelijk worden.

In de Europese richtlijn inzake elektronische handel wordt daarom onderscheid gemaakt tussen het opslaan van informatie (caching en hosting) en het doorgeven van informatie, dat *mere conduit* genoemd wordt. Wanneer er sprake is van onrechtmatige informatie die verwijderd moet worden van een server van een hostingprovider, dan zal die provider aan een verzoek van de officier of rechter-commissaris gehoor moeten geven. Wanneer de informatie zich echter op een andere server bevindt, en er dus sprake is van mere conduit, dan zal de provider die informatie niet ontoegankelijk maken. In dat laatste geval kunnen bij de internetprovider wel de NAW-gegevens van de betreffende klant opgevraagd worden, zodat de eisende partij zich rechtstreeks tot de klant kan richten.

Om die procedure eenvoudiger en duidelijker te maken, heeft internetprovider XS4ALL als eerste in februari 2007 een procedure voor klachten over uitingen op internet[1] gepubliceerd. In navolging daarvan heeft een groot aantal Nederlandse providers, samenwerkend in het programma *Samen tegen Cybercrime*, op 2 oktober 2008 een Gedragscode Notice-and-Take-Down[2] gepubliceerd, waarin beschreven staat hoe geklaagd kan worden over uitingen op internet en hoe met klachten wordt omgegaan.

58.3 Externe links

- Vereniging ISPConnect Nederland, Nederlandse branche- en belangenvereniging voor ISP's
- Internet Service Providers Association, Belgische belangenorganisatie

Hoofdstuk 59

IP-adres

Een **IP-adres**, waarin IP staat voor Internet Protocol, is een adres waarmee een NIC (*network interface card* of *controller*), of in het Nederlands 'netwerkkaart', van een host in een netwerk eenduidig geadresseerd kan worden binnen het TCP/IP-model, de standaard van “het” internet.

Elke computer die is aangesloten op het internet of netwerk heeft een nummer waarmee deze zichtbaar is voor alle andere computers op het internet. Men kan dit vergelijken met telefoonnummers. Om het mogelijk te maken dat computers elkaar kunnen vinden en identificeren, hebben deze hun eigen nummer nodig. Deze nummers zijn de IP-adressen. Een IP-adres op internet is meestal gekoppeld aan een bedrijf of instantie. Zo is het te achterhalen waar bewerkingen onder een IP-adres vandaan komen. Bij mensen die vanuit huis werken identificeert het IP-adres hun internetprovider. Bijdragen op het internet zijn hierdoor bijna nooit werkelijk anoniem. De persoon achter een IP-adres is in de meeste gevallen te achterhalen, soms direct, maar soms alleen met medewerking van justitie. Deze vraagt vervolgens bij de betreffende provider op wie dat adres op dat moment gebruikte.

59.1 Adresruimte

Tot nu toe gebruikt men voornamelijk IP-adressen die bestaan uit 32 bits, het zogenaamde Internet Protocol versie 4-systeem (IPv4). In de praktijk blijkt dit systeem echter te weinig bruikbare adressen op te leveren. Daarom heeft men Internet Protocol versie 6 (IPv6) ontwikkeld, met IP-adressen bestaande uit 128 bits.

59.2 IPv4

In IPv4 is een IP-adres een reeks van 32 bits. De adresruimte van IPv4 bevat daarom maximaal 2^{32} = 4.294.967.296 IP-adressen. Dat is minder dan er mensen op aarde zijn. In werkelijkheid is het beschikbare aantal adressen minder, want in de praktijk worden bepaalde adressen als broadcastadres of netwerkadres gebruikt en is een deel van de adresruimte als privé-adresruimte voor bijvoorbeeld testdoeleinden gereserveerd, zoals beschreven staat in RFC 1918. Dit deel wordt niet over het internet gerouteerd. Verder zijn hele reeksen IP-adressen toegekend aan bedrijven en providers, bijvoorbeeld een reeks van 65.536 adressen, terwijl dat bedrijf niet zo veel adressen nodig heeft.

Het is gebruikelijk een IP-adres uit IPv4 op te delen in vier groepen van 8 bits en deze weer te geven in de vorm van door punten gescheiden decimale getallen, bijvoorbeeld 192.0.2.197. Dit is korter dan de 32 bits en eenvoudiger te lezen. Elk van de vier getallen ligt tussen 0 en 255 (2^8 - 1), 0 en 255 beide inbegrepen. Voor de mens zijn zulke combinaties van vier getallen echter ook nog moeilijk te onthouden. Daarom wordt het DNS gebruikt om IP-adressen in leesbare en makkelijker te onthouden namen zoals *nl.wikipedia.org* om te zetten en vice versa.

In principe bestaat een IP-adres in IPv4 uit een netwerkgedeelte, gevolgd door een hostgedeelte. Het netwerkgedeelte geeft aan welk netwerk bedoeld is en het hostgedeelte geeft de host (bv. een pc of een router) aan binnen het netwerk.

De reeks van IP-adressen binnen een subnet wordt meestal als volgt weergegeven. In een adres dat decimaal wordt aangegeven met G.H.K.L/M, waarbij G-M gehele getallen zijn, geeft het getal M aan hoeveel bits van het adres voor het netwerkgedeelte zijn (M ligt dus tussen 0 en 32); de rest van de 32 bits is voor het hostgedeelte.

Bij bijvoorbeeld 192.0.2.197/32 zijn alle bits voor het netwerkgedeelte en is er sprake van een enkele host. Indien een subnet 192.0.2.0/24 als allocatie heeft, zijn de eerste 24 bits uit het adres, dus de eerste drie door punten gescheiden decimale getallen, voor het netwerkgedeelte, en de laatste 8 bits voor de hosts binnen het subnet. Hierdoor zijn er in dit voorbeeld 2^8=256 adressen voor adressering van individuele hosts. (N.B.: het eerste adres, 192.0.2.0, en het laatste, 192.0.2.255, vallen normaal gesproken af omdat ze dan het (sub-)netwerkadres resp. het broadcastadres zijn.)

59.2.1 NAT

Onder andere om de schaarste aan adresruimte binnen IPv4 tegemoet te komen, is network address translation (NAT), ook wel IP-masquerading genoemd, ontwik-

keld. Hiermee kunnen de hosts van een intranet met IP-adressen uit de privé-adresruimte van RFC 1918 worden geadresseerd, terwijl de NAT-router dit naar buiten toe presenteert als één enkel IP-adres van de routeerbare adresruimte, dus slechts één IP-adres hoeft werkelijk gerouteerd en toegekend te worden, terwijl honderden hosts hier gebruik van kunnen maken. Men kan dit vergelijken met het systeem van een interne telefooncentrale. Er is slechts één buitenlijn (één IP-adres) maar vele gebruikers die via die telefooncentrale verbonden zijn met de buitenwereld. Voor alle andere gebruikers op het internet is er maar één IP-adres zichtbaar. Een groot nadeel van NAT is dat standaard alleen uitgaande verbindingen mogelijk zijn. Het mogelijk maken van binnenkomende verbindingen vergt specifieke oplossingen die niet altijd even goed werken.

59.2.2 Speciale adressen

Speciale IP-adressen binnen IPv4 zijn onder meer:[1]

0.0.0.0 "Deze host op dit netwerk", mag standaard niet verzonden worden, behalve als bronadres in een procedure waarbij een host het eigen IP-adres leert.[2]

127.0.0.1 Het meest gebruikte adres voor localhost, maar andere adressen binnen 127.0.0.0/8 kunnen er ook voor gebruikt worden.

10.0.0.0/8, 172.16.0.0/12 en 192.168.0.0/16 De volgens RFC 1918 voor privé-netwerken gereserveerde reeksen van IP-adressen.

192.0.2.0/24, 198.51.100.0/24 en 203.0.113.0/24 Deze blokken zijn volgens RFC 5737 gereserveerd voor gebruik in documentatie.

59.3 IPv6

Een structurele oplossing voor de schaarste in adresruimte van IPv4 is te vinden in de opvolger hiervan: IPv6. In IPv6 zijn er 128 bits beschikbaar voor een IP-adres, en is de theoretische bovengrens dus 2^{128} ~ 3,4×10^{38} IP-adressen. Net als bij IPv4 geldt dat in de praktijk weer adressen gebruikt worden als netwerkadres en broadcastadres, maar evengoed is het aantal toe te kennen IP-adressen hiermee enorm groot: triljarden adressen per persoon.

59.4 Soorten adressen

Soorten IP-adressen waartussen men wel onderscheid maakt:

- Dynamisch IP-adres versus statisch IP-adres. Als een NIC een statisch IP-adres heeft, blijft dit adres telkens hetzelfde; als het een dynamisch IP-adres is, wordt het dynamisch toegewezen, bijvoorbeeld met het DHCP-protocol, en kan het in de loop van de tijd veranderen. Dynamische IP-adressen worden vaak voor inbelaccounts (dialups) en mobiele internetverbindingen gebruikt.
- Privé-IP-adres versus routeerbaar IP-adres. Een privé-IP-adres is een adres uit de in RFC 1918 beschreven adresruimte.
- IP-adres volgens IPv4 versus IP-adres volgens IPv6.

59.5 IP-blokkering

Omdat IP-adressen door internetapplicaties makkelijk te raadplegen zijn (meestal wordt hier de "REMOTE_ADDR"-variabele voor gebruikt), zijn veel internetapplicaties ook in staat een IP-adres te blokkeren van de website of om permissies in te trekken voor dat IP-adres. Dit kan bijvoorbeeld gebeuren bij het spelen van een internetgame, waarbij de gebruiker valsspeelt.

59.6 Privacy

Een IP-adres is op zichzelf geen persoonsgegeven, maar kan dat wel worden, in combinatie met andere gegevens.[3] In dat geval is de Databeschermingsrichtlijn inzake privacy van toepassing.

59.7 Zie ook

- TCP- en UDP-poorten
- Whois
- Zeroconf

Hoofdstuk 60

IRC-bot

Een **IRC-bot** is een bot die gebruikt wordt voor automatische taken op een Internet Relay Chat-*channel*, voor administratieve taken (buitenhouden van spammers, grof taalgebruik, kanaalbeheerders handhaven), statistieken (meest actieve personen, etc), het doorgeven van nieuws of het organiseren van spelletjes (vaak in de vorm van Trivia, zie Triviaal) of het delen van bestanden (Xdcc). Ook bestaan er bots die gebruikt worden om de controle over de computer over te nemen, deze bots worden vaak gebruikt door hackers.

Dergelijke bots worden vaak geschreven in de mIRC-script scripttaal, omdat deze taal zich volledig richt op IRC. Ook de op de Tcl-scripttaal gebaseerde Eggdrop wordt vaak ingezet. Dit is echter geen vereiste, een IRC bot kan in vrijwel iedere programmeertaal worden geschreven. Omdat het IRC protocol open is, is het voor iedereen mogelijk een IRC bot te maken.

60.1 IRCBot (kwaadaardig)

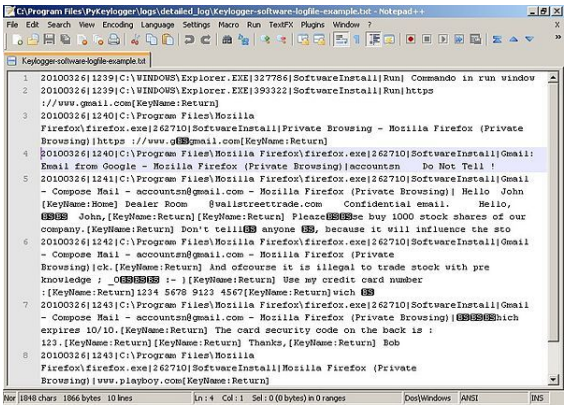
De term **IRCBot** wordt ook gebruikt voor kwaadaardige programma's. Deze bots geven een persoon, meestal een hacker via IRC toegang tot de computer waar de bot op is geïnstalleerd. Dit installeren gebeurt meestal zonder medeweten van de eigenaar van de computer. Deze IRC bots worden vaak, net als Trojaanse paarden, gebruikt om (persoonlijke) informatie van de computer te stelen, andere programmatuur te installeren, servers aan te vallen (DDoS) en spam te verzenden. Deze bots worden over het algemeen bewust door een persoon aangestuurd en zullen uit zichzelf geen actie ondernemen.

60.2 Externe links

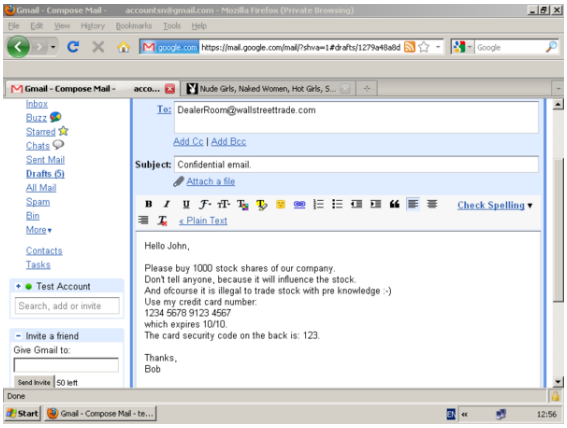
- (en) mIRC
- (en) mIRC scripts
- (en) Hawkee mIRC scripts

Hoofdstuk 61

Keylogger

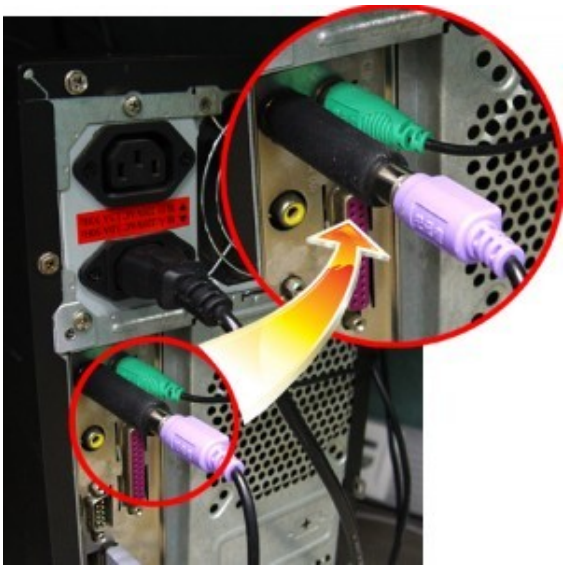


Een logfile van een software-keylogger



Een screen capture van een software-keylogger

Een hardware-keylogger (PS/2)



Een aangesloten hardwarematige keylogger

Een **keylogger** is een programma of een stuk hardware waarmee men de toetsaanslagen tot zelfs de muisbewegingen van een computergebruiker kan registreren.

61.1 Redenen voor het gebruik van keyloggers

Deze informatie kan worden gebruikt voor verscheidene doeleinden. Meestal probeert men door middel van keyloggers persoonlijke informatie te stelen. Hierbij gaat het vaak om wachtwoorden en gebruikersnamen of creditcardnummers. Ook belangrijke en vertrouwelijke e-mails kunnen onderschept worden. Tegenwoordig worden keyloggers ook ingezet op de werkvloer. Op deze manier kunnen werkgevers hun werknemers controleren. Een keylogger kan er bijvoorbeeld voor zorgen dat er een lijst van alle bezochte websites wordt blootgelegd. Zo kan de werkgever nagaan of zijn werknemers wel degelijk aan het werk zijn.

Een keylogger kan ook dienstdoen als back-up, namelijk als het computersysteem crasht. Deze functie van keylog-

gers is dan weer interessant voor grotere bedrijven waarbij crashes ernstige gevolgen kunnen hebben. Keyloggers kunnen reeds worden ondergebracht onder de noemer van spyware.

61.2 De werking van een keylogger

Het programma draait op de achtergrond waardoor de nietsvermoedende gebruiker geen last ondervindt of er ook maar iets van opmerkt. Een keylogger slaat zijn informatie op in een *logfile*. Deze kan via het internet bezorgd worden aan de opdrachtgever, bijvoorbeeld via e-mail. Je kunt het programma van een keylogger beveiligen door middel van een wachtwoord. Hierdoor kan enkel de opdrachtgever het programma gebruiken. Een keylogger kan aan een tijdschema worden onderworpen zodat de taken enkel uitgevoerd worden tijdens de uren dat de gebruiker meestal actief is. Naast de belangrijkste functies zijn keyloggers ook in staat om klembordtekst te loggen. Uitgebreidere keyloggersoftware kan ook regelmatig screen captures maken, waardoor gelogd wordt wat er op dat moment op het scherm te zien was.

61.3 Beveiligen tegen keyloggers

Software voor keyloggers staat niet standaard op een computer, maar wordt veelal geïnstalleerd door de hacker zelf, weliswaar via een omweg. Keyloggers kunnen doorgegeven worden via het installeren van software of via virussen en wormen. Vaak gebeurt dit zonder dat de gebruiker zich van kwaad opzet bewust is. Daarom is het voor gebruikers belangrijk de computer goed te beveiligen. Hier zijn enkele suggesties:

- Maak gebruik van de firewall. Keyloggers verspreiden hun informatie via het internet. Een firewall kan onbekende programma's die contact zoeken met het internet opmerken, om dan de gebruiker te waarschuwen.
- Installeer antivirussoftware en een programma dat spyware tegengaat. Deze zijn in staat om de aanwezigheid van keyloggers op te sporen. Eenmaal ze de aanwezigheid van keyloggers ontdekt hebben, kunnen ze ook gebruikt worden om deze keyloggers te verwijderen van de computer.
- Tegenwoordig bestaat er specifieke software om keyloggers op te sporen. *Dewasoft* bracht eerder al twee tools op de markt die deze taak op zich nemen.
- Voorzichtig zijn bij het installeren van software die nieuw voor je is. Het kan zijn dat bij deze software een virus zit of bij de installatie ervan ook een keylogger wordt geïnstalleerd.
- Het is zeer belangrijk om je browser up-to-date te houden. Deze updates kunnen hun inbreng hebben in het veiliger surfen.

61.4 Hardware-keylogger

Keyloggers bestaan niet alleen in de vorm van software, maar ze kunnen ook als hardware voorkomen. Het is een hulpstukje tussen de computer en de kabel van het toetsenbord. Deze keyloggers hoeven niet geïnstalleerd te worden via software en kunnen zelf ook niet opgemerkt worden door scanners. Ze hebben echter het nadeel dat ze waarneembaar zijn langs de buitenkant van de computer, maar voor mensen die weinig kennis van computers en hardware hebben is het zeer moeilijk om een keylogger op te merken.

61.4.1 Formaten

Een hardware-keylogger beschikt over een flashgeheugen. Dit kan variëren van 2MB tot 2GB. Een keylogger met een geheugencapaciteit van 2MB stemt ongeveer overeen met 1.000.000 toetsaanslagen. Keyloggers zijn verkrijgbaar in verschillende formaten:

- USB-aansluiting
- PS/2-aansluiting
- Men kan ze ook via een chip installeren in het toetsenbord zelf.

61.4.2 Extra functies en varianten

Keyloggers kennen heel wat varianten. Zo zijn er keyloggers met of zonder extra software. Deze software kan helpen om de instellingen te wijzigen naar de voorkeur van de gebruiker. Andere extra opties zijn bijvoorbeeld de timerfunctie en wifi. Door de timerfunctie kan de keylogger bijhouden op welke datum en welk uur de gebruiker iets getypt heeft. Wifi-keyloggers zijn heel wat duurder omdat zij hun informatie rechtstreeks kunnen doorsturen via het internet naar de opdrachtgever.

61.4.3 Draadloze keylogger

Naast hardware-keyloggers bestaan sinds kort ook draadloze keyloggers. Het geheel bestaat uit een kabel van het toetsenbord naar de computer van de gebruiker, de zender, en een ontvanger. In de zender zit een ingebouwde draadloze verbinding met de ontvanger. De opdrachtgever beschikt zelf over die ontvanger. Zo kan de zender alle verwerkte informatie doorsturen naar de ontvanger.

Het grote voordeel is dat als de zender eenmaal geïnstalleerd is, de opdrachtgever zich niet meer hoeft te vertonen

aan de computer van de gebruiker. Uiteraard werkt een draadloze verbinding maar vanaf een bepaalde afstand. De maximale afstand kan ongeveer 50 meter bedragen.

Met computers die iemand niet zelf beheert moet voorzichtig worden omgegaan. Een computer in een internetcafé zou bijvoorbeeld door een (vorige) gebruiker besmet kunnen zijn met een keylogger. Het kan dan nog steeds zo zijn dat er een antivirusprogramma actief is, maar dat alle meldingen met betrekking tot de keylogger handmatig uitgezet zijn.

61.5 Toekomst van de keylogger

Keyloggers zijn legaal verkrijgbaar en worden dus gebruikt voor verschillende doeleinden. Bijvoorbeeld door ouders om hun kinderen te controleren terwijl ze surfen op het net. Buiten de voordelen die keyloggers bieden, moet men toch nadenken over de gevolgen die ze met zich mee kunnen brengen. Aangezien keyloggers legaal zijn, zou het kunnen dat over enkele jaren een keylogger standaard wordt ingebouwd in een toetsenbord.

61.6 Zie ook

- Antikeylogger
- Spyware
- Trojaans paard
- Waarschuwingsdienst.nl

61.7 Referenties

- Oliver-Christopher Rochford, *Hacken voor dummies*, Pearson Education Benelux.
- Hoe verdedigen tegen keyloggers, mget.nl
- Keyloggers houden uw toetsaanslagen in de gaten, waarschuwingsdienst.nl

Hoofdstuk 62

Klikfraude

Onder klikfraude valt onder andere het moedwillig klikken op 'Gesponsorde Koppelingen' naast de zoekresultaten van Google.

Klikfraude is het verschijnsel waarbij derden moedwillig klikken op tekstadvertenties op internet met een pay-per-clickmodel (PPC) om de adverteerder armer en zichzelf rijker te maken. De term wordt met name in verband gebracht met Googles Adsense/Adwords-systeem.

62.1 Pay-per-click

Het pay-per-clickmodel is voor het eerst toegepast in 1997 door de website goto.com (nu overture.com). Het is een methode van adverteren waarbij webmasters ruimte bieden op hun websites voor (relevante) tekstadvertenties met klikbare links. De webmasters ontvangen een vergoeding voor elke keer dat bezoekers op een van deze advertenties klikken. Dit is een van de aspecten van dit systeem waardoor het gevoelig is voor fraude. De Engelse benaming voor deze klikfraude is overigens *bluffclicking*. Deze naam is voor het eerst gebruikt in de correspondentie met Google op 30 mei 2007 door een benadeelde site-eigenaar.

Bluffclicking: het doelloos klikken op AdSense-advertenties door verveelde en ook anonieme sitebezoekers. Door dit doelloos klikken kan de sitebezoeker ervoor zorgen dat de eigenaar van de site zijn reeds verworven tegoed kwijtraakt.

62.2 De praktijk

Klikfraude kan bijvoorbeeld simpelweg geschieden door zelf op een eigen website de advertenties te plaatsen en vervolgens links aan te klikken om hiermee inkomsten te genereren. Veelal is hierdoor slechts sprake van een beperkte winst en zal de fraude niet worden opgemerkt. Maar ook fraude op een veel grotere schaal komt voor. Hierbij kan worden gebruikgemaakt van scripts (kleine computerprogrammaatjes) om een menselijk klikgedrag te simuleren. Indien deze manier van frauderen wordt gedaan vanaf een enkele of een beperkt aantal computers (of IP-adressen) binnen een bepaalde regio, zal dit erg verdacht overkomen en is de kans dus groot dat men betrapt wordt.

Er is sprake van georganiseerde misdaad wanneer men een grote groep computers, verspreid over een groot geografisch gebied, inzet om de fraude te plegen. Dit kan zelfs met behulp van computers van onschuldige en onwetende gebruikers, waarop een trojaan is geïnstalleerd. Deze 'zombiecomputers' worden op deze wijze ingezet om eens in de zoveel tijd het klikken op een advertentie te simuleren om de inkomsten te genereren voor degene die de advertenties heeft geplaatst.

Ook een bedrijf als Google zelf vaart wel bij klikfraude, want zij steken (onbedoeld) ook hun aandeel van de advertentieopbrengsten in hun zak. Er zijn schattingen dat 14 tot 25 procent van alle klikken op online advertenties frauduleus zijn. Google zelf beweert echter dat deze cijfers sterk overdreven zijn en gebaseerd op foutief onderzoek. Zelf geeft Google echter de 'ware' cijfers niet prijs aan het publiek.

62.3 Externe links

- "Google wil niet reageren op bluffclicking" planet.nl 6 juni 2007
- "Klikfraude bedreigt zonnige toekomst online adverteren" - MKB.net 2 december 2006
- "Rapport bevestigt strijd Google tegen Klikfraude" - Tweakers.net, 22 juli 2006

- (en) Google Will Eat Itself

Hoofdstuk 63

Linux

Linux is een open-source-, Unix-achtig besturingssysteem gebaseerd op de Linuxkernel. De verschillende Linuxvarianten worden Linuxdistributies genoemd en zijn meestal gratis verkrijgbaar. De Linuxkernel wordt verspreid onder de GNU General Public License (GPL). Omdat Linuxdistributies in de regel gebruikmaken van het GNU-besturingssysteem, de standaard-C-bibliotheek en voldoen aan de POSIX-standaard, wordt het geheel ook wel **GNU/Linux** genoemd.

63.1 Geschiedenis

63.1.1 Unix

Het besturingssysteem Unix werd in 1969 door Ken Thompson, Dennis Ritchie, Douglas Mcllroy en Joe Ossanna van AT&T Bell Laboratories ontwikkeld. Unix werd voor het eerst uitgegeven in 1971, het was toen volledig geschreven in een assembleertaal, een normaal gebruik in die tijd. In 1973 werd Unix – toen heel vooruitstrevend – door Dennis Ritchie volledig herschreven in de programmeertaal C (met uitzonderingen voor de kernel en I/O). De beschikbaarheid van een besturingssysteem geschreven in een hogere programmeertaal zorgde voor een gemakkelijker overgang naar verschillende computerplatforms.

Door een juridisch probleem waardoor AT&T de broncode moest openstellen voor iedereen die het vroeg, groeide Unix vlug en werd het gebruikt door academische instituten en zaken. In 1984 scheidden de wegen van AT&T en Bell Laboratories. Vrij van de juridische problemen die ervoor zorgden dat de licentie voor iedereen vrij te verkrijgen was, begon Bell met het verkopen van Unix als een niet-vrij product.

63.1.2 GNU

In 1984 nam de Amerikaan Richard M. Stallman het initiatief tot het GNU-project, dat de ontwikkeling behelsde van een compleet, op Unix gelijkend besturingssysteem. Met een groep vrijwilligers, uitmondend in de Free Software Foundation, ging Stallman aan de slag.

Na enkele jaren waren er veel goede en vrije hulp-, ontwikkelings- en toepassingsprogramma's beschikbaar onder de GNU-vlag. Deze onderdelen van het GNU-project, zoals de macro-verwerker m4, de compiler gcc (voor C en andere programmeertalen) en de teksteditor emacs, werden al snel populair op andere Unix-achtige systemen. Maar de kernel van het nieuwe systeem (die inmiddels bekendstaat als De Hurd) was veel moeilijker te ontwerpen dan verwacht en ontbrak nog.

63.1.3 Linux

Linus Torvalds, Fins informaticus, begon met de ontwikkeling van Linux

In 1991 wilde de Fin Linus Torvalds, die op de universi-

teit kennis had gemaakt met Unix, ook een soortgelijk besturingssysteem hebben om thuis te gebruiken. Omdat commerciële pakketten te duur waren, was hij genoodzaakt Minix te gebruiken. Al snel voldeed dit besturingssysteem niet meer en besloot hij zijn eigen besturingssysteem te maken. Zijn eerste versie was niet echt een bruikbaar besturingssysteem, maar meer een speeltje voor hackers en programmeurs. Al snel werden er andere ontwikkelaars aangetrokken tot Linus' project en zo groeide Linux al snel uit tot een volledig productief besturingssysteem.

Linux is in feite geen volledig besturingssysteem, maar omvat alleen de kernel. De kernel zorgt er onder andere voor dat software en hardware kunnen samenwerken. Torvalds heeft alleen de kernel gemaakt en heeft als software bestaande GNU-software gebruikt. De kernel werd aangepast zodat de GNU-software hierop kon werken. Daarom wordt het besturingssysteem ook wel GNU/Linux genoemd. In de loop der jaren is er echter steeds meer niet-GNU-software bij gekomen (zoals software onder de BSD-licentie) en is volgens sommigen de naam GNU/Linux dan ook minder van toepassing. Essentiële onderdelen als glibc, fileutils en gcc zijn echter nog steeds GNU. Het volledige systeem wordt meestal kortweg Linux genoemd. Bovendien zijn er systemen (zoals vele embedded systemen) waar boven op de Linuxkernel geen GNU-tools gebruikt worden, waardoor de naam GNU/Linux dan helemaal niet van toepassing is.

In 1992 en 1993 groeide Linux uit tot een volledig functionele kernel en kreeg het ook steeds meer aandacht. Verschillende bedrijven begonnen eigen distributies te ontwikkelen. In 1994 kwamen de eerste nummers uit van het tijdschrift Linux Journal.

Sinds versie 1.0 van de Linuxkernel in 1994 is uitgekomen, is de kernel sterk verbeterd en stabieler geworden. Linux wordt inmiddels door veel bedrijven verkozen boven andere besturingssystemen en dit vooral in de servermarkt.[1] Ook voor embedded toepassingen zoals in mobiele telefoons is Linux populair en verder draaien 92% van de 500 snelste computers ter wereld op Linux. De grootste Linuxgebruiker is Google, met meer dan 100.000 servers.

63.2 Basisonderdelen

Er is een verschil tussen het besturingssysteem en de kernel. De basisonderdelen van een Linuxsysteem, zoals basistoepassingen, bibliotheken, compilers en hulpprogramma's, houden zich aan de POSIX-standaarden. Vaak zijn dit GNU-implementaties, maar ook alternatieven zoals Busybox en µClibc zijn mogelijk. Van de kernel bestaan vele versies, die volgens een bepaald systeem genummerd worden. Meer informatie daarover staat onder Linuxkernel.

Daarnaast heeft Linux op desktop-pc's tegenwoordig meestal een grafische gebruikersomgeving, draaiend onder het X Window System. Er zijn verscheidene van deze met elkaar concurrerende grafische omgevingen, waarvan de populairste GNOME (van het GNU-project) en KDE zijn; veel distributies bevatten beide. Onlangs zijn deze omgevingen voorzichtig toenadering tot elkaar gaan zoeken en wordt de samenwerking tussen de onder deze omgevingen draaiende programma's langzaam verbeterd.

63.3 Distributies

Om Linux te kunnen installeren op een thuiscomputer of server, kan men gebruikmaken van zogenaamde distributies. Zo'n distributie bestaat uit een verzameling basistoepassingen, bibliotheken en een Linuxkernel, vergezeld van een set installatieprogramma's, het X Window System en meestal een hoop extra programmatuur. Zulke *distro's* zijn vaak toegespitst op een bepaald toepassingsdoel. Bij sommige commerciële distributies, zoals bij Red Hat Enterprise Linux en Ubuntu, is er ondersteuning tegen betaling beschikbaar. De distributie is daarentegen meestal gratis: gebruikers kunnen optioneel helpdeskondersteuning en handleidingen aanschaffen.

63.4 Gebruikersgroepen

Sommige Linuxgebruikers verenigen zich in GUG's, GLUG's en LUG's, respectievelijk GNU Users Group, GNU/Linux Users Group en Linux Users Group.

63.5 Toepassing

Linux werd historisch gezien voornamelijk gebruikt als serversysteem voor bedrijven. Op desktopgebied heeft Linux nog geen sterke positie weten te veroveren: in 2012 had Linux een marktaandeel van 1,18% volgens NetMarketShare.[2][3] Een belangrijke reden hiervoor is dat de meeste computers met een vooraf geïnstalleerde versie van het Windowsbesturingssysteem verkocht worden. Hierdoor is Windows het vertrouwde besturingssysteem voor de meeste eindgebruikers. Het reeds aanwezige besturingssysteem waarvoor men betaalde bij aankoop zelf vervangen of laten vervangen door een Linuxdistributie die afwijkt van de vertrouwde gebruikerservaring is een stap die slechts weinig eindgebruikers zetten. Een mogelijke reden hiervan was dat Linux niet makkelijk geconfigureerd kan worden bij gebruik van minder gangbare hardwareonderdelen. Inmiddels is dit ook sterk verbeterd.

Op servergebied heeft Linux een uitstekende positie: het marktaandeel is aanzienlijk en vooral voor websites is Linux marktleider.[4] Het Linuxmarktaandeel is echter niet eenvoudig af te leiden vanuit de verkoopcijfers van ser-

verhardware, omdat in de regel Windows geïnstalleerd wordt.[5]

De installatie en verwijdering van software wordt in de meeste distributies afgehandeld door speciaal voor dit doeleinde ontwikkelde software: de pakketbeheersoftware. Dit stelt een gebruiker in staat om een keuze te maken uit duizenden pakketten die specifiek voor de betreffende distributie geconfigureerd zijn.

Linux wordt veel gebruikt in combinatie met Apache, MySQL en PHP, en Perl of Python. Deze combinatie van software wordt LAMP genoemd en is de basis van veel internetservers door de eenvoudige verkrijgbaarheid en open structuur.

Omwille van de lage kosten, hoge configureerbaarheid en beschikbaarheid op diverse platformen, wordt Linux ook meer en meer gebruikt op embedded systemen; men spreekt dan van embedded Linux. Mogelijke toepassingen zijn te vinden binnen settopboxen voor televisie, mobiele telefoons, routenavigatiesystemen en handheld computers zoals pda's. Linux wordt zo een concurrent van Symbian OS voor mobiele telefoons, en een alternatief voor Windows Mobile en PalmOS op handheld devices. Ook Googles besturingssysteem Android (voor mobiele telefoons en tablets) is op Linux gebaseerd.

Ook op supercomputers wordt Linux steeds populairder. Op de TOP500-lijst van supercomputers van juni 2012 draaide 90% van de snelste computers op Linux.[6]

63.6 Vakbladen

Bijna elk land kent wel zijn eigen *Linux Magazine*. Het Nederlandse blad *Linux Magazine* wordt uitgegeven door Reshift Digital.

63.7 Zie ook

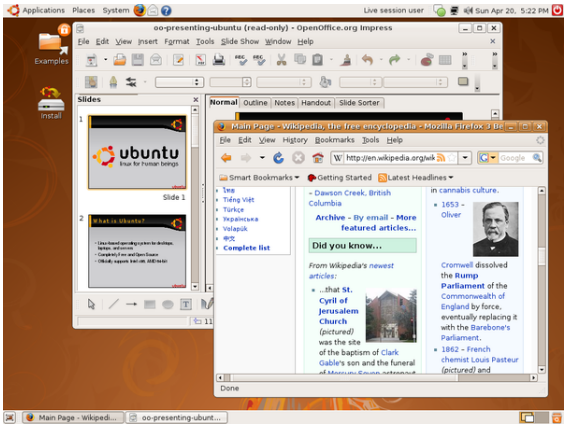
- Linux Professional Institute, een stichting die onafhankelijke certificeringen voor Linuxgerelateerde vaardigheden toekent
- Linux van A tot Z, voor een alfabetische lijst van gerelateerde artikelen
- Linuxbestandssysteem, voor de structuur van het bestandssysteem in Linux
- Linuxkernel, de belangrijkste component van elke Linuxdistributie
- Live-cd, een cd met een besturingssysteem erop, vaak toegepast bij Linuxdistributies
- Open source, de ideologie achter opensourcesoftware
- POSIX, vastgelegde standaarden die Linux probeert te volgen
- SELinux, een extra beveiligingslaag voor Linux
- Lijst van Linuxdistributies, voor een overzicht van verschillende besturingssystemen gebaseerd op de Linuxkernel

63.8 Externe links

- (en) The Linux Documentation Project, een website met veel (voornamelijk Engelstalige) documentatie over Linux
- (en) DistroWatch, een verzamelwebsite waarop veel Linuxdistributies terug te vinden zijn

Hoofdstuk 64

Live-cd



Ubuntu als Live-cd

Een **live-cd** is een besturingssysteem opgeslagen op een zelfstartende cd-rom. Het besturingssysteem kan worden gebruikt zonder installatie op een harde schijf. Na uitname van de cd-rom kan de computer weer normaal starten met het op de harde schijf aanwezige besturingssysteem. Naast live-cd's komen er steeds meer **live-dvd's** en andere *live-systems*. Daar past meestal meer op, voor het overige is de werking hetzelfde.

64.1 Toepassingen

Een live-cd heeft de volgende toepassingen:

- De meest gebruikte toepassing is om kennis te maken met een ander besturingssysteem, zonder dat het eerst geïnstalleerd hoeft te worden.
- Een live-cd kan gebruikt worden ter controle van de computer. Doordat er niets op de harde schijf wordt geschreven, kunnen veilig de gegevens op de computer bekeken worden.
- Wanneer een computer vanwege technische of softwaregebreken niet meer goed van de harde schijf start (of zelfs helemaal niet meer wil starten), biedt de live-cd vaak uitkomst op twee manieren:
    - Enerzijds kan men gewoon verder werken (onafhankelijk van de harde schijf);
    - Anderzijds kan men softwareproblemen op de harde schijf oplossen of belangrijke bestanden vanaf de harde schijf op bijvoorbeeld een USB-stick veiligstellen. De live-cd als probleemoplosser wordt ook wel "rescue cd" genoemd.
- Een live-cd kan gebruikt worden als reclamemateriaal, om bijvoorbeeld een presentatie te laten zien.
- Bij gebruik van computers die door meerdere personen worden gebruikt, kan men een live-cd gebruiken om altijd dezelfde systeeminstellingen te houden.

64.2 Gebruik

Een live-cd start iedere keer op dezelfde manier. Het starten duurt wat langer, omdat alle aanwezige hardware afgezocht en ingesteld moet worden. Omdat een cd-rom langzamer is dan een harde schijf, is het werken met een live-cd wat langzamer.
Daarnaast kan het starten van programma's langer duren, omdat deze meestal gecomprimeerd op de schijf staan.

Omdat de automatische herkenning van de hardware niet altijd goed gaat, hebben sommige live-cd's de mogelijkheid om bepaalde instellingen op een ander medium (diskette of USB-stick) te schrijven. Bij het starten worden dan de gegevens vanaf dat medium gebruikt.

Het nadeel van een live-cd is dat gegevens niet zomaar opgeslagen kunnen worden. Daar zijn verschillende oplossingen voor. Zo kan (een deel van) de harde schijf beschreven worden, zodat bijvoorbeeld gemaakte brieven gewoon opgeslagen kunnen worden. Daarnaast is het mogelijk om een live-cd te gebruiken in combinatie met een USB-stick of een diskette om nieuwe gegevens op te kunnen slaan.

Een bijzondere oplossing is de "multi-sessie live-cd", hierbij worden alle gewijzigde instellingen (zoals instellingen voor een printer) en de eigen documenten op dezelfde Live-cd geschreven bij het afsluiten van de computer. Puppy Linux bijvoorbeeld heeft die mogelijkheid. Op deze manier blijven instellingen en bestanden bewaard en is er geen verschil meer met werken op een harde schijf.

Puppy Linux voegt daarbij steeds een nieuwe sessie toe aan de eenmalig beschrijfbare cd-rom, waardoor deze wel op een gegeven moment vol raakt.

Een andere oplossing is het gebruik van het bestandssysteem UnionFS waarbij niet alleen gewijzigde instellingen, maar ook compleet nieuw geïnstalleerde pakketten opgeslagen worden op een speciaal gebied van de harde schijf. Zo kan zelfs een live-cd opgewaardeerd worden.

64.3 Soorten

Voor Linux bestaan vele live-cd's, waarvan Knoppix de bekendste is. Voor BSD bestaan ook Live-cd's, maar dit is minder gebruikelijk.

- Linux
  - Gebaseerd op Debian, hier bestaan er zeer veel van.
    - Knoppix
    - Knoppix for Kids
    - Games Knoppix
    - Damn Small Linux
    - Gnoppix
    - Ubuntu/Kubuntu/Edubuntu
    - sidux
  - Gebaseerd op Slackware Linux
    - NimbleX
    - Nonux
    - SLAX
  - Gebaseerd op Mandrake
    - SAM
    - PCLinuxOS
    - MCNLive
- Berkeley Software Distribution (BSD)
  - DragonFly BSD
  - FreeSBIE
- Windows
  - BartPE (enkel voor eigen gebruik)
- Gebaseerd op Solaris
  - OpenSolaris

64.4 Populariteit van Linux bij Live-cd's

Bij Live-cd's is Linux veruit het meest gebruikte besturingssysteem om de volgende redenen:

1. Er zijn verschillende vrij te gebruiken Linuxdistributies. Deze mogen door iedereen gratis worden gebruikt.

2. Linux is compatibel met alle typen bestandssystemen, en kan hiermee werken. Windows ondersteunt bijvoorbeeld HFS+ van Mac niet, en Mac kan geen gegevens naar NTFS van Windows schrijven (er wel vanaf lezen).

3. Linux gebruikt veel drivers voor hardware in de kernel of in bijgevoegde bestanden. Tijdens het opstarten kijkt Linux iedere keer opnieuw welke drivers nodig zijn. Daardoor zal Linux op veel computers werken, zonder dat een aparte driver geïnstalleerd hoeft te worden.

64.5 Mogelijke vormen van een Live-cd

Een normale cd-rom met 650 MB of 700 MB heeft voldoende ruimte voor een besturingssysteem met een webbrowser, een tekstverwerker, e-mail, etc. Het is natuurlijk ook mogelijk om een dvd van 4,7 GB of 8,5 GB te gebruiken, waardoor veel meer programma's op de schijf geplaatst kunnen worden.

64.6 Live USB

Vanaf ongeveer 2003 hebben USB-sticks voldoende geheugen om daarop ook een volledig zelfstartend besturingssysteem te plaatsen. De meeste computers kunnen vanaf 2005 opstarten vanaf een dergelijke USB-stick (dit vereist meestal een kleine aanpassing in het BIOS). Zo'n USB-stick wordt Live USB genoemd.

De live-cd wordt in 2010 nog veel gebruikt. Maar steeds meer wordt de USB-stick gebruikt om een besturingssysteem op te plaatsen. Bij Ubuntu, een populaire Linuxdistributie, is een optie in het menu aanwezig om een opstartbare USB-stick te maken. Er is echter nog geen gestandaardiseerde manier om van een bestand dat gedownload is een opstartbare USB-stick te maken. Hiervoor wordt meestal een programma gebruikt, gericht op een bepaald besturingssysteem. Er zijn echter ook universele programma's beschikbaar zoals UNetbootin of Universal USB Installer.

64.7 Zie ook

- SYSLINUX
- Lijst van Linuxdistributies

64.8 Externe links

- (en) Lijst van actieve Linuxdistributies, inclusief live-cd's.
- (en) Uitgebreide lijst van live-cd's bij FrozenTech.

Hoofdstuk 65

macOS

MacOS (vroeger Mac OS X en later OS X)[1] is een lijn van besturingssystemen van Apple en wordt sinds 2002 meegeleverd op alle nieuwe Apple Macintosh-systemen. Het is de opvolger van Mac OS 9, het laatste "Classic" Mac OS dat Apple gebruikte sinds 1984. In 2016 werd dit besturingssysteem opgevolgd door macOS.

Voor Apples serversystemen wordt OS X Server gemaakt. De basis van dit systeem is identiek aan de consumentenversie, maar het wordt geleverd met specifieke gereedschappen voor servers. Het mobiele besturingssysteem iOS is een aangepaste versie van *macOS*, en wordt gebruikt voor de iPhone, iPad, iPod touch en de tweede en derde generatie Apple TV.

65.1 Geschiedenis

Het Mac OS was aanvankelijk geprogrammeerd vanuit de gedachte dat men op een computer voornamelijk één programma tegelijk zou gebruiken. Het ondersteunen van gevorderde multitasking, oftewel de mogelijkheid om meerdere programma's *onafhankelijk* van elkaar te draaien op eenzelfde computer, bleek hierdoor erg moeilijk aan het systeem toe te voegen. De Macintosh-computers verloren veel aanhang door het ontbreken van deze mogelijkheid, die op vele andere systemen al gerealiseerd was.

Na verloop van tijd kwamen er nog meer verouderde elementen van het Macintosh-besturingssysteem aan het licht. Het werd steeds duidelijker dat het eenvoudiger zou zijn een compleet nieuw systeem te ontwerpen, dan alle problemen uit het bestaande systeem te verhelpen. In 1999 werd aanvankelijk, op beperkte schaal, alleen een server-versie uitgebracht. Deze versie is voorzien van hulpprogramma's voor werkgroepbeheer en vereenvoudigde toegang tot netwerkdiensten, zoals een mail-, een Samba- en een DNS-server. In maart 2001 werd ook een versie van Mac OS X voor consumenten uitgebracht zonder deze diensten. Het is grotendeels gebaseerd op NeXTStep, het besturingssysteem voor NeXT Computers, dat op zijn beurt gebaseerd is op een BSD-kern.

Het oude Mac OS kon echter nog wel gebruikt worden in een emulatie, genaamd Classic. Met ingang van de Intel-Macsystemen werd de Classic-omgeving verwijderd uit het besturingssysteem en werd een transparant PowerPC-emulatiesysteem toegevoegd, genaamd Rosetta. Dit liet oudere programma's die zijn geschreven voor de PowerPC-processor werken op een Mac met Intelprocessor, wat zorgde voor een simpelere overgang naar de nieuwe systemen. In OS X 10.7 ("Lion") wordt Rosetta niet meer meegeleverd.

Mac OS X bestaat uit twee delen: XNU (een microkernelontwerp gebaseerd op de Mach 3.0-microkernel en de 4.4-BSD-systemservice[2]) en Aqua, een grafische gebruikersomgeving die door Apple is ontwikkeld.

Een variant van OS X, genaamd iOS, wordt door Apple gebruikt in zijn iPhone, iPad en iPod touch-producten. Omdat deze producten geen gebruik maken van Intel- of PowerPC-processor, betekent dit dat een aangepaste versie van OS X is ontwikkeld voor ARM-processors.

65.2 Naamgeving

Mac OS X is de opvolger van Mac OS 9. Het teken "X" in de naam verwijst naar het Romeinse cijfer tien. Sommige mensen lezen het teken echter als de letter 'x'. Dit wordt in de hand gewerkt doordat veel Unix-gerelateerde systemen een naam hebben die eindigt op een 'x'; bijvoorbeeld AIX, IRIX, Linux, Minix, Ultrix en Xenix. Daarnaast wordt de grafische Unix-interface het X Window System genoemd. Een andere reden is de tendens van Apple om naar specifieke versies te verwijzen met een decimaalnotatie, bijvoorbeeld met Mac OS X 10.4.

Voormalige versies van Mac OS X worden vernoemd naar grote katachtigen en worden sinds versie 10.2 (*Jaguar*) ook onder deze naam geadverteerd en verkocht. Zo wordt Mac OS X-versie 10.6 door Apple en Macgebruikers gewoonlijk *Snow Leopard* genoemd, en versie 10.7 *Lion*. Vanaf versie 10.7 is "Mac" uit de naam verdwenen, en gaat het besturingssysteem verder onder de naam "OS X". Sinds OS X 10.9 verving Apple de naamgeving aan de hand van katachtige door locaties in California.

Vanaf versie 10.12 is de naam van OS X gewijzigd naar macOS. Het besturingssysteem heeft een nieuwe naam gekregen om beter in lijn te liggen met iOS, tvOS en watchOS.

65.3 Versies

65.3.1 Public Beta Kodiak

Op 13 september 2000 lanceerde Apple een bètaversie van Mac OS X (intern Kodiak genaamd) om feedback van het publiek te krijgen. De publieke bèta markeerde de eerste publieke beschikbaarheid van de Aqua-interface en Apple heeft intussen al enorm veel veranderingen aangebracht op basis van de feedback van de klanten. De publieke beta werd stopgezet toen Mac OS X 10.0 Cheetah lanceerde.

65.3.2 Mac OS X 10.0 Cheetah

In maart 2001 lanceerde Apple de eerste versie van Mac OS X, genaamd Cheetah. De initiële versie was traag, onvolledig en had enorm weinig applicaties ten tijde van de lancering. Terwijl vele critici suggereerden dat het besturingssysteem nog niet klaar was voor gebruik door het grote publiek, herkenden ze het belang van de lancering als een basis om te verbeteren. De Macintosh community zag de lancering al als een enorme vervulling, omdat pogingen om het Macintosh besturingssysteem compleet te hernieuwen al sinds 1996 bezig waren, en vertraagd werden door eindeloze problemen.

65.3.3 Mac OS X 10.1 Puma

Later dat jaar, in september 2001, werd de versie 10.1 van Mac OS X gelanceerd. De release werd gekenmerkt door verhoogde prestaties en bijkomende applicaties, zoals de mogelijkheid om dvd's af te spelen. Apple lanceerde de 10.1 als een gratis upgrade-cd voor 10.0 gebruikers en als een betaalde versie voor gebruikers van Mac OS 9. Het werd al snel ontdekt dat de upgrade cd's ook als volledige installatie cd's konden gebruikt worden door een bepaald bestand aan te passen. De upgrade cd werd later opnieuw uitgegeven in een verminderde versie die ervoor zorgde dat de installatie op Mac OS 9 niet meer mogelijk was. Op 7 januari 2002 kondigde Apple aan dat Mac OS X op het einde van die maand het standaard besturingssysteem zou worden voor alle Apple computers.

65.3.4 Mac OS X 10.2 Jaguar

Op 24 augustus 2002 werd OS X-versie, oftewel *Jaguar*, gelanceerd. Het was de eerste versie die een "family pack" introduceerde. Met dit family pack mocht een gebruiker Mac OS X op maximaal 5 verschillende computers installeren.

65.3.5 Mac OS X 10.3 Panther

Op 24 oktober 2003 werd OS X-versie 10.3, oftewel *Panther*, gelanceerd, welke in vergelijking met de vorige versie 150 nieuwe technologieën en programma's bevatte.

65.3.6 Mac OS X 10.4 Tiger

In april 2005 werd OS X-versie 10.4, oftewel *Tiger*, gelanceerd. Deze versie bevatte onder andere vernieuwingen op het gebied van zoeken met het programma Spotlight en vergemakkelijkte regelmatig terugkerende handelingen met Automator. Daarnaast kon de gebruiker met Dashboard een aantal *widgets* op het scherm weergeven, waarmee in één oogopslag het weer, wereldtijden, beurskoersen en vluchtinformatie te zien zijn. Verder is sinds versie 10.3 Exposé opgenomen, een hulpmiddel waarmee men met een druk één toets - vroeger F9, bij nieuwe Macs F3 - alle geopende vensters gelijktijdig verkleind ziet, op F10 alle geopende vensters in het huidige programma in het klein ziet en met F11 het bureaublad ziet.

65.3.7 Mac OS X 10.5 Leopard

26 oktober 2007 verscheen Mac OS X 'Leopard' 10.5 als opvolger van 'Tiger'. Naast toegevoegde functies als Time Machine, voor het maken van back-ups, Quick Look en Cover Flow voor het sneller weergeven van bestandsinformatie is Boot Camp hierbij een van de standaardvoorzieningen. Dit laatste programma maakt het mogelijk om op Macs met Intel-processoren naast Mac OS X ook Microsofts Windows te installeren (doorgaans voor het draaien van computergames of programma's die voor OS X niet verkrijgbaar zijn). Via alternatieve 'virtualisatie'-pakketten als VMWare en Parallels is het ook mogelijk om veel Windows-programma's rechtstreeks binnen OS X te laten werken, zonder te hoeven herstarten in Windows via Boot Camp.

65.3.8 Mac OS X 10.6 Snow Leopard

Op 28 augustus 2009 kwam Mac OS X Snow Leopard (10.6) op de markt. Dit systeem was erop gericht bestaande functies te verbeteren in plaats van meer functies toe te voegen. De grootste troeven van dit systeem zijn dat het minder plaats inneemt dan Leopard - 7 GB volgens Apple, een verbeterde interface voor Exposé, sneller back-ups maken, sneller uitzetten en sneller ontwaken uit sluimerstand. Een groot deel van de bespaarde ruimte is te danken aan het "opruimen" van het systeem. Zo werden de ondersteuning voor PowerPC-processoren en AppleTalk geschrapt, en zijn de ontwerpbestanden verwijderd die in Leopard ten onrechte in de programmabestanden zaten bijgesloten. De systeemprocessen en vrijwel alle meegeleverde applicaties bij Snow Leopard zijn

omgezet naar 64 bit en de Finder is geheel opnieuw geprogrammeerd in de programmeertaal Cocoa.

65.3.9 OS X 10.7 Lion

OS X 10.7 Lion werd aangekondigd op het WWDC in 2011

OS X 10.7, genaamd *Lion*, werd in oktober 2010 door Steve Jobs aangekondigd tijdens het mediaspektakel 'Back to the Mac'. Deze nieuwe versie van OS X is op 20 juli 2011 op de markt gebracht. OS X bevat meer dan 250 nieuwe toevoegingen. Veel wijzigingen en toevoegingen zijn gebaseerd op de werking van *iOS*. OS X wordt vanaf deze versie zonder het voorvoegsel 'Mac' genoemd.[1]

Belangrijke UI-wijzigingen en toevoegingen zijn: *Launchpad* (startscherm voor alle applicaties, zoals het home-scherm op iOS-apparaten), automatisch verborgen schuifbalken, ondersteuning van multiple full-screenapps, *Mission Control* (overzichtelijke samenvoeging van *Exposé*, *Spaces*, *Dashboard* en full-screenapplicaties) en uitgebreide ondersteuning voor 'gestures' (touchpad-gebaren).

Verder zullen het systeem en de programma's altijd starten in de staat waarin ze eerder afgesloten zijn. Ook is het standaard niet nodig om documenten of projecten op te slaan; dit wordt zonder tussenkomst van de gebruiker afgehandeld door OS X. Met *Versions* is het eenvoudig mogelijk om de huidige versie van een document te vergelijken met oudere, automatisch opgeslagen, versies. Deze weergave is vergelijkbaar met *Time Machine* en is met name geschikt om oude gedeelten van het document te kopiëren naar de huidige versie.

In OS X 10.7 *Lion* is de ondersteuning voor Rosetta stopgezet; de PowerPc-apps zijn in *Lion* niet meer bruikbaar. Ook is de applicatie Front Row niet meer beschikbaar.

Ook bevat OS X 10.7 *Lion* een nieuwe versie van het standaardmailprogramma *Mail*. De belangrijkste wijzigingen hierin zijn: een nieuwe intelligente zoekfunctie, een lijstweergave van alle mailtjes met inleiding zoals ook in *iOS* het geval is en een nette weergave van conversaties (meerdere replies/thread).

OS X 10.7 *Lion* is 3,74 GB groot en was tot augustus 2011 enkel beschikbaar via de Mac App Store. Later werd het ook mogelijk om een USB-stick met Mac OS X Lion te bestellen.[3][4]

Met de release van OS X 10.7.2 kwam er tevens ondersteuning voor iCloud, Apples dienst voor cloud computing, waarin documenten, contacten kunnen worden gesynchroniseerd en iOS-apparaten via gps kunnen worden gelokaliseerd.

65.3.10 OS X 10.8 Mountain Lion

OS X 10.8, genaamd *Mountain Lion*, werd op 16 februari 2012 aangekondigd via de website van Apple en is sinds 25 juli 2012 te downloaden via de Mac App Store.[5] Het besturingssysteem bevat vooral veel nieuwe functies die hun oorsprong vinden in iOS, Apples besturingssysteem voor mobiele apparaten.

65.3.11 OS X 10.9 Mavericks

OS X 10.9 genaamd *Mavericks*, werd op 10 juni 2013 aangekondigd via de website van Apple. Apple stopt met namen van katachtige dieren en belooft om de eerstvolgende tien jaar gebruik te maken van namen die naar de roots van Apple verwijzen: California. Er zijn zo'n 200 nieuwe functies. Mavericks is sinds 22 oktober 2013 gratis te downloaden via de Mac App Store.

65.3.12 OS X 10.10 Yosemite

OS X 10.10, genaamd *Yosemite*, is de opvolger van OS X Mavericks. De naam, alsook de vernieuwde grafische gebruikersinterface, werd op de jaarlijkse WWDC van juni 2014 onthuld. Yosemite is sinds 16 oktober 2014 gratis te downloaden via de Mac App Store.

65.3.13 OS X 10.11 El Capitan

OS X 10.11, genaamd *El Capitan*, is de opvolger van OS X Yosemite. Bij deze nieuwe versie van OS X ligt de focus vooral op performance en gebruiksvriendelijkheid. *El Capitan* werd op 8 juni 2015 voorgesteld tijdens het jaarlijkse WWDC en is sinds 30 september 2015 gratis te downloaden via de Mac App Store.

65.3.14 macOS 10.12 Sierra

MacOS 10.12, genaamd *Sierra*, is de opvolger van OS X El Capitan. Het besturingssysteem krijgt een nieuwe naam om beter in lijn te liggen met iOS, tvOS en watchOS.

65.4 Zie ook

- Lijst van BSD-distributies

65.5 Externe link

- Officiële website

Hoofdstuk 66

Mailserver

Een **mailserver** is een server die verantwoordelijk is voor het verwerken van e-mail. Een andere, meer technische benaming voor een mailserver is **Mail Transfer Agent** (MTA). De term MTA wordt niet alleen voor internetmail (RFC's 2821 en 2822) gebruikt maar ook voor andere mailprotocollen (bijvoorbeeld X.400).

Een mailserver voert over het algemeen twee verschillende taken uit: e-mail uitwisselen met clients en e-mail routeren naar andere mailservers. Voor deze twee taken worden over het algemeen verschillende protocollen gebruikt: POP3 en IMAP voor het eerste, SMTP voor de laatste. Het uitwisselen van e-mail met een client is de taak die uitgevoerd wordt door een Mail Submission Agent (MSA) en Mail Delivery Agent (MDA). De meeste mailservers vervullen zowel de rol van MTA als MSA en MDA. Er is wel speciale software voor de rol van MDA beschikbaar, een voorbeeld hiervan is procmail.

Een gebruiker die e-mail verstuurt of ontvangt heeft over het algemeen geen directe interactie met een mailserver, maar gebruikt hiervoor een Mail User Agent (MUA) ofwel e-mail-client. Het is wel mogelijk om een mailserver direct aan te spreken door een Telnet-sessie op poort 25 te openen en direct SMTP-commando's te geven.

Tegenwoordig heeft een mailserver naast het transporteren van e-mail vaak ook de taak om deze te controleren op virussen, en om ze indien nodig te markeren als spam (ongewenste e-mail).

66.1 Lijst van MTA software

66.1.1 Unix-achtige besturingssystemen

- Apache James
- Atmail
- CommuniGate Pro
- Courier Mail Server
- Exim
- Haraka
- MailerQ
- MMDF
- MeTA1
- Message Systems
- OpenSMTPD
- Postfix
- Smail
- ZMailer
- qmail
- qpsmtpd
- sendmail

66.1.2 Microsoft Windows

- Axigen
- EVO Mail Server
- IBM Domino
- JAMES
- Kerio Connect
- Lotus Notes van IBM
- MDaemon
- MailEnable
- Mercury
- Microsoft Exchange Server
- Novell GroupWise
- SmarterTools
- SurgeMail
- hMailServer

Hoofdstuk 67

Man-in-the-middle-aanval

Een **man-in-the-middle-aanval** is een aanval waarbij informatie tussen twee communicerende partijen onderschept wordt zonder dat beide partijen daar weet van hebben. Hierbij bevindt de computer van de aanvaller zich tussen de twee communicerende partijen. De berichten kunnen daarbij mogelijk gelezen en veranderd worden. Ook kunnen berichten worden verzonden die niet door de andere partij zijn geschreven. De naam van de aanval verwijst naar de derde persoon die in het midden tussen de twee partijen *staat* en de langskomende berichten bekijkt en aanpast. Voorbeelden hiervan zijn het onderscheppen van e-mail en ander dataverkeer tussen twee of meerdere computers. Ook het onderscheppen van brieven en telefoongesprekken kan men zien als man-in-the-middle-aanvallen.

Het Diffie-Hellman-sleuteluitwisselingsprotocol zonder authenticiteit is niet bestand tegen een man-in-the-middle-aanval.

67.1 Voorbeeld

Stel dat Alice en Bob met elkaar via e-mail berichten willen uitwisselen. Alice stuurt een e-mail naar Bob, maar Trudy onderschept de e-mail doordat zij toegang heeft tot de e-mailserver. Indien Alice en Bob geen encryptie gebruiken, is Trudy in staat het bericht te lezen en eventueel te veranderen. Als ze het bericht aanpast, heeft Bob hier geen weet van, want hij kan niet controleren of het werkelijk Alice is die het bericht heeft geschreven. Ook in situaties waar wel sprake is van beveiligde communicatie – dat wil zeggen dat Alice en Bob eerst elkaars identiteit aan elkaar kenbaar maken – kan Trudy tussenbeide komen en de identificatie ongemerkt beïnvloeden.

Uit gelekte geheime informatie kan een MITM-aanval gereconstrueerd worden die werd uitgevoerd bij BICS, een dochtermaatschappij van de Belgische telecommaatschappij Belgacom, die oa. VoIP en dataroaming aanbiedt in Afrika en het Midden-Oosten. Door een hack op de servers van BICS kon de Britse geheime dienst man-in-the-middle aanvallen uitvoeren bij webbezoeken via de smartphone.[1]

67.2 Zie ook

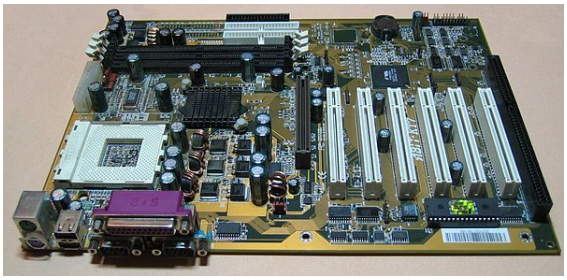
- Cryptografie

67.3 Externe link

- (en) Man-in-the-middle attack, OWASP

Hoofdstuk 68

Moederbord



Moederbord in ATX-formaat, ABIT KT7

Een **moederbord** in een personal computer (ook wel: *systeembord*, *mainboard*, *mobo* of in het geval van Apple Inc.: Logic Board) is een printplaat met elektronica waarop andere (insteek-)printplaten kunnen worden gemonteerd. In de loop der jaren is steeds meer functionaliteit in het moederbord ondergebracht. Rond 1989 bevatte het moederbord voornamelijk de processor, het werkgeheugen en interruptvoorzieningen, alle overige functies werden met insteekkaarten verzorgd. Anno 2016 treft men op een moederbord vaak een complete pc aan, inclusief geluids- en netwerkkaart, en in een aantal gevallen ook de videokaart en CPU. Hierdoor kunnen systemen goedkoper en compacter gebouwd worden.

68.1 Onderdelen

Enkele onderdelen die men op een modern moederbord vindt:

- De processor, ofwel de centrale verwerkingseenheid (*CVE*, Engels: *CPU*, Central Processing Unit).
- Het BIOS (Basic Input/Output System): in EEPROM opgeslagen programmatuur voor het opstarten van het systeem, waarbij het systeem ook een aantal zelftests (POST) uitvoert. In veel gevallen is er ook een optie aanwezig om instellingen van het BIOS te wijzigen, bijvoorbeeld om bepaalde geïntegreerde functies uit te schakelen wanneer deze niet worden gebruikt.
- De chipset, in de vorm van de northbridge en southbridge. Op de northbridge zit de processor aangesloten en, indien aanwezig, ook de PCI-E-sloten (deze kunnen ook gedeeltelijk op de southbridge zitten), en op de southbridge alle *langzame* onderdelen zoals de PCI-bus, USB-poorten en soms PCI-E sloten.
- Werkgeheugen (RAM, Random Access Memory) in de vorm van DDR SDRAM, SDRAM of, bij oudere moederborden, DIMM's, RIMM's en SIMM's.
- Connectoren voor uitbreidingskaarten zoals AGP, PCI, PCI-E, PCI-X, ISA, AMR
- Tegenwoordig standaard geïntegreerd: geluidskaart, netwerkkaart
- Op sommige moederborden, met name Micro-ATX, geïntegreerd: videokaart

68.2 Modellen

Systeemborden zijn verkrijgbaar in verschillende modellen en formaten: AT, ATX, Mini-ATX, MicroATX en Mini-ITX. Ook werden er BTX-moederborden verkocht, maar vanwege de incompatibiliteit met ATX werd BTX geen succes. BTX was een vormfactor waarbij de componenten heel anders geschikt stonden om optimaal te kunnen afkoelen. Er zijn wel fabrikanten van computerbehuizingen die de ATX-moederborden in de behuizing anders oriënteren voor een beter koelresultaat, waaronder Corsair.

Tegenwoordig zijn er drie grote processormerken waarop de CPU-sockets zijn gebaseerd: AMD, Intel en VIA. Zo zijn er voor Intel de Sockets 3, 5, 7 (ook voor AMD), Slot I, Slot II, PGA-370 (ook VIA), 478, Xeon, LGA-775, de LGA-1156 voor de Core i5 en Core i7 (800-serie), de LGA-1366 voor de Core i7 (900-serie), de LGA-1155 voor de 2e en 3e generatie van Core i3, i5 en i7, LGA-1150 voor de 4e en 5e generatie Core-processoren en sinds 2015 ook de LGA-1151-socket voor de 6e generatie Core-processoren.

Voor AMD zijn er de sockets: 7 (ook Intel), super socket 7, Slot A, Socket A (ook wel T-462 genoemd), 754, 939, AM1, AM2, AM2+, AM3, AM3+, FM1, FM2, FM2+, socket 940 en socket F.

VIA fabriceert tegenwoordig ook zelf moederborden met eigen processoren geïntegreerd, VIA Epia genaamd. VIA fabriceert onder andere de volgende processoren: VIA C3, VIA Eden, VIA Antaur. Vroeger fabriceerde VIA ook de VIA Cyrix, die vooral voor oudere moederborden met socket 3, 5, 7 en 370 geschikt waren.

Het moederbord kan, zoals veel elektronica, niet tegen statische elektriciteit. Het is niet aan te raden met een hand een blank metalen deel van het moederbord of van een elektronische component aan te raken tijdens werkzaamheden. Het wordt aangeraden je van tevoren statisch te ontladen. Dit kan bijvoorbeeld door de aarding van een stopcontact aan te raken. Beter is echter het gebruik van een antistatische mat en een geleidend polsbandje verbonden met een goede aardleiding.

Als het moederbord toch met een blote hand wordt aangeraakt, kan de persoon ontladen in het moederbord waardoor elektronica niet meer (goed) functioneert.

Hoofdstuk 69

Nettiquette

Netiquette (of **netiquette**)[1] is een samenvoeging van de woorden netwerk en etiquette. De nettiquette omvat de ongeschreven richtlijnen en gedragsregels voor het gebruik van internet.

69.1 Regels

De regels uit de nettiquette zijn informeel in te delen in twee categorieën: technologisch en cultureel bepaalde regels.

- Technologische regels zijn gebaseerd op het feit dat niet iedereen dezelfde technologie op het internet gebruikt.
- Culturele regels zijn gebaseerd op de wereldwijdheid van internet: wat de één ontzettend grappig vindt, is voor de ander een grove belediging.

In de praktijk blijkt dat rechttoe rechtaan zeggen wat men denkt, zonder de mogelijkheid van het overbrengen van toon en gelaatsuitdrukking, zeer snel kan leiden tot misverstanden en hevige woede. Bij e-mail is het daarom verstandig terughoudend te zijn, met name in de manier waarop kritiek wordt verwoord. De nettiquette kan verschillen per forum, nieuwsgroep of chatprogramma. Over het algemeen wordt het overdadig gebruik van hoofdletters beschouwd als schreeuwerig en storend. Op veel fora wordt het gebruik van hoofdletters en interpunctie zeer gewaardeerd, terwijl dit bij andere fora en chatprogramma's zoals MSN, niet het geval is. Er zijn onderwerpen die riskant blijven: politiek, religie en seks, terwijl informatica (beheersystemen, programmeertalen, e.d.) als voor vakspecialisten wordt ervaren.[2]

69.2 De tien geboden

Op SOFWeb[3] zijn regels te vinden om een goede 'Netizen' (net-burger) te zijn. Vertaald komen deze tien geboden op het volgende neer:

1. Denk aan het menselijke aspect achter de computer.
2. Houd online dezelfde gedragsstandaard aan als in het gewone leven.
3. Weet waar je bent in cyberspace; pas je toonzetting aan bij de omgeving waar je op bezoek bent.
4. Respecteer tijd en bandbreedte van de gebruiker.
5. Zorg ervoor dat je je goed presenteert online.
6. Deel deskundige kennis.
7. Help mee aan het binnen de perken houden van 'flames' en laat emotionaliteit voor wat het is.
8. Respecteer de privacy van anderen.
9. Maak geen misbruik van je macht.
10. Vergeef andere mensen hun fouten.

69.3 Nettiquette bij digitale berichten en e-mail

- E-mail komt overeen met een gewone brief. Een passende aanspreking en ondertekening moet dus ook gebruikt worden.[4]
- In de onderwerpregel van de e-mail wordt ingegeven waarover het bericht gaat. Verstuur nooit een e-mail zonder onderwerp.
- De regellengte van het e-mailbericht mag maximaal uit 72 tekens bestaan (exclusief citatiesymbolen). Hierdoor blijft het bericht goed leesbaar op het beeldscherm van de ontvanger.
- Verstuur de e-mail altijd als gewone tekst in plaats van HTML.
- Gebruik in het digitale of e-mailbericht geen hoofdletters om iets te benadrukken. Hoofdletters zorgen ervoor dat de ontvanger het bericht schreeuwerig interpreteert.

- Wanneer een e-mail naar veel personen en/of personen die elkaar niet kennen verstuurd wordt, vul dan de e-mailadressen in het BCC-veld in. Door het BCC-veld te gebruiken worden de e-mailadressen niet kenbaar gemaakt aan anderen.
- Bij het schrijven van een e-mail ontbreekt lichaamstaal. Er moet dus voorzichtig worden omgegaan met humor. Wanneer iets als een grap wordt bedoeld, kan gebruik worden gemaakt van een emoticon. Let wel, emoticons kunnen enkel in informele berichten.
- Plak bij beantwoorden alleen de tekst aan waarover het onderwerp gaat. Knip onnodige zinnen weg, bij voorkeur vervangen door "[...]" om te laten blijken dat je iets hebt weggehaald. Knip sowieso de ondertekening van de vorige schrijver weg.
- Mocht het onderwerpveld weinig meer te maken hebben met het originele onderwerp, verander dan het onderwerpveld in een nieuw onderwerp.
    - Bijvoorbeeld: *Onderwerp: Re: wekelijkse planningoverleg*
    - Mocht het zo zijn dat de e-mailwisseling niet meer over 'plannen' gaan, maar over bierbrouwen ofzo; verander het onderwerp op deze wijze: *Onderwerp: zelf bier brouwen (was: wekelijkse planning)*
    - En als er op déze e-mail een antwoord komt dan wordt het onderwerp dit: *Onderwerp: Re: zelf bier brouwen*
- Zo min mogelijk: Re, RE, Forw, Antw, achter elkaar. Dus géén: *Re: Antw: FW: Re: een leuk fotootje uit mijn ICQ- floppies*

69.4 Zie ook

- Usenet

69.5 Externe link

- (en) *ietf.org* - RFC1855: Netiquette Guidelines, al sedert oktober 1995. Bezocht op 11 april 2014.

Hoofdstuk 70

Nieuwsgroep

Een **nieuwsgroep** is een communicatiekanaal op Usenet. Het is vergelijkbaar met de discussiefora zoals die op veel websites te vinden zijn, maar de nieuwsgroepen vormen geen rechtstreeks onderdeel van het wereldwijde web waar men met een webbrowser naartoe kan surfen. Nieuwsgroepen worden ook wel *discussiegroepen* genoemd.

Er zijn vele tienduizenden nieuwsgroepen die gaan over de meest uiteenlopende onderwerpen. Het geeft iedereen de mogelijkheid om informatie te verspreiden en zeer serieus te discussiëren, maar ook om volstrekte nonsens te verkondigen.

De nieuwsgroepen zijn ook een plek waar mensen elkaar vrijwillig helpen om een probleem op te lossen, vaak in verband met computers en het internet, maar het kan ook gaan over een ziekte van een goudvis, problemen met wetgeving of wat dan ook.

70.1 Infrastructuur

Nieuwsgroepen maken vaak gebruik van het Usenet-netwerk en zijn onder andere bereikbaar via het NNTP-protocol. In tegenstelling tot veel andere netwerkdiensten maakt dit systeem geen gebruik van een centrale server. Berichten worden volgens een peer-to-peer-systeem van server naar server doorgegeven.

70.2 Benodigde software

Om nieuwsgroepen te kunnen lezen, heeft u in principe een newsreader (ook wel nieuwslezer genoemd) nodig. Een overzicht hiervan staat op de newsreader-pagina. U kunt ook gebruikmaken van een e-mailclient zoals Mozilla Thunderbird of Outlook Express.

U kunt nieuwsgroepen lezen via de nieuwsservers van uw provider of van enkele 'openbare' servers, zoals die van euro.net en van de Freie Universität Berlin. Wanneer u slechts over een internetbrowser beschikt, kunt u ook gebruikmaken van Google Groups.

70.3 Verschillende nieuwsgroepen

Nieuwsgroepen zijn geordend volgens een hiërarchie. Men begint op topniveau (bijvoorbeeld *nl* of *news*) en hierachter komen dan steeds meer gespecialiseerde termen. Een voorbeeld is *nl.comp.software.newsreaders* (i.e. een Nederlandstalige nieuwsgroep over newsreaders).

70.3.1 Big8

Onder **Big8** verstaan we de (acht) oorspronkelijke, internationale hiërarchieën, te weten comp.*, humanities.*, misc.*, news.*, rec.*, sci.*, soc.* en talk.*. (bijvoorbeeld *talk.religion*, *talk.politics*, *talk.origins*)

70.3.2 nl.* en be.*

Net zoals bij de domeinnamen bestaan er ook landenhiërarchieën. Die van Nederland en België zijn de nl.*- en de be.*-hiërarchie.

Om nieuwe nieuwsgroepen aan te maken in de nl.*-hiërarchie bestaat er een oprichtingsprocedure, die onder andere een discussie en stemming in *nl.newsgroups* omvat.

70.3.3 alt.*

De alt.*-hiërarchie is een verzameling voor alles wat niet onder één van de andere hiërarchieën valt. Met name alt.binaries.* is bekend, omdat er (in tegenstelling tot de meeste andere nieuwsgroepen) naast tekst ook *binary's*, zoals muziek, films en foto's gepost mogen worden. Omdat dergelijke nieuwsgroepen meestal een groot volume aan data opleveren, zullen niet alle newsservers die groepen voeren.

70.4 Binaire nieuwsgroepen

Nieuwsgroepen worden steeds meer gebruikt voor het verspreiden van binaire bestanden, ook al is dat niet de oorspronkelijke bedoeling van nieuwsgroepen.

Die populariteit wordt onder meer veroorzaakt doordat bestanden van usenet door een onbeperkt aantal gebruikers kunnen worden gedownload waarbij de downloadsnelheid slechts afhankelijk is van de bandbreedte van de internetverbinding en usenetserver van de downloader. Dit in tegenstelling tot *Peer-to-peer* (P2P) uitwisselingsnetwerken waarbij de downloadsnelheid wordt gelimiteerd door de uploadsnelheid van de gebruikers die het bestand delen. Een ander voordeel is dat voor het downloaden van nieuwsgroepen niet is vereist dat ook wordt geüpload, hetgeen bij de meeste P2P netwerken wel het geval is.

Omdat nieuwsgroepen oorspronkelijk bedoeld zijn voor het verspreiden van tekstberichten, zijn er een aantal beperkingen aan het verspreiden van binaire bestanden via nieuwsgroepen:

1. Op nieuwsgroepen kunnen alleen tekstbestanden worden geplaatst en geen binaire bestanden. Binaire bestanden moeten daarom door de uploader eerst worden omgezet in tekst (het zogenaamde “coderen”). De tekstbestanden worden vervolgens geüpload naar de nieuwsgroep. De downloader dient de gedownloade tekstbestanden ten slotte om te zetten naar het oorspronkelijke binaire formaat (het zogenaamde “decoderen”). Coderen en decoderen kan op verschillende manieren. Vroeger werden meestal de technieken Uuencode en Base64 gebruikt. Het nadeel van deze technieken was dat de bestandsgrootte van het tekstbestand tot 30% groter was dan het oorspronkelijke binaire bestand. Deze overhead zorgt voor een langere downloadtijd. Tegenwoordig wordt meestal de techniek yEnc gebruikt, die een minimale overhead oplevert.

2. De maximale grootte van een bericht in een nieuwsgroep is beperkt. Als het bericht te groot is, dan wordt het niet geaccepteerd door de server. Een binair bestand is vaak veel groter dan deze maximale grootte. Deze beperking kan worden omzeild door het binaire bestand op te splitsen in meerdere kleine (tekst)berichten.

3. Omdat de overdracht tussen nieuwsservers onderling niet 100% gegarandeerd is kunnen er berichten verloren gaan. Als dit delen van een gecombineerd bestand zijn kan dit niet gereconstrueerd worden. Hierom worden vaak extra bestanden meegeport waarmee bijvoorbeeld met parchive de ontbrekende delen alsnog aangemaakt kunnen worden.

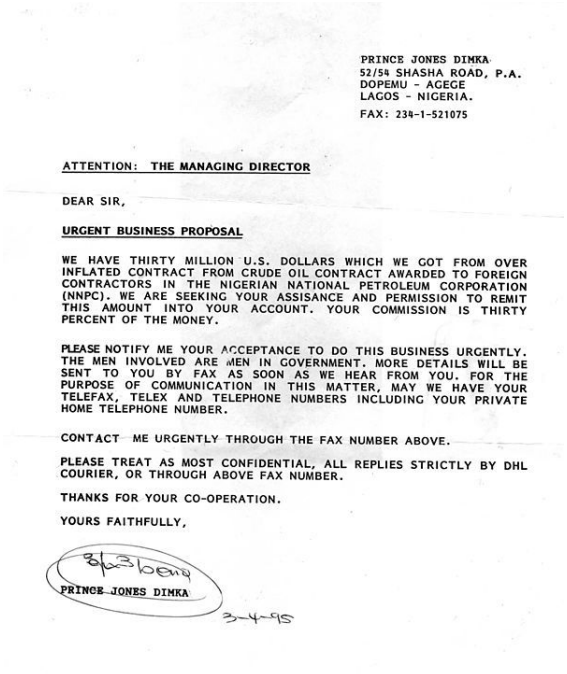
Binaire newsreaders zijn gespecialiseerd in het downloaden van binaire bestanden. Deze binaire newsreaders automatiseren het decoderen van de gedownloade tekstbestanden en het combineren van de gedecodeerde bestanden naar het oorspronkelijke binaire bestand.

70.5 Externe links

- Groepen en charters van de be-hiërarchie
- Google Groups

Hoofdstuk 71

Nigeriaanse oplichting



PRINCE JONES DIMKA
52/54 SHASHA ROAD, P.A.
DOPEMU - AGEGE
LAGOS - NIGERIA.
FAX: 234-1-521075

ATTENTION: THE MANAGING DIRECTOR

DEAR SIR,

URGENT BUSINESS PROPOSAL

WE HAVE THIRTY MILLION U.S. DOLLARS WHICH WE GOT FROM OVER INFLATED CONTRACT FROM CRUDE OIL CONTRACT AWARDED TO FOREIGN CONTRACTORS IN THE NIGERIAN NATIONAL PETROLEUM CORPORATION (NNPC). WE ARE SEEKING YOUR ASSISANCE AND PERMISSION TO REMIT THIS AMOUNT INTO YOUR ACCOUNT. YOUR COMMISSION IS THIRTY PERCENT OF THE MONEY.

PLEASE NOTIFY ME YOUR ACCEPTANCE TO DO THIS BUSINESS URGENTLY. THE MEN INVOLVED ARE MEN IN GOVERNMENT. MORE DETAILS WILL BE SENT TO YOU BY FAX AS SOON AS WE HEAR FROM YOU. FOR THE PURPOSE OF COMMUNICATION IN THIS MATTER, MAY WE HAVE YOUR TELEFAX, TELEX AND TELEPHONE NUMBERS INCLUDING YOUR PRIVATE HOME TELEPHONE NUMBER.

CONTACT ME URGENTLY THROUGH THE FAX NUMBER ABOVE.

PLEASE TREAT AS MOST CONFIDENTIAL, ALL REPLIES STRICTLY BY DHL COURIER, OR THROUGH ABOVE FAX NUMBER.

THANKS FOR YOUR CO-OPERATION.

YOURS FAITHFULLY,

PRINCE JONES DIMKA

3-4-95

Voorbeeld van een Nigeriaanse oplichtingsbrief

Voorschotfraude, ook wel gekend als **Nigeriaanse oplichting** is een vorm van oplichting. Het slachtoffer wordt 'gouden bergen' beloofd als hij eerst (relatief) kleine onkosten wil voorschieten. De 'kosten'-truc wordt herhaald tot het slachtoffer afhaakt, waarna de oplichters spoorloos verdwijnen. De term 'Nigeriaanse oplichting' wordt in overdrachtelijke zin ook gebruikt voor oplichtingspogingen vanuit andere landen.

Deze vorm van oplichting is eeuwenoud. Een voorloper deed de ronde in 1900. Een zogenaamde rijkaard zat ergens gevangen en kon niet bij zijn geld om zijn proceskosten te betalen. Het slachtoffer werd gevraagd in ruil voor een beloning het geld tijdelijk onder zich te houden. Uiteindelijk moest ook hier geld voorgeschoten worden.

Met de komst van het internet en de bijhorende internetfraude zijn de oude communicatiemiddelen, fax en brief, nagenoeg geheel vervangen door massale e-mailspam en berichten via community-netwerksites.

71.1 Mooi verhaal

De eerste stap is het versturen van een stortvloed aan e-mails (spam) naar alle mogelijke adressen. Er wordt meestal gewerkt met standaardteksten en varianten daarop. De afzender beweert bijvoorbeeld een hoge overheidsfunctionaris te zijn, een executeur-testamentair, een stervende rijkaard, een bankmedewerker of een loterij. Het betreft een som van vaak miljoenen euro's of dollars, waarbij de hulp wordt ingeroepen van de ontvanger bij een of andere transactie. Er wordt een beloning in het vooruitzicht gesteld en er wordt met aandrang gevraagd aan de ontvanger om zo snel mogelijk contact op te nemen. Er wordt vaak van webmailadressen gebruikgemaakt, zoals Hotmail, Yahoo Mail en Gmail.

De e-mails zijn te herkennen doordat het voorstel "te goed om waar te zijn" is, de oplichters weinig aandacht besteden aan de eerste e-mails (taalfouten), het voorstel gelinkt is met het "exotische" buitenland en gebruikmaakt van betalingsmethodes zoals Western Union.

In 2005 kreeg deze vorm van oplichting de Ig Nobelprijs voor Literatuur - *Presented to the Internet entrepreneurs of Nigeria, for creating and then using e-mail to distribute a bold series of short stories, thus introducing millions of readers to a cast of rich characters — General Sani Abacha, Mrs. Mariam Sanni Abacha, Barrister Jon A Mbeki Esq., and others — each of whom requires just a small amount of expense money so as to obtain access to the great wealth to which they are entitled and which they would like to share with the kind person who assists them.*

71.2 Gevolgen

De oplichting kan het slachtoffer financieel volledig ruïneren. Sommige slachtoffers steken zichzelf diep in de schulden. Dit draagt ook bij tot het blijven betalen: in de ogen van het slachtoffer is er geen weg meer terug nadat er zoveel schulden zijn gemaakt, en is het beloofde bedrag de enige uitweg. In de extreemste gevallen raken ze alles wat ze bezitten kwijt en blijven bovendien met een flinke restschuld achter.

Wanneer iemand tot de ontdekking is gekomen dat hij is

opgelicht, is de kans erg klein dat hij zijn geld terugziet. De oplichters maken gebruik van niet-traceerbare kanalen en laten zich ook op een niet-traceerbare manier betalen, bijvoorbeeld via Western Union. Ook zelf of via een privédetective op onderzoek uitgaan, heeft meestal geen andere gevolgen dan dat de kosten nog verder oplopen. Zelfs in de zeldzame gevallen waarin het tot arrestaties komt is het geld meestal 'verdwenen'.

Naast de financiële schade is er vaak ook emotionele schade. Het slachtoffer durft niemand meer te vertrouwen. Ook komt het soms voor dat het slachtoffer wanhopig blijft vastklampen aan de droom van het geld en de oplichters blijft betalen, ook als een derde hem inmiddels op de feiten heeft gewezen. Sommige slachtoffers hebben zelfmoord gepleegd, zoals de Engelsman Leslie Fountain die zichzelf in november 2003 in brand stak na tot de ontdekking te zijn gekomen dat hij was opgelicht.[1][2][3] Een ander dodelijk incident vond plaats in februari 2003 op de Nigeriaanse ambassade in Praag. De 72-jarige Tsjech Jiří Pasovský schoot twee ambassademedewerkers neer, waarvan één dodelijk, nadat hij was opgelicht voor $ 550 000 en hij van de Nigeriaanse consul-generaal te horen had gekregen dat Nigeria hem dat niet zou terugbetalen.[4]

Er zijn ook gevallen aan de orde geweest waarin een slachtoffer, al dan niet op uitnodiging van de oplichters, naar het betreffende Afrikaanse land afreisde en gegijzeld werd. Bovendien zijn er ook verschillende gevallen van moord bekend (in de periode 1994-97 alleen al 15 gevallen). De meest bekende '419 moord' was die op de Griekse George Makronalli. Hij werd door oplichters naar Zuid-Afrika gelokt, gegijzeld, en uiteindelijk vermoord toen zijn familie het losgeld niet betaalde.[5]

Slachtoffers die zelf de onkosten niet kunnen betalen komen soms in de verleiding geld te verduisteren om zo de onkosten te betalen. Ze doen dit bijvoorbeeld door via een bankrekening van de werkgever te betalen, of uit onder beheer staande gelden van derden. Men denkt immers dat het saldo binnen korte tijd weer kan worden aangevuld. Het geld komt echter niet, en sommige slachtoffers zijn zelf strafrechtelijk vervolgd omdat ze verduistering hadden gepleegd teneinde de 'onkosten' te kunnen betalen. Een van de bekendste voorbeelden hiervan was de oplichting van de Braziliaanse bankdirecteur Nelson Sakaguchi door de Nigeriaanse oplichter Emmanuel Nwude. Van 1995 tot 1998 betaalde Sakaguchi $ 242 miljoen aan Nwude. Dit geld was afkomstig van Sakaguchi's werkgever, Banco Noroeste Brazil, die hierdoor failliet ging. Deze zaak was een van de omvangrijkste fraudezaken ooit en leidde uiteindelijk tot 2 doden, een civiele- en strafprocedure tegen Sakaguchi. Nwude werd eveneens vervolgd door de Nigeriaanse autoriteiten en is uiteindelijk tot 25 jaar gevangenisstraf veroordeeld. Het grootste deel van het geld is terugbetaald.

Wanneer het slachtoffer persoonlijke informatie heeft gestuurd is het mogelijk dat die ook wordt gebruikt om mensen op te lichten, bijvoorbeeld via identiteitsdiefstal. Hierdoor kan het slachtoffer zelfs jaren later nog in de problemen komen.

71.3 Bestrijding

71.3.1 Nederland

De bestrijding van deze fraude is in Nederland in handen van het KLPD. De zaak is zeer gecompliceerd en de prioriteit ervan ligt niet hoog. Hoewel er af en toe een succes wordt geboekt, blijft het dweilen met de kraan open.[6][7]

71.4 Zie ook

- Internetfraude

Hoofdstuk 72

Online betalen

Door de toenemende digitalisering is het tegenwoordig mogelijk om **online te betalen**. Dit kan onder andere met iDEAL, met PayPal en met een creditcard. Online betalen zorgt ervoor dat je op ieder moment van de dag, zolang er internet aanwezig is, een betaling kan regelen. Steeds meer betalingen worden online geregeld en online wordt ook een steeds groter bedrag uitgegeven.[1]

De groeiende verwerkingscapaciteit en complexiteit van informatietechnologie hebben er echter voor gezorgd dat privacy een steeds belangrijker onderwerp is geworden [2] Online betalen brengt namelijk een risico met zich mee dat dit de privacy van gebruikers kan aantasten door gaten in de beveiliging.[3] Onder privacy valt het verkrijgen, distribueren van persoonlijke/ niet geautoriseerde informatie.[4] Om privacy te waarborgen is het belangrijk om een veilige verbinding te maken tussen de bank en de gebruiker. De bank heeft hier een belangrijke rol in door te zorgen voor een uitstekende beveiliging middels encryptie, autorisatie en firewalls.[3]

72.1 Zie ook

- Internetbankieren

Hoofdstuk 73

PayPal

PayPal is een online betaalsysteem, dat bij zijn oprichting oorspronkelijk bedoeld was voor betalingen tussen pda's.

Het systeem fungeert als intermediair voor online en mobiele betalingen tussen personen onderling, online verkopers en webwinkels. Om te betalen is alleen een e-mailadres nodig. Betalingen kunnen gedaan worden vanaf een bankrekening, creditcard of van ontvangen geld op de PayPal-rekening. Er kan ook geld worden overgeschreven naar een eigen bankrekening.

73.1 Ontwikkeling

Het bedrijf, met zijn hoofdkwartier in San Jose (Californië), werd in 1998 onder de naam Confinity opgericht door Peter Thiel, Luke Nosek en Max Levchin. In eerste instantie richtte het bedrijf zich op applicaties voor de Palm Pilot-pda. Het product PayPal werd in 1999 gelanceerd.

De populaire veilingsite eBay kocht PayPal in oktober 2002 op, omdat ongeveer 50% van de eBay-gebruikers het al gebruikte. PayPal was daarmee veel populairder dan eBays eigen BillPoint. Sinds de lancering van de Nederlandstalige versie van PayPal in 2006, toont de Nederlandse markt een forse stijging. Het aantal rekeninghouders in Nederland groeide van 1 miljoen in maart 2007 naar 2,7 miljoen in maart 2010[1]. Het bedrijf won van 2009 tot 2013 al vijf maal op rij de Nederlandse Thuiswinkel Award voor de beste financiële dienst op het internet en in België de BeCommerce Award in 2010. In 2015 stoot eBay PayPal af en gaat het als onafhankelijk bedrijf naar de beurs.[2]

Betalen met PayPal is voor de betaler gratis, maar de ontvanger betaalt een aandeel als provisie, ter grootte van 3,4% + € 0,35 van het overgeschreven bedrag. Een betaling van 20 euro ontvangen kost daarmee ongeveer 1 euro. Grootafnemers kunnen in aanmerking komen voor een lager tarief. Informatie over de gebruikte betaalrekening of creditcard komt niet ter beschikking van de verkoper.

73.2 Kritiek op PayPal

Sinds 7 december 2010 ligt PayPal samen met VISA, Mastercard, Western Union en Bank of America onder vuur als financiële instellingen die overboekingen aan WikiLeaks blokkeren. Deze maatregel wordt door critici als willekeurig en onwettig gezien.

73.3 Kopersbescherming

PayPal biedt bescherming aan de koper van producten op eBay, Marktplaats of op andere websites gekocht en betaald zijn met PayPal, maar niet zijn geleverd. Indien een product is ontvangen dat sterk afwijkt van de beschrijving (zoals namaakartikelen of beschadigde artikelen) kan de koper dat product terugsturen. De koper moet vervolgens een bewijs van verzending aan PayPal kunnen overleggen zodat de prijs van het product niet op hem verhaald kan worden.

Deze bescherming zorgt ervoor dat een verkoper zich moet indekken. Het belangrijkste voor de verkoper is om elk verkocht product betaald via PayPal, traceerbaar te verzenden. Er zijn kopers die het niet ontvangen van het product aanvechten via PayPal zodra ze merken dat het pakket niet traceerbaar is, waardoor de verkoper aan PayPal geen bewijs van verzending kan leveren en hij de betaling terug moet storten. Sommige oplichters maken hier misbruik van door goederen te kopen, ze in persoon op te halen en vervolgens hun geld terug te eisen, omdat de goederen zogenaamd niet ontvangen zouden zijn.

73.4 Fraude

Veiligheid, betrouwbaarheid en discretie zijn noodzakelijk bij allerhande verrichtingen via het internet.

PayPal stelt de discretie van de persoonlijke gegevens en/of de financiële status veilig[3] door:

- eigen servers voor de opslag van gevoelige informatie;

- onzichtbaar maken van de financiële informatie voor bijvoorbeeld webwinkels;[4]
- opgave van het persoonlijk e-mailadres bij elke verrichting;
- gegevenscodering bij alle dataverkeer.

73.4.1 Externe risico's

Hoewel PayPal maatregelen neemt tegen fraude, bestaan er nog externe invloeden waardoor hackers de persoonlijke gegevens kunnen misbruiken:

- door middel van frauduleuze e-mails en nepwebsites proberen hackers onder naam van een legaal bekende organisatie allerhande persoonlijke gegevens te verkrijgen (phishing en spoofing);
- via oude bankafschriften/persoonlijke documenten kunnen hackers de nodige gegevens achterhalen;
- bij het doorgeven/noteren van persoonlijke gegevens in een niet-vertrouwde omgeving kunnen omstaanders misbruik maken van de genoemde informatie.

73.5 Innovatie

In 2009 werd de PayPal-webservices opengesteld voor externe ontwikkelaars, waardoor er ook mobiele applicaties voor persoonlijke betalingen gemaakt kunnen worden. De iPhone-app bevat onder meer de zogenaamde "Bump"-functionaliteit, waarmee de ene iPhone-bezitter geld kan overmaken aan een andere iPhone-bezitter door de apparaten tegen elkaar te "bumpen". Ook voor Android en BlackBerry OS ontwikkelde PayPal een applicatie. Ook werd er een Mobiele Shopgids-app uitgebracht, een soort gouden gids voor m-Commerce in Nederland.

Een doorontwikkeling vormen eerste mobiele websites en applicaties (iPhone en Android) met PayPal Mobiel. Zo kan de consument mobiele bioscoopkaartjes kopen in de app van Pathé, maar kan er mobiel betaald worden voor kleding, wijn, ansichtkaarten, schoenen, bloemen, maar ook condooms binnen de applicatie van Condoom Anoniem.

Amerikaanse bestuurders van PayPal hebben laten weten dat PayPal offline gaat, zodat het bedrijf een betaalwijze voor in fysieke winkels kan leveren, een zogeheten Point of Sale (POS)-oplossing. Een stap hiertoe is een grootschalige pilot in Californië in samenwerking met het bedrijf Bling. Consumenten kunnen betalen in winkels en bedrijfskantines door hun mobiele telefoon langs een NFC-lezer bij de kassa te halen.

73.6 Externe link

- Officiële site

Hoofdstuk 74

Pharming (internet)

Pharming is een oplichtingstechniek die erin bestaat internetgebruikers te misleiden door hun internetverkeer met een bepaalde website ongemerkt om te leiden naar een andere (malafide) website.

Bij pharming wordt een DNS-server aangevallen (meestal door een methode die "DNS cache poisoning" wordt genoemd) en wordt het IP-adres van een bepaalde domeinnaam gewijzigd. De nietsvermoedende surfer typt het bekende webadres in, maar komt op een nagebootste site terecht. Indien dit bijvoorbeeld de site van een bank is, kan een kwaadwillige hacker vervolgens gevoelige gegevens ontfutselen. Om pharming tegen te gaan is DNSSEC ontwikkeld.

Pharming is mogelijk door een kwetsbaarheid in de DNS-serversoftware. DNS-servers zijn servers die domeinnamen omzetten in werkelijke IP-adressen die bestaan uit vier getallen. Voorbeeld: *nl.wikipedia.org* verwijst naar IP-adres 145.97.39.133. Als een hacker erin slaagt de tabel van een DNS-server te wijzigen, kan men door het intypen van bijvoorbeeld *nl.wikipedia.org* op een heel andere webserver belanden. De internetgebruiker merkt hier niets van; ook antivirusprogramma's of antispywaresoftware beschermen niet tegen pharming. De bescherming moet komen van de beheerder van de website. Banken beschikken in het algemeen over goed beveiligde sites. De gebruiker moet erop letten dat het adres van de site exact overeenkomt met de site van de bank. Websites beveiligd met SSL starten met https:// in de URL.

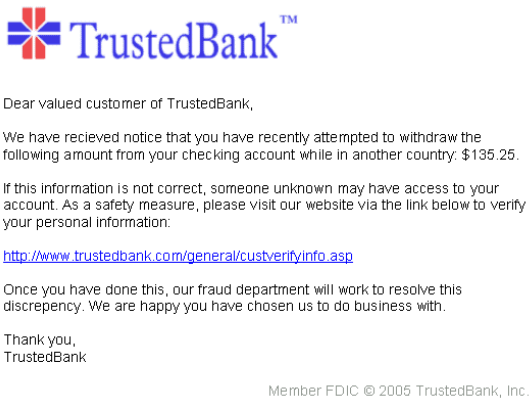
De term "pharming" is gekozen analoog met de term phishing. Beide methoden worden ook gebruikt voor identiteitsfraude. Hoewel pharming gelijkenissen kan vertonen met phishing, is deze techniek verraderlijker omdat de surfer geheel te goeder trouw naar een valse website kan worden gestuurd.

74.1 Zie ook

- Phishing
- Skimmen

Hoofdstuk 75

Phishing


TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Voorbeeld van phishing-e-mail

Phishing (naar analogie van *phreaking*, is het afgeleid van *fishing*: “vissen”, “hengelen”) is een vorm van internetfraude. Het bestaat uit het oplichten van mensen door ze te lokken naar een valse (bank)website, die een kopie is van de echte website, om ze daar – nietsvermoedend – te laten inloggen met hun inlognaam en wachtwoord of hun creditcardnummer. Hierdoor krijgt de fraudeur de beschikking over deze gegevens met alle gevolgen van dien. De fraudeur doet zich hierbij voor als een vertrouwde instantie, zoals een bank. De meeste vormen van phishing gebeuren via e-mail. De slachtoffers worden hierbij met een e-mail naar deze valse website gelokt. De mail bevat een link naar de (valse) website met het verzoek om zogenaamd “de inloggegevens te controleren”.

Een variante vorm van phishing is *spear fishing*, waarbij de persoonlijke gegevens (naam, e-mailadres, telefoonnummer) van het slachtoffer worden gebruikt om hem een gevoel van vertrouwen te geven.

75.1 Methode

Bij phishing wordt dikwijls gebruikgemaakt van URL-spoofing. Dit is het nabootsen van de URL van bijvoorbeeld een bank, zodat de gebruiker denkt de echte site te bezoeken, terwijl de URL die van de bedrieger is.

Sinds het gebruik van het IDN-systeem (Internationalized domain name), waarbij niet-ASCII-tekens kunnen worden gebruikt in domeinnamen, kan phishing hiervan gebruikmaken door een echte domeinnaam na te bootsen met gelijkwaardige buitenlandse tekens, zodat de gebruiker niet merkt dat het adres niet klopt.

Zelfs met een gewone ASCII-URL kan bedrog gepleegd worden: zo lijkt het adres www.googIe.com, waarin de kleine letter l vervangen is door een hoofdletter i (I), erg op www.google.com, en kan het er, afhankelijk van het lettertype, zelfs exact gelijk uitzien.

De meeste banken maken tegenwoordig gebruik van een Extended Validation-certificaat: in moderne internetbrowsers wordt het eerste gedeelte van de adresbalk weergegeven met een groene achtergrond, zodat de gebruiker zeker weet dat hij op de echte pagina zit.

Meestal ontvangt het slachtoffer een mail waarin hem gevraagd wordt zijn account bij bijvoorbeeld een bank na te kijken en te bevestigen. Ook wordt er wel gebruikgemaakt van instant messaging, soms wordt er telefonisch contact opgenomen. Fraudeurs maken veelvuldig gebruik van nepsites van financiële instellingen, eBay en PayPal. Phishing is moeilijk te achterhalen, mensen op het internet moeten vooral zelf opletten en nooit ingaan op een mailverzoek waarin gevraagd wordt persoonlijke (financiële) gegevens te geven; zoals bankrekeningnummer, pincode, BSN of creditcardgegevens. Het eerste geval van phishing dateert uit 1996.

75.1.1 Kenmerken

In een phishing-bericht zijn vaak de volgende elementen te vinden:[1][2]

- De mail is niet aan de klant persoonlijk gericht, maar begint met een algemene opening als “geachte klant”.
- De mail bevat taal- en stijlfouten.
- Er wordt gesuggereerd dat het account “geverifieerd” (op juistheid onderzocht en bevestigd) moet worden met de inloggegevens van de klant.

- Er wordt gedreigd met gevolgen als niet onmiddellijk gehoor gegeven wordt aan de mail.
- De link waarnaar wordt verwezen bevat subtiele verschillen met de originele link, zoals een andere extensie of andere schrijfwijze.

Een veelgebruikte methode is dat de fraudeur een e-mail stuurt met een bijlage waarin een keylogger of andere malware zit verborgen. De mail functioneert dan als een Trojaans paard. Zodra de gebruiker de bijlage heeft geopend, wordt – op de achtergrond – de keylogger geactiveerd. Hierdoor kan de fraudeur via internet zien welke wachtwoorden de gebruiker gebruikt bij het inloggen bij zijn of haar bank.

75.1.2 Als slachtoffer

Wie slachtoffer is van phishing, wordt aanbevolen:

- om de bank op de hoogte te brengen van het ontvangen bericht en van de phishingactie;
- om codes van de online bankaccount te veranderen of deze te blokkeren;
- om alle gegevens die bewijs kunnen leveren van de feiten en de geleden schade te verzamelen:[3]
- om onmiddellijk aangifte te doen bij de politie.

75.2 Incidenten

- In maart 2007 kreeg een groot aantal klanten van ABN AMRO te maken met een phishing-mail. Deze bevatte een Trojaans paard waarmee de inloggegevens van de klant achterhaald konden worden.
- In oktober 2009 werd phishing gebruikt om de wachtwoorden van enkele duizenden gebruikers van maildiensten zoals Hotmail en Gmail te achterhalen.[4]
- De Nederlandse Vereniging van Banken heeft op 13 oktober 2010 een mediacampagne gelanceerd. Die helpt onder het motto: “als je weet hoe ze werken, kun je je ertegen wapenen”. De mediacampagne geeft inzicht in hoe internetcriminelen te werk gaan en wat je eraan kunt doen.
- ING-klanten slachtoffer van poging tot phishing. [5]
- Begin 2015 berichtte de Belgische Federatie van de Financiële sector dat er 85% minder fraudegevallen waren in 2014 (277 gevallen) ten opzichte van 2013 (1772 gevallen).[6]

75.3 Zie ook

- Pharming
- Skimmen

75.4 Externe links

- (en) Phishing-test
- (nl) veiligbankieren.nl

Hoofdstuk 76

Portaal (internet)

In internetverkeer wordt **portaal** gebruikt als een webpagina die dienstdoet als "toegangspoort" tot een reeks andere websites, die over hetzelfde onderwerp gaan. Soms dus synoniem van start- of hoofdpagina, maar meestal ook als vertrekpunt en overzichtstabel voor verdere navigatie binnen een onderwerp.

De Engelse naam, die ook veel in Nederlandse teksten gebruikt wordt, is ***portal***.

76.1 Achtergrond

Veeleer dan te proberen een eenduidige en algemeen geldige definitie te geven, volgen hierna enkele veel gebruikte definities of pogingen tot definitie.

> *Een webtoepassing die via een eenvormige gebruikersinterface toegang geeft tot een gevarieerd aanbod aan informatiebronnen.*
>
> *Meer dan een webpagina met links naar andere toepassingen.*
>
> *De universele, verpersoonlijkte toegang tot elke toepassing of informatiebron.*
>
> *Beveiligde en verpersoonlijkte toegang tot inhoud en toepassingen.*

In de praktijk komt het erop neer dat een bezoeker gericht informatie wil vinden over een bepaald onderwerp, en het zoeken via een zoekmachine als google een te breed scala aan websites terug geeft.

76.2 Functies

Alhoewel dus afwijkende definities gehanteerd kunnen worden, wordt algemeen aangenomen dat een portaalsite in grote mate over volgende functies moet kunnen beschikken:

- Authenticiteit bevestigen
- Verpersoonlijkbaar zijn (personalisatie)
- Inhoud beheren
- Toegang verlenen tot toepassingen
- Groeperen en integreren
- Zoeken en catalogiseren
- Samenwerken bevorderen
- Meertaligheid
- Distribueerbaar via diverse kanalen

Het bedrijfsportaal en het gemeenschapsportaal zijn twee brede categorieën van portaalsites. Deze sites bieden dan een startpagina met nuttige links en informatie voor de medewerkers van het bedrijf of de leden van de gemeenschap.

Hoofdstuk 77

Pretty Good Privacy

Pretty Good Privacy (lett: *vrij goede privacy*) wordt meestal afgekort tot PGP en is een van de veel gebruikte vercijferingsmethodes op internet. De standaard die aan PGP ontsproten is wordt thans OpenPGP genoemd en er zijn tegenwoordig vele programma's, zowel commercieel als open source, die deze standaard implementeren en ook grotendeels onderling compatibel zijn.

OpenPGP-cryptografie is gebaseerd op een schema van asymmetrische cryptografie, oorspronkelijk op het RSA-principe. Dit houdt in dat er twee verschillende sleutels zijn, één voor vercijferen en één voor ontcijferen van de informatie.

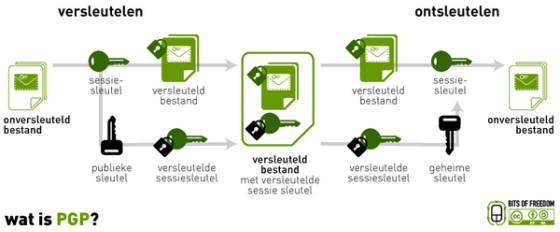
Er zijn vele OpenPGP-servers die van duizenden mensen de publieke sleutel opgeslagen hebben. Met die sleutel en een OpenPGP-programma kan men een vertrouwelijk bericht sturen naar een van de personen die op die server hun publieke sleutel op hebben laten slaan. Daarnaast is het ook mogelijk om sleutels als tekst te exporteren en te importeren zodat deze bijvoorbeeld op de website van de eigenaar geplaatst kan worden.

Hoewel dit principe erg veilig is, is het wel zaak te bedenken welke garantie er geboden wordt: iemand heeft een sleutel gemaakt en tekent daar berichten mee of laat mensen daar berichten mee vercijferen. Dit betekent dus niet automatisch dat deze sleutel toebehoort aan de persoon aan wie wij denken dat hij behoort. Om deze reden kennen veel OpenPGP-implementaties publieke sleutels een vertrouwenswaarde toe, die door de gebruiker gewijzigd kan worden nadat deze via een betrouwbaar kanaal (telefoon, ontmoeting) geverifieerd heeft dat de sleutel inderdaad van de vermoede persoon afkomstig is.

GPG, ook wel GnuPG, is een juist niet gepatenteerd alternatief voor PGP. GPG is te gebruiken bij Microsoft Outlook, Mozilla Thunderbird, Apple Mail, Eudora en veel andere mailprogramma's door plug-ins te downloaden en aan de programmatuur toe te voegen. De Thunderbird plug-in heet Enigmail. De zwakste schakel bij berichtenversleuteling is meestal het wachtwoord dat de eindgebruiker kiest, niet de software. Het ideale wachtwoord is een lange reeks cijfers, hoofdletters, kleine letters en symbolen.

Voor GNOME bestaat er een frontend voor GPG genaamd Seahorse voor het beheer van de sleutels.

77.1 Werking van PGP



Wat is PGP (Pretty Good Privacy)?

Als een gebruiker een stuk tekst wil vercijferen met PGP, dan comprimeert PGP de tekst meestal eerst. Hierdoor wordt zowel de plaats die het bestand inneemt op de harde schijf verminderd als de tijd die nodig is om het te versturen.

Dan maakt PGP een IDEA-sessiesleutel aan, een sleutel die gegenereerd wordt door de willekeurige bewegingen van je muis en de toetsen die je aanslaat. Met deze sessiesleutel wordt de tekst vercijferd. De sessiesleutel zelf wordt met de publieke sleutel van de beoogde ontvanger versleuteld, waarna beide delen verstuurd worden.

Decryptie werkt precies andersom. De ontvanger gebruikt zijn of haar geheime sleutel om de versleutelde sessiesleutel te ontcijferen. Daarna ontcijfert PGP met behulp van de sessiesleutel de ontvangen tekst.

77.1.1 Sleutels

Een sleutel is een waarde waarmee je cryptografisch algoritme een tekst versleutelt. Het is in principe een erg groot getal, waarvan de lengte gemeten wordt in bits. Uitgaande van een goed cryptografisch algoritme geldt: hoe langer de sleutel, hoe veiliger de versleuteling.

Hoewel de publieke en de geheime sleutel wiskundig aan elkaar gerelateerd zijn, is het erg lastig om de geheime sleutel af te leiden wanneer men alleen de publieke sleutel weet. Het is in theorie voor iemand die genoeg tijd en rekenkracht tot zijn beschikking heeft mogelijk om deze afleiding te maken. In de praktijk kan dit echter alleen bij (erg) kleine sleutels. Bij grotere sleutels is de reken-

kracht van de huidige computers niet voldoende om de afleiding binnen een bruikbare tijd te maken. De keuze van de lengte van de sleutel is dus een afweging tussen veiligheid enerzijds en gebruikssnelheid anderzijds, waarbij het optimum afhangt van de waarschijnlijkheid dat iemand de betreffende boodschap zou willen kraken.

Sleutels worden versleuteld opgeslagen. PGP slaat de sleutels in twee bestanden op; één voor de publieke sleutels en één voor de geheime sleutels. Deze bestanden worden sleutelringen genoemd. Wanneer je PGP gebruikt, zul je in het algemeen de publieke sleutels van jouw ontvangers toevoegen aan jouw publieke sleutelring. Jouw geheime sleutels worden opgeslagen in jouw geheime sleutelring. Wanneer je deze ring kwijtraakt, kun je geen data meer ontcijferen waarvoor je deze sleutels nodig hebt.

77.1.2 Digitale handtekeningen

Wanneer een gebruiker een bericht wil voorzien van een digitale handtekening, dan voegt hij of zij een met zijn of haar geheime sleutel versleutelde tekst toe aan het bericht. Hierdoor kan een ontvanger controleren of het bericht echt afkomstig is van de verzender door het te ontcijferen met de publieke sleutel van de verzender.

Een groot voordeel van publieke-sleutelcryptografie is dat het zorgt voor een systeem waarmee digitale handtekeningen kunnen worden gebruikt. Hierdoor kan een ontvanger zowel verifiëren of het bericht echt van de verwachte verzender afkomt (authenticiteit) als controleren of de data nog intact is (data-integriteit). Daarnaast zorgt het er ook voor dat een verzender niet kan ontkennen dat hij of zij een bericht gestuurd heeft (non-repudiation).

77.2 Referenties

- PGP internationaal

77.3 Zie ook

- GPG (Alternatieve opensource versie die niet gepatenteerd is)
- RSA
- Enigmail (OpenPGP in Mozilla Thunderbird)

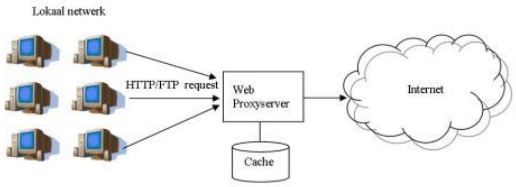
77.4 Externe links

- GnuPG: een open source-implementatie van OpenPGP
- WinPT: een windowsprogramma om GnuPG makkelijker te gebruiken
- Een aantal redenen waarom Phil Zimmermann PGP schreef

Hoofdstuk 78

Proxyserver

Een **proxyserver** is een server die zich bevindt tussen de computer van een gebruiker en de computer waarop de door de gebruiker gewenste informatie staat (het Engelse woord “proxy” betekent *gevolmachtigd tussenpersoon*). Wil iemand op een computer waarop een proxyserver is ingesteld een andere computer bereiken, dan gebeurt dit niet rechtstreeks, maar via deze proxyserver. Het doel van deze tussenstap is afhankelijk van het type proxyserver.



web proxyserver

78.1 Typen proxyserver

Er zijn globaal gezien drie typen proxyservers.

78.1.1 Web proxy

Dat is de meest voorkomende server, waarbij alle clients in een lokaal netwerk gezamenlijk via een proxyserver het internet opgaan, waarbij al het HTTP- en/of FTP-verkeer gecachet wordt, met een belangrijk snelheidsvoordeel voor de clients in het netwerk die webpagina’s opvragen uit de cache (of tussenbuffer) van de proxyserver.

78.1.2 Open proxy

Een **open proxy** is een proxyserver die verbindingen toestaat van clients en ze voorziet van willekeurige IP-adressen. Deze open, transparante proxy’s worden bijvoorbeeld gebruikt door mensen die hun privacy om welke reden dan ook willen beschermen, of om bij een website te kunnen komen die ontoegankelijk is vanaf het netwerk waarvan zij gebruikmaken. Open proxy’s kunnen ook misbruikt worden door spammers en mensen die op andere manieren misbruik maken van het internet.

78.1.3 Reverse proxy

De proxyserver werkt hier van buiten naar binnen, dus andersom. Dit wordt ook wel “web server acceleration” genoemd. Hierbij wordt de proxyserver ingezet om de belasting vanuit het internet naar de webserver(s) gelijkmatiger te verdelen, zowel om beveiligings- als om “loadbalancing"-redenen.

78.2 Transparante proxyserver

Een proxyserver is **transparant** als hij voor de gebruikers (clients) 'doorschijnend' en daarmee onzichtbaar is. Er zijn enkele voordelen aan deze opstelling:

- De proxyserver hoeft niet ingesteld te worden in de browsers van alle gebruikers.
- Het gebruik van de proxyserver is verplicht.
- Gebruikers hoeven niet te weten dat ze via een proxyserver surfen.

Wanneer een webaanvraag gestuurd wordt, zal de router dit doorsturen naar de proxyserver die de aanvraag verder zal afhandelen. Professionele routers hebben ondersteuning voor transparante proxyservers. Dit is ook mogelijk via een Linux-router.

78.3 Doel

78.3.1 Filteren van informatie

Zo kan een bedrijf alle werknemers via een proxyserver met internet verbinden en voorkomen dat bepaalde webpagina's door die werknemers bekeken kunnen worden. Hierbij gaat het om het afhandelen van aanvragen van binnen naar buiten. Vaak wordt dan een internetfilterprogramma gekoppeld aan de proxyserver.

78.3.2 Beveiliging

Bovendien kan de proxyserver als (onderdeel van) een firewall de toegang tot computers van werknemers van buitenaf bemoeilijken en zo als beveiliging gebruikt worden. Deze afhandeling van aanvragen van buiten (internet) naar binnen wordt “reverse proxy” genoemd.

78.3.3 Minder IP-adressen

Publieke IPv4-adressen op het internet zijn schaars en kosten dus geld. Door gebruik te maken van een proxyserver of NAT-router kunnen de computers op het bedrijfs- of thuisnetwerk een intern (gratis) IP-adres toegewezen krijgen. Zulke IP-adressen vallen in een (of meerdere) van de volgende reeksen:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Hoewel er duizenden pc’s b.v. het IP-nummer 192.168.0.2 zullen hebben, bestaan IP-nummers uit deze reeksen niet op het publieke internet.

78.3.4 Betere netwerkprestaties

In dit geval wordt de proxyserver gebruikt als tijdelijke opslagruimte. Bezoekt persoon X een website, dan wordt een kopie van de bezochte pagina’s opgeslagen op de proxyserver. Wil persoon Y daarna dezelfde website bezoeken, dan krijgt hij de eerder gemaakte kopie te zien. Bezoekt Y een nog niet door de proxyserver opgeslagen webpagina, dan wordt alsnog contact opgenomen met de eigenlijke website.

Het voordeel van de laatste methode is dat het netwerk minder vaak contact hoeft te maken met de oorspronkelijke website. Y ontvangt het resultaat doorgaans sneller en het netwerk wordt ontlast. Het nadeel is dat de getoonde informatie mogelijk niet de meest actuele stand van zaken weergeeft.

Veel internetproviders maken gebruik van dit type proxyserver en vragen hun klanten in hun webbrowser een proxyserver in te stellen. Op deze manier kunnen zij het gebruik van bandbreedte beperken en de snelheid van hun dienst vergroten. Of die klant ook daadwerkelijk profiteert van het gebruik van een proxyserver is afhankelijk van de omvang van de proxyserver en van het type websites dat hij bezoekt. Wijkt zijn internetgedrag sterk af van dat van andere klanten, dan is de kans dat de door hem opgevraagde website zich in de cache van de proxyserver bevindt klein en kan deze tussenstap voor hem juist een vertraging opleveren bij het bereiken van zijn doel. Wanneer de verbinding van de proxyserver met de website echter een hogere bandbreedte heeft dan de verbinding tussen proxyserver en client, kan dit alsnog een aanzienlijke snelheidswinst opleveren.

78.3.5 Misbruik

Een zeer groot deel van de spam die tegenwoordig op het internet verstuurd wordt, maakt gebruik van open proxy’s. Veelal installeren spammers open proxy’s op Microsoft Windows-computers met behulp van virussen die voor dit doel zijn ontworpen. Mensen die misbruik maken op IRC-netwerken maken ook vaak gebruik van open proxy’s om hun identiteit te verhullen.

78.3.6 Detectie

Omdat het gebruik van open proxy’s veelal samenhangt met misbruik van Internetdiensten, is er een aantal manieren ontwikkeld door systeembeheerders om open proxy’s te blokkeren van het gebruik van diensten. IRC-netwerken(Internet Relay Chat) zoals het blitzed network testen systemen van clients automatisch voor bekende types van open proxy’s. Zo kan ook een mailserver zo geconfigureerd worden, dat deze zenders van e-mails automatisch test op open proxy’s.

Van diverse open proxy’s zijn lijsten beschikbaar die op het Internet worden bijgehouden, zoals die van de DNSBL.

78.4 Software

Veelgebruikte software voor proxyservers:

- Squid cache (UNIX/Linux)
- Apache HTTP Server kan dienen als proxyserver.
- Privoxy (opensource)
- Microsoft Internet Security and Acceleration Server (Windows 2000/2003)
- Proxomitron - proxy, veel gebruikt om reclame te verwijderen.
- Tor (netwerk) - een proxy-service die toegang geeft tot 'onion' sites en de gebruiker door meerdere proxyservers leidt.

Hoofdstuk 79

Ransomware

Voorbeeld van ransomware

Ransomware is een chantagemethode op internet door middel van malware. Letterlijk vertaald betekent ransom: *losgeld*. Ransomware is een programma dat een computer (of gegevens die erop staan) blokkeert en vervolgens van de gebruiker geld vraagt om de computer weer te 'bevrijden'. Betalen blijkt echter niet (altijd) tot ontsluiting van de computer te leiden, zo waarschuwt de Nederlandse overheid.

79.1 Werking

De computers van de slachtoffers worden geïnfecteerd zoals ook andere virussen worden verspreid. Bij het heropstarten van de computer krijgt de gebruiker een scherm te zien met een boodschap. In deze boodschap krijgt het slachtoffer te lezen dat zijn of haar computer geblokkeerd werd en pas na betaling weer wordt vrijgegeven. Vaak wordt de indruk gewekt dat het bericht afkomstig is van een betrouwbare (overheids)instantie en dat er een boete moet worden betaald wegens misbruik van het internet. Maar de politie en opsporingsdiensten gaan zo niet te werk. Wie ransomware op zijn computer heeft, is voor de politie dus niet ineens een verdachte. De criminelen zijn enkel op het geld uit en zullen de computer na de betaling mogelijk vrijgeven. Er zijn meerdere gevallen bekend waarbij de computer daarna werd ontgrendeld, daarentegen zijn er ook genoeg gevallen van computers die niet werden ontgrendeld.

79.2 Varianten

De ransomware kan in drie vormen voorkomen:

- systeem gijzelen;
- bestand gijzelen;
- combinatie van beide.

79.3 Preventie

De kans op besmetting kan worden verkleind door:

- Actuele software gebruiken. De fabrikanten van software brengen regelmatig updates uit om beveiligingslekken te dichten, zoals Microsoft Windows, Adobe Reader, Flash Player ...
- Niet surfen op het internet als je ingelogd bent op een account met administrator-rechten
- Niet surfen op het internet zonder up-to-date antivirusprogramma.
- Gebruik van een firewall.
- Niet openen van verdachte bijlagen in e-mails.
- Niet downloaden en installeren van nepprogramma's of van gehackte (illegale) software.
- Activeer geen links zoals “klik hier”.

Besmetting is niet volledig te voorkomen. Soms raken computers besmet via een reguliere website, die door criminelen is gehackt.

79.4 Ecopsvirus

Een voorbeeld van ransomware is het Ecopsvirus. Hierbij wordt het Belgisch overheidsmeldpunt voor internetmisbruik eCops misbruikt. Het virus blokkeert de computer, en toont een site die zogezegd van de Belgische politie

afkomstig is. De gebruiker zou zogezegd illegale activiteiten uitgevoerd hebben, en dientengevolge is zijn computer geblokkeerd. In de site staat een link om een boete te betalen, maar dit is enkel om de gebruiker geld afhandig te maken. Antivirusscanners herkennen het virus als JS/Blacole.

79.5 Ontsmetting en aangifte

Wie slachtoffer is geworden van ransomware, doet er altijd goed aan om aangifte te doen bij de politie. De politie adviseert om hiervoor een afspraak te maken met het wijkteam en van tevoren aan te geven dat het om cybercrime gaat, zodat de juiste experts beschikbaar zijn.

79.6 Zie ook

- Cyberpolitie-virus

79.7 Externe link

- Federal Computer Crime Unit: fenomeenfiche Ransomware
- Ransomware on the rise (FBI)

Hoofdstuk 80

Recht om vergeten te worden

Het **recht om vergeten te worden** ofwel **vergeetrecht** is een recht voor burgers van de Europese Unie om bepaalde verouderde of onjuiste privacygevoelige informatie te laten verwijderen uit de zoekresultaten van zoekopdrachten op een persoonsnaam bij een internetzoekmachine, een bedrijf dat online gegevens bijhoudt, een online organisatie of een website. Het gaat in artikel 17 om het verwijderen van internet data bij de bron. Ze moeten hiervoor contact opnemen met de eigenaar van de zoekmachine zelf, zo heeft het Europees Hof van Justitie op 13 mei 2014 besloten.[1]. Een website heeft dus niet noodzakelijkerwijs een speciale knop waardoor een database alle gegevens wist. Let dus op dat een site niet slechts de mogelijkheid tot het deactiveren van content van een profiel of zoekmachine biedt.

80.1 Aanleiding

Het vergeetrecht is voorgekomen uit het zogenaamde Costeja-arrest van het Europese Hof van justitie op 13 mei 2014 (zaaknummer C-131/12). De aanleiding was een zaak aangespannen door een Spanjaard. Via zoekgigant Google was een krantenartikel te vinden uit 1998 waarin de gedwongen verkoop van bezittingen van de Spanjaard werd aangekondigd. Omdat de man vond dat de informatie zijn relevantie intussen had verloren – en daarom alleen nog maar zijn reputatie schaadde – begon hij een proces tegen de krant en Google.[2]

Het vergeetrecht is gebaseerd op de Europese Privacyrichtlijn (Richtlijn 95/46/EG) die door Nederland is geïmplementeerd in de Wet bescherming persoonsgegevens (WBP). Specifiek de artikelen 36 en 40 uit het WBP vormen in de Nederlandse wetgeving de basis voor het vergeetrecht en leggen gegevensverwerkers verplichtingen op als er sprake is van ofwel onjuiste of niet ter zake doende gegevens ofwel bijzondere persoonlijke omstandigheden van de persoon van wie er gegevens verwerkt worden.

Het vergeetrecht houdt echter een conflict in tussen twee zogenaamde fundamentele rechten uit het Europees Verdrag voor de Rechten van de Mens (ERVM) te weten artikel 8 uit het ERVM, het recht op privacy en artikel 10 uit het ERVM, het recht op vrijheid van informatie.

80.2 Verzoeken

Google biedt inmiddels de mogelijkheid gebruik te maken van het recht om vergeten te worden, en wel door het beschikbaar stellen van een online formulier waarmee internetgebruikers in de EU een verzoek kunnen indienen. Dergelijke verzoeken kunnen ervoor zorgen dat bepaalde links met informatie verwijderd worden uit de Google-zoekresultaten. Om een verzoek in te dienen moet een geldige kopie van een identiteitsbewijs worden ingeleverd, evenals een link naar de informatie, en moet een reden worden opgegeven waarom de informatie gedateerd, irrelevant of ongepast zou zijn. Het recht om vergeten te worden wordt echter niet effectief beschermd en vaak worden de verzoeken afgewezen op grond van het algemeen belang.[3]

80.3 Andere Media

De online service http://www.justdelete.me geeft aan hoe makkelijk of moeilijk het is voor een gebruiker om een profiel of andere gegevens te verwijderen. Bedenk dus eerst goed waar je je gegevens achterlaat. Sites met een indicatie rood (moeilijk te verwijderen profiel) of zwart (onmogelijk te verwijderen profiel) bevinden zich in de gevarenzone wat betreft de privacy.

80.4 Wereldwijd

Op 15 juni 2015 werd bekend dat de Franse rechter Google nog 14 dagen de tijd gaf om het recht om vergeten te worden wereldwijd te maken. De Franse autoriteit voor gegevensbescherming is naar de rechter gestapt en heeft deze situatie aan de rechter voorgelegd. Momenteel is het zo dat het recht om vergeten te worden per land dient te worden ingediend. Indien een verzoek slaagt, wordt het resultaat dan ook alleen in de landelijke Google-pagina verwijderd. Mocht het recht om verge-

ten te worden wereldwijd worden, wordt het daarmee een stuk effectiever.[4]

Hoofdstuk 81

Scriptkiddie

Een **scriptkiddie** is een persoon die zich misdraagt op het internet. Hij maakt daarbij gebruik van technieken en hulpmiddelen die door anderen zijn ontwikkeld. Vaak zijn die bedacht door crackers. Een scriptkiddie heeft meestal geen verstand van de onderliggende technieken en is slechts een gebruiker van andermans middelen. Deze term wordt sinds halverwege de jaren 90 van de 20e eeuw gebruikt.

De stereotiepe scriptkiddie is een puber van het mannelijke geslacht die over een krachtige computer beschikt. Scriptkiddies handelen vaak vanuit een baldadige motivatie en voor de “kick”. Ze zijn zich meestal niet bewust van de gevolgen van hun eigen handelen of hebben weinig boodschap aan de gevolgen/overlast voor andere internetgebruikers.

Scriptkiddies veroorzaken overlast. Veel van de misbruikmeldingen op het internet worden veroorzaakt door scriptkiddies. Ze komen echter vaak kennis en kunde te kort om daadwerkelijk een gevaar te vormen voor mensen die hun computer en/of systemen goed up-to-date houden.

Veel computervirussen en -wormen worden als het werk gezien van scriptkiddies.

Een in Nederland bekend voorbeeld van het werk van een scriptkiddie is het zogenaamde Anna Kournikova-virus. Dit virus was door een computerverkoper uit Sneek met een paar muisklikken in elkaar gezet door gebruik te maken van een kant-en-klare virusontwerpomgeving. Dit virus heeft wereldwijd economische schade toegebracht maar leidde slechts tot een kleine werkstraf voor de maker.

81.1 Zie ook

- Computercriminaliteit
- Cracker
- Hacker
- Spoofing

Hoofdstuk 82

Server

Een aantal Wikipediaservers.

Een **server** is een computer of een programma dat diensten verleent aan clients. In de eerste betekenis wordt met server de fysieke computer aangeduid waarop een programma draait dat deze diensten verleent.

In de praktijk komen er verschillende combinaties van hardware en serverprogramma's voor:

- Dedicated server: op een computer draait 1 serverprogramma. Dit zal vooral het geval zijn voor taken die veel resources vragen, zoals een database.
- Clustered server: een aantal aan elkaar gekoppelde computers (een cluster) draait een serverprogramma. Dit zal over het algemeen gebeuren om veel clients tegelijk te kunnen bedienen. Een typisch voorbeeld hiervan is een webserver voor een drukke website.
- Een server waarop meerdere serverprogramma's draaien. Dit is vrij algemeen het geval bij UNIX systemen.
- Een computer die zowel client- als servertaken vervult.
- Een cloud server dat met al de computers die erop aangesloten zijn een soort 'wolk van computers' vormt, waarbij de eindgebruiker niet weet op hoeveel of welke computer(s) de software draait of waar die precies staan.

Andere termen die gebruikt worden voor serverprogramma's zijn daemon (UNIX) en service (Windows).

82.1 Hardware

Over het algemeen worden servers voorzien van aangepaste hardware, andere dan bijvoorbeeld bij computers voor thuisgebruik. Verschillen zijn over het algemeen:

- Voeding: Dit is meestal gewoon een ATX-voeding, soms is er ook een extra voeding aanwezig die dient als back-up. Beide voedingen kunnen hot-swappable zijn.
- Geheugen: In servers wordt meestal ECC-geheugen gebruikt. Vaak gaat dit gepaard met grote hoeveelheden RAM geheugen.
- Processor: Het belangrijkste onderdeel van de server. Hierbij wordt vaak gebruikt van een Intel Xeon Processor, of een AMD Opteron Processor, hoewel soms ook meer gangbare processoren voor reguliere computers gebruikt worden.
- Harde schijf: Meestal het oude SCSI of nieuwere SAS schijven op 10.000 of 15.000 RPM. Tegenwoordig worden ook wel SSD's gebruikt die zijn aangesloten via een Serial ATA connector, vanwege de lage toegangstijden en hogere snelheden.
- Moederbord: Moederborden voor servers zijn veelal groter van formaat om 2 of zelfs 4 losse processoren te ondersteunen. Daarnaast is er vaak veel meer ruimte voor geheugen en ook wordt vaak ECC geheugen ondersteund.
- Behuizing: Omdat de meeste servers in een datacenter staan, worden vaak rackservers gebruikt. Deze servers kunnen in een rack geschoven worden, waardoor er zo veel mogelijk servers per vierkante meter kunnen staan. Toch bestaan er ook towerservers en bladeservers.

82.2 Gangbare servertypen

- Bestandsserver
- Applicatieserver
- Webserver
- Mailserver
- Databaseserver
- Time-server
- Printerserver
- FTP-server
- DHCP-server
- DNS-server
- Proxyserver
- IRC-server
- Gameserver
- Virtual private server
- Telnet-server
- Opensource-server
- Media streaming server

82.3 Zie ook

- Client

Hoofdstuk 83

Social engineering (informatica)

Social engineering of **social hacking**, is een techniek waarbij een computerkraker een aanval op computersystemen tracht te ondernemen. Dit door de zwakste schakel in de computerbeveiliging, namelijk de mens, te kraken. De aanval is gericht op het verkrijgen van vertrouwelijke of geheime informatie, waarmee de hacker dichter bij het aan te vallen object kan komen. De beroemdste kraker die van deze techniek gebruikmaakte, is Kevin Mitnick. Hij heeft zijn ervaringen verwoord in het boek The Art of Deception.

83.1 Doelen

Kenmerkend voor social engineering is dat er geen aanval op de techniek zelf wordt uitgevoerd. Een aanvaller tracht om:

- de nieuwsgierigheid van een slachtoffer te wekken
- medelijden bij een slachtoffer te wekken
- een slachtoffer bang te maken

De aanvaller doet zichzelf voor als iemand anders. Dit doet de aanvaller met het doel om via de aangenomen, vertrouwenwekkende, rol informatie te verkrijgen die op een andere manier niet of met aanzienlijk meer inspanning of hogere kosten te krijgen is.

83.2 Technieken

Er zijn drie aanvalstechnieken:

83.2.1 Persoonlijk contact

De hacker probeert persoonlijk contact te leggen met het slachtoffer. Hij kan zich bijvoorbeeld voordoen als helpdeskmedewerker en de gebruiker opbellen met het verzoek aan diens gebruikersnaam en wachtwoord door te geven om een probleem te verhelpen. Vooraf aan dit contact verzamelt de hacker gerelateerde informatie over het slachtoffer zodat hij het slachtoffer een overtuigend verhaal kan vertellen. Hiervoor worden zoekmachines als Google, sociale netwerksites als Facebook en andere informatiebronnen op het internet gebruikt. Dit is in de praktijk een eenvoudige en effectieve techniek.

Een actueel voorbeeld is de kwestie rond het gebruik van de *pretext* techniek (het voorwenden iemand anders te zijn) door de onderzoekers die voor de CEO van Hewlett-Packard door analyse van het privé telefoon en e-mail gebruik van mededirecteuren en journalisten hebben achterhaald wie verantwoordelijk was voor het laten uitlekken van strategische informatie naar de pers.

83.2.2 E-mail

Een hacker verstuurt een e-mailtje met een belangwekkende tekst. Deze techniek wordt onder meer uitgevoerd bij de phishing aanval, waarbij gebruikers ertoe worden verleid om op een authentiek ogende site vertrouwelijke gegevens zoals pincodes en creditcardnummers op te geven. Ook de vele e-mail wormen, zoals Sober en Klez, hanteren deze techniek, waarbij een vertrouwenwekkend of bangmakend mailtje de gebruikers ertoe verleidt om ongemerkt een trojaans paard te laten installeren. De aanvaller kan daarmee vervolgens de computer controleren en gebruiken voor zijn eigen doeleinden, zoals het versturen van spam.

Vishing is de telefoonvariant van phishing waarbij de aanvaller geen mail stuurt, maar telefonisch contact opneemt met het slachtoffer.

83.2.3 Rondsnuffelen

De computerkraker probeert vertrouwelijke informatie te krijgen door het snuffelen in vuilnisbakken, containers en prullenbakken. Deze techniek heet dumpster diving. Ook probeert een aanvaller rond te neuzen op de diverse plaatsen bij kopieermachines waar wel eens vertrouwelijke documenten worden weggegooid, of verzameld. Hierbij zal de hacker wel eerst een vorm van insluiping moeten uitvoeren om het gebouw waar de vertrouwelijke gegevens te vinden zijn binnen te komen.

83.3 Maatregelen

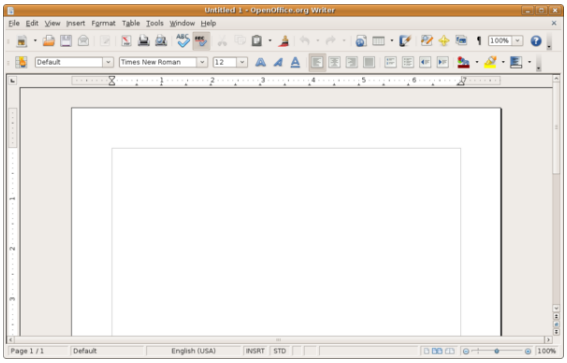
De belangrijkste maatregel tegen social engineering is het creëren van beveiligingsbewustzijn (security awareness). Daarbij is het enerzijds van belang de eindgebruikers te informeren over het belang van informatiebeveiliging en hen anderzijds te trainen op het herkennen van oneigenlijk gebruik.

83.4 Externe links

- Webwereld (2004) *Een wachtwoord in ruil voor een chocoladereep*
- Onderzoek naar lekken bij HP

Hoofdstuk 84

Software



OpenOffice.org Writer

Software of **programmatuur** is een gangbaar woord voor computerprogramma's. Naast toepassingen voor de mainframes, pc's en spelcomputers, bevatten ook apparaten als televisies, telefoons, telefooncentrales, auto's en machines sinds de jaren zeventig steeds vaker software.

Software kan worden ingedeeld naar toepassingsgebied of gebruikersgroep.

Het begrip “software” komt uit het Engels, en is de tegenhanger van hardware (apparatuur), waarmee alle “tastbare” apparatuur wordt bedoeld.

Het onderscheid tussen hardware en software bestond al voordat de computer bestond, al worden de termen in die zin niet vaak gebruikt. Een radiotoestel is hardware, het radioprogramma is software. Een grammofoon is hardware, de grammofoonplaat bevat software. Dit illustreert dat de hardware onbruikbaar is zonder software.

84.1 Privésoftware

Thuis op de pc of spelcomputer:

- Webbrowsers
- Computerspellen
- Educatieve software
- Audioprogrammatuur

84.2 Kantoorsoftware

Kantoorsoftwarepakketten bestaan vaak uit

- Tekstverwerker
- Spreadsheet
- Databaseprogramma
- Presentatiesoftware
- Projectplanning

Kantoorsoftware draait meestal op een computer. Bekende toepassingen zijn Microsoft Office en LibreOffice. Er kan ook een CAD-systeem in een kantoorpakket zitten.

84.3 Bedrijfssoftware

Bedrijfssoftware zijn grotere softwarepakketten, vaak voor meerdere gebruikers. Voorbeelden zijn:

- ERP-systeem Enterprise Resource Planning
- SCM-systeem Supply Chain Management
- CRM/EMM-systeem Customer Relationship Management / Enterprise Marketing Management
- HRM-systeem Human Resource Management
- Propriëtaire software, dit is vaak maatwerk, zoals het Elektronisch patiëntendossier, of de software van de belastingdienst, grote banken, industrie etc., software gemaakt voor een bedrijf. Voor technisch en wetenschappelijk onderzoek worden zeer specifieke toepassingen vaak binnen de organisatie zelf ontwikkeld.
- PDM-systeem Product Data Management
- EDM/ECM-systeem Enterprise Document / Content Management
- Praktijkmanagementsysteem voor artsen, tandartsen, apothekers en overige zorgverleners.

84.4 Systeemsoftware

Systeemsoftware wordt ook wel een besturingssysteem genoemd, met als bekende voorbeelden Windows, Macintosh en Unix. Dit zijn alle programma's die nodig zijn voor het functioneren van het systeem, bijvoorbeeld programma's om bestanden te kopiëren (*cp* of *copy*), te verwijderen (*rm* of *del*), mappen aan te maken en de inhoud van een bestandssysteem zichtbaar te maken (*ls* of *dir*). Typische onderdelen zijn BIOS, *device drivers*, *interrupt service routines*. Deze laag wordt ook wel *low level software* genoemd.

1. De kernel: deze implementeert alle diensten die voor het hele systeem beschikbaar (moeten) zijn zoals *multitasking*, geheugenbeheer en semaforen.
2. Programmabibliotheken met specifieke functionaliteit, zoals netwerkabstracties (bv. TCP/IP), implementaties van specifieke bestandssystemen, grafische routines en basisbibliotheken voor specifieke computertalen (libc, bijvoorbeeld).
3. Daemons, processen die weliswaar niet bij de kernel horen, maar wel noodzakelijk zijn voor het functioneren van het systeem zoals programmamanagers, printermanagers, windowmanagers en cronachtige programma's. Daemons worden (in de regel) door het systeem zelf gestart en zijn voortdurend actief.

- Netwerkprogrammatuur (bijvoorbeeld voor internet), FTP, NNTP- en IRC-servers en -cliënten.
- Om te kunnen werken hebben computers ten minste *firmware* nodig, bijvoorbeeld het BIOS van een pc, maar in de regel bevat een computer een grote verscheidenheid aan software. De uitzondering hierop is een embedded system, dat over het algemeen uitsluitend op *firmware* berust.

84.5 Hardwareplatform

De ontwikkeling van software is naarmate die dichter bij de hardware staat, nauwer verweven met het *platform* waarop het werkt. Op het allerlaagste niveau dient de ontwikkelaar van dit soort software op de hoogte te zijn van de werking van de hardware, terwijl het op het hoogste niveau vaak mogelijk is software zo te schrijven dat die op een groot aantal verschillende platforms kan worden gebruikt, door handig gebruik te maken van verschillende abstractielagen. Goede voorbeelden hiervan zijn Qt en de POSIX-standaard.

84.6 Realtimesoftware

Realtimesoftware geldt als een speciaal geval, waarin niet alleen het uiteindelijke resultaat, maar ook scherpe tijdsrestricties gelden. Voor alle software is van enig belang hoe snel de resultaten beschikbaar komen; in een tekstverwerker een paar minuten moeten wachten om naar een volgende pagina te bladeren, zou niet aanvaardbaar zijn. Zakelijke en administratieve software, alsook simulatie van wiskundige modellen worden echter niet als realtime beschouwd. Er is geen directe relatie met processen buiten het softwaresysteem. Over het algemeen wordt een onderscheid gemaakt tussen

- *Soft real time*, waarbij alleen een maximumresponstijd geldt, die afhankelijk is van de eisen; een voorbeeld is de navigatie- en doelzoeksoftware voor geleide wapens.
- *Hard real time*, waarbij het systeem 'deterministisch' moet zijn.

Hoewel vele realtimetoepassingen eveneens *embedded* zijn, zijn de twee begrippen geenszins equivalent.

84.7 Ingebouwde software

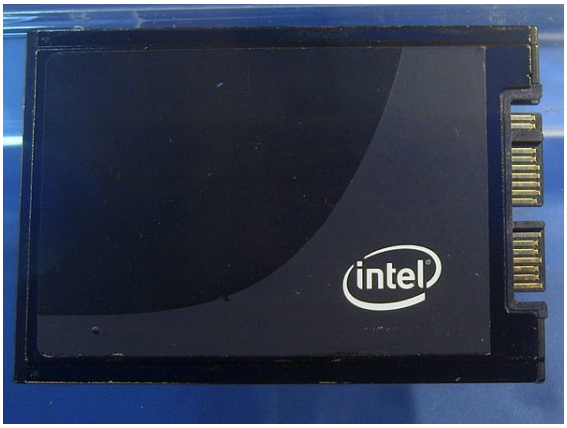
Ingebouwde oftewel Embedded software is software die is ingebouwd in apparaten, zoals auto's, (antiblokkeersysteem) thermostaten, televisies, camera's, mobiele telefoons, *Active Suspension*, navigatiesystemen, dataloggers, gps-cliënten, remote sensors, satellieten.

84.8 Zie ook

- Opensourcesoftware en vrije software zie een Lijst van opensourcesoftware
- Programmeren
- Changelog
- Testen
- Vapourware
- Applicatie-architectuur
- Grafische programmatuur
- Simulaties
- Sjoemelsoftware

Hoofdstuk 85

Solid state drive



Een prototype van een SSD

mSATA-SSD

Een **solid state drive**[1] of **solid state disk** (SSD) is een medium waarop digitaal gegevens bewaard kunnen worden met behulp van niet-vluchtig (zoals flash) of vluchtig geheugen (bijvoorbeeld SDRAM). SSD's worden voornamelijk gebruikt in computertoepassingen waar traditioneel een harde schijf gebruikt werd. SSD's staan bekend om hun korte zoek- en toegangstijd. Tegenwoordig hebben SSD's een toegangstijd van amper 0,1 milliseconde.

85.1 Snelheid

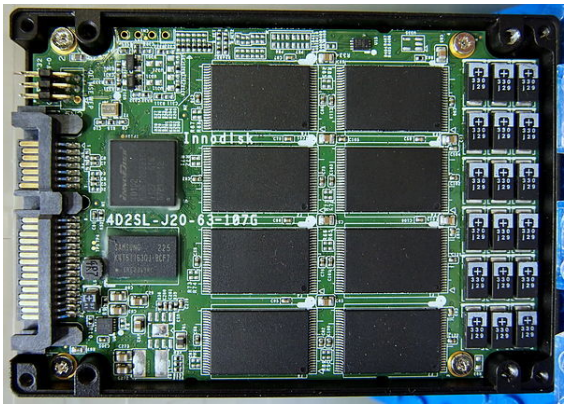
Kenmerkend aan solid state drives is dat er geen bewegende onderdelen gebruikt worden die wel in harde schijven te vinden zijn, zoals een roterende schijf of bewegende lees- en schrijfkoppen. Hierdoor treden er (weinig tot) geen mechanische fouten meer op en behoort het wachten op de schijf en het positioneren van de koppen tot het verleden. Gegevens kunnen - onafhankelijk van waar ze zijn opgeslagen - altijd even snel gevonden worden. Defragmenteren is niet meer nodig; bestanden die uit duizenden fragmenten bestaan worden nagenoeg net zo snel gelezen als een aaneengesloten bestand. Ook het wegschrijven van gegevens gaat veel sneller bij een SSD ten opzichte van een harde schijf. Er zitten vaak meerdere geheugenmodules in een SSD, die onafhankelijk van elkaar data kunnen wegschrijven.

Een SSD kan worden aangesloten via een SATA-aansluiting op een moederbord. Er zijn ook al SSD's die via PCI en PCI Express worden aangesloten op het moederbord. Deze kunnen nog hogere snelheden halen, maar zijn vaak ook duurder dan de via SATA aangesloten exemplaren. Ze zijn dan ook voornamelijk bedoeld voor bedrijven in plaats van consumenten.

Vanwege de hoge snelheden worden SSD's vaak als opstartschijf gebruikt, hierbij zet men het besturingssysteem op de SSD. Het voordeel hiervan is dat het besturingssysteem veel sneller opstart. Ook zware programma's die veel data nodig hebben om goed te werken, worden vaak op SSD's gezet. Een pc kan veel winst halen uit een SSD omdat de harde schijf meestal een bottleneck vormt voor een computer met recente hardware. Dit komt doordat de standaard draaisnelheid van harde schijven al jarenlang 7.200 RPM is. Er bestaan ook schijven van 10.000 of 15.000 RPM, maar ook deze zijn trager dan SSD's. Het is moeilijk om harde schijven nog sneller te maken door de rotatiesnelheid te verhogen, aangezien bij nog hogere draaisnelheden van de interne schijf er te grote krachten optreden die storingen kunnen opwekken. Het is wel mogelijk harde schijven op andere manieren sneller te maken, bijvoorbeeld door de datadichtheid (hoeveelheid gegevens per vierkante centimeter) te verhogen.

85.2 SSD intern

Een solid state drive wordt gebruikt voor opslag van gegevens. Daarvoor is geheugen nodig. Bij SSD's heeft men hiervoor de keuze uit twee soorten geheugens: DRAM en flashgeheugen.



Binnenkant SSD-loopwerk

85.2.1 DRAM

DRAM is hetzelfde soort geheugen als het geheugen dat als werkgeheugen (RAM) in een computer gebruikt wordt. Een op DRAM gebaseerde SSD is daardoor ook relatief eenvoudig te upgraden, namelijk door er modules in te steken die een grotere capaciteit hebben.

Het nadeel van DRAM-SSD's is dat ze ofwel een batterij ofwel een aparte stroomtoevoer nodig hebben, aangezien het geheugen vluchtig is. Zonder deze voorziening zou een DRAM-SSD bij het uitvallen van de stroom alle gegevens verliezen.

85.2.2 Flashgeheugen

SSD's met flashgeheugen zijn doorgaans trager dan SSD's met DRAM, maar ze zijn wel goedkoper.

Een SSD met flashgeheugen is opgebouwd uit:

- het flashgeheugen zelf: dit is voor de opslag van gegevens;
- een geheugencontroller: deze zorgt ervoor dat de SSD gegevens kan wegschrijven in of verwijderen van het flashgeheugen;
- cache: een SSD gebruikt hiervoor een kleine hoeveelheid DRAM. Dit verhoogt de prestaties van de SSD: gegevens kunnen gebufferd worden vóór ze door de geheugencontroller worden weggeschreven naar het flashgeheugen;
- een batterij: deze zorgt ervoor dat de SSD de gegevens die nog in de cache staan niet verliest als de computer per ongeluk uitvalt door een elektriciteitsstoring. De batterij zorgt er dan voor dat de data ofwel wordt weggeschreven ofwel wordt bewaard totdat er weer stroom is.

85.3 MLC versus SLC

Solid state drives zijn onder te verdelen in twee typen: SLC en MLC. Een SSD bestaat uit verschillende cellen. Iedere cel heeft een analoge waarde. Deze analoge waarde, doorgaans een lading, spanning of weerstand, wordt onderverdeeld om tot een digitale waarde te komen.

Bij Single-Level-Cell SSD's (SLC) wordt de analoge waarde van een cel verdeeld in twee bereiken: een hoog bereik en een laag bereik. Hierdoor slaat iedere cel effectief één bit op (0 of 1).

Bij Multi-Level-Cell SSD's (MLC) wordt de analoge waarde in meer bereiken verdeeld. Hierdoor worden effectief meer bits per cel opgeslagen. Met vier analoge waarden zijn dat twee bits per cel (00, 01, 10 of 11), met acht waarden zijn dat er drie (000, 001, 010, 011, 100, 101, 110 of 111) enzovoorts.

Dit verschil heeft tot gevolg dat SLC's betrouwbaarder, duurzamer en sneller zijn, terwijl MLC's juist als voordeel hebben dat ze data veel compacter kunnen opslaan. Hierdoor kunnen MLC's met dezelfde opslagcapaciteit goedkoper worden geproduceerd dan SLC's.[2]

85.4 TRIM

Wanneer SSD's veel gebruikt worden, worden ze trager. Bij het schrijven in eerder gebruikte ruimte moet dit gebied eerst gewist worden, en deze handeling kost extra tijd. Daarom heeft men een nieuwe technologie ontwikkeld die dit tegengaat, namelijk TRIM. TRIM zorgt ervoor dat het besturingssysteem zoekt naar gebieden op de SSD die niet meer gebruikt worden. Vervolgens krijgt de controller van de SSD opdracht om deze gebieden alvast te wissen, zodat er zonder vertraging weer op geschreven kan worden.

De recentste SSD's zijn bijna allemaal uitgerust met deze TRIM-functie. Het is aan te raden om bij aanschaf te kijken of een SSD deze technologie ondersteunt. Vóór TRIM was er wel al een alternatieve techniek die de SSD resette. Het nadeel hiervan was dat deze techniek alle data wiste die op de SSD stond, waardoor hij niet praktisch was om te gebruiken.

TRIM is geïntegreerd in de Linuxkernel vanaf versie 2.6.33, OS X vanaf versie 10.7 *Lion*[3] en bij Windows vanaf Windows 7 en vanaf Windows Server 2008 R2.

85.5 Voor- en nadelen

Dit zijn de voornaamste voor- en nadelen van een SSD ten opzichte van een harde schijf.

85.5.1 Voordelen

- Snelheid: een SSD heeft een zeer korte toegangstijd en zeer hoge lees- en schrijfsnelheid.
- Stilte: doordat een SSD geen bewegende onderdelen bevat, produceert een SSD geen geluid.
- Gewicht: een SSD is vele malen lichter dan een harde schijf.
- Zuiniger: een SSD heeft minder vermogen nodig om te werken dan een harde schijf.
- Koeler: geen bewegende onderdelen dus minder warmteproductie.

85.5.2 Nadelen

- Prijs: een SSD is (gerekend in prijs per gigabyte) nog steeds duurder dan een harde schijf (vroeger zelfs vele malen duurder).
- Degradatie (alleen voor flashgeheugens): na een aantal malen schrijven en wissen verliezen de cellen hun geheugencapaciteit. MLC's kunnen ongeveer 5000 keer beschreven worden. TRIM zorgt ervoor dat alle cellen ongeveer gelijk belast worden. Zo gaat de hele schijf langer mee.

Opgeloste nadelen:

- Capaciteit: de capaciteit van een SSD was lange tijd niet zo groot als die van een harde schijf. Met de introductie van 2TB-SSD's[4] en hoger, tot 32 TB,[5] is dit probleem echter opgelost.
- Verlies van snelheid: als geen maatregelen (zoals bijvoorbeeld TRIM) getroffen worden, wordt een SSD na veel herschrijven van data trager. TRIM wordt bij de meeste besturingssystemen standaard geactiveerd voor SSD's.

85.6 Toepassingen

Verwacht wordt dat SSD's langzaam de mechanische harde schijven zullen vervangen. SSD's die gebaseerd zijn op vluchtig geheugen zoals SDRAM worden gekenmerkt door snelle toegang. Er zijn SSD's met toegangstijden van minder dan 0,01 milliseconde; meer dan 400 keer zo snel als de snelste harde schijven met anno 2012 een toegangstijd van 4 milliseconden. Voor consumenten die een doorsnee SSD kopen ligt de toegangstijd rond de 0,1 milliseconde. Omdat de prijs per gigabyte opslagcapaciteit vooralsnog hoger is dan bij conventionele harde schijven wordt een SSD soms gecombineerd met een "gewone" harde schijf voor het opslaan van (grote hoeveelheden) data.

Solid state drives kunnen applicaties die in hun snelheid beperkt worden door beperkingen van de harde schijf versnellen. Ze worden ook gebruikt als "boot disk" (opstartschijf). Ook hier spelen de hogere lees- en schrijfsnelheden een rol.

Ook kunnen SSD's nuttig zijn in computers die al de maximum toegelaten hoeveelheid RAM gebruiken. Sommige x86-architecturen hebben bijvoorbeeld limieten van 4 GB aan RAM. Door gebruik te maken van een wisselbestand op een SSD kan dit probleem omzeild worden. Door beperkingen op de bandbreedte van de bus waarmee zo'n SSD met de rest van de computer verbonden is zal de SSD weliswaar niet de snelheid van het hoofdgeheugen halen, maar de snelheid blijft vele malen hoger dan wanneer het wisselbestand op een conventionele harde schijf zou staan. Dit komt echter de levensduur van de SSD niet ten goede, gezien het beperkte aantal schrijfcycli bij flashgeheugencellen.

Op DRAM gebaseerde SSD's kunnen ook als cache gebruikt worden. Wanneer data naar een harde schijf weggeschreven moet worden, zal het overeenkomstige blok als gewijzigd (jargon: *vuil* of *dirty*) gemarkeerd worden. Alle gewijzigde blokken kunnen dan naar de harde schijf gesynchroniseerd worden op basis van een van de volgende strategieën:

- tijd, bijvoorbeeld elke 10 seconden;
- drempel, wanneer het percentage gewijzigde blokken een bepaalde vooraf gedefinieerde waarde overschrijdt;
- een combinatie hiervan.

Eind 2011 werd de eerste supercomputer met 1024 SSD's in gebruik genomen, goed voor de 48e plaats in de top 50 van supercomputers.[6]

85.7 SSHD

Indien een solid state drive als flashgeheugen in één fysieke unit wordt gecombineerd met een mechanische harde schijf, spreekt men van een hybride schijf of solid state hybrid drive (SSHD). Het aanwezige, vaak kleine flashgeheugen wordt ingezet als cachegeheugen. De rest van de schijf wordt gevormd door de harde schijf, die vaak een hogere opslagcapaciteit heeft. Hierbij combineert men de snelheid van een SSD met een goedkopere en ruimere harde schijf.

85.8 Zie ook

- USB-stick
- Extern geheugen

Hoofdstuk 86

Spam (post)

Een mailbox gevuld met spam

Spam is een verzamelnaam voor ongewenste berichten en is ook bekend als **Unsolicited Commercial E-mail** en **Unsolicited Bulk E-mail**. Onder deze term vallen ongewenste e-mails en reclameboodschappen op websites (onder andere fora). Spam is moeilijk te definiëren. Niet ieder initiatief van een persoon of organisatie om contact te leggen is spam. Spam onderscheidt zich van andere vormen van commerciële communicatie, omdat een bericht wordt gestuurd aan een groep die veel groter is dan de potentiële doelgroep. Omdat deze afbakening te maken heeft met de proporties, zou je verwachten dat het moeilijk is om te bepalen of een bericht spam is. Vanwege de enorme schaal waarop *spammers* opereren is het in de meeste gevallen echter zeer duidelijk.

Kenmerken van spamberichten:

- Berichten worden in grote hoeveelheden verstuurd, naar duizenden mensen tegelijkertijd.
- Het spammen heeft een commercieel doel. Meestal bevatten de berichten daarom een verwijzing naar een product of website.
- De berichten worden verstuurd of geplaatst zonder toestemming of medeweten van de website, of de ontvanger.

De economische bestaansreden van spam is terug te vinden in de zeer lage kosten voor het versturen van e-mail of het plaatsen van een ongewenste reactie op een website. Een spammer kan rendabel miljoenen spamberichten versturen om slechts één product te verkopen. Het kost ongeveer 150 euro om 20 miljoen spamberichten te verzenden, dat zijn meer dan 100 000 spamberichten per euro.[1] Er is wereldwijd een levendige handel in bestanden met vele miljoenen e-mailadressen.

De kosten worden evenwel verplaatst naar de ontvangers: tegenover een kleine groep geïnteresseerden staan zeer veel mensen die tijd verliezen met het verwijderen van berichten uit hun mailbox.

86.1 Ergernissen

Veel internetgebruikers ergeren zich aan spam. Het verwijderen van die berichten kost veel tijd. Wereldwijd veroorzaakt spam enorme schade, onder meer bij Internet Service Providers. De ergernis is onder Amerikanen wel enigszins afgenomen, zo constateert onderzoeksbureau Pew Research Center in 2007. Slechts 18 procent van de ondervraagden beschouwt spam als een groot probleem. In 2003 was dat nog 25 procent.

86.2 Geschiedenis

De eerste bekende spam werd verstuurd op 3 mei 1978. Het was een bericht van het toenmalige Digital Equipment Corporation (DEC, overgenomen door Compaq en nu een onderdeel van Hewlett-Packard). Marketingmedewerker Gary Thuerk stuurde een aankondiging van een 'open huis', naar aanleiding van de lancering van nieuwe modellen DEC-20-computers, naar iedereen op het toenmalige ARPANET aan de westkust van de Verenigde Staten.

86.2.1 Etymologie

Oorspronkelijk was spam de merknaam van een bepaald soort ingeblikt vlees dat nog steeds bestaat en dat in Nederland bekendstaat onder de naam Smac. De Britse komieken van Monty Python gebruikten het in een sketch om het toen actuele verbod op 'unsolicited advertising' (sluikreclame) op televisie aan de kaak te stellen. In een lunchroom waar aan alle gerechten ongevraagd spam

werd toegevoegd, en waarin een groepje Vikingen uit volle borst zingt: "*Spam spam spam spam. Lovely spam! Wonderful spam!*", werd normale conversatie door de spam-zangers vrijwel onmogelijk gemaakt, net als bij ongevraagde e-mail. Ook bij de aftiteling werd te pas en te onpas het woordje “spam” vermeld. Monty Python liet daarmee zien dat de wellicht wenselijke restricties aan reclame-uitingen op gespannen voet staan met het recht op vrije meningsuiting. In de latere e-mail-spamdebatten deden e-mailmarketeers ook vaak een beroep op het recht op vrije meningsuiting.

Wikipedia spamfilter

Als tegenhanger van de bekende term *spam* wordt sinds kort in kleine kring de term *ham* gebruikt. Dit is de *goede kwaliteit* vlees als tegenhanger van de *slechte kwaliteit* van spam. *Ham* is alle e-mail die geen *spam* is. Het is niet noodzakelijkerwijs e-mail die de ontvanger wil ontvangen of waar de ontvanger om gevraagd heeft. Deze term wordt op dit moment in diverse spamfilterpakketten toegepast, veelal bij een techniek waarbij de ontvanger onderscheid kan maken tussen ham en spam om de filter zelflerend te maken.

SPAM is een geregistreerd handelsmerk van Hormel Foods Corporation, maar het woord *spam* is zo gebruikelijk geworden dat het niet langer door het merkenrecht beschermd wordt.

86.3 Maatregelen tegen spam

86.3.1 Politiek en spam

De politieke strijd voor het verbieden van spam wordt tegengewerkt door directmarketing-bedrijven, die een commercieel belang hebben bij het verzenden van reclame per e-mail. Langzaam maar zeker is ook bij deze beroepsgroep een omslag waar te nemen en groeit het besef dat alleen reclame die op verzoek van de ontvanger wordt toegestuurd (opt-in) aanvaardbaar is. Deze vorm van reclame is overigens gemakkelijk te vermijden doordat deze bedrijven hun afzenderadres niet verbergen. Men kan dus programmatuur installeren om op dit afzenderadres te filteren.

Inmiddels is een Europese richtlijn aangenomen die spam moet tegengaan: “Het gebruik van automatische oproepsystemen zonder menselijke tussenkomst (automatische oproepapparaten), fax of e-mail met het oog op direct marketing kan alleen worden toegestaan met betrekking tot abonnees die daarin vooraf hebben toegestemd.” (richtlijn 2002/58/EG d.d. 12 juli 2002, artikel 13, lid 1). Ter implementatie van deze richtlijn in Nederlandse wetgeving is een ontwerpwetsvoorstel gereed. Dit is in februari 2011 voor advies aan de Raad van State voorgelegd. Daarin wordt een regeling getroffen die communicatie voor directmarketingdoeleinden via e-mail onderwerpt aan het opt-insysteem.

Ondertussen krijgt het spamprobleem weinig aandacht in de Nederlandse politiek. Bij de Tweede Kamerverkiezingen van januari 2003 was op de website van slechts twee van de grote partijen iets over het thema spam te vinden:

- GroenLinks “kiest voor opt-in en tegen spam”
- De SP wil dat Internet Service Providers “hun mailservers zo inrichten dat gebruikers zo veel mogelijk gevrijwaard blijven van ongevraagde commerciële e-mail ('spam') en e-mailbommen.”

Over het spamstandpunt van CDA, VVD, PvdA, LPF en D66 was op de website niets te vinden.

Op 20 april 2004 nam de Eerste Kamer een wet aan die het versturen van spam binnen Nederland verbiedt. De wet was een initiatief van minister Brinkhorst van Economische Zaken en brengt de Nederlandse situatie in overeenstemming met een Europese richtlijn. Deze aanpassingen in de Telecommunicatiewet 1998 werden op 19 mei 2004 actief. OPTA zal zorgen voor de handhaving van de wet en mag boetes opleggen. Helaas komt de meeste spam uit het buitenland, waar de Nederlandse wet niet van toepassing is.

Een aantal anti-spamorganisaties, zoals Spamvrij.nl, vonden de wet niet ver genoeg gaan omdat deze alleen consumenten beschermt; aan bedrijven mag wel spam gestuurd worden. Daarnaast trokken ze de kwaliteiten van OPTA voor deze taak in twijfel.

86.3.2 OPTA-acties

Artikel 11.7 Telecommunicatiewet, door juristen aangeduid als het *spamverbod*, schrijft voor dat bedrijven slechts reclame mogen sturen als de klant hier zelf om heeft gevraagd (opt-in). Het mag niet zo zijn dat alleen middels een actie van de klant (bijvoorbeeld door het wegklikken van een al aangevinkt vierkantje) er geen reclame wordt toegestuurd. De klant moet via een actieve handeling (bijvoorbeeld het aanklikken van een nog niet aangevinkt vierkantje) zelf om het toezenden van de reclame vragen. Bestaande klanten die informatie ontvangen moeten kosteloos kunnen aangeven dat ze dit niet meer willen (opt-out). Ook moet de afzender duidelijk aangeven dat het bericht van hem komt. OPTA is bevoegd boetes op te leggen met een maximum van € 450 000.

Op 28 december 2004 legde de OPTA in Nederland de eerste boetes op aan de verzenders van spam, waaronder de hoogste 42 500 euro bedroeg aan iemand die vier

verzendingen had uitgevoerd. Hij had onder andere spam verstuurd waarin werd opgeroepen medicijnen te kopen. Verder was het boek Mein Kampf aangeprezen met gebruik van de naam van spambestrijder Rejo Zenger.

Een ander bedrijf kreeg een boete van 25.000 euro opgelegd voor het verzenden van mail uit naam van 'Tekstbureau voor Marketingteksten'.

De Stichting Yellow Monday, die gebruikmaakte van de naam 'Purple Friday' kreeg een boete van 20.000 euro voor het versturen van spam per sms, waardoor de ontvanger zonder toestemming gegeven te hebben 1,10 euro per bericht moest betalen.

86.3.3 Samenwerking

Spam is een wereldwijd, grensoverschrijdend probleem. Dat heeft men door; binnen de grenzen van de Europese Unie wordt er al op meerdere vlakken samengewerkt door verschillende landen, waar het CNIL-protocol en de Telecommunicatiewet voorbeelden van zijn. Zo deelt men informatie over de locatie van spammers om deze vervolgens op te kunnen pakken. De samenwerking verloopt echter nog niet optimaal. Door grote verschillen in het vervolgen van spammers en de prioriteitenstelling van landen in de opsporing van spammers ontstaat er een gat in de spamdefensie binnen Europa. Samenwerking vanuit Europa met landen waarvandaan veel spam wordt verstuurd zoals de Verenigde Staten, Zuid-Korea, Rusland en China is er nauwelijks.

86.3.4 Technische maatregelen

Technische maatregelen tegen spam bestaan uit:

- *greylisting*, een techniek om een bepaalde klasse servers te blokkeren;
- *blacklisting*, het blokkeren van bekende servers van spammers; en
- het filteren van inkomende e-mail.

Spammers wapenen zich tegen deze maatregelen door zeer veel verschillende servers te gebruiken en door allerlei kenmerken van de e-mail te manipuleren. Het afzenderadres is vaak vervalst, zodat reageren op spam geen zin heeft. De ontvanger merkt dit vaak doordat hij op hetzelfde moment een aantal berichten ontvangt die vrijwel (meestal net niet helemaal) gelijkluidend zijn en die van verschillende afzenders afkomstig lijken te zijn.

86.3.5 Opt out?

Wanneer een spambericht met een periodiek karakter de ontvanger de mogelijkheid biedt aan te geven dat hij het periodiek niet meer wil ontvangen, dan wordt gesproken van een opt-outsysteem. De afmeldmogelijkheid is in de praktijk echter onbetrouwbaar. Sommige spammers zien de afmelding als een bevestiging dat het e-mailadres actief gebruikt wordt, waardoor het op de adresmarkt in waarde stijgt en nog meer spam naar dat adres gestuurd zal worden.

Ontvangt u spam van een bekende afzender, bijvoorbeeld van een postorderbedrijf waar u wel eens iets besteld heeft, dan is de afmeldmogelijkheid waarschijnlijk wel betrouwbaar. In de VS bestaat de **can spam act**, die de afzender verplicht bij een opt-out de opt-out **binnen 10 dagen** uit te voeren. Op niet-nakoming daarvan staan hoge geldboetes en gevangenisstraffen.

86.3.6 Het verbergen van e-mailadressen

Om iemand te kunnen spammen heeft men e-mailadressen nodig. Om deze te verkrijgen is er onder andere software beschikbaar die op fora en op websites gaat zoeken naar e-mailadressen.

Het is daarom niet wenselijk om een eigen e-mailadres in ongewijzigde vorm te publiceren via een bericht op usenet of op een website. Het is zeker aanbevolen hierbij grote voorzichtigheid in acht te nemen wanneer het gaat om adressen van derden, zodat deze personen niet onnodig veel spam zouden ontvangen.

Men kan toch zijn e-mailadres publiceren met een aanzienlijk lagere kans op spamming, en wel door het e-mailadres te vervormen. Als stelregel geldt hierbij dat hoe meer de tekst afwijkt van een e-mailadres, hoe kleiner de kans op spam wordt. Het is al lang niet voldoende meer “NOSPAM” in het e-mailadres te plaatsen, of het @-symbool te vervangen door “AT”. Een aantal mogelijkheden:

- voornaam.naam@isp.VERWIJDER_DIT.com
- De eenvoudigste en bekendste wijze is het @-symbool vervangen door de letters AT (zelfde uitspraak, ander teken), of een andere benaming, of "(AT)", "*AT*", enz. Men hoopt dat iemand die 'voornaam.naam AT isp.com' ziet staan zal begrijpen dat het 'voornaam.naam@isp.com' is. Eventueel kan ook een afbeelding van een @-symbool gebruikt worden.
- het gebruik van JavaScript waarbij het e-mailadres in code verstopt wordt. Zo <SCRIPT TYPE="text/javascript"> document.write('naam@' + 'isp.com') </SCRIPT> (mits JavaScript aan staat) gelezen als naam@isp.com.

Gebruik altijd een adres dat niet zou kunnen bestaan, anders loopt u het risico anderen te duperen. De DNS-standaard schrijft hiertoe voor een adres te gebruiken dat

op ".invalid" eindigt. De vraag is echter of goedwillende gebruikers zullen begrijpen dat dit deel van het adres moet worden verwijderd. Een mogelijke oplossing is een patroon als:

- **naam@isp.com.verwijder.invalid**

Bij al deze vervormde adressen moet worden aangetekend dat spammers er wellicht vroeg of laat toe over gaan de vervormingen automatisch te herkennen en te 'decoderen'. Het softwarematig herkennen en verwijderen van het woordje 'invalid' is wel heel eenvoudig.

86.3.7 Gebruik van BCC

Om e-mailadressen niet onnodig te verspreiden, wordt aangeraden om e-mails bestemd voor een grote hoeveelheid ontvangers aan zichzelf te adresseren en de eigenlijke ontvangers alleen in het BCC-veld op te nemen. Die ontvangen dan een zo genoemde blindkopie (BCC, blind carbon copy). De adressen in het BCC-veld zijn voor de ontvangers niet zichtbaar.

Veel mensen ontvangen kettingbrieven die ze aan zo veel mogelijk vrienden doorsturen. Daarbij vermelden ze niet alleen de adressen van alle geadresseerden, maar bovendien citeren ze het volledige bericht, inclusief de adressen van de vorige generaties. Een dergelijk bericht is een goudmijn voor een spammer.

86.3.8 Meer maatregelen om zelf spam te voorkomen of te bestrijden

Het is raadzaam om voorzichtig om te gaan met e-mailadressen, maar toch is het onmogelijk om vrij te blijven van spam.

Een spamfilter is daarvoor een van de technische mogelijkheden. Deze filters bestaan zowel voor e-mailprogramma's, zoals Outlook (Express) of Thunderbird, als voor mailservers. Tegenwoordig installeren veel providers spamfilters op hun servers.

Spamfilters zijn grofweg op te delen in 2 soorten. De eerste categorie probeert aan de hand van kenmerken spam te herkennen. Een bericht wordt gescand op die kenmerken en krijgt aan de hand daarvan een aantal punten. Als het aantal punten hoger ligt dan een bepaalde drempelwaarde zal het bericht als spam worden gemarkeerd en bijvoorbeeld alvast in de map verwijderde berichten worden gezet. Meestal kan de gebruiker zelf bepalen wat diegene met het bericht wil doen. Mogelijke kenmerken zijn woordenlijsten met spamkernwoorden, maar ook het vaststellen of de e-mailadressen aan bepaalde regels voldoen. Tot slot wordt er vaak gebruikgemaakt van zwarte lijsten.

De tweede categorie kiest voor een statistische benadering (vaak Bayesiaans). Deze filters zijn zeer nauwkeurig en hebben een zeer klein aantal valse positieven, maar moeten wel getraind worden. De gebruiker moet zelf honderden berichten verzamelen en aangeven of deze spam of ham (het tegenovergestelde van spam) zijn.

Moderne filters combineren vaak verschillende technieken.

Een spamfilter gooit zelden een bericht weg. Uit vrees voor een valse positief worden de berichten op een of andere manier als spam gemarkeerd en naar de geadresseerde gestuurd. De overlast blijft dus.

Die markering bestaat soms uit een toevoeging aan de onderwerpregel. Blijkt het bericht geen spam te zijn en wilt u het beantwoorden, dan moet u deze toevoeging handmatig verwijderen. Sorteert uw mailprogramma de berichten op onderwerp, dan wordt deze sortering door een dergelijke toevoeging onmogelijk gemaakt.

Andere spamfilters voegen in de body van het bericht een melding toe, zoals "dit bericht is gecontroleerd en in orde bevonden". Dergelijke meldingen worden soms al door slimme spammers toegevoegd voordat ze het bericht versturen.

Ook een interessante manier van spambestrijding is het gebruik van de zogenaamde boxtrapper. Bij dit systeem wordt elke nieuwe afzender eenmalig verplicht om zijn/haar e-mailadres te verifiëren door het beantwoorden van een controle-e-mail of het bezoeken van een speciale webpagina. Doet een afzender dit niet, dan zal de mailserver alle post van de afzender weigeren. Omdat spammers vrijwel altijd gebruikmaken van een vals afzendadres, wordt vrijwel alle spam in de kiem gesmoord. Ondanks de bijna waterdichte werking worden boxtrappers nog weinig toegepast, voornamelijk omdat ze (vanuit het standpunt van de afzender) als gebruiksonvriendelijk te boek staan.

Nadeel van boxtrapping is dat het niet werkt bij automatisch ontvangen berichten. Het komt vaak voor dat men zijn gegevens op een website moet invoeren en dat de website ter controle een e-mail stuurt waarop u moet reageren. Een dergelijk bericht wordt door de boxtrapper geblokkeerd, en het controlebericht, dat naar de afzender gaat, wordt niet gelezen.

Verder leert de praktijk dat veel mensen wel een e-mail kunnen versturen, maar niet weten te reageren op het controlebericht, bijvoorbeeld omdat het in het Engels is gesteld. De kans is trouwens niet denkbeeldig dat het controlebericht zelf door een spamfilter wordt opgevangen.

Als iemand met een boxtrapper zelf een bericht stuurt naar iemand die ook een boxtrapper gebruikt, dan resulteert dat in eindeloos heen-en-weer sturen van controle-e-mails tussen de boxtrappers.

Een andere ontwikkeling is ingezet door Yahoo!. Dit internetbedrijf heeft een techniek ontwikkeld genaamd domain keys. Deze techniek is strikt genomen geen antispammethode, maar een manier om te kunnen verifiëren

of de afzender inderdaad de afzender is. Op het moment dat er voldoende gebruikers zijn is dat een goede discriminerende factor tegen spam, omdat spammers vaak gebruikmaken van valse e-mailadressen.

Er bestaan commerciële websites om wenskaarten te versturen. Ze zijn populair met verjaardagen en in de tijd van Kerstmis. De verzender typt zijn eigen e-mailadres en het adres van zijn vrienden op de website. Zodoende springt hij niet alleen met zijn eigen adres, maar ook met het adres van anderen onzorgvuldig om. De ontvanger krijgt een e-mail met de boodschap dat hij de wenskaart op de website van de exploitant kan vinden. Klikt hij daarop om de webpagina te openen, dan weet de exploitant van de website dat het e-mailadres geldig is. Het advies is dus: gebruik geen website om iemand gelukwensen te sturen en als je zo'n gelukwens ontvangt, bedwing dan je nieuwsgierigheid en open de webpagina niet.

Om spam via e-mail te voorkomen worden ook wegwerp-e-mailadressen gebruikt.

Het is raadzaam om bij het bestrijden van spam een actieve houding aan te nemen en de spamberichten die u ontvangt te rapporteren bij diverse onlinediensten zoals SpamCop. Dit heeft een aantal voordelen, het helpt onder andere om spamfilters en blocklijsten up-to-date te houden waar anderen weer van kunnen profiteren doordat hetzelfde spambericht op dat moment bekend is en gefilterd kan worden. Daarnaast zullen spammers merken dat berichten die naar uw adres gestuurd worden gerapporteerd worden en zullen ze voortaan uw e-mailadres vermijden, waardoor de hoeveelheid spam in uw mailbox afneemt.

86.4 Nieuwe vormen van spam

Recent lijkt er een evolutie ingezet waarin spam niet enkel voorkomt in e-mails (of nieuwsgroepen), maar in verscheidene internettoepassingen, waaronder het web. Een populair doelwit lijken internetfora te zijn. Naast het gewoonlijke doel van spam om ongevraagd reclame te maken, heeft spam op het web vaak een extra doel: doordat de spam op veel websites gekopieerd wordt, verwijzen er veel links naar de website van de spammer, waardoor deze website in de rankings van zoekmachines stijgt, zie ook Googlebom.

Spammen op het web is omslachtiger dan via e-mail (of in nieuwsgroepen). Om spam via e-mail te versturen volstaat het de e-mailadressen van de slachtoffers te kennen. Om op het web te kunnen spammen, dient men naast de websites van de slachtoffers ook een bug op de website te kennen zodat men spam op de website kan toevoegen.

Een werkwijze die gevolgd wordt om op het web te spammen is dat men met een bot een zoekmachine scant naar een populair computerprogramma met een bekende bug. Als de bot een website met het programma gevonden heeft, exploiteert de bot de bug.

Een veelvoorkomend voorbeeld is dat nieuwe gebruikers op internetfora aangemaakt worden en dat deze gebruikers een spambericht in hun handtekening hebben en/of een spambericht op het forum posten. Doorgaans blijven er meer spamberichten achter naarmate het minder duidelijk is dat het om spam gaat.

Een voorbeeld van een dergelijke onduidelijke spam die veel (nietszeggende) berichten heeft nagelaten is de aanmaak van de gebruiker “Ninel2006aZ” op talloze phpBB-internetfora. Deze spam lijkt begonnen te zijn op 2 augustus 2006. De bot lijkt op zoek te zijn gegaan naar websites die een al dan niet gemodificeerde versie van het phpBB-internetforum hosten met de zoekstring “options html is off bbcode is on smilies are on” in een of andere zoekmachine. Op 13 augustus 2006, 6 uur 10 CET geeft de zoekstring “Ninel2006aZ” 324000 resultaten in Google terwijl de zoekstring “Ninel2006aZ PHPBB” 267000 resultaten weergeeft.

Dit voorbeeld lijkt een gecoördineerde aanval op het PHPBB te zijn geweest, waarbij er gedurende 10 dagen ongeveer 20 nieuwe accounts per minuut op verschillende phpBB-fora werden aangemaakt. Deze aanval ging gepaard met andere aanvallen op de PHPBB-fora, maar andere aanvallen zijn doorgaans duidelijker spam en veroorzaken ook minder blijvende Google-hits. Het grote aantal hits (in een zoekmachine) van dit voorbeeld illustreert de impact van een nieuw fenomeen van “www-spammen”.

Sterk in opkomst is aandelenspam, waarin gebruikers worden aangemoedigd om een bepaald aandeel te kopen, zodat de koers stijgt. De verzender van de spam heeft vooraf al een grote hoeveelheid van dat fonds ingeslagen.

86.5 Zie ook

- CAN-SPAM Act of 2003
- DNSBL - een systeem waarbij mailservers die een bron van spam zijn of kunnen zijn in een blacklist plaatsen
- E-mailmarketing is een verzamelnaam voor zowel spam als andere commerciële boodschappen.
- Shell account
- Spambot
- Spamkoning
- Spim (ongewenste berichten via instant messaging), scam en phishing (oplichting, of poging tot oplichting via e-mail).

86.6 Externe links

- Het officiële aangifteloket van E-cops (België): ecops.be

- Het officiële aangifteloket van OPTA (Nederland):
  spamklacht.nl

Hoofdstuk 87

Spamfilter

"spam"filter

Een **spamfilter** is een stuk software dat spam en computervirussen probeert te herkennen en te verwijderen uit een set e-mails. Normaal gezien leest een spamfilter de e-mail in, besluit of het spam is, en zal op basis daarvan besluiten actie nemen.

Spamfilters worden vaak gebruikt door de ontvanger in combinatie met een e-mailclient, of door de internetprovider direct op de mailserver.

Bekende spamfilters zijn K9 en SpamAssassin. Voor de zakelijke markt zijn Proofpoint, Cisco en Microsoft de grootste spelers.

Een spamfilter is een type mailfilter. Mailfilters kunnen ook voor andere doeleinden dan het herkennen van spam gebruikt worden, bijvoorbeeld het automatisch sorteren van e-mails in bepaalde mappen, of het zoeken naar illegale activiteiten.

Doordat het filters zijn is het onvermijdelijk dat een spamfilter te veel (fout-positief) of te weinig (fout-negatief) filtert.

87.1 Beoordeling

In zijn eenvoudigste vorm is spamfilteren een voorbeeld van automatische tekstclassificatie: binnenkomende e-mailteksten worden geanalyseerd en geclassificeerd als "spam" of "normaal".

Spamfilters werken doordat zij in de e-mails bepaalde patronen herkennen. Enkele voorbeelden zijn:

- Woorden die vaak in spam voorkomen, zoals 'Viagra' en 'Sex'. Vooral als deze termen in het onderwerpveld voorkomen, is het bericht verdacht.
- Een bijlage met een dubbele extensie waarin een rij spaties voorkomt, zoals **Leuke mop.txt .exe**. De afzender hoopt dat de ontvanger denkt dat het een onschuldig txt-bestand is, terwijl het in werkelijkheid een exe-bestand is.
- Een groot aantal berichten die vrijwel gelijkluidend zijn maar verschillende afzenders hebben. Dit werkt vooral goed als het spamfilter bij de internetprovider geplaatst is, omdat daar veel berichten vergeleken kunnen worden.

Geavanceerdere spamfilters maken gebruik van een bayesiaans netwerk, waarbij de gebruiker van een aantal e-mails aangeeft of ze als spam beschouwd moeten worden. Het filter probeert hier dan uit te 'leren' welke eigenschappen van de e-mails vooral bij spam voorkomen, en welke niet. Op basis hiervan zal de software de e-mails filteren. Het nadeel hiervan is dat het filter in het begin nog niet zo secuur zal zijn, doordat het nog in de leerfase is. Om dit te ondervangen kunnen bedrijven softwaresystemen voor e-mailmanagement inzetten die naast spamfilterfunctionaliteit ook grote hoeveelheden e-mail automatisch kunnen sorteren en verwerken.

87.2 Actie

Wordt een bericht als spam herkend, dan zijn er verschillende mogelijkheden:

- Het bericht komt in een aparte map, hetzij in de e-mailclient, hetzij op de website van de provider. In het laatste geval komt het bericht niet in de POP-box van de ontvanger, maar de ontvanger kan op de website aangeven dat hij het bericht tóch wenst te ontvangen.
- Het bericht wordt voorzien van een waarschuwing in de onderwerpregel. Die waarschuwing luidt meestal **{SPAM!!}**, **[SPAM]** of iets dergelijks.
- Het bericht wordt ongemerkt verwijderd.
- De bijlage wordt verwijderd en de ontvanger krijgt daarvan een melding.
- De bijlage wordt zonder melding verwijderd.

Meestal heeft de ontvanger de mogelijkheid bepaalde berichten of afzenders als veilig te markeren. Meldt hij bijvoorbeeld dat mail van een bepaalde afzender betrouwbaar is, dan zal het spamfilter die berichten ongemoeid laten.

87.3 Bezwaren

Bijna alle internetproviders passen spamfilters toe. Dit staat lijnrecht tegenover het beleid bij de papieren post, waar het bij wet streng verboden is iets aan een poststuk te veranderen. Het is dan ook niet verwonderlijk dat ontvangers van e-mail zich ergeren aan de fout-positieve gevallen (*false positives*), waarbij een normaal bericht door de provider als spam wordt gefilterd en tegengehouden.

87.4 Zie ook

- Greylisting, een techniek om spam te weren voordat het de mailserver bereikt

Hoofdstuk 88

Spoofing

Spoofing is het vervalsen van kenmerken met als doel om tijdelijk een valse identiteit aan te nemen. Dit kan bijvoorbeeld gaan om e-mail, website, IP-adres en biometrische kenmerken.

88.1 E-mail spoofing

E-mail spoofing is een term die gebruikt wordt om frauduleuze e-mailactiviteiten te beschrijven. Deze activiteiten houden in dat specifieke eigenschappen van het e-mailbericht, zoals *From* (Van), *Return-Path* (Afzender) en *Reply-To* (Antwoorden naar) worden gewijzigd. Hierdoor lijkt het alsof de e-mail afkomstig is van een andere bron. E-mail spoofing is een veelgebruikte techniek voor het versturen van spam.

Ook zijn er computervirussen die e-mail spoofing gebruiken om zichzelf te verspreiden. Het virus gebruikt een ander adres dat het op de geïnfecteerde computer heeft aangetroffen als afzender. In sommige gevallen maakt het virus ook zelf een e-mailadres aan. Yaha.E is niet het eerste virus dat de afzender vervalst. Het Klez.H-virus deed dat zelfs structureel en is daardoor tot op heden lastig te bestrijden. Mensen van wie de computer geïnfecteerd is, kunnen moeilijk worden gewaarschuwd, omdat hun e-mailadres voor de meeste ontvangers onbekend is.

88.2 Website spoofing

Website spoofing is het nabootsen van een bestaande, algemeen bekende website met de bedoeling om kritiek te uiten op de organisatie achter de originele website. In werkelijkheid wordt het geleid door eindgebruikers met bijvoorbeeld frauduleuze bedoelingen (phishing).

88.2.1 URL-spoofing

Is het nabootsen van een bestaande URL, zodat de gebruiker denkt de echte site te bezoeken, terwijl de URL die van een bedrieger is. Het nabootsen kan bestaan uit spelfouten in het webadres, of het gebruik van letters uit een andere taal die lijken op die van het oorspronkelijke adres. De gebruiker wordt in de meeste gevallen naar de valse website gelokt via een e-mail of een hyperlink op een andere website. Het komt ook voor dat een website eruitziet als het origineel, maar dat het een parodie betreft. Deze zijn meestal onschuldig, omdat deze zichtbaar verschillen van de originele website.

88.3 Andere vormen van spoofing

Naast het “spoofen” van een e-mailadres of website is een soortgelijke truc ook mogelijk met IP-adressen. Hierbij kan een aanvaller het IP-adres van iemand anders aannemen. Deze techniek is op internet echter alleen in zeer uitzonderlijke situaties toe te passen en wordt daarom bijna nooit gebruikt (IP-spoofing).

88.4 Externe link

- (en) Meer informatie over IP spoofing

Hoofdstuk 89

Spyware

Spyware is de naam voor computerprogramma's (of delen daarvan) die informatie vergaren over een computergebruiker en deze doorsturen naar een externe partij. Het doel van spyware is meestal om geld te verdienen. De term komt van het Engelse woord *spy*, dat spion betekent, en het achtervoegsel *ware*, dat aangeeft dat het om software gaat.

De opkomst van spyware is mede het gevolg van het illegaal kopiëren van software. De programmamakers zoeken, nu ze minder inkomsten uit verkopen halen, naar andere manieren om geld te verdienen. Het toevoegen van spyware aan een programma is een manier. Zo zijn er bijvoorbeeld twee versies van het peer-to-peerprogramma Kazaa: het ene kost geld, het andere bevat spyware. Naast deze commerciële vorm van spyware bestaat er ook een vorm met meer criminele doeleinden.

Meestal weten gebruikers niets van de spywarefunctie van een programma. Er zijn echter varianten waarbij gebruikers wel over de spywarefunctionaliteiten ingelicht worden. Vaak vindt dit dan op een listige wijze in de algemene voorwaarden plaats. Detectieprogramma's kunnen gebruikt worden om de spyware na installatie te ontdekken en eventueel te verwijderen. Deze werking is anders dan bij virusscanners. Deze voorkomen namelijk de installatie van ongewenste programma's. Men moet wel oppassen voor slechte, valse en malafide spywaredetectieprogramma's. Een aantal van deze programma's werkt slecht of probeert de gebruiker aan te zetten tot het kopen van een betaalde variant, ofwel door middel van het geven van valse positieven, ofwel door zelf spyware of adware te installeren.

Spyware is een van de grootste gevaren geworden voor computers waarop Windows gebruikt wordt. Dit geldt speciaal voor gebruikers van Internet Explorer, vanwege de nauwe integratie van deze webbrowser met het Windows-besturingssysteem.

89.1 Malwarevarianten

Spyware mag niet verward worden met andere soorten *malware*, ook al zijn er vaak wel bepaalde overlappingen. Het specifieke aan spyware is dat het gaat om spioneren: het aftappen van gegevens. Meestal wordt de informatie gebruikt voor reclamedoeleinden.

Adware laat reclameboodschappen aan de gebruiker zien. Deze kunnen door middel van spyware op de gebruiker afgestemd zijn, maar dat is niet altijd het geval. Adware bevat dus soms spywarefunctionaliteit maar niet altijd.

Ook phishing is anders dan spyware. Door misleidende informatie proberen de phishers de gebruikers te laten geloven dat ze de website van een bedrijf (bijvoorbeeld een bank) bezoeken, terwijl het in werkelijkheid een vervalste webpagina betreft. Vervolgens vragen de phishers of de gebruikers gegevens aan hen willen verstrekken. Deze werkwijze is dus anders dan bij spyware.

Een Trojaans paard is software die, zonder medeweten van de gebruiker, op zijn computer geïnstalleerd wordt en op die computer handelingen kan gaan verrichten. De handelingen die verricht worden, worden door het programma zelf aangestuurd. Deze handelingen kunnen onder andere bestaan uit het aanrichten van schade. Deze malwarevariant doet dus meer dan enkel gegevens vergaren.

Een keylogger registreert toetsaanslagen op een computer en kan de vergaarde gegevens doorsturen naar een andere computer. Dit is vaak een vorm van spyware.

Een autodialer is een programma dat automatisch het inbelnummer op een computer verandert. Vaak wordt dit veranderd in een nummer waarvoor een hoog bedrag per minuut betaald moet worden. Dit is geen spyware omdat het geen gegevens verzamelt.

89.2 Spyware en virussen

Spywareprogramma's lijken in zekere zin op computervirussen. Beide worden geïnstalleerd zonder dat de gebruiker daar weet van heeft en beide hebben nadelige gevolgen voor de gebruiker. Ook veroorzaken ze vaak instabiliteit van het besturingssysteem. Maar er zijn toch wat verschillen.

Een virus kopieert zichzelf; het zal proberen andere computers te infecteren. Spyware kopieert zichzelf in het algemeen niet. Virussen verspreiden zichzelf (met hulp van

computergebruikers die onvoorzichtig met hun computer omgaan) op een zo onopvallend mogelijke manier om niet ontdekt te worden. Spyware wordt verspreid door programma's juist duidelijk aan te prijzen, zodat ze door onwetende gebruikers worden uitgevoerd.

Spyware installeert zichzelf op zo'n manier dat het steeds mee opstart als de computer gestart wordt, waarbij het processortijd en geheugen gebruikt en het systeem instabiel kan maken.

Spywareprogramma's kunnen bijvoorbeeld bijhouden welke websites er worden bezocht, welke e-mails worden verstuurd, welke programma's geïnstalleerd zijn, enzovoort. Spyware kan in virussen zitten, maar meestal zit het bijgeleverd bij bepaalde programma's (zoals Bonzi Buddy, CometCursor en Kazaa). Ook bepaalde cookies kunnen als spyware worden beschouwd: iemands surfgedrag over diverse websites kan worden getraceerd als de reclamebanners op die diverse websites vanuit één centrale server worden verzorgd.

89.3 Bekende programma's die spyware mee installeren

- Kazaa
- Kazaa lite (minder dan Kazaa weliswaar, maar draait men Spybot Search & Destroy na het installeren van Kazaa Lite, dan vindt deze enige spyware en na verwijdering hiervan door Spybot S&D werkt Kazaa Lite niet meer)
- DivX (behalve voor de betaalde versies en de 'standaard'-versie zonder de encoder)
- eXeem™ (volgens sommige gebruikers gaat eXeem vergezeld van spyware, niet bevestigd)
- Morpheus
- Grokster
- Messenger Plus! (optionele sponsor, in de laatste versie is er geen sponsor meer aanwezig)
- BSPlayer (de gratis variant)
- KMSPico.

89.4 Spyware en de wet

89.4.1 Nederland

Strafbaarheid

Het gebruik van spyware is onder bepaalde omstandigheden strafbaar. Zo is het bij wet verboden om zonder toestemming een computerprogramma op iemands harde schijf te installeren. De juridische term hiervoor is computervredebreuk en staat vermeld in artikel 138ab Wetboek van Strafrecht en artikel 144a Wetboek van Strafrecht BES. Een lacune in de wet is dat deze spyware toelaatbaar acht wanneer de algemene voorwaarden melding maken van de spyware — zelfs als dit op een zeer onduidelijke wijze gebeurt. Daarnaast maakt spyware computers instabiel door slecht programmeerwerk. Dit valt onder het strafrechtelijk delict 'vernieling van geautomatiseerde bestanden door schuld'.

Tevens verzamelt spyware persoonsgegevens zonder toestemming, hetgeen in strijd is met de privacywetgeving: 'de Wet bescherming persoonsgegevens'. Ook kan spyware in strijd zijn met artikel 4.1 van 'Het besluit universele dienstverlening en eindgebruikersbelangen'. Deze bepaling luidt als volgt:

1. Een ieder die door middel van elektronische communicatienetwerken toegang wenst te verkrijgen tot gegevens die zijn opgeslagen in de randapparatuur van een abonnee of gebruiker van openbare elektronische communicatiediensten dan wel gegevens wenst op te slaan in de randapparatuur van de abonnee of gebruiker van openbare elektronische communicatiediensten, dient voorafgaand aan de desbetreffende handeling de abonnee of gebruiker:

a. op een duidelijke en nauwkeurige wijze te informeren omtrent de doeleinden waarvoor men toegang wenst te verkrijgen tot de desbetreffende gegevens dan wel waarvoor men gegevens wenst op te slaan **en**

b. op voldoende kenbare wijze gelegenheid te bieden de desbetreffende handeling te weigeren.

Handhaving

Een gebruiker kan zelf het bedrijf in rechte aanspreken over diens handelwijze. Ook is het College bescherming persoonsgegevens bevoegd een boete per overtreding op te leggen wanneer de privacywetgeving is overtreden. Daarnaast is de OPTA bevoegd om op te treden en boetes op te leggen. Tot slot is ook het OM belast met de opsporing.

Een struikelblok in de handhaving van de gestelde regels is dat men meestal niet kan nagaan waar de spyware vandaan komt. In de gevallen waarin dit wel lukt, blijkt meestal het bedrijf buiten Europa gevestigd te zijn, en zullen instanties als het College bescherming persoonsgegevens, het Openbaar ministerie en de OPTA machteloos staan.

In Europa is enkel één Duitse rechtszaak aangaande spyware bekend (Hertz versus Claria). In de VS zijn meerdere rechtszaken gevoerd met uiteenlopende uitspraken.

De eerste Nederlandse (en Europese) maatregel tegen spyware: OPTA heeft boetes opgelegd van in totaal 1 miljoen euro. Het gaat over de besmetting van 22 miljoen computers. De spyware heet DollarRevenue. Het betreft

een overtreding van art. 4.1 van het bovenvermelde besluit. De boetes zijn opgelegd volgens art. 15.4 en art. 15.10 van de Telecommunicatiewet. Een deel van deze boetes moet betaald worden door de directeurs zelf.[1] Door een bezwaarprocedure moeten de boetes pas betaald worden nadat een rechter hierover uitspraak gedaan heeft. De verdachten beweren dat het bewijs illegaal werd verzameld. OPTA heeft de namen van de bedrijven en hun directeurs niet bekendgemaakt omdat het niet duidelijk is of OPTA dergelijke informatie openbaar mag maken.[2]

Hoofdstuk 90

SQL-injectie

De term **SQL-injectie** (Engels: *SQL injection*) wordt gebruikt voor een type kwetsbaarheid van computerapplicaties, meestal webapplicaties. Applicaties die informatie in een database opslaan maken vaak gebruik van SQL om met de database te communiceren. SQL-injectie kan gebeuren als invoer van gebruikers op onvoldoende gecontroleerde wijze wordt verwerkt in een SQL-statement. Om de precieze werking van SQL-injectie te begrijpen is het belangrijk om te weten hoe SQL werkt.

90.1 Rol van de apostrof in SQL

In SQL heeft de apostrof een belangrijke functie, namelijk het afbakenen van niet-numerieke gegevens. Om bijvoorbeeld alle personen met de naam “Jansen” te selecteren uit een tabel wordt het volgende statement gebruikt

```
SELECT * FROM persoon WHERE achternaam = 'Jansen'
```

In een applicatie waar gezocht kan worden naar personen, zal de gebruiker in het zoekveld uitsluitend “Jansen” invullen. In de applicatie wordt op basis van deze invoer bovenstaande code naar de database gestuurd.

Interessant wordt het als de gebruiker een apostrof in het zoekveld invult, bijvoorbeeld "'t Hart”. In een correct statement moet dan namelijk de apostrof worden verdubbeld, of voorzien van een backslash (\).

```
SELECT * FROM persoon WHERE achternaam = '"t Hart' SELECT * FROM persoon WHERE achternaam = '\'t Hart'
```

Als dat niet gebeurt, dan levert het een incorrect SQL-statement op, en volgt een foutmelding van de database. Maar het betekent ook dat de applicatie niet beschermd is tegen SQL-injectie.

90.2 SQL-injectie

SQL-injectie bestaat er uit dat een gebruiker in het invoerveld tekens invoert die ervoor zorgen dat een ongewenste SQL-query wordt uitgevoerd. Daarbij wordt vaak gebruikgemaakt van de apostrof. Dit kan alleen als bij het genereren van de SQL-code op basis van gebruikersinvoer de apostrof niet goed wordt afgevangen.

De gebruiker typt bijvoorbeeld “Jansen' OR 'a' = 'a” in het zoekveld. Het resulterende statement is dan

```
SELECT * FROM persoon WHERE achternaam = 'Jansen' OR 'a' = 'a'
```

Omdat "'a' = 'a'" altijd waar is, voldoet nu elk record aan de gestelde voorwaarde.

Met bovenstaand voorbeeld kan de hacker extra informatie ophalen uit de database. Dezelfde methode levert ook de mogelijkheden om nieuwe informatie aan de database toe te voegen, bestaande informatie aan te passen en informatie te verwijderen. Daarvoor is informatie nodig over de structuur (namen van tabellen en kolommen) van de database. De naamgeving van tabellen en kolommen is meestal logisch om werken met de database voor een reguliere gebruiker eenvoudig te houden en daardoor voorspelbaar. Daarnaast kan de hacker ook diverse zaken uitproberen om bijvoorbeeld een gebruikersaccount met beheerders-rechten aan te maken. Lukt dit, dan kan de hacker de totale controle over de computer overnemen, met alle gevolgen van dien.

90.3 Preventie

Door middel van het geven van de minimaal noodzakelijke rechten van de gebruiker en de SQL-server kan het ongewenst aanpassen van gegevens en het uitvoeren van ongewenste commando’s op het systeem moeilijker gemaakt worden.

90.3.1 Afwijzen van verkeerde invoer

Men kan alleen bepaalde tekens en strings toestaan in de invoer en alles wat een betekenis heeft in een SQL-commando afwijzen (bijvoorbeeld de tekens en strings: insert drop ' -- ; enzovoorts, maar ook char zodat niet via een omweg een ' in de invoer kan voorkomen). Zui-

ver numerieke gebruikersnamen en wachtwoorden moeten afgewezen worden, omdat die automatisch omgezet kunnen worden in strings met ongewenste betekenissen.

90.3.2 Backslash

De injectie met SQL-code kan eenvoudig tegengegaan worden door het juist verwerken van informatie die door een gebruiker wordt aangeleverd. In de programmeertaal PHP kan dat bijvoorbeeld via mysqli_real_escape_string(). Deze functie vangt (my)SQL-specifieke karakters af door er een backslash (\) voor te plaatsen. Hierdoor weet het systeem dat enkel het letterteken bedoeld wordt, en niet meer de scheidende functie van het afbakenen van gegevens. Een stukje voorbeeld-programmeertaal in PHP kan er als volgt uitzien:

<?php $result = mysqli_query($verbinding, “SELECT * FROM persoon WHERE achternaam = '" . mysqli_real_escape_string($verbinding, $_POST['achternaam']) . "'"); ?>

90.3.3 Statement

Een andere methode om injectie tegen te gaan is door middel van een voorgedefinieerd statement. Hierbij wordt in het aanroepende programma het statement opgebouwd met een variabele. De inhoud van de variabele wordt dan gekoppeld aan de gebruikersinvoer.

Bijvoorbeeld (in de taal Java):

In plaats van

1. Connection con = (maak verbinding met de database)
2. Statement stmt = con.createStatement();
3. ResultSet rset = stmt.executeQuery(“SELECT * FROM persoon WHERE achternaam = '" + invoer + "';");

is het beter om het volgende te gebruiken

1. Connection con = (maak verbinding met de database)
2. PreparedStatement pstmt = con.prepareStatement(“SELECT * FROM persoon WHERE achternaam = ?");
3. pstmt.setString(1, invoer);
4. ResultSet rset = pstmt.executeQuery();

90.3.4 Databasepermissies

Schade kan beperkt worden door alleen de strikt nodige permissies te verlenen. Bijvoorbeeld kan men het op SQL-server onmogelijk maken bepaalde tabellen te lezen:

deny select on sys.sysobjects to webdatabaselogon; deny select on sys.objects to webdatabaselogon; deny select on sys.tables to webdatabaselogon; deny select on sys.views to webdatabaselogon;

90.4 Externe link

- (en) Advanced SQL injection (SQL Server)

Hoofdstuk 91

Streaming media

Streaming media zijn media die rechtstreeks via computernetwerken (zoals het internet) worden gedistribueerd. Het proces wordt *streamen* genoemd en wordt gebruikt bij het webcasten en is een populaire distributiemethode bij het op verzoek bekijken van webvideo's. Tijdens het streamen wordt continu een gedeelte van de data in een buffer geplaatst, opdat een programma dit kan afspelen. Hierdoor kunnen de ontvangen media (video en audio) direct geconsumeerd worden zonder dat de gehele uitzending gedownload is.

91.1 Geschiedenis van het streamen

De vroegst bekende stream is de webcast *koffiepotcamera van Cambridge* die werd gebruikt om te zien of de koffie al doorgelopen was. Deze bestond al in 1991, lang voordat het wereldwijd web bekendheid kreeg. In Nederland zijn Stef Van der Ziel en Adam Curry pioniers. In 1994 produceerde Van der Ziel de eerste Nederlandse webcast, later volgden diverse andere Nederlandse partijen en verzorgde de VPRO webcastprojecten rond evenementen.

Microsoft geloofde niet in het Internet. Manager Rob Glaser nam daarom alle mensen met mediakennis mee en startte RealNetworks. In 1996 kwam het bedrijf met RealAudio uit. Voor het eerst was het mogelijk om redelijke kwaliteit live-audio via smalbandinternet te distribueren, door middel van een propriëtaire codec, reflectieserver en mediaspeler. Andere initiatieven zoals VDO werden door RealNetworks opgekocht. In 1997 kwam RealNetworks ook met video-ondersteuning. In 1998 nam Microsoft een licentie op RealVideo-technologie om deze in de eigen Media Player in te bouwen. Kort daarop lanceerde RealNetworks RealVideo G2, waardoor de licentie van Microsoft weinig waarde meer had. In 1999 lanceerden Apple en Microsoft hun streamingmediaproducten, respectievelijk gebaseerd op Apples QuickTime - dat al sinds 1991 bestond - en het bij Microsoft ontwikkelde Netshow, later Windows Media gedoopt.

Omdat geen van de drie productlijnen van RealNetworks, Microsoft en Apple onderling uitwisselbaar waren, werd gevreesd voor een 'mediaplayeroorlog'. Om acceptatie bij de consument voor streamingdiensten te bevorderen besloot de Motion Pictures Expert Group (bekend van MPEG−1, MPEG-2 en dus ook MP3) de strijdende partijen uit te nodigen voor deelname aan MPEG-4. RealNetworks stelde het RTSP/RTP-protocol voor als standaard voor distributie. Dat werd geaccepteerd. Apple stelde het QuickTime atom-gebaseerde bestandsformaat voor. Dat werd geaccepteerd. Microsoft stelde haar MPEG-4-videocodec voor, maar dat werd afgewezen. Mede omdat na publicatie de codeccode werd gestolen en omgedoopt tot DivX trok Microsoft zich terug uit de MPEG-4-standaardisatie. Microsoft MPEG-4 is dan ook niet uitwisselbaar met de ISO- of ISMA MPEG-4-producten op de markt en is door Microsoft zelf al tot onderhoudsversie verklaard.

RealNetworks' technologiestrategie berust inmiddels niet meer op het eigen RealVideo-formaat, maar op ondersteuning van meerdere formaten, ook die van Apple en Microsoft. De ondersteuning van deze formaten is overigens niet officieel en ligt technologisch één à twee generaties achter. Apple committeerde zich aan de open MPEG-4- en 3GPP-standaarden en Microsoft positioneerde het proprietary Windows Media-formaat. De mediaspeleroorlog werd inmiddels afgespeeld op terreinen buiten de desktop-pc met 3GPP dominant op de mobiele markt. In de hd-dvd- en settopboxmarkt was de strijd onbepaald tussen Windows Media en H.264 (MPEG-4). In 2008 besloot Microsoft om H.264 toe te voegen aan Silverlight [1]. In 2010 introduceerde Google zijn eigen codec WebM. Maar in 2012 verkiest Mozilla ook H.264 boven WebM [2].

91.2 Codec

Codecs zorgen voor een efficiënte distributie van beeld en geluid. In het algemeen zijn codecs voor streaming media 'lossy' waarbij geluids- en beeldinformatie beperkt voor vloeiende distributie. De keuze voor een codec is afhankelijk van de bandbreedte van de verbinding en de rekenkracht van de hardware voor compressie en afspelen. Streamingcodecs schalen van GSM (9,6 Kbps) tot hd-tv (4-10 Mbps). Andere bekende codecs zijn MPEG-1 (waaronder MP3), MPEG-2 en FLAC. Spe-

cifieke streamingmediacodecs zijn RealVideo Windows Media, MPEG-4 (opgevolgd door H.264), FLV en AAC. Op internet worden voor uitwisseldiensten MP3 en OGG voor audio gebruikt en Xvid voor video.

91.3 Bestandsformaat

Het bestandsformaat is de opbouw en beschrijving van een bestand. Het bevat naast (volgens de genoemde codecs gecomprimeerde) audio- en videobestanden ook zogeheten metagegevens: technische beschrijvingen van de audio- en videobestanden, inhoudelijke beschrijvingen van het document, en tot slot biedt een bestandsindeling mogelijkheden tot interactieve functies. Voorbeelden zijn de .MOV QuickTime-containerindeling, waar ook de .MP4-, MPEG-4-, en .3GP-bestandsindelingen op zijn gebaseerd. 3GP is de standaard voor video op mobiele telefoons. Andere, minder uitgebreide bestandsindelingen zijn .ASF (ook bekend als .WMV) van Microsoft en .RM van RealNetworks. Zogeheten DivX-bestanden maken gebruik van de eenvoudige .AVI-bestandsindeling met daarin een als DivX-gecodeerd videospoor en MP3-audiospoor. DivX 6 introduceerde een eigen bestandsindeling (.divx) waardoor net zoals bij MPEG-4-ondertiteling, markeringen en andere interactieve functies mogelijk werden. Het FLV-formaat is een proprietaryformaat van Macromedia en gebruikt H.263 of ON2 VP6 als videocodec en MP3 als audiocodec.

Vrijwel alle producenten van mobiele telefoons ondersteunen het 3GPP-formaat. Deze industriestandaard is een afgeleide van MPEG-4 met specifieke kenmerken voor zaktelefoons zoals vaste afspraken voor schermgrootte en video- en audiocodecs. 3GPP is ook het formaat dat gebruikt wordt voor DVB-H (Digital Video Broadcasting voor Handhelds). Uitzondering zijn vooralsnog de Microsoft Mobile gebaseerde smartphones, die een klein marktaandeel vormen en primair het Windows Media-formaat ondersteunen: optioneel kan echter 3GPP afspeelsoftware worden geïnstalleerd.

91.4 Opnemen

Voor het opnemen van geluid- en beeldmateriaal is een geluids- en/of videokaart nodig met een ingang, zoals composiet video, S-Video, DV of SDI. De opgenomen audio of video wordt geconverteerd (of getranscodeerd) naar het gewenste bestandsformaat.

91.5 Afspelen

Om af te spelen wordt een mediaspeler gebruikt dat *streaming media* ondersteunt.

ITunes is vooral populair door de ondersteuning van podcasts en vodcasts.

Windows Media Player wordt vaak gebruikt in omgevingen waar afscherming vereist is, vanwege DRM-voorzieningen.

QuickTime Player heeft voordeel van het meeliften van distributie via digitale fototoestellen, de populaire Apple iPod en het populaire Apple iTunes. Naast het eigen QuickTime-formaat worden meer dan 100 audio-, video- en afbeeldingsformaten ondersteund. Apple stimuleert het gebruik van de MPEG-4-standaard boven het eigen MOV-formaat. De QuickTime Player kent een Pro-versie, die tegen een geringe vergoeding zeer veel additionele features biedt, zoals knippen en plakken op metaniveau en het exporteren van audio en video naar tientallen high-end- en streamingformaten. De QuickTime Player wordt vaak verward met QuickTime, wat een uitgebreide multimedia-architectuur is die als framework boven op het OS draait waardoor programma's van derden een rijke bibliotheek aan multimediafuncties kunnen gebruiken. Voorbeelden hiervan zijn iTunes, iMovie, Final Cut Pro, Word, Powerpoint, Premiere, Photoshop, Director en honderden multimedia-georiënteerde programma's voor zowel pc als Mac.

RealPlayer heeft onder het publiek een slechte naam opgebouwd wegens instabiliteit en vermeende 'spyware'. Vanwege de hoge kosten van streamingdistributietechniek zijn er nog maar weinig aanbieders die het Real-formaat gebruiken. Het marktaandeel van deze player is hierdoor dalende. Ook RealPlayer bouwt steeds meer op de onderliggende Windows Media- en QuickTime-architecturen voor het kunnen ondersteunen van diverse mediaformaten.

Er zijn softwareprogramma's die gebruikmaken van Windows Media Player, RealPlayer en andere spelers. Deze pakketten maken het gebruikersvriendelijker om net als op de normale televisie te zappen tussen kanalen.

VideoLAN is een opensource-videoplayer. Deze ligt momenteel onder vuur omdat de ontwikkelaars, in tegenstelling tot andere ontwikkelaars, geen licenties willen afdragen voor het gebruik van MPEG-4. VideoLAN vraagt eindgebruikers zelf de verantwoordelijkheid te nemen om een eenmalige vergoeding voor het gebruik van technologie aan de MPEG-4 licentiehouders te betalen maar faciliteert dit niet. In de praktijk zien eindgebruikers deze bepaling in de VideoLAN EULA over het hoofd, en daarnaast zijn de licentiehouders niet ingesteld op het zaken doen met particulieren maar met technologie-ontwikkelaars.

In de woonkamer zijn settopboxen met hardware-afspeelprogramma's meer van toepassing.

91.6 Integreren in de browser

Het inbedden van de mediaspeler-plugin binnen een HTML-omgeving gebeurt vaak met ActiveX (Internet Explorer-familie) of EMBED (Mozilla-familie). De mediaspeler wordt dan niet als extern programma gestart, maar binnen de webpagina getoond. Hiermee kan de aanbieder de video in een eigen vormgegeven html-speler aanbieden.

91.7 Virtueel knippen en plakken

Het is mogelijk om random op een willekeurig tijdstip in VOD-streams te beginnen. In plaats van eerst het volledige bestand te moeten downloaden kan de server vanaf elk tijdsmoment beginnen te spelen. De *Virtuele Snijmachine*[3] is een publieke webgebaseerde tool die het mogelijk maakt om fragmenten virtueel uit een VOD-stream te knippen. Er wordt geen werkelijk gedeelte van de video gekopieerd (deze blijft in zijn geheel op de server staan), maar er wordt een metafile gegenereerd waarin de VOD-stream-URL, de starttijd en de doorlooptijd staan vermeld. Dit bestand opent automatisch de juiste mediaspeler en zorgt ervoor dat alleen het fragment wordt afgespeeld. Werkt met de meest gangbare mediaspelers.

91.8 Afscherming

Soms is het gewenst audio of video content af te schermen. De redenen hiervoor kunnen onder meer privacy, geheimhouding, rechten of commerciële exploitatie zijn, zoals het huren van een online speelfilm. Er zijn meerdere mogelijkheden om streams af te schermen. Soms wordt een combinatie gebruikt:

- Obscurity: het niet vertellen of verbergen van de URL (locatie) van het streamingbestand. Een website probeert de bron af te schermen. Deze vorm van afscherming wordt ten zeerste afgeraden omdat de URL snel te achterhalen is en via Usenet, IRC en andere sociale netwerken snel verspreid kan worden.
- Wachtwoordbeveiliging: bestanden, of mappen met bestanden worden op de streamingserver afgeschermd door middel van een gebruikersrechtenmanagement. Omdat distributieservers van verschillende fabrikanten hun eigen methodiek hiervoor op na houden is dit ook geen aan te raden oplossing. Gebruikers moeten meerdere wachtwoorden onthouden, of dubbel invoeren, of beheerders moeten complexe koppelingen bouwen en drievoudig gebruikersbeheer gaan implementeren. Gebruikers kunnen wachtwoorden gaan delen. Voor sommige mediaservers zijn plug-ins beschikbaar die met gebruikersdatabanken kunnen worden gekoppeld.
- Netwerkafscherming: Een server wordt binnen een afgeschermd netwerk (intranet, VPN) geplaatst, of toegang tot de server wordt beperkt tot een beperkt aantal IP-ranges. Hiermee kan op betrekkelijk eenvoudige wijze afscherming voor een bepaalde groep worden geregeld. Afscherming is echter niet op persoonlijk niveau (authenticatie) mogelijk.
- Slagboom: Een slagboom is een server die tussen de streamingserver(s) en het netwerk (vaak is dit het internet) wordt geplaatst. De website genereert een unieke sessiecode en plakt deze achter de URL. De slagboom geeft enkel toegang tot de URL indien de sessiecode geldig is. Na verloop van de sessie dient de gebruiker via de website een nieuwe aan te vragen. Een eenvoudige firewall kan deze functie invullen, maar performance hiervan is laag. Er is ook een slagboom oplossing op TCP/IP-stack-niveau, welke hogere performance biedt. Deze slagboom is een zeer efficiënte, gebruiksvriendelijke en platformonafhankelijke afschermingsoplossing en volstaat overal waar encryptie van de content geen vereiste is.
- DRM: De zwaarste afschermingsmethode is Digital Rights Management, wat in de volgende sectie wordt behandeld.

91.9 Digital Rights Management

Met Digital Rights Management (DRM) worden de datastromen en bestanden met een sleutel onleesbaar gemaakt. Alleen de kijkers met een passende sleutel zijn in staat om de stromen en bestanden te openen. Het is echter niet mogelijk de sleutel te kopiëren, te delen of te overhandigen aan een ander. Men kan een eigen sleutel bemachtigen door bijvoorbeeld eerst een transactie te voltooien. Dit kan een financiële transactie zijn, maar ook reguliere authenticatie. In de sleutel zitten zogeheten 'business rules' opgeslagen. Deze regels bepalen hoe vaak en hoelang de datastroom of het bestand te bekijken of te beluisteren is. De licentieserver (die de sleutel heeft uitgegeven) kan eventueel controleren of de sleutel nog geldig is en of de regels in de sleutel wellicht dienen te worden aangepast. De pc kan ook tijdelijk de rol van licentieserver over nemen en de licentie sublicenseren aan bijvoorbeeld een mp3-speler.

DRM stelt de eigenaar of openbaarmaker in staat om alleen degenen die betaald hebben voor content toegang tot deze content te bieden. In combinatie met streamingmediaservers is het kijk- en luistergedrag exact te meten. Microsoft en RealNetworks hebben een operationele *proprietary* DRM-oplossing die verweven is met de eigen streamingmediacodecs, codeerprogramma's en afspeelprogrammatuur. De specificaties voor een industriestandaard MPEG-4-DRM-oplossing zijn gereed en toepassingen worden op het moment van schrijven ontwik-

keld. Voor mobiele toepassingen is er de OMA DRM-specificatie. Apple hanteert voor de populaire iTunes Music Store de *proprietary* FairPlay-DRM-techniek, maar maakte op 5 januari 2009 bekend dat de hele Store DRM-vrij zou worden.

91.10 Hosting en distributie

Om te streamen is een eigen streamingserver of een account op een streamingserver van een provider nodig. De kosten van streamingsoftware lopen flink uiteen. Sommige software is gratis en open source, maar heeft een enorme leercurve; andere software (RealServer, Flash Media Server) kan gestapeld oplopen tot 400.000 euro. Streamingproviders bieden gedeelde accounts (abonnement), dedicated servers (huur), mediaserverclusters of verspreide servers. Sommige aanbieders lijken goedkoop, maar rekenen achteraf hogere bedragen voor gegenereerd dataverkeer.

Ook de werkelijk beschikbare bandbreedte dient toereikend te zijn. Shared servers dienen een eigen 100Mbps-link naar het internet te hebben. Dedicated servers dienen over 100 Mbps of zelfs een of meerdere gigabitverbindingen te beschikken. Het service level agreement (SLA) bevat de voorwaarden van de dienstverlening, waaronder de garantie voor de beschikbaarheid van de server(s), of deze actief gemonitord worden en de snelheid waarmee een defect of crash wordt hersteld.

De Flash Media Server II kostte circa 4500 dollar per 150 connecties. Als men een dergelijke server ongelimiteerd aan een gigabitverbinding (1000 gelijktijdige kijkers op 1 Mbps) wilt aanbieden, kost dit de gebruiker veel geld aan softwarelicenties. Daarom bieden sommige hostingproviders FLV-hosting als progressive download aan. Het nadeel van deze methode is dat er geen random toegang tot fragmenten mogelijk is, geen goede metingen kunnen worden verricht. Inmiddels starten innovatieve mediahostingbedrijven met streamingalternatieven voor FLV-bestanden die wel random access en snelle bursting bieden. Adobes Flash Media Server III wordt gesplitst in een betaalbare (4500 dollar) ongelimiteerde mediaserver en een duurdere (meer dan 10.000 dollar) interactieve server.

Een nadeel aan de Flash Media Server is dat hij alleen geschikt is voor het streamen naar de Flash-plug-in of spelers die overweg kunnen met de Flashprotocollen. Een nieuwe generatie multi-screenoplossingen is daarom in opkomst. Multi-screen is de term die wordt gebruikt voor het kunnen streamen van content naar verschillende type apparaten, spelers en plug-ins vanaf dezelfde server. Wowza Streaming Engine is een gevestigde naam in de multi-screenwereld. De opensourceserver Mistserver vormt hiervoor een alternatief. Anders dan andere opensourceserverproducten (Red5, crtmpserver) is dit het eerste product wat een multi-screenoplossing aanbied in een Plug & Play-formaat.

Nieuw is p2p-distributie. Elke kijker wordt hierbij ook een zender. Bedrijven als Octoshape is het gelukt om p2p ook geschikt te maken voor live-uitzendingen.

In 2005 is het volumeverkeer over de AMS-IX verdubbeld. De grootste groeier was streamingverkeer (met 80%). Aangenomen wordt dat van de 100Gbps-dataverkeer, circa 10 Gbps al streams is. Streamingverkeer groeide in 2005 sneller dan peer-to-peer, downloads, usenet, e-mail en surfen bij elkaar. In 2006 wordt een nog snellere groei verwacht. Om die reden wordt streamingverkeer steeds vaker via peering (via het AMS-IX-knooppunt) verwerkt, of decentraal gedistribueerd. Traditioneel worden servers centraal geplaatst achter een backbone. Echter, door de servers decentraal (netwerktopologisch) bij internetproviders te plaatsen worden de backbones ontlast en zijn er nauwelijks kosten meer voor dataverkeer. Bovendien kan er beter worden geschaald, en kan een kwaliteitsgarantie worden afgegeven, alhoewel sommige centrale clusters zeer goedkoop zijn en al hoge performance bieden.

Om de centrale servers goed te kunnen beheren, contentbeheer eenvoudig te houden, gebruikers te kunnen verdelen over de vele servers en centraal de logbestanden te kunnen verwerken is een zogeheten 'CDN'-managementserver nodig. De meeste exploitanten van een CDN ontwikkelen en exploiteren deze technologie exclusief voor zichzelf, Akamai en Vitalstream zijn hier voorbeelden van. Inmiddels zijn commerciële CDN-producten gelanceerd, waarmee elke provider of omroep tegen lage kosten en een korte 'time to market' zijn eigen CDN kan uitrollen.

91.11 Zie ook

- Downloaden versus streamen
- Uploaden
- Client-servermodel
- Podcast

91.12 Externe bronnen

- Officiële Flash Media Server website
- Officiële Mistserver website
- Officiële Wowza Media Systems website
- Officiële Jet-Stream website

Hoofdstuk 92

TCP/IP

TCP/IP is een verzamelnaam voor een reeks netwerkprotocollen die gebruikt worden voor het grootste deel van de netwerkcommunicatie tussen computers. Het internet is het grootste en bekendste TCP/IP-netwerk. De naam TCP/IP is een samentrekking van de twee bekendste protocollen die deel uit maken van de TCP/IP-protocol*stack* (= protocol*stapel*): het Transmission Control Protocol (TCP) en het internetprotocol (IP). TCP/IP wordt uitgesproken als "TCP over IP" of meestal *"tiesiepie ajpie"*.

92.1 Geschiedenis

Het internet is een open netwerk. Op dit netwerk maakt men gebruik van het TCP/IP-protocol om gegevens uit te wisselen. TCP/IP is een pakketgeschakeld protocol waarbij de gegevens in kleine pakketjes onafhankelijk van elkaar worden verzonden. De communicatiesoftware plaatst de pakketten weer in de juiste volgorde, detecteert eventuele fouten in de ontvangst om indien nodig bepaalde pakketten opnieuw te vragen totdat alle pakketten ontvangen zijn.

Deze manier van werken liet toe om bij de voorloper van internet, ARPANET, informatie in kleine pakketjes te versturen langs verschillende wegen. Zoals zo vaak ging het hier om de oplossing voor een militair probleem. In geval van een oorlog, en bij het platleggen van sommige computers in een netwerk, was het nodig dat de overige computers toch hun gegevens konden blijven uitwisselen. Was een deel van het netwerk er niet meer, dan werden de gegevens langs een andere weg naar elkaar toegestuurd. Dit maakte het netwerk minder kwetsbaar. De doelstelling van de militairen was een netwerk dat altijd bleef werken.

Toch werd na een tijd dit netwerk te licht bevonden en zijn de militairen overgestapt naar MILnet. Van toen af werd dit protocol tussen de verschillende universiteiten die met elkaar verbonden waren gemeengoed.

92.2 Kenmerken

Het internet is een zogenaamd pakketgeschakeld netwerk, zonder garantie op enige service. Een pakketje gegevens kan zonder meer verloren gaan, sterker, bij overbelasting van een bepaalde lijn wordt zelfs aangeraden pakketjes weg te gooien. Over dit onbetrouwbare netwerk wordt met behulp van het TCP-protocol een ogenschijnlijk betrouwbare dienst gelegd, waarbij TCP in de gaten houdt of TCP-pakketjes (in de juiste volgorde) aankomen, en indien niet, geen bevestiging (acknowledge) stuurt. Indien bij de zender een welbepaalde wachttijd (timeout) verstrijkt, zonder dat er een bevestiging binnen is, dan stuurt deze het pakketje opnieuw.

Vanwege deze kenmerken is TCP/IP erg geschikt voor netwerkdiensten waar geen garantie over de zekerheid en timing vereist is wanneer bepaalde data aan dient te komen. Bijvoorbeeld, bij het downloaden van een fotootje van internet, maakt het niet uit dat er door pakketverlies enige data verloren gaat, zolang dit door TCP maar gecorrigeerd wordt.

Bij een telefoongesprek gelden heel andere wensen. Hier is gewenst dat ieder pakketje exact op het juiste moment aankomt. Pakketjes dienen liefst niet weggegooid te worden, maar als dat toch gebeurt, is het zinloos om ze opnieuw te verzenden, de hapering in het geluid heeft dan al plaatsgevonden. Hiervoor kan dan weer gebruikgemaakt worden van het UDP-protocol dat losse pakketjes zendt en zo onder de herverzend-eigenschappen van TCP uitkomt. Omdat echter nog steeds geen enkele garantie bestaat over de timing en zekerheid van de aankomst van gegevens zijn bepaalde eigenschappen inherent aan het systeem.

92.3 Lagen

De TCP/IP-protocolstack wordt officieel onderverdeeld in vijf lagen, met elk een eigen functionaliteit. De onderste laag, de *fysieke laag*, wordt vaak onderverdeeld in een eigenlijke fysieke laag en een datalinklaag.

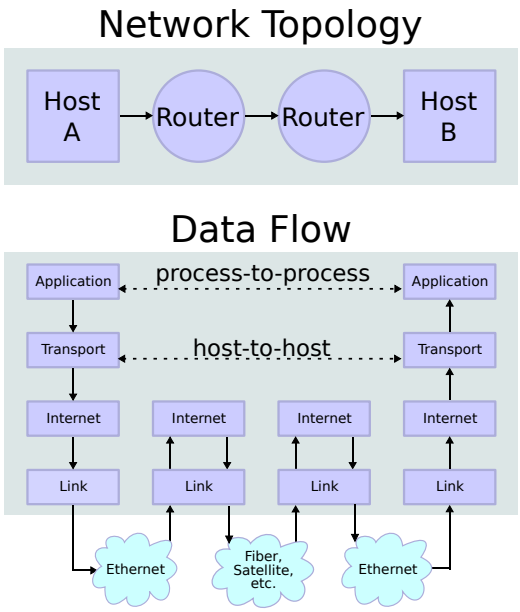
Ook is er discussie over hoe de lagen uit de TCP/IP-stack overeenkomen met de 7 lagen die het (vooral theo-

retische) OSI-model voorschrijft. Vaak vallen in de literatuur de drie bovenste OSI-netwerklagen (Toepassing, Presentatie, en Sessie) samen met de toepassingslaag uit het TCP/IP-protocol.

Volgende tabel geeft het klassieke OSI-model weer, met daarbij telkens een aantal bijhorende protocollen uit de TCP/IP-stack:

Hieronder volgt een vereenvoudigde TCP/IP-stack, met enkele protocollen:

92.4 Bekende aan TCP/IP gerelateerde protocollen



TCP/IP-gerelateerde protocollen

92.4.1 Applicatielaag

In de applicatielaag bevinden zich de internettoepassingen als e-mail POP3, SMTP en FTP. Deze toepassingen hebben meestal een client-server structuur.

> Echo, Finger, Gopher, HTTP, HTTPS, IMAP, IRC, NNTP, NTP, POP3, QOTD, RTP, RTSP, SNMP, SSH en SCP, SMTP, Telnet, XDMCP

92.4.2 Transportlaag

De transportlaag zorgt voor de communicatie tussen processen die zich op de hosts bevinden. Elke internetapplicatie is voor wat betreft de transportlaag gebouwd op ofwel TCP- ofwel UDP-protocol. Als volledig foutvrije transmissie is vereist wordt TCP gebruikt, als snelheid of het minimaliseren van overhead belangrijker is wordt UDP gebruikt.

> TCP, UDP, DCCP, GTP, SCTP

92.4.3 Netwerklaag

De bedoeling van deze laag is om de aangeboden data van bron naar doel te versturen ongeacht het protocol of type data, enkel ervoor zorgen dat alles netjes toekomt op de plaats van bestemming. Via de netwerklaag wisselen clients en servers tijdens TCP-handshakes onderling TCP/IP-pakketten uit om netwerkverbindingen tot stand te brengen of te verbreken. Er wordt gezocht naar de meest geschikte weg om de data te versturen. Ook wel Internetprotocol genoemd.

92.4.4 Datalinklaag

> Point-to-Point Protocol, SLIP, IEEE 802.3, IP-over-ATM-tunnel, SDH, IEEE 802.11 en 802.11i

92.4.5 Fysieke laag

Deze laag maakt de fysieke connectie tussen de netwerken mogelijk, zij bevat alle gegevens van een LAN- en WAN-netwerk die nodig zijn om een connectie te verwezenlijken.

> telefoonlijn, coaxkabel, twisted pair, glasvezel, wifi

Hoofdstuk 93

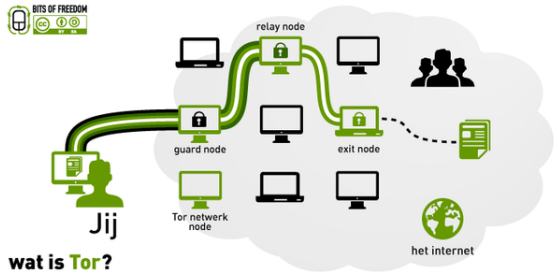
Tor (netwerk)

Tor (kort voor **The onion router**) is een open netwerk voor anonieme communicatie gebaseerd op een techniek genaamd Onion routing. Onion routing is een technologie ontwikkeld in 1995 door het United States Naval Research Laboratory.[1] Het netwerk is een van de systemen die Edward Snowden gebruikte om geclassificeerde documenten openbaar te maken.

Het Tor-netwerk is bedoeld om te voorkomen dat anderen door analyse van het berichtenverkeer kunnen achterhalen wat de herkomst en bestemming van berichten is.[2]

De Tor-client is opensourcesoftware en het gebruik van het Tor-netwerk is gratis.

93.1 Werking



Wat is Tor (The onion router)?

Het netwerk is gebaseerd op zogenaamde *onion-servers*; computers die als tussenstations dienen tussen de afzender en de bestemming. De naam “Onion Routing” is geen willekeurige naam. “Onion”, wat “ui” betekent, staat voor de manier waarop de data op het Tor-netwerk worden voorgesteld. Het principe is dat berichten volgens een willekeurig pad via verschillende onion-servers naar hun bestemming reizen, waarbij iedere server een versleutelde “laag” van de routinginformatie ontcijfert, vergelijkbaar met de schillen van een ui die verwijderd worden.[3] Deze data wordt dan doorgestuurd naar de volgende server totdat de volledig ontcijferde data bij de ontvanger aankomen.

Doordat bij iedere tussenstap alleen de routinginformatie voor de voorafgaande en de volgende server in ongeëncrypteerde vorm aanwezig is, is het onderweg nergens mogelijk om de oorsprong en de bestemming van het bericht te bepalen. Voor de computer op de eindbestemming lijkt het alsof het bericht van de laatste onion-server komt.[4] Bij de laatste server is alleen maar te bepalen wat de data bevat en niet waar ze vandaan komen. Doordat het Tor-programma willekeurige servers kiest waarlangs het de data verstuurt, is het heel moeilijk om een bepaalde computer af te luisteren.[5]

93.2 Veiligheid

Zoals bij vele encryptiemethoden kent ook Tor enkele zwakke punten. Op de website staat een waarschuwing dat alleen Tor gebruiken niet genoeg beveiliging geeft voor sommige doeleinden en dat de gebruiker zelf ook op enkele dingen moet letten zoals het negeren van browser-plug-ins en cookies.[6]

Men kan echter ook een Tor-exitnode opzetten en zodoende een gedeelte van het Tor-verkeer afluisteren. Dit werd in augustus 2007 aangetoond door de Zweedse beveiligingsconsultant Dan Egerstad, die via een vijftal Tor-exitnodes honderden gebruikersnamen en wachtwoorden van diplomatieke diensten van ambassades ontdekte. Na het publiceren van 100 van deze logins werd Dan Egerstad op 16 november 2007 gearresteerd door de Zweedse politiedienst.[7][8][9]

Het is beter nog een extra encryptiemethode te gebruiken voor de data om extra veilig te zijn. Proxy's zijn namelijk nooit compleet veilig, ook al is het bij Tor zo dat het internetverkeer door meerdere proxy’s of 'nodes' wordt gestuurd.[10]

93.3 Gebruikers

Het netwerk wordt onder andere gebruikt voor militaire toepassingen (vandaar de belangstelling van de US Navy voor deze technologie), maar ook voor civiele toepassingen, zoals het beschermen van de privacy van dissidenten. Zo zouden journalisten die kritiek geven op totalitaire regimes die geen persvrijheid kennen, hun anonimiteit en

veiligheid kunnen waarborgen.[11][12]

De mogelijkheden van anonieme communicatie (bijvoorbeeld op het deep web) kunnen ook misbruikt worden, omdat kwaadwillenden zoals computerkrakers, distributeurs van kinderpornografie en drugshandelaren, indien ze gebruikmaken van Tor moeilijker opgespoord kunnen worden.

93.4 Zie ook

- Onion routing
- .onion
- Orbot
- Tails

93.5 Externe link

- Tor-hoofdpagina

Hoofdstuk 94

Trojaans paard (computers)

Een **Trojaans paard** is in de computerwereld een functie die verborgen zit in een programma dat door de gebruiker wordt geïnstalleerd. Deze functie kan toegang tot de geïnfecteerde computer verschaffen aan kwaadwillenden en zo schade toebrengen aan de computergegevens of de privacy van de gebruiker. In het jargon gebruikt men ook wel het Engelse *Trojan horse* of kortweg *trojan*. Het is genoemd naar het Paard van Troje waarin Griekse soldaten de stad Troje binnenkwamen om de poorten van de stad van binnenuit te openen.

Een Trojaans paard is dus geen programma dat zelfstandig beschadigingen aan de geïnfecteerde computer veroorzaakt, zoals een computervirus. Een Trojaans paard moet bovendien door de gebruiker worden gekopieerd en kopieert zichzelf niet naar andere computers, zoals een worm wel doet.

Trojaanse paarden worden vaak verstuurd als bijlage bij een e-mail, of vermomd als liefdesbrief of pornografisch materiaal, maar ze kunnen ook via chatprogramma's worden verspreid of verstopt zitten in programma's die gedownload worden van een website of een p2p-programma.

94.1 Kenmerken

Een Trojaans paard is een (klein) programma dat, vermomd als een nuttig programma, zichzelf vaak op de harde schijf nestelt. Een hacker kan zich via een client-console toegang verschaffen tot een pc. Hij is in zo'n geval in staat om alle randapparatuur te besturen en om de gegevens op de harde schijf te bewerken, te kopiëren of zelfs te verwijderen.

94.1.1 Verschil tussen een virus, een worm en een Trojaans paard

Wormen en virussen zeggen iets over de methode van verspreiding, niet over datgene wat verspreid wordt. Het verschil tussen een worm en een virus zit hem in het feit dat een worm zich zonder de hulp van een gebruiker kan verspreiden. Een virus kan in sommige gevallen een Trojaans paard met zich meedragen.

94.2 Mogelijke schade

Met een Trojaans paard wordt de pc opengezet voor andere gebruikers. Dit geeft hun de mogelijkheid om:

- Wachtwoorden en gebruiksnamen op het systeem te achterhalen.
- De harde schijf te gebruiken om bestanden te delen, wijzigen of verwijderen.
- De pc gebruiken in een DDOS-aanval (Distributed Denial Of Service).
- De processor gebruiken voor intensieve rekentaken.
- De muisaanwijzer te laten verdwijnen, het scherm te spiegelen of om te keren.
- De computer te laten crashen.
- Spammails te versturen vanaf de pc. Men noemt zo'n pc dan een spambot of zombie.
- Woorden in bijvoorbeeld zoekbalken neerzetten.
- Creditkaartnummers en bankgegevens te verzamelen.
- De hele computer overnemen en de toetsaanslagen registreren.
- De computer lid maken van een zogenaamd botnet.
- Reclame op verschillende websites laten zien.
- Het BSOD laten zien.
- Naar websites gaan die men niet bedoeld heeft.

94.3 Preventie

- Opletten met uitvoerbare bestanden (.exe) of scripts (.vbs) die als bijlage via e-mail ontvangen worden.
- Geen verdachte applicaties van het internet downloaden/installeren.

- Alle binnenkomende post en gedownloade documenten scannen met een recente versie van antimalwaresoftware.

Zelfs als al deze voorzorgsmaatregelen genomen worden, is het niet uitgesloten dat het systeem gekraakt wordt. Elke barrière die opgeworpen wordt, verkleint de kans op inbraak.

94.3.1 Personal firewall

Een personal firewall houdt in de gaten welke applicaties met het internet mogen communiceren. Mocht het zo zijn dat er op de een of andere manier een Trojaan op het systeem terecht is gekomen, dan zal hij zichzelf kenbaar moeten maken. Een personal firewall zal herkennen dat de Trojaan met het internet wil communiceren en zal de gebruiker vragen of hij de applicatie toestemming wil geven. Het is meestal aan de gebruiker om te herkennen dat het om een Trojaans paard gaat. Het herkennen van een Trojaans paard is niet eenvoudig, omdat de Trojanen zichzelf proberen te vermommen met een onopvallende naam zoals 'server.exe' of zichzelf in te bedden in een bestaande applicatie.

94.4 Detectie en verwijdering

Er zijn drie manieren om een Trojaan te detecteren en vervolgens te verwijderen:

- Door een anti-trojan-scanner (zoals TDS-3 of BOClean) op het systeem los te laten. Sommige virusscanners kunnen gebruikt worden om Trojans mee op te sporen.
- Handmatige detectie en verwijdering.
  - Kijken in het register welke programma's er opgestart worden.
  - Kijken in Autoexec.bat of er programma's opgestart worden.
  - Zoeken in het bestand win.ini naar "run="-codes die programma's opstarten.
  - Zoeken in het bestand system.ini naar codes die programma's opstarten.

    Als op een van bovenstaande locaties een verwijzing gevonden wordt naar een programma in Joakim von Brauns Trojan Database dan moet er actie worden ondernomen en de desbetreffende verwijzingen en programma's van het systeem verwijderd worden. Het is overigens vaak niet mogelijk om de Trojaanse paarden terug te vinden in 'taakbeheer' (bij Windows NT/2000), omdat de Trojaan zich verborgen houdt. Op Windows 98, Me, XP en Vista kan ook gebruikgemaakt worden van start ⇒ uitvoeren ⇒ msconfig.
- Door na te gaan welke poorten open staan en door welke programma's deze gebruikt worden. Om te begrijpen wat een poort is, moet eerst het internetprotocol (IP) begrepen worden. Alle informatie die op het internet verzonden wordt, wordt eerst in kleine stukjes geknipt: IP-pakketjes. Om ervoor te zorgen dat de computer weet welk pakketje voor welke applicatie (bv. e-mail, FTP of HTTP) bestemd is, wordt aan elk pakketje een nummer gehangen: het poortnummer. Als op de computer deze poort openstaat, wordt het pakketje bij de juiste applicatie afgeleverd.

94.5 Bekende poorten

Bekende poorten die door Trojaanse paarden gebruikt worden, zijn onder andere:

- Back Orifice - poort 31337
- Netmonitor - poort 7301
- Ripper - poort 2023
- Remote Shell Trojan - poort 5503

94.6 Banking trojans

Voor cybercriminelen is er een ruim aanbod van software waarmee bankrekeningen kunnen geplunderd worden. Een voorbeeld van zo'n *banking trojan* is Zeus. Zeus is een Trojaans paard dat bankinformatie steelt. De diverse botnets van Zeus hebben miljoenen computers gecompromitteerd in 196 landen (vooral in Egypte, VS, Mexico, Saoedi-Arabië en Turkije. In de criminele wereld wordt Zeus verkocht voor 3000 tot 4000 dollar. Bij criminelen die gespecialiseerd zijn in financiële fraude is Zeus zeer populair. Zeus steelt de informatie die in HTTP-formulieren wordt ingevoerd, accountgegevens die zijn opgeslagen in de Windows Protected Storage, en certificaten van FTP- en POP-abonnementen. Het modificeert HTML-pagina's van websites, zoekt naar bestanden en uploadt deze, wijzigt bestanden van lokale gastheren en vernietigt cruciale registratiesleutels.

Door het succes van Zeus verschenen er talrijke copycats op de markt die probeerden Zeus te imiteren. In concurrenten zoals SpyEye is een "kill Zeus" ingebouwd waardoor botnets van Zeus kunnen worden overgenomen. Dit leidde tot een botnetoorlog. Criminele groepen vechten hun onderlinge strijd uit door het kapen van elkaars botnets.[1]

Hoofdstuk 95

Uitgebreid gevalideerd SSL-certificaat

PayPal-EV-certificaat in Mozilla Firefox

Een **uitgebreid gevalideerd SSL-certificaat** of **EV-certificaat** (EV-SSL, Engels: *Extended Validation Certificate*) is een X.509-certificaat uitgegeven door een certificaatautoriteit (CA) via het public key infrastructure-systeem. Een EV-certificaat voldoet aan specifieke eisen omtrent identiteitscontrole. Aan deze eisen moeten uitvoerig voldaan zijn voordat een certificaat wordt toegekend door een CA. Certificaten uitgegeven door een CA onder de EV-richtlijnen zijn niet structureel verschillend van andere certificaten en bieden bijgevolg geen betere encryptie dan andere, goedkopere certificaten. Ze zijn echter wel voorzien van een CA-specifieke identificatie zodat EV-ondersteunde software deze certificaten kan herkennen.

De criteria die gebruikt worden om EV-certificaten uit te geven zijn bepaald in de *Guidelines for Extended Validation Cerficates* (richtlijnen voor EV-certificaten). De richtlijnen worden opgesteld door het CA/Browser Forum, een nonprofitorganisatie. Deze organisatie bestaat uit belangrijke certificaatautoriteiten, ontwikkelaars van internetsoftware en vertegenwoordigers van controleberoepen en juridische beroepen.

95.1 Compatibele software

Ondersteuning voor de meeste EV-certificaten is ingebouwd in Google Chrome, Internet Explorer, Mozilla Firefox, Opera en Safari.[1]

95.2 Zie ook

- Cryptografie
- Secure Sockets Layer (SSL)

95.3 Externe links

- (en) CA/Browser Forum
- (en) Richtlijnen voor het uitgeven van EV-certificaten

Hoofdstuk 96

Update (software)

Updaten betekent letterlijk actualiseren in het Engels. Het kan van toepassing zijn op alles wat naar een nieuwere variant is bijgewerkt. Echter in de context van het algemene spraakgebruik, duidt het op het bijwerken van software middels een patch.

96.1 Update vs upgrade

Er is een groot verschil tussen een update en een upgrade:

- Een update wordt meestal uitgebracht om ontoelaatbare tekortkomingen, zoals bugs (programmeerfoutjes) of beveiligingsrisico's te herstellen of om een klein deel van het programma te wijzigen. Een upgrade brengt meestal grotere veranderingen met zich mee, zoals volledig nieuwe functionaliteit, een nieuwe gebruikersinterface ...
- Updates zijn meestal te herkennen aan het feit dat het tweede of een later getal van het versienummer met 1 verhoogd wordt. Bijvoorbeeld van 1.1 naar 1.2 of van 1.12 naar 1.13 of van 1.7.2 naar 1.7.3.
  Bij een upgrade verhoogt normaal het eerste getal van het versienummer en wordt het tweede getal terug op 0 gezet. Bijvoorbeeld van 1.5 naar 2.0
- Voor een update hoef je normaal niet te betalen, zelfs niet als het om een commercieel programma gaat. Deze dient immers om een ondeugdelijk product te verbeteren. Voor een upgrade moet je echter meestal bijbetalen (indien het om een commercieel programma gaat). Dikwijls moet je echter niet zoveel betalen als wanneer je het programma voor het eerst zou aanschaffen.
- Updates hebben *meestal* een kleinere omvang dan upgrades.

96.2 Hoe updaten

Er zijn verschillende manieren om een programma te updaten. Welke van toepassing is, verschilt van programma tot programma:

- Men moet een nieuw installatiebestand downloaden en over de vorige versie installeren. Deze werkwijze is erg omslachtig omdat iedere keer het volledige programma opnieuw moet worden geïnstalleerd. Deze werkwijze komt vooral bij kleine programma's voor.
- Men downloadt een installatiebestand dat enkel die bestanden vervangt die daadwerkelijk vernieuwd zijn. Deze werkwijze wordt vooral toegepast door de middelgrote softwarebedrijven.
- Het programma kan zelfstandig de nieuwe updates downloaden en installeren. Deze techniek wordt vooral door de grote softwarebedrijven gebruikt.

De meeste Linuxdistributies beschikken over een updatefunctionaliteit via het pakketbeheersysteem.

96.3 Wanneer updaten

Het wordt aangeraden periodiek te updaten naar de nieuwste versie, of wanneer er problemen zijn met de huidige versie. Deze update brengt meestal buiten het zicht van de gebruiker belangrijke wijzigingen aan. De gebruiker zal zelden het verschil met de vorige versie zien, maar de nieuwe versie zal meestal stabieler zijn (beter werken). Bij updates van besturingssystemen kan het voorkomen dat er gevolgen zijn van het updaten. Sommige functies zijn dan bijvoorbeeld buiten werking gesteld of reageren anders.

Upgrades zijn daarentegen veel grotere wijzigingen. Er moet beter nagedacht worden of het voordelig is om deze te installeren.

Hoofdstuk 97

Valse beveiligingssoftware

Valse beveiligingssoftware (*rogue security software* in het Engels) is een vorm van malware. Gebruikers geloven dat ze een virus op hun computer hebben staan en zo wordt geprobeerd hen te laten betalen voor bepaalde software die het probleem zogezegd zal oplossen. Eigenlijk doen deze programma's niets of bevatten ze virussen. De gebruikers worden meestal in de val gelokt door reclamebanners op het internet waarin ze te lezen krijgen dat ze virussen hebben.

97.1 Geloofwaardigheid

Om zo veel mogelijk mensen te kunnen oplichten, lijken de namen vaak heel geloofwaardig en oprecht. Vaak lijken ze sterk op die van een écht beveiligingsproduct. Bijvoorbeeld, de top vijf namen in de periode van juli 2008 tot juni 2009 waren:

- SpyGuard 2008
- AntiVirus 2008
- AntiVirus 2009
- MacShield
- Spyware Secure
- XP AntiVirus
- SpySheriff

Niet alleen de naam brengt internetgebruikers op een dwaalspoor. Vaak worden er bekende en legale betaalsystemen gebruikt om deze software aan te kopen wat het geheel geloofwaardig maakt.

De gevaarlijkste van alle *valse beveiligingssoftware* is Navashield. Navashield lijkt heel goed te werken, maar als Navashield een tijdje op de computer geïnstalleerd staat, verandert het in een monster. Het programma produceert een vervelend klokgeluid en geluiden van uitlachen (ook wel *spammen* door de luidsprekers). Ongeveer elke tien seconden opent Navashield pornowebsites.

Hoofdstuk 98

Videokaart

Asus Nvidia 7600 GS

Een **videokaart** of **grafische kaart** is een interface tussen een computer en het beeldscherm. Het belangrijkste onderdeel van moderne grafische kaarten is de GPU, die zoveel mogelijk grafische taken overneemt van de processor (CPU). Niet alle computers hebben anno 2016 nog een discrete ('losse') videokaart. De meeste pc's, laptops en tablets die worden geproduceerd, hebben een videokaart die is geïntegreerd in de processor of het moederbord. Losse grafische kaarten worden normaal gesproken in de computer zelf ondergebracht.

98.1 Soorten videokaarten

Grofweg zijn er twee typen videokaarten te onderscheiden:

- Onboard: De elektronica is in het moederbord of de processor geïntegreerd. Deze versie bezit vaak geen eigen geheugen, maar gebruikt het werkgeheugen van het systeem. Deze oplossing biedt standaardprestaties. Omdat de video een deel van het gewone werkgeheugen gebruikt wordt deze oplossing wel Shared Memory Architecture (SMA) genoemd. Dit is afhankelijk van de hoeveelheid die in BIOS is in te stellen. Nieuwere desktop-processors van zowel Intel als AMD bevatten geïntegreerde grafische functionaliteit die de onboard-videokaart in het moederbord overbodig maken.
- Insteekkaart: Deze kaarten worden op het moederbord aangesloten door middel van een bus of een poort. In chronologische volgorde, met steeds betere prestaties, zijn de de volgende architecturen gangbaar in pc-systemen:
  - ISA (Industry Standard Architecture). Deze kaarten worden niet meer geproduceerd.
  - PCI (Peripheral Component Interconnect). Deze worden nog wel geproduceerd, maar niet veel meer. De kaarten zijn niet erg krachtig naar moderne maatstaven.
  - AGP (Accelerated Graphics Port). Deze worden nog wel gemaakt, maar door de lagere bandbreedte ten opzichte van PCI-Express worden ze in geavanceerde systemen niet meer toegepast.
  - PCI-Express (Peripheral Component Interconnect Express). De verbeterde, seriële versie van PCI.

Met de CGA-kaart in 1981 begon de ontwikkeling van videokaarten voor IBM-compatibele pc's. Zie Standaard voor weergavemodus voor de verdere geschiedenis.

Videokaarten zijn sterk in ontwikkeling. Elke nieuwe generatie kaarten levert in het algemeen dubbel de prestaties van de vorige. Steeds meer mensen gebruiken hun computer om spellen op te spelen en zijn bereid daar geld aan uit te geven. De druk om steeds snellere videokaarten te ontwikkelen en de mogelijkheid om grafisch geavanceerdere spellen te ontwerpen versterken elkaar.

98.2 Opbouw

Een videokaart bestaat uit deze onderdelen:

98.2.1 Graphics Processing Unit (GPU)

Een GPU is een speciale processor ontworpen voor het verwerken van grafische data. De GPU berekent de beeldopbouw en versnelt het renderen van 3D-beelden. De prestaties van een GPU kunnen worden uitgedrukt in

flops (doorgaans gigaflops, gezien de snelheid). Enkele onderdelen in moderne GPU's zijn onder andere:

- TMU's (Texture Units): plaatsen, zoals de naam al zegt, de textures over een 3D-model.
- ROP's (Render back-ends): processoren voor raster-operaties zoals blending en anti-aliasing.
- Stream Processors (shaders): verantwoordelijk voor visuele effecten en vortexoperaties. Bij de betere videokaarten zijn hiervan vele aanwezig in de GPU. Ze vervangen het vroegere pixelpipelineprincipe.
- De geheugeninterface. Verzorgt de communicatie met het gebruikte VRAM.

De belangrijkste fabrikanten zijn nVidia en AMD.

98.2.2 Videogeheugen (VRAM)

Hierin wordt een digitale representatie van het beeld opgeslagen, alsmede sjablonen hiervoor, zoals textures. Hoe meer geheugen er op een videokaart zit, hoe meer voorbewerkte beeldonderdelen erin passen. Hierdoor hoeven minder compromissen tussen snelheid en detailweergave gesloten te worden. Een groot videogeheugen is bij hoge resoluties belangrijker, want hoe hoger de resolutie, des te meer pixels er zijn en hoe meer geheugen er moet zijn om de textures op te kunnen slaan. Ook gebruikt anti-aliasing veel geheugen. Dit wordt vooral gebruikt in spellen. Een kaart met een groter geheugen is alleen aanmerkelijk sneller als die een meer geavanceerde chipset bezit. De grootte van het geheugen wordt uitgedrukt in bytes en de snelheid in hertz (Hz). De bandbreedte van het geheugen wordt uitgedrukt in gigabyte per seconde (GB/s) en kan berekend worden door de busbreedte in bits te vermenigvuldigen met de snelheid in hertz.

Net als het RAM gebruikt het videogeheugen DDR-technologie.

- HBM: Voor het eerst toegepast in 2015 in de Fury-serie van AMD. HBM is, in tegenstelling tot vorige VRAM-standaarden, op de videochip zelf vastgezet. Hierdoor zijn hogere snelheden en een lager verbruik mogelijk terwijl de grafische kaart juist kleiner wordt.
- GDDR5X: Dit wordt toegepast vanaf 2016 in sommige kaarten, zoals de GTX 1080 van NVIDIA. GDDR5X heeft meer bandbreedte dan GDDR5, maar lagere productiekosten dan HBM.
- GDDR5: Dit wordt toegepast vanaf 2008 op bepaalde AMD(ATI)-videokaarten, zoals de HD4870. Het is DDR-geheugen, dat twee maal 32 keer per klokperiode data kan verwerken. Onder andere nVidia's Fermi-architectuur en de serie ATI Radeon HD5000 en oudere HD4870/HD4890 maken gebruik van dit type geheugen. Het draait dan ook meestal rond de 4,7 GHz tot 5,1 GHz.
- GDDR4: uitgevonden in 2006 en wordt toegepast sinds 2007. Het is DDR-geheugen, dat 32 keer per klokperiode data kan verwerken. GDDR4-geheugen werkt op lagere spanningen dan GDDR3, DDR2- en DDR-geheugen.
- GDDR3: In 2005 de meest gebruikte soort. Dit is DDR-geheugen, dat twee keer per klokperiode data kan verwerken. GDDR3-geheugen werkt op lagere spanningen dan DDR2- en DDR-geheugen.
- DDR2: Sneller dan DDR-geheugen doordat het vier keer per klokperiode data kan verwerken. DDR2-geheugen wordt echter vele malen warmer dan DDR- en GDDR3-geheugen, waardoor de toepassing op grafische kaarten wordt beperkt.
- DDR-geheugen: Trager dan GDDR3, maar goedkoper. DDR-geheugen zit vaak op de goedkopere kaarten.
- Gedeeld: Hierbij wordt geheugen van de computer zelf gebruikt. Dit is trager, maar wel goedkoper dan DDR op de videokaart.

98.3 Aansluitingen

De meest voorkomende aansluitingen tussen de videokaart en monitor zijn:

- Digital Visual Interface (DVI)
- S-Video (tv-uitgang)
- VGA (D-Sub)
- HDMI
- DisplayPort

98.4 Koelers

Tegenwoordig zijn videokaarten standaard met een koeler uitgerust. Deze koelt voornamelijk de GPU en het VRAM. Hoe hoger het verbruik van de videokaart, des te meer warmte hij produceert. Temperaturen boven de 80 graden Celsius vormen geen uitzondering. Verder gebruiken oude videokaarten vaak meer stroom in verhouding tot hun prestaties.

De drie meest voorkomende vormen van koeling zijn:

- Passieve koeling: Hierbij is een groot koelprofiel met ribben toegepast. Het profiel neemt de warmte van de GPU en andere onderdelen op en geeft de warmte

weer af aan de omringende lucht. Passieve koelers maken geen geluid. Ze zijn vaak van koper gemaakt, omdat dit de warmte beter geleidt dan aluminium.

- Actieve luchtkoeling: een ventilator is boven op het koelprofiel geplaatst. Deze blaast de warme lucht tussen de koelribben weg. Dit is effectiever dan passieve koeling. Deze vorm van koeling produceert geluid. De warme lucht kan weggeblazen worden in de computerkast, maar kan ook naar buiten geblazen worden.

- Waterkoeling: Hierbij wordt met vloeistof de warmte van het koelblok op de videokaart naar een radiator elders getransporteerd. Waterkoeling wordt gebruikt als actieve luchtkoeling niet toereikend is, zoals bij overklokken het geval kan zijn. Dankzij het grote koeloppervlak van de radiator is er minder luchtverplaatsing nodig zodat waterkoeling ook stiller is. Waterkoeling is duur in aanschaf en vraagt ook geregeld onderhoud. Er zijn grafische kaarten waarbij de waterkoeling al door de fabrikant gemonteerd is.

Een videokaart met een passieve koeling hoeft niet altijd een stillere computer op te leveren. De warmte van de videokaart verwarmt in dat geval de computer van binnen. Er is dan alsnog een ventilator nodig om de warme lucht naar buiten te blazen. Een ventilator op de videokaart die de warme lucht meteen naar buiten blaast kan soms een stillere computer opleveren.

98.5 Extra stroomtoevoer

De PCI-E x16-sleuf kan maximaal 75 watt leveren. Dit is voor sommige videokaarten te weinig. Deze kaarten bezitten een of meer extra voedingsaansluitingen via een kabeltje. Hieraan zit meestal een 6 pinsconnector (stekker). Sommige videokaarten vragen nog meer stroom en passen een 8 pinsconnector toe. Ook de combinaties 2x6 pins, 2x8 pins, 1x6 pins+1x8 en 3x8 pins komen voor. Deze stroom moet rechtstreeks vanaf de voeding komen. Hiervoor is een sterke en moderne voeding nodig. Verder gebruiken oude videokaarten een 4 pin-Molexconnector.

98.6 Meerdere videokaarten tegelijk in gebruik

In een computer kunnen meerdere videokaarten geplaatst worden. Deze kunnen samenwerken voor betere prestaties, zoals bij een SLI- of Crossfire-opstelling. Ze kunnen ook onafhankelijk van elkaar gebruikt worden om meerdere gebruikers tegelijkertijd te laten werken zoals bij multiseat.

98.6.1 SLI en Crossfire

Het is mogelijk om twee, drie of zelfs vier videokaarten te laten samenwerken bij de beeldopbouw. Het rekenwerk wordt dan verdeeld over de aan elkaar gekoppelde kaarten. Deze technologie heet SLI bij nVidia-videokaarten en Crossfire bij ATI-kaarten. De snelheidswinst is beperkt, doordat er rekenkracht voor extra overhead wordt gebruikt.

SLI van Nvidia werkt alleen met identieke kaarten met dezelfde chipset. Zo kan een Asus 8800GT met een MSI 8800GT gecombineerd worden, maar geen Asus 8800GT met een Asus 7900GT. Die twee kaarten worden meestal met een (verharde) kabel aan elkaar verbonden.

ATI's Crossfire werkt anders. Bij Crossfire maakt het niet uit welk merk/chipset gebruikt wordt, mits die Crossfire ondersteunt. Een nadeel is dat Crossfire zich terugschakelt naar de traagste kaart, daarom is het het beste om twee identieke kaarten te nemen.

De snelheidsverschillen tussen SLI en Crossfire zijn minimaal.

98.6.2 Multiseat

Als meerdere videokaarten in een computer geplaatst worden, is het mogelijk om met meerdere gebruikers op dezelfde computer te werken. Dit wordt aangeduid met multiseat. Elke gebruiker heeft dan een eigen beeldscherm, muis en toetsenbord. Het aantal gebruikers kan variëren van twee tot acht of nog meer.

Voor Microsoft Windows zijn er enkele programma's die dat mogelijk maken.

In Linux is multiseat mogelijk zonder extra programma, doordat de processen in Linux onafhankelijk van elkaar werken. In de praktijk is het echter niet eenvoudig te realiseren. In een multiseat-opstelling in Linux wordt soms voor iedere gebruiker Microsoft Windows door middel van virtualisatie opgestart. Zo lijkt het alsof iedere gebruiker zijn eigen Windows-computer heeft.

Er bestaan ook videokaarten met bijvoorbeeld verscheidene aansluitingen voor beeldschermen. Een multiseat-opstelling is echter eenvoudiger te realiseren met aparte videokaarten.

98.7 Fabrikanten

Een aantal GPU-fabrikanten, van groot naar klein:

- Intel: hoewel Intel voornamelijk CPU's produceert, hebben ze ook grafische kaarten (zoals de Larrabee, voor de professionele markt) en geïntegreerde grafische processoren (die aanzienlijk mindere prestaties leveren dan discrete grafische kaarten).

- nVidia: nVidia maakt de GeForce-serie voor de consument en de Quadroserie voor professioneel gebruik.
- AMD, vroeger ATI: AMD maakt de Radeonserie voor de consument en de Fire/FireGL-serie voor de professionele markt.
- Matrox-chipsets en -kaarten voor de professionele markt. Dit zijn kaarten die meestal speciaal ontworpen zijn voor meer dan één monitor.
    - De fabrikanten verwerken de GPU samen met de andere videokaartonderdelen. Enkele voorbeelden zijn: XFX, EVGA, ASUS, HIS, Point-Of-View, Gainward, Chainteck, Gecube, Expert Vision, Leadtek, MSI, Sapphire en Club3D. Er zit weinig verschil tussen de kaarten van deze fabrikanten: meestal een ander softwarepakket, type geheugen en prijs. Soms wijkt een fabrikant af van de standaardkaart en verandert de klokfrequenties door ze standaard over te klokken. Dit wordt vaak aangeduid met *OC* (overclocked). Ook kiezen sommige fabrikanten een andere koeler, die geluidsarmer is of beter koelt.
- 3Dlabs die richt zich op de professionele markt, maar is een kleinere speler.
- S3, die de Chromeserie maakt. Deze kaarten onderpresteren, vergeleken bij hun directe concurrenten.

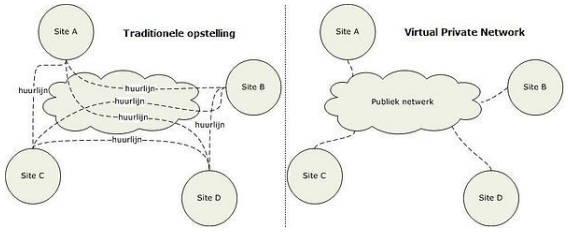
98.8 Zie ook

- GPGPU
- CUDA

Hoofdstuk 99

Virtueel Particulier Netwerk

Een **Virtueel Particulier Netwerk** of **Virtueel Privénetwerk** (Engels: *Virtual Private Network, VPN*) is een goedkope manier om een Local Area Network (LAN) over een bestaande verbinding, een Wide Area Network (WAN), zoals het internet, uit te bouwen met behoud van vertrouwelijkheid.



WAN topologie

99.1 Data

Deze dienst maakt gebruik van een reeds bestaand netwerk, doorgaans het internet, om informatiedeling tussen geografisch gescheiden netwerken mogelijk te maken alsof er een dedicated network was. De verzonden data kunnen het best beveiligd worden zodat de integriteit, autorisatie en authenticiteit van de data over dit onderliggende netwerk gewaarborgd blijven. De eindgebruikers zullen in principe niet merken dat er een VPN gebruikt wordt. Technisch zijn er ondertussen tal van protocollen uitgewerkt die deze dienst beschikbaar maken. Het bekendste en courantste protocol vandaag de dag is IPsec.

99.1.1 Malafide gebruik

Met VPN kan de gebruiker zich onbeperkt van IP-adressen voorzien. Dit wordt vaak gebruikt door gebruikers die verbannen worden van bijvoorbeeld een forum of chatbox (IP-blokkade) of wiki-site. Door via VPN een ander IP-adres te gebruiken, kan zo'n gebruiker toch terugkeren naar dit forum of deze chatbox. Daarom stellen beheerders tegenwoordig vaak beperkingen aan het gebruiken van dit soort netwerken.

99.2 Technologisch abstract

Een VPN is een netwerk dat door een ander netwerk (gewoonlijk het internet)[1] getunneld wordt. Hierdoor wordt de theoretische topologie vereenvoudigd, de praktische routering daarentegen zal complexer worden afhankelijk van het onderliggende netwerk. Een VPN tracht de voordelen van het onderliggende netwerk te gebruiken en de nadelen ervan te compenseren. De primaire problemen met het datatransport over een onderliggend netwerk zijn de veiligheid en de betrouwbaarheid. Door encryptie en controlemaatregelen (bijvoorbeeld CRC) kan een goed uitgewerkt VPN toch de integriteit, autorisatie en authenticiteit van de verzonden data verzorgen. Al deze beveiligingsmaatregelen moeten bovendien zo transparant mogelijk geïmplementeerd worden, opdat de eindgebruikers er eenvoudig gebruik van kunnen maken. Verder moet er ook rekening gehouden worden met wetten[2] die van kracht zijn omtrent de privacy van data.

99.3 Evolutie

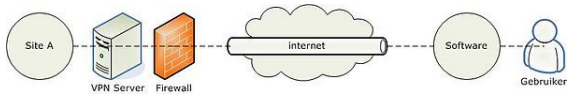
Door de opkomst van de ICT werden binnen veel bedrijven de computer en het Local Area Network (LAN) al snel noodzakelijk. Hier hield de informatisering echter niet op. De LAN's van verschillende vestigingen of afdelingen moesten met elkaar verbonden worden om het delen van informatie mogelijk te maken en om uniforme netwerkdiensten aan te kunnen bieden (dataopslag, e-mail etc.). Daarnaast heeft het ook voordelen als een verkoper onderweg of een thuiswerker toegang kan krijgen tot dit netwerk. De bedrijven moesten dan inbellijnen of huurlijnen regelen om zo het Wide Area Network uit te bouwen waarbinnen deze voordelen en diensten mogelijk waren. Dit was duur. Vanuit dit inzicht groeide het idee om een reeds bestaand netwerk (met name het internet) aan te wenden bij de uitbouw van een WAN. Hierdoor vallen de kosten van de verschillende huurlijnen weg en wordt het netwerk algemeen toegankelijker. De bedrijven kunnen zo hun operationele kosten verminderen door de netwerkdiensten voor een WAN uit te besteden aan een

internetprovider.

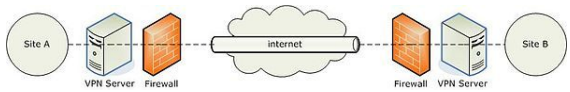
99.4 Classificaties

Er zijn tal van indelingen die gemaakt kunnen worden om VPN's van elkaar te onderscheiden. De voornaamste classificaties zijn hieronder opgesomd:

99.4.1 Opstelling



Remote-access VPN



Site-to-site VPN

Er zijn twee courante opstellingen waarin een VPN geconfigureerd kan worden. Ten eerste is er de remote-access-VPN. Hierbij zal een gebruiker toegang krijgen tot de private LAN van een organisatie door middel van een VPN. In de eerste plaats valt dan te denken aan werknemers die thuis of onderweg toegang willen hebben tot het private bedrijfsnetwerk. Ten tweede is er de site-to-site-VPN. Hierdoor kan een organisatie de netwerken van geografisch gescheiden vestigingen met elkaar verbinden. Het resultaat van deze verbinding wordt een intranet-VPN genoemd. Een andere mogelijkheid is dat verwante organisaties (bijvoorbeeld leveranciers en magazijniers) elkanders netwerk onderling verbinden om zo een intelligent geheel te bekomen, opdat de productiviteit stijgt. Dit betreft een extranet-VPN. Daarnaast bestaan er natuurlijk nog andere opstellingen afhankelijk van de reële situatie. Deze zijn meestal te herleiden tot een variant op de bovengenoemde opstellingen.

99.4.2 IETF

De Internet Engineering Task Force (IETF) onderscheidt enkele verschillende VPN's. Het deelt de verschillende technologieën in op basis van het beheer van en tussen de verschillende netwerknodes. Hierdoor kan dan geclassificeerd worden op basis van zaken als beveiliging of quality of service (QoS). Bij een netwerk dat centraal beheerd wordt, spreekt de IETF[3] van een intranet. Als er meerdere beheersposten in het spel komen, dan wordt gesproken over een extranet. Deze indeling sluit logisch nauw aan bij de gelijknamige classificaties van de site-to-site-indeling.

Daarnaast definieert IETF ook nog een provider-provisioned-VPN. Een PPVPN[4] is een totaalpakket voor een VPN-dienst die een internetprovider aanbiedt via zijn netwerk (zijnde het internet of specifiek aparte lijnen voor VPN). Het is specifiek gericht op bedrijven en organisaties die een WAN wensen uit te bouwen. In de praktijk betekent dit meestal dat de internetprovider een service level agreement (SLA) afsluit waarbinnen de kwaliteit van het datatransport verzekerd wordt.

99.4.3 Beveiligingsmodel

Het onderliggende netwerk dat gebruikt wordt zal ofwel 'vertrouwd' of 'niet vertrouwd' worden door het VPN. Het valt aan te raden om het onderliggende netwerk simpelweg niet te vertrouwen, zeker niet als dit het internet is. Het VPN-protocol moet dan in technologieën voorzien om de beveiliging te verzorgen. Als men toch het onderliggende netwerk vertrouwt, wordt er gesproken over een 'trusted VPN' (of een 'Actual Private Network'). Hierbij wordt de beveiliging volledig afgehandeld door het onderliggende netwerk, zonder eigen controlemogelijkheden.

Een essentieel stuk van de beveiliging is de authenticiteit van de data. Dit wil zeggen dat de originaliteit en de herkomst van de data betrouwbaar moeten zijn. Een beveiligingsmodel kan ervoor kiezen om eerst de authenticiteit van de deelnemers aan de VPN-verbinding te controleren alvorens de eigenlijke verbinding op te zetten. Een andere mogelijkheid is om de authenticiteit te verzorgen bij de eigenlijke transmissie.

99.5 Beveiliging

VPN-technieken kunnen ook worden gebruikt om de beveiliging van een eigen netwerk te verbeteren, maar ze zijn in de eerste plaats ontworpen om veilig transport over een onveilig netwerk mogelijk te maken.

99.5.1 Topologie

In de eerste plaats zal het private netwerk gescheiden moeten worden van het onderliggende netwerk door middel van een firewall. Deze module zal zowel binnenkomend als uitgaand verkeer analyseren en zo nodig stoppen: de module kan als een filter worden beschouwd. De firewall moet strategisch opgesteld staan in de verbinding tussen het private en publieke netwerk. Een firewall biedt een hardwarematige isolatie van het private netwerk om ongewenste bezoekers te vermijden. Het is imperatief dat openingen in de firewall voor VPN-doeleinden de algemene beveiliging niet ondermijnen.

Vlak achter deze firewall zal er bij site-to-site-VPN een AAA-server (authenticiteit, autorisatie en accounting) moeten volgen die VPN-pakketten kan vertalen, zodat

die ofwel op het private netwerk kunnen routeren, ofwel klaar zijn om verzonden te worden over het publieke netwerk. Dit wordt praktisch geïmplementeerd door een daemon die het VPN-protocol verzorgt op een dedicated-VPN-server. Bij remote-access-VPN zal de gebruiker lokaal op zijn eigen computer software moeten gebruiken om het VPN-protocol uit te voeren. Een firewall kan eventueel ook softwarematig geïmplementeerd worden.

99.5.2 Encryptie

Encryptie wordt bij tal van protocollen gebruikt om geheimhouding van data te realiseren. Bij encryptie zullen de data getransformeerd worden naar een onleesbare vorm, de zogenaamde cyphertekst. Door middel van een sleutel kan de ontvanger dan een omgekeerde transformatie uitvoeren, waardoor de tekst weer leesbaar wordt. De meest performante encryptietechnieken vandaag de dag zijn 3DES en AES. AES heeft altijd de voorkeur vanwege zijn sterkere crypto-eigenschappen in vergelijking met 3DES. 3DES is verouderd en mag alleen gebruikt worden als er geen mogelijkheden zijn om AES te gebruiken.

99.5.3 Tunneling

Bij tunneling wordt een pakket voor het private netwerk geëncapsuleerd binnen een nieuw pakket om over het publieke netwerk verzonden te worden. Een eerste reden hiervoor is om het originele pakket compatibel te maken met het publieke netwerk. Deze stap kan met de werking van een bridge vergeleken worden. Een andere reden is de beveiliging van het originele pakket. Het originele pakket kan namelijk volledig versleuteld worden, waarna het geëncapsuleerd zal worden binnen een nieuw pakket. Het geëncapsuleerde pakket zal dan verzonden worden via het onderliggende netwerk en na aankomst uitgepakt worden, zodat met het originele pakket verder gewerkt kan worden. Tunneling is een veelgebruikte techniek bij tal van VPN-implementaties.

99.6 Voordelen

99.6.1 Technologische voordelen

Het succes van een goed uitgewerkt VPN hangt in beduidende mate af van het internet. Tal van de voordelen van een VPN vinden namelijk hier hun beginsel. Door de brede beschikbaarheid van het internet zal het private netwerk algemeen toegankelijker worden. Verder zal de verbinding tussen de verschillende uiteinden van een VPN-verbinding maar moeilijk verbroken kunnen worden, daar de routering over het internet zoveel verschillende alternatieven biedt. Hierdoor neemt de betrouwbaarheid toe. Daarnaast zal het internet ook nog een deel van de schaalbaarheid voor zijn rekening nemen; het kan een grote variëteit qua datatransport aan. Een ander deel van de schaalbaarheid zal de technologie zelf moeten oplossen. Te denken valt bijvoorbeeld aan het aantal gebruikers die tegelijkertijd een VPN opzetten of de grootteorde van de getransporteerde data. Verder moet de technologie ook nog de veiligheid garanderen. De kern van deze voordelen is samengevat in de volgende opsomming:

- Algemeen toegankelijk
- Veilig (authenticiteit, autorisatie & integriteit)
- Betrouwbaar
- Schaalbaar

99.6.2 Praktische voordelen

Voor de bedrijven of organisaties die een WAN opzetten door middel van een VPN zijn er tal van praktische voordelen, vooral in vergelijking met de alternatieven (huurlijnen etc.). Ten eerste zal iedere medewerker het private netwerk eender waar ter wereld kunnen benaderen via het internet. Op de macroschaal zal dit de algemene productiviteit ten gunste komen. Verder is het opzetten en onderhouden van een VPN goedkoper dan bij de alternatieven. Al wat er nodig is, is dedicated hardware en software gecombineerd met toegang tot het internet. In vergelijking met de alternatieven is dit een investering die snel zal renderen. De kern van deze voordelen wordt in de volgende opsomming gegeven:

- Globaal beschikbaar
- Verhoogde productiviteit
- Goedkoper
- Snelle return on investment

99.7 Protocollen

- IPsec, IP security, ontwikkeld door IETF, werkt op basis van twee headers: de Authentication Header (AH) en Encapsulating Security Payload (ESP), verplicht gebruik bij IPv6
- SSL/TLS, Secure Sockets Layer/Transport Layer Security, geschikt voor tunneling, niet specifiek ontwikkeld voor VPN-doeleinden
- L2F, Layer Two Forwarding, ontwikkeld door Cisco, geschikt voor tunneling, geen encryptie mogelijk, niet specifiek ontwikkeld voor VPN-doeleinden
- PPTP, Point to Point Tunneling Protocol, ontwikkeld door Microsoft, geschikt voor remote-access-VPN

- L2TP, Layer Two Tunneling Protocol, combinatie van L2F en PPTP, geschikt voor remote-access-VPN, kan simultaan meerdere tunnels onderhouden voor een gebruiker
- OpenVPN, een open standaard vergelijkbaar met SSL VPN
- IKEv2, een nieuwe soort VPN. Gebouwd op Oakley protocol en ISAKMP.

Hoofdstuk 100

Virtuele gemeenschap

Een **virtuele gemeenschap**, **internetgemeenschap** of **online gemeenschap** is een groep mensen die communiceren en/of samenwerken, met behulp van het internet of een andere informatietechnologie, in plaats van elkaar in levenden lijve te ontmoeten. In het Nederlands taalgebied wordt voor de term 'gemeenschap' ook regelmatig 'community' (meervoud: communities) gebruikt, ontleend aan het Engels.

100.1 Algemeen

Hoewel het begrip virtuele gemeenschap pas rond de eeuwwisseling algemeen bekend werd, is het verschijnsel dat mensen zich met elkaar verbonden voelen via een communicatiemedium veel ouder. (Brief)schrijvers in Europa tijdens en na de renaissance voelden zich waarschijnlijk evenzeer met elkaar verbonden als hedendaagse internetgebruikers. De komst van computernetwerken heeft sinds de jaren zeventig de communicatiesnelheid sterk verhoogd. Bij de toenemende populariteit van het internet in de jaren tachtig en negentig hebben veel meer mensen met diversere achtergronden toegang tot elkaar.

100.1.1 Begin

De eerste interessegroepen op het internet hadden contact via e-mail en Usenet. Programmeurs hebben daarnaast gezocht naar mogelijkheden om als geografisch verspreide groep tezamen aan een project te werken, daaruit zijn hulpmiddelen als Git en wiki's ontstaan.

Met de komst van computernetwerken voor bedrijven ontstonden producten als Lotus Notes om het samenwerken van vele medewerkers op verschillende locaties te vereenvoudigen.

100.1.2 Beschrijving in literatuur en wetenschap

Progressieve denkers zoals de Amerikaan Charles Cooley in het begin van de 20e eeuw stelden zich een maatschappij voor waarin de leden sterk met elkaar waren verbonden door middel van een stijgend gebruik van massamedia. Ook bekend is de term 'gemeenschap zonder verwantschap' (Engels: *community without propinquity*), naar voren gebracht door de socioloog Melvin Webber in 1963.

In 1985 ontwikkelde zich in Sausalito, nabij het Californische San Francisco een elektronische discussieclub genaamd The WELL (een afkorting van *The Whole Earth 'Lectronic Link*). Deze door Stewart Brand en Larry Brilliant gestarte gemeenschap kan als een van de eerste internetgemeenschappen beschouwd worden. Daarnaast worden de eerste mailinglijsten als een van de eerste virtuele gemeenschappen beschouwd. Een van de eerste Nederlandse community's die als zodanig gezien wordt, is De Digitale Stad, waarvan ook De Digitale Metro deel uitmaakte.

Howard Rheingold was de eerste die in 1993 in zijn boek *The Virtual Community* (Nederlands: "De virtuele gemeenschap") deze term gebruikte.

100.1.3 Commercialisering

Onder het Web 2.0-concept ontdekten verschillende bedrijven het ontstaan en gebruik van virtuele gemeenschappen als bron van economische winst. In 2005 waren dat bijvoorbeeld Flickr, Hyves en delicious. In 2012 werd het online sociale landschap bepaald door netwerken als Facebook, Twitter, Instagram en het opkomende Google+.

Kenmerkend aan deze vormen van gemeenschap is de laagdrempelige toegang die doorgaans geen geld kost voor het gemeenschapslid. De winst ontstaat uit de door leden gegenereerde informatie, bijvoorbeeld in de vorm van eigen interesses, sociale contacten of ook inhoud zoals foto's, video's en teksten die de gebruikers ter uitbating aan het bedrijf schenken. Advertenties zijn een verdere inkomstenbron.

100.1.4 Open source

In de stijl van de opensourcebeweging ontstonden meerdere samenwerkingsprojecten waarbij de leden van de

virtuele gemeenschap samen werkten aan een bepaald doel, zoals bijvoorbeeld Wikipedia.

100.1.5 Mengvormen

In forums deelt men op websites informatie over bepaalde onderwerpen zoals aanvankelijk via Usenet en e-maillijsten. De controle over een forum ligt gewoonlijk bij de website-eigenaar.

Sommige online spelletjes hebben zich tot virtuele gemeenschappen ontwikkeld. Zie bijvoorbeeld MMORPG's.

100.2 Overwegingen

In commerciële virtuele gemeenschappen is het gebruik van de eigen naam doorgaans verplicht. Elders is (pseudo)anonimiteit mogelijk. Dat biedt de gebruiker mogelijkheden zich zo te presenteren als hij zelf wil. Anderzijds zijn overheden veelal huiverig voor zulke anonimiteit uit angst dat de grenzen van de vrijheid van meningsuiting overschreden zouden kunnen worden of dat criminele samenzweringen te zeer vergemakkelijkt worden.

Bij virtuele gemeenschappen is er sprake van een gemengde werkelijkheid wanneer de werkelijke wereld en een virtuele (schijnbare) wereld sterk met elkaar vermengd zijn. Deze vermenging geeft dan een indruk van een complete werkelijkheid. Onder psychologen en sociologen wordt gediscussieerd over de gevolgen en mogelijke gevaren daarvan.

100.3 Soorten virtuele gemeenschappen

- BBS'en
- Instant messaging
- IRC
- Internetforums
- Mailinglijsten
- Micronaties
- Online computerspellen
- Opensourcesoftware
- Peer-to-peer
- Sociaalnetwerksites
- Usenet
- Webstrips
- Weblogs
- Wiki's

100.4 Externe link

- (en) *The Virtual Community* van Howard Rheingold

Hoofdstuk 101

Wachtwoord

Het inlogformulier op Wikipedia vraagt naar de gebruikersnaam en wachtwoord

Een **wachtwoord** (in computerjargon spreekt men ook over **paswoord** of **password**[1][2]) is een afgesproken woord of zin waaraan belanghebbenden elkaar herkennen. Het wachtwoord is geheim voor buitenstaanders.

Een wachtwoord wordt zo ook gebruikt om toegang te verschaffen tot bijvoorbeeld gebouwen of computers die met digitale middelen zijn beveiligd. Het wachtwoord is alleen bekend aan degene die toestemming heeft om het te gebruiken.

In de ICT is het wachtwoord normaliter gekoppeld aan een gebruikersnaam die identificeert wie er toegang mag hebben.

Door het achterhalen van een wachtwoord kan een derde persoon onterecht gebruikmaken van andermans informatie. Het wachtwoord kan achterhaald worden door dit af te kijken, door een wachtwoordenbestand te ontcijferen, of door verschillende eenvoudige wachtwoorden te proberen. Om die reden wordt in de meeste professionele omgevingen een zogenaamd *complex* wachtwoord vereist dat regelmatig door de eigenaar ervan moet worden gewijzigd.

Een variant op het wachtwoord is het sjibbolet waarmee men, bijvoorbeeld in oorlogstijd, vriend van vijand onderscheidt. Een voorbeeld is *"scilt ende vriend"* waarmee volgens de legende franskiljons tijdens de Brugse metten ontmaskerd zouden zijn,[3] of *"Scheveningen"* dat tijdens de Duitse aanval op Nederland in 1940 eenzelfde functie had.[4]

101.1 Wachtwoordcomplexiteit

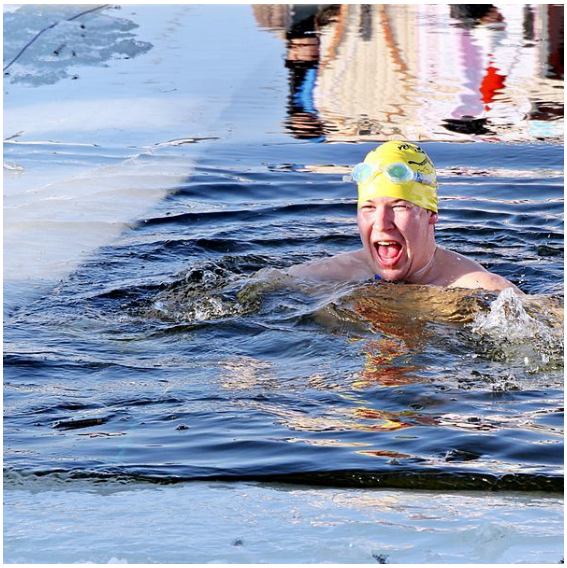
Een goed wachtwoord is niet te eenvoudig en niet te kort. Eenvoudige, korte wachtwoorden worden namelijk veel gebruikt en zijn dus snel te achterhalen.[5] Een goed wachtwoord is niet eenvoudig te raden, en kan bovendien niet op methodische wijze worden achterhaald, aangezien dit onhaalbaar lang (decennia) zou duren. Er zijn een aantal mogelijkheden om een eenvoudig wachtwoord, bijvoorbeeld *"zon"*, te vinden:

- Willekeurig raden.[6] Voorbeelden zijn: je achternaam, de naam van je partner, namen van huisdieren, een geboortedatum, en je favoriete muziekartiest, sportman of voetbalploeg. Dit is een zeer eenvoudige methode om wachtwoorden te raden, maar ook zeer eenvoudig om te vermijden.
- Een *brute-force*-aanval. Hierbij worden domweg alle mogelijkheden (bijvoorbeeld *aaa*, *aab*, *aac*, *aad*, ..., *zol*, *zom*, ***zon***) geprobeerd.
- Gebruik van een woordenboek of -lijst. Hierbij wordt een lijst van veel voorkomende woorden nagelopen (bijvoorbeeld *zonder*, *zolder*, *zowel*, *zondag*, ***zon***). Alternatief kan ook een volledig woordenboek nagelopen worden. Dit is eenvoudig te vermijden door geen standaardwoorden te gebruiken.

Daarnaast kan het wachtwoord geraden worden door er gewoon naar te vragen. Dit wordt 'social engineering' genoemd.

101.1.1 Veilige wachtwoorden

Het is erg moeilijk om een 'veilig' wachtwoord te onthouden. Een eerste mogelijkheid is een willekeurige combinatie van letters (kleine letter en hoofdletter), cijfers en leestekens. Dit bemoeilijkt het raden omdat er veel meer mogelijkheden zijn. Deze combinaties zijn vaak moeilijk te onthouden en moeilijk om in te geven op draagbare toestellen. Voorbeelden zijn "*SleJnn12][*" of "*qSK12$%j*"



"IJsberen met gele badmuts" *is een veilig wachtwoord dat toch eenvoudig te onthouden is.*

Een andere mogelijkheid is een lang wachtwoord opgebouwd uit een combinatie van al dan niet bestaande woorden, ook wel wachtzinnen of *pass phrases* genoemd.[7] Een eenvoudige manier om een dergelijk lang wachtwoord te kiezen, is een zin van een aantal willekeurige woorden. Bijvoorbeeld *"IJsberen met gele badmuts"*. Dit is een wachtwoord dat eenvoudig te onthouden is, maar door de 25 karakters toch moeilijk genoeg is om brute-forceaanvallen af te slaan.[8] Wachtzinnen kunnen echter ook aangevallen worden door alle mogelijk zinnen van bijvoorbeeld vier woorden te proberen met behulp van een woordenboek. In het Engels wordt vaak over wordlists gesproken. Deze lijsten kunnen gemakkelijk 75 miljoen woorden uit verschillende talen bevatten. Ze kunnen ook gebruikt worden om gebruikers te beschermen door nieuw bedachte wachtwoorden met de lijst te vergelijken.[9]

De sterkte van wachtzinnen en wachtwoorden van verschillende lengtes en complexiteit kunnen vergeleken worden. Een wachtzin van vier woorden is ongeveer even sterk is als een wachtwoord van zes tot acht willekeurige tekens,[10], mits de woorden op willekeurige wijze gekozen worden. Bijvoorbeeld door de keuze van de woorden door zes dobbelstenen te laten bepalen zoals bij Diceware[11] Een wachtzin als *"kenner franje hup mantra"* is door die willekeurig gekozen woorden niet te vergelijken met een Nederlandse zin. De woorden hebben geen onderling verband en de zin heeft geen taalkundige betekenis. Als toch voor een grammaticaal juiste zin gekozen wordt (zoals het genoemde voorbeeld *"IJsberen met gele badmuts"*), dient de zin langer te zijn dan een wachtzin van willekeurig woorden.

101.2 Versleuteling

Over het algemeen worden wachtwoorden gehasht opgeslagen.

Het hashen van wachtwoorden is een vorm van cryptografie. Een bekendere vorm van cryptografie is cryptografische encryptie (versleuteling) waarbij bijvoorbeeld een tekst met behulp van een sleutel onleesbaar (versleuteld) gemaakt wordt. Het bijbehorende decryptie algoritme zorgt voor omkeerbaarheid: (alleen) als de sleutel is doorgegeven, kan de oorspronkelijke tekst weer teruggekregen worden. Bij hashen wordt echter een cryptografische algoritme gebruikt dat niet omkeerbaar is (net zoals bij een checksum). Het algoritme kan wel een gehashte vorm van het wachtwoord berekenen. Maar andersom bestaat er geen algoritme waarmee het oorspronkelijke wachtwoord weer teruggekregen kan worden. De enige mogelijkheid is alle mogelijke wachtwoorden een voor een te proberen (te hashen) en het resultaat met de gehashte vorm te vergelijken. Iemand die het algoritme kent en toegang heeft tot het bestand waarin de wachtwoorden gehasht opgeslagen zijn, weet dus nog niet wat de wachtwoorden zijn. Bij UNIX is het zelfs regel dat het bestand voor iedereen leesbaar is.

Is iemand zijn wachtwoord vergeten, dan kan de systeembeheerder een nieuw wachtwoord voor hem instellen. Veel websites op het internet sturen desgevraagd een nieuw wachtwoord per e-mail op. Veilige websites slaan enkel de hash op en houden het wachtwoord zelf niet bij, daarom moet je een nieuw wachtwoord kiezen.

101.3 Zie ook

- Eenmalig wachtwoord
- Rainbow table
- John the Ripper

Hoofdstuk 102

Webbrowser

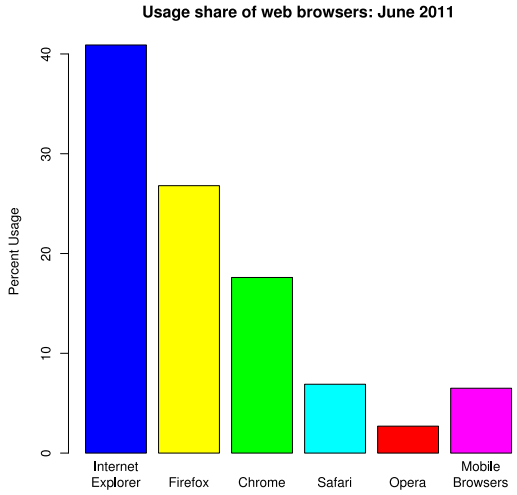
De browser Mozilla Firefox.

Een **webbrowser** (ook wel **(internet)browser**, **bladerprogramma**[1] of **bladeraar**[1] genoemd) is een computerprogramma om webpagina's te bekijken. Populaire browsers zijn Internet Explorer, Mozilla Firefox, Google Chrome, Safari en Opera. Minder bekende, alternatieve browsers zijn Camino, Konqueror, CoolNovo, Lunascape en Seamonkey. Het gebruik van een browser is in de volksmond synoniem aan *surfen op het internet*. Een webbrowser kan zijn opgenomen in een internet suite.

102.1 Webbrowser

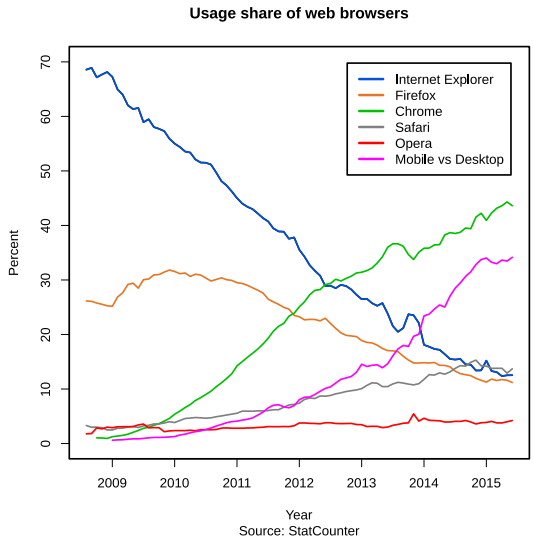
Een browser zet webpagina's, die door een webserver zijn aangeleverd, om in een voor mensen leesbare vorm. Vaste elementen van een webpagina zijn verschillende soorten opmaak van tekst, plaatjes en links naar andere webpagina's. Deze links kunnen worden gebruikt om naar andere pagina's te surfen. Er zijn webbrowsers die dergelijke documenten voorlezen, andere zetten ze om in puntjes op een braillemachine, maar de meeste browserinstallaties geven een *webpagina* weer op een computerscherm en kunnen ook animaties en geluid weergeven. Sommige webbrowsers zijn geïntegreerde pakketten, waarin bijvoorbeeld ook een e-mailclient en een Usenetclient zitten. Vrijwel alle browsers hebben de mogelijkheid om weblocaties op te slaan (bladwijzers), bestanden te downloaden, een geschiedenis bij te houden van waar de gebruiker geweest is en om verschillende soorten media weer te geven. Sommige browsers voegen hier nog andere dingen aan toe zoals meerdere tabbladen, pop-upblockers, advertentiefiltering en automatisch zoeken op een zoekmachine.

102.2 Geschiedenis



Het marktaandeel van webbbrowsers.
Internet Explorer
Mozilla Firefox
Google Chrome
Safari
Opera
Overige

De eerste browser heette *WorldWideWeb* en werd geschreven door de uitvinder van het world wide web, Sir Tim Berners-Lee in 1990 en geïntroduceerd aan zijn collega's bij CERN in maart 1991.[2] De eerste echt populaire browser was NCSA Mosaic, een grafische browser die oorspronkelijk alleen werkte op het Unix-platform, maar al snel ook op Apple Macintosh en Windows. Versie 1.0 kwam uit in 1993. Marc Andreessen, de leider van het Mosaic-team, nam ontslag om zijn eigen bedrijf op te kunnen gaan richten: Netscape Communications Corporation.



Verandering in het marktaandeel van webbrowsers volgens StatCounter.

In 1994 kwam de eerste versie van de Netscape Navigator uit en nam al snel in populariteit toe. Microsoft reageerde hierop door zelf een browser te kopen van het bedrijf Spyglass Inc. en deze te gaan ontwikkelen onder de naam Microsoft Internet Explorer (IE). Dit startte de zogenaamde *browseroorlog*.

In de strijd om de meeste gebruikers werden er veel nieuwe technologieën bedacht door beide bedrijven. Doordat de *uitbreidingen* niet werkten in de browser van de concurrent had dit tot gevolg dat veel webpagina's maar in een van beide programma's goed werkten. Vanaf versie 3.0 van beide programma's begon Microsoft toch langzamerhand de overhand te krijgen, omdat haar browser zich beter aan de standaarden hield en doordat deze over meer functies beschikte. In 1998 eindigde de oorlog omdat het duidelijk was dat Microsofts sterke stijging niet meer te stoppen was. Dit kwam grotendeels doordat Microsoft haar browser bij Windows inbouwde. In de jaren daarna vergrootte Microsoft haar marktaandeel tot meer dan 95%.

Om het tij te keren maakte Netscape haar browser open source. Na enkele moeilijke jaren resulteerde dit in 2002 in de Mozilla Suite. Ook splitste er zich in dat jaar een onderdeel vanaf dat later Mozilla Firefox zou worden. In 2004 werd de 1.0-versie van Firefox uitgebracht. Deze werd snel populairder en voor het eerst in jaren was er een daling in het marktaandeel van IE te zien.

102.3 Standaarden en protocollen

Er wordt getracht browsers aan de standaarden van de standaardorganisatie voor het world wide web, W3C, te laten voldoen. Helaas slagen de meeste browsers niet volledig in het foutloos implementeren van deze standaarden. Het gevolg is dat veel webpagina's code bevatten om in verschillende browsers toch vergelijkbare lay-out en functionaliteit te bieden. Soms wordt er browser sniffing gebruikt om te detecteren welke browser gebruikt wordt, soms conditional comments (Internet Explorer gebruikt deze techniek) of zogenaamde CSS-filters (doorgaans "CSS hacks" genaamd).

Iedere browser maakt gebruik van het HTTP en van HTTPS om te communiceren met de server. Veel browsers bieden tevens voorzieningen om gebruik te maken van FTP- of P2P- en IRC-protocollen zoals het door Opera ondersteunde BitTorrent-protocol. *"Resources"* (pagina's, afbeeldingen, video's etc.) op het internet worden aangegeven door een URL (Uniform Resource Locator), een type URI (Uniform Resource Identifier). Dit is te zien aan het eerste gedeelte van de URL, http://nl.wikipedia.org bijvoorbeeld. Webpagina's worden opgemaakt in HTML of XHTML, vaak in combinatie met CSS. Deze informatie wordt vervolgens verwerkt door de render-engine van de browser om zo de pagina weer te geven. In een pagina zijn vaak afbeeldingen te vinden, meestal worden de types PNG, JPEG of GIF gebruikt.

102.4 Zie ook

- Lijst van webbrowsers
- Bookmarklet
- Plug-in

102.5 Externe links

- (en) Overzicht van historische webbrowsers

Hoofdstuk 103

Weblog

Een **weblog** of **blog** is een persoonlijk dagboek op een website dat regelmatig, soms meermalen per dag, wordt bijgehouden. Meestal gaat het om teksten die in omgekeerd chronologische volgorde verschijnen. De auteur, ook *blogger* genoemd, biedt in feite een logboek van informatie die hij wil meedelen aan zijn publiek, de bezoekers van zijn weblog. Meestal gaat het om tekst, maar soms ook foto's (een fotoblog), video (vlog) of audio (podcast). Weblogs bieden hun lezers vaak de mogelijkheid om – al dan niet anoniem – reacties onder de berichten te plaatsen of een reactie via een Trackback-mechanisme achter te laten.

Het is het persoonlijke of juist het gespecialiseerde karakter dat weblogs interessant maakt voor bezoekers.

Sinds eind 2006 is *microbloggen* populair, een combinatie van bloggen en instant messaging. De bekendste site hiervoor is Twitter. Er bestaan klonen van, zoals Jaiku en Tumblr.

103.1 Geschiedenis

Het concept van een weblog of een groepsweblog ontstond op natuurlijke wijze uit de 'online dagboeken' die mensen vanaf 1994, na de uitvinding van het HTTP-protocol (http), begonnen bij te houden. Jorn Barger is de bedenker van het woord 'weblog' op 17 december 1997. Het ging indertijd immers om het 'loggen van wat er op het web gevonden werd'. Het woord 'blog' werd bedacht door Peter Merholz, die bij wijze van grap het woord *weblog* schreef als *we blog* in de zijbalk van zijn Engelstalig weblog peterme.com rond mei 1999. In augustus 1999 werd het bedrijf Blogger opgericht, met de site www.blogger.com. Omdat Blogger als een van de pioniers de term 'to blog' publiek uitdroeg, spreken de meeste Amerikanen nu van 'blogs' in plaats van weblogs.

Het voor zover bekend eerste Nederlandstalige weblog, Daily Wacko, begon op 1 december 1997.[1] Het betrof hier aanvankelijk een parodienieuwsbrief op de dagelijkse e-mail-nieuwsbrief *Daily Planet*, welke door internetjournalist Francisco van Jole voor internetprovider Planet Internet werd gepubliceerd.[2] De karikatuur *Daily Wacko* groeide later uit tot een meer op zich op zichzelf staand weblog. In het boek *Bloghelden* van auteur Frank Meeuwsen staat beschreven dat onder pioniers van het Nederlandse webloggen het weblog Alt0169.com als *eerste weblog van Nederland* wordt beschouwd. Dit uit de websites *Het Dagelijkse Nieuws* (Jeroen Bosch) en *Pjoe.net* (Joep Vermaat) samengesmolten weblog zou het meeste invloed hebben gehad op de Nederlandse blogosfeer.[3]

Een van de eerste groepsweblogs was Camworld. Jesse James Garrett, een editor van *Infosift*, begon eind 1998 met het bijhouden van een lijst van interessante sites die hij bezocht. De lijst met URL's verstuurde hij naar Cameron Barrett, die de lijst publiceerde op de site *Camworld*. Meer personen begonnen met het insturen van interessante links.

103.2 Vast publiek

Veel weblogs trekken na verloop van tijd een vast publiek, – uiteenlopend van enkele tientallen tot duizenden bezoekers per dag – dat regelmatig komt kijken of er nieuws is verschenen. Bovendien lezen webloggers zelf vaak veel andere – wereldwijd verspreide – weblogs, waardoor nieuws zich via dit medium erg snel verspreidt. Zo speelden weblogs een belangrijke rol in de periode dat de aanslag op de Twin Towers in New York gepleegd werd. Terwijl traditionele nieuwssites door de ongekende belangstelling al snel onbereikbaar raakten, deden webloggers verslag van de gebeurtenissen, die bij sommigen vrijwel onder hun ogen plaatsvonden.

103.3 Bekende personen

In de media neemt webloggen een steeds grotere plaats in. Bekende bloggers zijn bijvoorbeeld presentatoren of cabaretiers, maar ook politici houden weblogs bij die druk bezocht worden en waarvan de inhoud regelmatig de media haalt.

Het weblog van de Cubaanse blogger Yoani Sánchez wordt vertaald in vele talen, waaronder het Nederlands. Zij ontving voor haar blogs de Prins Claus Prijs.

103.4 Software

De meeste webloggers maken voor het bijhouden van hun log gebruik van gratis online diensten, waarvan Blogger het populairst is. Hun grootste concurrent is WordPress. Blogger en WordPress zijn internationaal georiënteerd, in Nederland was er voor het Nederlandse taalgebied een organisatie die web-log heet en die dezelfde diensten aanbiedt. Deze organisatie werd (samen met de blogs van de Volkskrant) later overgenomen door Sanoma, maar de migratie verliep niet geheel vlekkeloos[4] en het nieuw ontstane weblog.nl (zonder streepje) is in 2013 gestopt. Ook punt.nl timmert in Nederland aan de weg en steeds meer organisaties bieden de mogelijkheid tot webloggen aan zoals vrouw.nl, en blogse.nl.

In België is de bekendste aanbieder Skynetblogs van Skynet (Belgacom).

Via deze sites kunnen gebruikers die geen ervaring hebben met het maken van webpagina's op een gemakkelijke manier via een webinterface hun artikelen plaatsen. Naarmate zulke gebruikers meer ervaren raken, kiezen ze vervolgens vaak alsnog voor een geheel zelfgemaakte weblog. Zij ruilen hun gratis host in voor een eigen HTML-site met daarin een zelfgemaakte weblog.

Webloggers met meer ervaring gebruiken daarentegen over het algemeen speciaal daarvoor ontwikkelde software zoals WordPress (dat naast een eigen dienst dus ook losse software aanbiedt), MovableType, Pivot of Drupal. Met deze software, die op een eigen serverruimte dient te worden geïnstalleerd, kan men zijn weblog geheel naar eigen inzicht vormgeven. Het merendeel van deze software is gratis.

103.5 Techniek

103.5.1 RSS

Een slinkend aantal internetters[5] surft niet dagelijks naar de webpagina's van de weblogs, maar gebruikt daar een RSS-lezer voor. RSS staat voor Really Simple Syndication en het is een XML-toepassing, waarmee tal van sites te controleren zijn op updates. Om RSS te gebruiken is een RSS-lezer benodigd. Dit zijn veelal programma's die op een pc draaien. Google had een online RSS-dienst: Google Reader.

103.5.2 Trackback

Wanneer een blog reageert op of verwijst naar een item uit een andere blog, en beide bloggers ondersteunen een trackback, dan wordt de originele blogger door middel van een "trackback ping" hiervan op de hoogte gebracht. Onderaan het originele blogartikel wordt dan naar deze andere blogs doorverwezen.

103.5.3 Permalink

Een permalink is een permanente link naar een blogartikel. Aangezien de artikelen gesorteerd worden naar datum, kan het zijn dat een nieuwsfeit op een bepaald moment op de hoofdpagina staat, maar een maand later daar niet meer terug te vinden is. Een permalink verandert niet.

103.6 Soorten weblogs

- Babysite: een weblog die door ouders wordt gemaakt voor hun baby.
- Mamablog: weblog gericht op moeders en vaak ook vaders.
- Clublog: feitelijk meer een uitgebreide vorm van een gastenboek dan een zuivere weblog. Het verschil zit hem in het enigszins besloten karakter van een clublog. Het is weliswaar geen besloten log (en is dus voor eenieder toegankelijk), maar verreweg de meeste bezoekers van een clublog zullen deel uitmaken van een bepaalde club, vereniging of organisatie waarvan de leden nieuwtjes en wetenswaardigheden over hun club publiceren.
- Corporate blog of businessblog: een themablog dat officieel aan een specifiek bedrijf is verbonden. Het blog kan zowel intern als extern zijn en het blog dient daarbij vooral als communicatie- en marketingkanaal. Het blog wordt geschreven door een werknemer of een ingehuurde redacteur.
- Facelog: Ook wel *space blog* genoemd. Dit type van weblogs is geïntegreerd in Social-networkingsites zoals het Facebook en Hyves. Dit type blog combineert 2 elementen die beiden onder social networking vallen, enerzijds het Facebook-principe en anderzijds het logprincipe. Mogelijkheden tot modificatie worden gelijk getrokken aan normale blog sites, integratie van bijvoorbeeld YouTube en foto's zal tot de mogelijkheden gaan behoren.
- Fashionblog: Op fashion blogs delen veelal vrouwen hun laatste mode aankopen en informatie over de laatste trends. Ook komt het vaak voor dat inspiratie foto's worden gedeeld en soms worden webshops gepromoot. Een bekend fenomeen op fashion blogs zijn de 'outfit of the day' posts waarin wordt getoond wat de blogster die dag draagt.
- Filmblog: Geeft dagelijks filmnieuws, filmbesprekingen, trailers en filmposters.
- Fotoblog: een weblog dat bestaat uit foto's met al dan niet een korte beschrijving of commentaar.
- Klasblog: een weblog waarop leerlingen en leerkrachten berichten, en foto's plaatsen over wat er

zoal in de klas gebeurt, meestal aangevuld met studietips en informatie. Deze blog trekt meestal enkel leerkrachten (al dan niet van de klas waarover de klasblog gaat), leerlingen van de klas en familie van de leerlingen.

- Lifelog: een weblog waarop regelmatig berichten geplaatst worden over gebeurtenissen in het leven van de beheerder van de lifelog. Een soort online dagboek.
- Linkdump of linklog: een weblog dat niet zozeer drijft op eigen content, maar vooral links brengt naar andermans leuke, grappige, ontroerende of sexy bijdragen. Doorgaans worden deze wel voorzien van persoonlijk commentaar. Op linkdumpweblogs wordt doorgaans minder gereageerd dan op de zogenaamde lifelogs of shocklogs.
- Moblog: een weblog dat wordt bijgehouden vanaf een mobiel gadget met een camera (zoals veel mobiele telefoons en smartphones), vaak vooral met foto's die vanaf die telefoon zijn genomen.
- Muzieklog: een weblog over muziek in de breedste zin des woords. Het aanbod is gevarieerd; op sommige muzieklogs verschijnen alleen besprekingen van nieuwe albums en artiesten, terwijl anderen zich richten op specifieke genres, artiesten, stromingen of zich beperken tot het plaatsen van linkjes naar albums.
- Nieuwslog: een online krant in weblogvorm waardoor de interactiviteit met betrekking tot het nieuws toeneemt. Een nieuwslog wordt meerdere keren per dag geüpdatet, speelt in op actualiteiten en is vaak onderhouden door meerdere redactieleden.
- Politiek weblog: een persoonlijke weblog van een politicus of een weblog van een politieke partij.
- Reisblogs: weblogs die gewijd zijn aan specifieke reizen die mensen ondernemen, het internetequivalent van een reisdagboek. Soms wordt het weblog onderweg bijgehouden, maar veel vaker achteraf op basis van een tijdens het reizen bijgehouden dagboek.
- Shocklog: probeert door middel van een schokkende en agressieve inhoud veel publiek te trekken, of door onafhankelijk en niet gehinderd door gevestigde journalistieke grenzen van het oldschoolnetwork in de branche met een scherpe pen verslag te doen van de actualiteit en wat er in de wereld speelt.
- Stadsblog: een weblog waarop berichten geplaatst worden met als onderwerp een bepaalde stad of gemeente. Typisch komen hierbij lokale actualiteiten aan bod, zoals allerlei culturele en sportieve evenementen, of persoonlijke observaties rond de gemeente/stad. Het doel van een stadslog omvat het kritisch volgen van de gebeurtenissen in een gemeente/stad zonder zelf politiek gekleurd te zijn. Zulke stadslogs komen vaak tot stand vanuit een samenwerkingsverband tussen een aantal lokale loggers.
- Superblogger: een verzameling weblogs onder 1 hoofdsite waarin individuele gebruikers een compleet blogsysteem per weblog toegewezen krijgen in plaats van een aangepaste multisite met veelal beperkte mogelijkheden. Een superblogger typeert zich door zeer veel instelmogelijkheden voor complexe blogs met verregaande interactie tussen bloggers onderling en tussen blogger en bezoeker.
- Themablog: een weblog waarop berichten staan over een onderwerp of professie. De mensen die schrijven hebben een passie voor het onderwerp en hebben vaak veel kennis van het onderwerp. Er zijn tegenwoordig webloguitgevers die deze vorm van weblogs professioneel inzetten.
- Tv-blog: een weblog dat informeert over allerlei zaken die te maken hebben met televisie (programma's, kijkcijfers, marktaandelen ...)
- Wijkvlog: ligt in het verlengde van een stadsblog, waarbij de focus uitgaat naar een wijk of buurt in de stad. Bekend zijn bijvoorbeeld de *Hoodvlogs* van Ismail Ilgun.

103.7 Nederlandstalige blogs

103.7.1 Nederland

In 2006 waren de bekendste (meting op basis van Google-hits) weblogs:

1. GeenStijl
2. Flabber
3. Retecool.com
4. Jaggle
5. VKmag/Volkomenkut.com
6. Villamedia
7. KlokkenluiderOnline
8. Merelroze
9. Sargasso
10. Bieslog

Samen met de 'pioniers' Alt0169.com, tonie.net en sikkema.net werden de eerste drie uit bovenstaand lijstje ook vermeld in het NRC Next artikel 'Sites die Nederland veranderden'.[6] In 2007 werd weblog Frankwatching.com gekozen als beste Nederlandse weblog door The Best of the Blogs. De publieksprijs ging naar het Volkskrantblog,[7] hoewel dit eigenlijk een verzameling is van vele honderden weblogs.

In 2009 heeft hyped.nl een onderzoek gedaan naar de waarde van de grootste weblogs in Nederland en een lijst gepubliceerd met de 30 waardevolste blogs. Bovenaan de lijst staat wederom GeenStijl.[8] Daarnaast zijn er diverse blog-netwerken, waarop bezoekers/gebruikers eigen weblogs kunnen aanmaken en bijhouden.

Volgens hoogleraar journalistiek aan de Rijksuniversiteit Groningen (RUG) Marc Chavannes heeft Nederland weinig relevante weblogs die leiden tot een maatschappelijk debat. Als correspondent in de US maakte hij op grote schaal gebruik van politieke en wetenschappelijke blogs. Deze waren volgens hem sneller, grondiger en levendiger in het politieke debat dan kranten en tv. Volgens Peter Verweij, docent journalistiek van de Hogeschool Utrecht, ligt dat aan de afkeurende houding van de traditionele media en deels aan de blogs: “Media hebben er alles aan gedaan om weblogs te kleineren in Nederland, en weblogs zelf hebben er ook aan bijgedragen dat de blogosfeer vaak niet serieus wordt genomen.”

Dutch Bloggies organiseerde sinds 2001 jaarlijkse verkiezingen voor de beste Nederlandse weblogs en hielden na een slotfeest in 2011[9] na tien jaar op met bestaan.

103.7.2 Vlaanderen

Eind 2006, begin 2007 ontstonden de Bwards (spreek uit 'bie-wards') als een niet commercieel alternatief voor de verkiezing van beste blog door het tijdschrift Clickx in de context van de *Site Van Het Jaar* verkiezing. Voor de eerste editie kon iedereen zijn favoriete blog nomineren. Tijdens een evenement op 23 maart 2007[10][11] in HETPALEIS te Antwerpen werden de winnaars bekendgemaakt. Het was het eerste publieke en gratis evenement waar voornamelijk Vlaamse bloggers elkaar ontmoetten. De tweede editie kende een lagere opkomst. Vanaf 1 januari 2008 tot 10 februari 2008 kon er gestemd worden[12]. De bekendmaking vond plaats op zaterdag 1 maart 2008[13]. Nadien is het initiatief gestopt.

In 2012 heeft het magazine Weekend, wat een bijlage is van Knack, voor de eerste keer de *Weekend Blog Awards* georganiseerd. Geïnteresseerden konden blogs voorstellen, waarna een jury een preselectie maakte voor verschillende rubrieken die nauw aansluiten bij de thema’s die in Weekend aan bod komen : Deco en design, Travel, Food, Photography, Entertainment, Niche, Cityblog, Personal, Beauty en Fashion. 3116 mensen hebben hun favoriete blog genomineerd, 12.579 mensen hebben hun stem uitgebracht. Deze stemmen werden voor 40% meegeteld, de overige 60% bestond uit de stemmen van een vakjury, bestaande uit redactieleden van het magazine. Onder de winnaars waren er nieuwe blogs zoals alledagenhonger.be, joliette.be en coffeeklatch.be, maar ook bekendere blogs zoals gentblogt.be en defilmblog.be[14]. Het Franstalige zustertijdschrift Le Vif Weekend organiseerde tegelijkertijd een gelijkaardige verkiezing van Franstalige blogs[15].

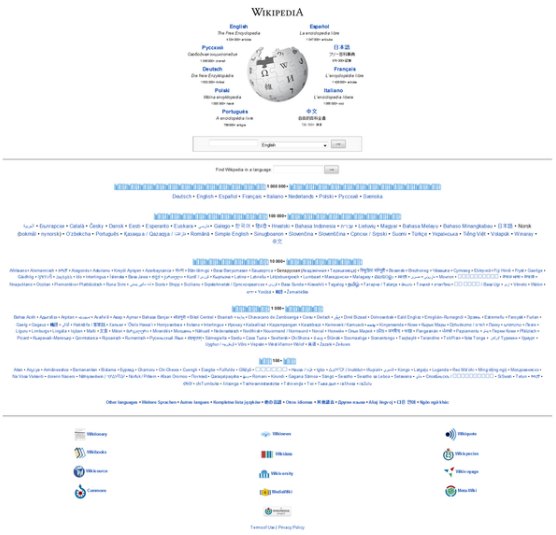
In Vlaanderen is de grootste blogsite bloggen.be.

103.8 Zie ook

- Blogkermis
- Blogsoftware:
  - Drupal
  - PostNuke
  - WordPress
  - Joomla!
- Contentmanagementsysteem (CMS) (*inhoudsbeheersysteem)*
- Wiki
- Online blogprogramma’s
  - Blogger
  - Windows Live Spaces
  - WordPress

Hoofdstuk 104

Website



Portaal van de Wikipedia-website op http://www.wikipedia.org

Een **website** is een verzameling samenhangende webpagina's met gegevens, zoals tekst, afbeeldingen of video's, die opgeslagen worden of in het gebruikte jargon 'gehost' (= letterlijk: 'geherbergd, onderdak geboden') worden. De website is vervolgens op een of meer webservers gezet en is (meestal) opvraagbaar gemaakt via internet. Het woorddeel *web* in *website* verwijst naar het wereldwijd web en het Engelse *site* betekent plek. Een *website* wordt ook wel aangeduid met het Engelstalige leenwoord **site**, dat in het Nederlands is aanvaard. Tevens bestaan er de Nederlandse woorden **weblocatie** of **webstek** voor. Deze woorden worden echter niet vaak gebruikt.

104.1 Webbrowser

Een webbrowser vertaalt het HTTP-bericht in bruikbare informatie voor de gebruiker zoals het tonen van een webpagina.

104.2 Domeinnaam

Om een website te kunnen vinden op het internet is er een centrale registratie waar bijgehouden wordt op welke computer een website ofwel domein opgevraagd kan worden met een webbrowser. Een domeinnaam is een naam in het Domain Name System (DNS), het naamgevingssysteem op internet waarmee netwerken, computers, webservers, mailservers en andere toepassingen worden geïdentificeerd. Deze naam verwijst naar een computeradres dat uit nummers bestaat. Het DNS functioneert als het telefoonboek van het computernetwerk. De vertaling van de naam naar het betreffende nummer geschiedt middels DNS-servers, alle verdere datacommunicatie tussen computers maakt gebruik van dat nummer. Informatie over een domein kan opgevraagd worden via Whois (who is).

Elke website is op de een of andere manier verbonden aan een unieke domeinnaam. De internationale Wikipedia bijvoorbeeld heeft als domein 'wikipedia.org'. Meestal wordt het subdomein 'www' gebruikt (zoals 'www.wikipedia.org'). Vaak wordt foutief verteld dat dit altijd het geval is. Dit is echter niet waar: de Nederlandstalige Wikipedia bijvoorbeeld heeft als subdomein 'nl' (dit geeft dan nl.wikipedia.org). In Nederland verzorgt Stichting Internet Domeinregistratie Nederland de uitgifte en registratie van .nl-domeinnamen en bewaakt de kwaliteit van domeinregistratie in Nederland. Voor particulieren is het niet mogelijk om via de SIDN direct een domeinnaam te registreren. Dat kan alleen via de aangesloten bedrijven (dit kunnen zowel binnen- als buitenlandse bedrijven zijn). In 2013 waren er ruim vijf miljoen .nl-domeinen.[1]

104.3 Webpagina

Een webpagina is een document, typisch geschreven in (X)HTML dat vrijwel altijd beschikbaar is via HTTP, een protocol waarmee een webserver communiceert met een client (meestal de webbrowser van een gebruiker).

Een kerneigenschap van het wereldwijde web vormt de hyperlink, een deel van het concept Hypertext; hiermee kan een gebruiker direct naar een specifieke tekst of andere digitale entiteit springen.

De webpagina's van een website zijn meestal toegankelijk via een specifieke node (URI). Vaak wordt deze specifieke startnode de hoofdpagina of homepage genoemd. De URI's van de webpagina's zijn meestal georganiseerd in een hiërarchie. De hyperlinks tussen de webpagina's geven echter per gebruiker een andere representatie van de betreffende website.

104.4 Standaarden

Alle publiek toegankelijke websites worden over het algemeen collectief benoemd als het "wereldwijde web" wat weer een deel van een bepaalde laag van het internet vormt.

Belangrijke standaarden rondom het wereldwijde web (www) worden onder andere beheerd en uitgebreid door voorstellen door het World Wide Web Consortium, beter bekend als het W3C. De directeur van het W3C is Tim Berners-Lee, die in 1991 HTML voorstelde, als subset van het complexere SGML als vervolg op de hypertext-achtige uitvoering Gopher (het www is daarmee nog steeds geen hypertext-systeem). Naast verschillende andere initiatieven bleek HTML uiteindelijk het succesvolst.

104.5 Geschiedenis

Ook al werd HTML voorgesteld als opvolger van Gopher in 1989 met als publieke uiting 1991, toch was het rond 1993 nog steeds zo dat Gopher de meest gebruikte manier was om het wereldwijd beschikbare informatienetwerk te gebruiken. In mei 1993 waren er dan ook slechts 50 websites wereldwijd. Men had nog steeds het idee dat het wereldwijde web voornamelijk gebruikt zou worden door universiteiten met dure en complexe hardware.

Pas toen Mosaic verscheen (1993), de eerste webbrowser met een grafische interface in plaats van een tekstgebaseerde interface, veranderde dit langzaam. De meeste wetenschappers in die tijd gebruikten beeldschermen waarop men geen grafische elementen kon tonen en bovendien was de verbinding nog erg traag en bandbreedte kostbaar.

Naarmate verbindingssnelheid toenam en (grafische) hardware goedkoper werd, nam de omvang van het aantal websites alsmede het aantal gebruikers toe en werden parallel hieraan nieuwe functionaliteiten toegevoegd in en rondom HTML.

Een webpagina in 1993 kon slechts: 1. informatie tonen in opmaakvorm; en: 2. beelden tonen. Daarnaast kon men "dynamische documenten" maken door middel van: 3. formulieren. Om deze formulieren te verwerken werd de standaard CGI opgesteld, de common gateway interface (versie 1.1 in 1995). Deze specificatie diende ondersteund te worden door de webserver en maakte het mogelijk om zogenaamde CGI-scripts aan te roepen, vaak geschreven in de taal Perl, diverse shell-talen, de taal AWK of zelfs de taal C. Via de HTTPD-browser van Microsoft was het zelfs al mogelijk op die manier CGI-scripts te linken aan Visual Basic om Windows-applicaties als spreadsheets of databases aan te roepen.

Deze CGI-scripts betekenden ook het begin van beveiliging in websites omdat het vanaf dat moment mogelijk was om "de achterkant" van de website te bereiken via snode wegen.

Met HTML versie 3.0 kwamen zaken als tabellen, lijsten en diverse andere noviteiten die toegepast konden worden binnen webpagina's.

Op softwarevlak kregen websites de volgende uitbreidingen en mogelijkheden:

- aan de clientzijde: meer mogelijkheden in markup via HTML en stylingmogelijkheden via CSS
- aan de clientzijde: meer scriptondersteuning zoals clientside-JavaScript, Perl-script en Tcl-script
- aan de clientzijde: meer objectondersteuning zoals Java-applets en Flash Player
- aan de serverzijde naast CGI ook serverside scripting zoals ASP (meestal VB Script), PHP en Serverside JavaScript
- aan de serverzijde meer directe integratiemogelijkheden met het achterlandschap zoals databases die ofwel via een tussenlaag informatie presenteren aan de gebruiker of direct informatie presenteren aan de gebruiker

Diverse termen als dynamische HTML of AJAX (Web 2.0) zijn niets meer dan combinaties van bovenstaande uitbreidingen.

104.6 Toegankelijkheid

Websites worden in toenemende mate geschikt gemaakt voor mensen met een beperking; hierbij wordt er rekening mee gehouden dat blinden bijvoorbeeld geen afbeeldingen kunnen zien maar wel graag willen weten wat er op de illustratie wordt afgebeeld door een begeleidende tekst. Een van de belangrijkste richtlijnen voor het ontwikkelen van toegankelijke websites zijn de zogenaamde Web Content Accessibility Guidelines. Een belangrijk neveneffect van het toegankelijk maken van websites voor gehandicapten is de betere vindbaarheid in internetzoekmachines zoals Google.

104.7 Structuur van een website

104.7.1 Hoofdpagina

Elke website heeft een hoofdpagina, ook wel index, homepage of startpagina genoemd. De hoofdpagina biedt een navigatie om door de rest van de site heen te gaan. De homepage kan, maar hoeft niet, een samenvatting te geven van de belangrijkste informatie die op de website staat, bijvoorbeeld in de vorm van categorieën, meest bezochte pagina's, het laatste nieuws etc. De hoofdpagina dient als uitvalbasis voor de bezoeker. Een bezoeker kan bijvoorbeeld via de homepage van het ene naar het andere onderdeel navigeren.

Een webserver is vaak zo ingesteld dat als alleen het domein wordt aangevraagd en niet een specifiek document, er toch een document naar de gebruiker wordt gestuurd. Meestal is dit de hoofdpagina, alhoewel eind jaren 1990 een zogeheten 'splash page' ook vaak voorkwam. Dit laatste was een document waar de gebruiker niets aan had, maar waarin de aanbieder bijvoorbeeld een logo kon tonen of een animatie kon afspelen.

104.7.2 Hiërarchie

Vaak is een website hiërarchisch ingedeeld. Een site wordt daarbij onderverdeeld in onderwerpen en eventueel subonderwerpen, die elk hun eigen pagina krijgen. Door eerst naar de homepage te gaan, dan naar een onderwerppagina en dan naar een subonderwerppagina volgt de gebruiker de hiërarchie van een site. Een aanbieder kan dit gevolgde pad zichtbaar maken. Dit wordt wel broodkruimelnavigatie genoemd.

104.8 Beheer van een website

104.8.1 Beheer via CMS

Een website wordt vaak beheerd met een online content management systeem (CMS). Een dergelijk systeem geeft de gebruiker de gelegenheid om op een simpele manier (zonder direct in HTML te programmeren) een website bij te houden. Een CMS bestaat meestal uit een zogenaamd managementgedeelte of administratiegedeelte, waar een gebruiker via een gebruikers- of inlognaam en wachtwoord kan inloggen. Vervolgens kan de gebruiker, afhankelijk van het toegangsniveau, nieuwe pagina's aanmaken, afbeeldingen uploaden, forumdiscussies beheren etc.

104.9 *Distributed denial-of-service*-aanval

Voor distributed denial-of-service (DDoS)-aanvallen op websites wordt vaak een botnet gebruikt,[2] maar het kan ook gaan om meerdere personen die hun acties coördineren, iets wat bijvoorbeeld gebeurt bij aanvallen van de zogenaamde *Anonymous*-beweging of de Syrisch Elektronisch Leger.[3] In reactie hierop werd het publiek-private Nationaal Cyber Security Centrum[4] opgericht, Europol startte het European Cybercrime Centre[5] en het Team High Tech Crime van de nationale recherche werd uitgebreid van 30 naar bijna 120 mensen en deed het Ministerie van Defensie een oproep in 2013 voor 150 white hats als cyberreservisten.[6][7] De AIVD en MIVD starten in 2014 met de Joint SIGINT Cyber Unit, een aftap- en cybercommando onder de codenaam Symbolon met 350 mensen.[8] en hebben voor 17 miljoen euro niet toegestane systemen om grootschalig telefoon- en internetverkeer op te kunnen vangen en verwerken besteld.[9] Voor 2013 werden er op ruim vijf miljoen .nl-domeinen.[1] 39 DDoS aanvallen gemeld in Nederland.[10] inclusief vermeende aanvallen die enkel een storing betroffen.[11]

104.10 Zie ook

- Black hat
- Distributed denial-of-service
- Domeinkaper
- Typosquatting

104.11 Referenties

104.12 Externe links

- (nl) Kwaliteitsrichtlijnen voor websites van de Nederlandse overheid
- (en) World Wide Web Consortium (W3C)

Hoofdstuk 105

Whois

Verdeling Whois-servers

Whois (uitspraak: who is) is een protocol om gegevens van een domeinnaam of IP-adres te achterhalen door middel van een query/vraag aan een database. In een whois staan meestal de naam en contactgegevens van de eigenaar, de provider en nameservers van de DNS-servers.

Traditioneel werden whois-zoekopdrachten gedaan met een command line-programma (IETF standaard RFC3912) , maar tegenwoordig zijn er ook veel websites die deze service bieden.

Deze resultaten kunnen per domein verschillen.

105.1 Whois-servers (IP-adressen)

Voor IP-adressen gelden de volgende whois-servers:

105.2 Whois-servers domeinextensies

Voor domein-extensies zijn er ook whois-servers. Voor de meeste land-extensies geldt dat er één centrale whois-server is. Voor gTLD's als .com, .net en .org is het meestal gedistribueerd: er is dan één centrale whois-server (van het registry) die doorverwijst naar de instantie die daadwerkelijk het domein geregistreerd heeft. In onderstaand overzicht wordt alleen de server van het registry vermeld, en niet die van onderliggende registrars.

105.3 Externe links

- IP Whois

Hoofdstuk 106

Wi-Fi

Wi-Fi is een certificatielabel ('logo') voor producten voor draadloze datanetwerken, die werken volgens de internationale standaard IEEE 802.11 (*draadloos ethernet* of *wifi*). Dergelijke producten maken gebruik van radiofrequenties in de 2,4GHz- en/of 5,0GHz-band die onder voorwaarden zonder licentie gebruikt mogen worden. De eisen voor dit logo worden vastgelegd door de Wi-Fi Alliance.

Een product komt in aanmerking voor het Wi-Fi-logo als door een onafhankelijk certificatiebureau is aangetoond dat aan bepaalde eisen op het gebied van functionaliteit, prestatie en interoperabiliteit is voldaan. Met name het laatste is van belang voor de consument, omdat dit garandeert dat producten met het Wi-Fi-logo samenwerken met producten van andere fabrikanten.

Hotspot in luchthaven

106.1 Naamgeving

Wi-Fi werd oorspronkelijk uitgesproken als 'waifi'. Tegenwoordig wordt het uitgesproken als [wifi]? of [wɑjfɑj]?.[1] De naam Wi-Fi is een duidelijke knipoog naar de uit de audiowereld bekende term hifi, hetgeen staat voor High Fidelity. De naam Wi-Fi staat, in tegenstelling tot wat velen denken, niet voor Wireless Fidelity.[2] In het verleden gebruikte de Wi-Fi Alliance de term Wireless Fidelity zelf wel in de leuze “The Standard for Wireless Fidelity”. Vanaf eind 2000 werd deze leuze niet meer gebruikt in marketingmateriaal. In online beschikbare documenten werd de term nog wel gebruikt, onder meer in een document uit februari 2004: "... wireless fidelity (Wi-Fi) network equipment.”[3] De Wi-Fi Alliance raadt tegenwoordig af deze term te gebruiken en noemt het gebruik ervan een te betreuren fout.

In de dagelijkse praktijk wordt de term, in dit geval geschreven als *wifi*, steeds vaker gebruikt als synoniem voor een draadloos thuisnetwerk in het algemeen.[4] De schrijfwijze met een koppelteken (*wi-fi*) komt in het Nederlands ook voor.[5]

106.2 Topologieën

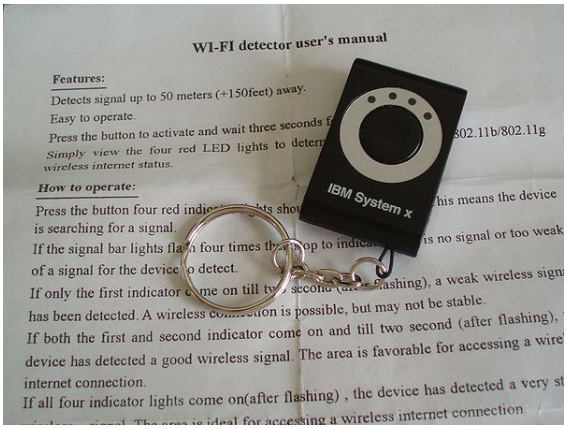
Wi-Fi definieert twee verschillende topologieën: ad hoc en infrastructuur. In ad-hocmodus communiceert een 802.11-client direct met een andere client. De maximale afstand tussen deze stations is daarmee automatisch begrensd tot het bereik van de beide zenders/ontvangers (afhankelijk van vele factoren, echter meestal maximaal zo'n 30 meter). In infrastructuurmodus wordt gewerkt met basisstations, in 802.11-termen access point genoemd. De basisstations zijn onderling verbonden door een ethernet-infrastructuur. Mobiele stations kunnen overschakelen van het ene naar het andere access point ('roamen'), zonder de verbinding met het netwerk te verliezen (vergelijk gsm).

Veel publiek toegankelijke locaties zoals vliegvelden, hotels en bibliotheken installeren basisstations waardoor de mobiele computergebruiker op deze locaties over internettoegang beschikt en gebruik kan maken van informatiediensten van de betreffende organisatie. Dergelijke (semi-)openbare basisstations worden ook wel *inbelpunt* of *hotspot* genoemd. Er zijn zowel gratis inbelpunten, als inbelpunten waarvoor een abonnement of een toegangskaartje tegen betaling nodig is. Kleine ondernemers kunnen met een geringe investering lokaal een wi-fi-netwerk opzetten.

De bandbreedte en het bereik van wifi zijn groter dan

die van bluetooth. Om deze redenen is wifi een van de belangrijkste toegangsmethoden voor een alom aanwezig draadloos internet. Een keerzijde van wifi, met name vergeleken met bluetooth, is het relatief hoge energieverbruik. Dit is bij kleine apparaten met een beperkte batterijcapaciteit, zoals pda's, een probleem.

106.3 Toegestaan



Wifi-detector als sleutelhanger

Wi-Fi-apparatuur valt binnen de EU onder de CEPT-regeling voor Short Range Devices. De voorwaarden voor licentievrij gebruik stellen beperkingen aan het uitgezonden vermogen (in Nederland anno 2015: 100 mW e.i.r.p. ("equivalent isotropically radiated power") voor de 2,4GHz-band, 200 mW e.i.r.p. voor de banden van 5,1-5,3 GHz en 1 W e.i.r.p. voor de banden van 5,4-5,7 GHz).[6]

In sommige landen is 500 mW toegestaan. Er zijn daarom ook wifi-apparaatjes te koop van 500 mW, waarbij men soms een bereik claimt van 1000 meter. Met speciale richtantennes is met 100 mW een afstand van 500 meter te overbruggen.

106.4 Versleuteling

Een belangrijk aandachtspunt bij wifinetwerken is de beveiliging van de door de ether verzonden informatie. Een wifiverbinding kan door middel van verschillende technieken worden versleuteld. De twee prominente standaarden zijn WEP en WPA. De WPA-standaard is in juni 2004 gestandaardiseerd als IEEE 802.11i, en WPA2, een verbetering op WPA, is sinds 2006 wijd in gebruik en vereist voor apparatuur met Wi-Fi-certificatie. WEP-beveiliging blijkt in de praktijk makkelijk te kraken; WPA of WPA2 worden daarom aanbevolen. WPA is slechts met zeer veel moeite te kraken, en WPA2 niet of nauwelijks.

106.5 Wi-Fi Protected Setup (WPS)

Het blauwe WPS-knopje aan de achterkant van een Cisco Systems E2500-wifirouter.

WPS is bedacht om de draadloze verbinding te kunnen configureren zonder ingewikkelde sleutels (WEP key of WPA keys) in te hoeven typen. Er zijn twee manieren: *Push Button* en *WPS Personal Identification Number (PIN)*. Bij de *Push Button*-methode moet er binnen circa 1 minuut) een speciale WPS-knop op de draadloze router en op de laptop ingedrukt worden. Beide apparaten wisselen vervolgens automatisch de sleutel uit en de verbinding komt tot stand. De meeste *wireless USB dongles* ondersteunen push-button-setup. Laptops, pc's, iPads en dergelijke ondersteunen *Push Button* niet omdat de speciale knop ontbreekt. De tweede methode, 'PIN', vereist het intypen van een pincode. Dat kan op twee manieren:

- de pc/laptop genereert automatisch een pincode die ingetypt moet worden in de draadloze router, of
- de draadloze router genereert een pincode die ingetypt moet worden op de laptop (in Windows, Apple iOS of Linux).

De eerste methode is omslachtig omdat eerst een pincode gegenereerd wordt door de laptop, dan moet ingelogd worden op de router en pas dan kan de pincode ingevuld worden. De tweede methode is makkelijker omdat altijd dezelfde pincode gebruikt wordt die vaak op een sticker onder op de router of in de handleiding staat en dus rechtstreeks overgetypt kan worden.

De pincode is geen willekeurig getal maar bestaat uit 8 cijfers. De eerste 7 mogen willekeurig gekozen worden (0..9), de laatste is een "checksum digit". Deze wordt als volgt berekend: tel de cijfers op de oneven posities bij elkaar op, vermenigvuldig het getal met 3, tel daarbij op de cijfers op de even posities, bereken de rest bij delen door 10, en trek die rest af van het getal 10. Voorbeeld: PIN=66323211. De eerste 7 cijfers zijn 6632321. De som van de cijfers op oneven posities is 6+3+3+1=13. Vermenigvuldiging met 3 levert 39. De som van de cijfers op de even posities is 6+2+2=10. Opgeteld levert dit 39+10=49. Delen door tien levert rest 9. Rest 9 aftrekken van 10 levert 1; het laatste cijfer van de PIN is dus 1.

106.6 Verstoring

De gebruikte licentievrijbanden van 2,4 GHz en 5 GHz worden gedeeld door verschillende gebruikers. De 2,4GHz-band is dezelfde band waarin ook magnetrons (voor verhitten van onder meer voedsel) werken, maar vele draadloze toepassingen maken gebruik van dezelfde band, zoals draadloze muizen en toetsenborden, video-overdracht (beveiligingscamera's en tweede televisie-aansluitingen), draadloze deurbellen, garagedeuropeners, hoofdtelefoons en veel andere apparatuur. Bij ingebruikname van deze apparatuur wordt aangeraden om de verschillende kanalen binnen de 2,4GHz-band te bekijken en het kanaal met de minste storing te kiezen. De 5GHz-band kent (2009) minder concurrerende gebruikers, maar doordat het gebruik van deze band naar verwachting zal toenemen zal de onderlinge verstoring ook groter worden. De effecten die de gebruiker kan merken zijn: wegvallende data-verbindingen, beeldverstoring, niet-functionerende draadloze bediening. Het betreft hier onderliggende verstoring in dezelfde frequentieband die gebruikt mag worden en wordt daarom niet gezien als een schending van de EMC-normen, die de onderlinge storing met andersoortige apparatuur beschrijft.

106.7 Wifi-standaarden

Er zijn verschillende wifi-standaarden:

- IEEE 802.11a werkt in de 5,8GHz-band en de bandbreedte is maximaal 54 Mbps.
- IEEE 802.11b werkt in de 2,4GHz-band en de bandbreedte is maximaal tot 11 Mb/s. Deze technologie is al geruime tijd (sinds medio 2005) niet meer in de handel en wordt als achterhaald beschouwd. Toch worden er nog veel laptops gemaakt die dit type wifi-standaard ondersteunen.
- IEEE 802.11g is de opvolger van 802.11b en werkt in de 2,4GHz-band, de bandbreedte is maximaal 54 Mbps. De producten die gebruikmaken van 802.11g kunnen ook met de 802.11b-standaard overweg.
- IEEE 802.11n werkt in de 2,4- en de 5,8GHz-band en meerdere antennes. De bandbreedte van de n-versie is minimaal 150 Mb/s, en kan oplopen tot 600 Mb/s. Dit is 10 keer sneller dan de voorloper van de standaard (802.11g). In augustus 2009 werd de IEEE 802.11n een officiële standaard. Tot die tijd bestond er al enkele jaren apparatuur die met de voorlopige standaard werkte (IEEE 802.11n draft 2.0). Het Engelse woord 'draft' staat voor 'concept'. Van 2006 tot 2009 was er allerlei apparatuur die voldeed aan de IEEE 802.11n draft.
- IEEE 802.11u maakt roaming over wifinetwerken mogelijk. Een apparaat kan daarvoor gebruikmaken van externe wifinetwerken om automatisch contact te leggen met internet.

106.8 Ontwikkeling in Nederland

Nederland heeft een belangrijke rol gespeeld in de standaardisatie van de initiële IEEE 802.11-standaard en de ontwikkeling van chipsets en producten:

- De NCR / AT&T / Lucent Technologies / Agere Systems vestiging te Nieuwegein, bekend onder de afkorting WCND (Wireless Communication Network Division), is actief betrokken geweest bij de standaardisatie, heeft specifieke geïntegreerde schakelingen ontwikkeld en heeft geruime tijd kaartjes en Access Points ontwikkeld en (laten) produceren. Na meer dan 15 jaar actief te zijn geweest in deze technologie, is de vestiging in Nieuwegein in december 2004 gesloten en heeft Agere Systems zich vrijwel geheel teruggetrokken uit de wifi-technologie. Een deel van de divisie is toen doorgegaan naar Motorola voor de chipontwikkeling van WiMAX en is daarna grotendeels overgegaan naar Broadcom om verder te werken aan de nieuwe wifistandaarden en -chips.
- De voormalige No Wires Needed / Intersil / GlobespanVirata / Conexant vestiging te Bilthoven heeft eveneens een belangrijke bijdrage geleverd aan verscheidene standaards en implementeerde voor de ARM-microprocessor een 802.11-MAC die wordt gebruikt in vele clients en access points. De vestiging in Bilthoven is opgeheven na outsourcing naar India. Vanuit de vestiging in Bilthoven zijn nieuwe bedrijven ontstaan die zich bezighouden met Wi-Fi zoals Signalutions en Avinity.
- De Airgo Networks vestiging te Breukelen is actief betrokken bij de ontwikkeling van IEEE 802.11n (Pre-N) geïntegreerde schakelingen.

106.9 Gezondheidsrisico's

Het Internationaal Agentschap voor Kankeronderzoek van de Wereldgezondheidsorganisatie plaatste in 2011 hoogfrequente elektromagnetische velden van o.a. mobiele telefoons en wifi in categorie 2B: 'mogelijk kankerverwekkend'.[7] In 2005 bleek uit een meta-analyse van studies waarin onderzoek was gedaan naar in totaal 725 personen die beweerden te leiden aan elektrosensitiviteit dat geen bewijs kon worden gevonden voor hun claims.[8] Volgens de Nederlandse overheid brengt elektromagnetische straling geen gezondheidsrisico's met zich mee.[9]

De Britse Health Protection Agency (HPA) rapporteerde in 2014 dat de frequentie van wifi-netwerken onge-

veer gelijk is aan dat van FM-radio, tv en mobiele telefoons. Aangezien wifi-netwerken niet continu data verzenden, stelt de organisatie dat er in de praktijk minder blootstelling is aan wifistraling dan de straling van mobiele telefoons.[10] In 2007 stelde de organisatie in reactie op een verontrustende mediareportage van het tv-programma *Panorama* dat waarschuwde voor wifi-straling in klassen, dat er onderzoek nodig was naar gezondheidseffecten van wifi-straling.[11] Na voltooiing van dit onderzoek concludeerde de HPA in september 2011 dat tijdens een typerende les het draadloos netwerk nauwelijks actief is en de blootstelling daarmee relatief gezien gering is.[12]

In Nederland liet de gemeente Alphen aan den Rijn onderzoek uitvoeren door de Universiteit Wageningen nadat ambtenaren de straling aanwezen als mogelijke oorzaak van de boomaantastingen. De eerste publicatie van onderzoeksresultaten in november 2010 suggereerde dat de elektromagnetische straling een rol zou spelen bij verslechterende gezondheid van bomen: in de laboratoriumsituatie bleek dat bladeren van esboompjes, na ruim drie maanden te zijn blootgesteld aan de straling van zogenaamde Wi-Fi Access Points, verdrogen en afsterven. Toch kon er geen verband worden vastgesteld met de verslechterde gezondheid.[13] Uit een vervolgonderzoek, waarin meer rekening werd gehouden met andere factoren, bleek dat er geen oorzakelijk verband kan worden vastgesteld tussen elektromagnetische straling (door wifi-routers en UMTS- en DVB-T-zenders) en boomaantastingen zoals bastknobbels, bastscheuren, bastnecrose en bastbloeding.[14][15]

106.10 Zie ook

- Wifi-MAC-laag
- WiMAX
- ZigBee

106.11 Externe links

- Wi-Fi Alliance
- Interview met de Nederlandse grondleggers van wifi Cees Links en van de IEEE 802.11-norm Vic Hayes.

Hoofdstuk 107

Witwassen

Witwassen is het uitvoeren van transacties teneinde de illegaliteit van geldsommen te maskeren. Het doel van witwassen is om illegaal verkregen vermogen te kunnen besteden of investeren zonder dat bewezen kan worden dat het bezit illegaal was. Zodoende kan voorkomen worden dat het geld door justitie of belastingdienst in beslag wordt genomen.

Witwassen is in vrijwel alle landen strafbaar als misdrijf. Wie zich hiermee bezighoudt riskeert strafvervolging, bestuursrechtelijke sancties en tuchtsancties.

107.1 Herkomst van het geld

Het gaat om vermogensvoordelen afkomstig van criminele activiteiten zoals drugshandel, mensenhandel, diefstal, sociale en fiscale fraude.

In sommige landen is de lijst van zogenaamde basismisdrijven (misdrijven die een bestraffing wegens witwassen kunnen opleveren) beperkt tot een zeker aantal, in andere landen kunnen alle misdrijven aanleiding zijn tot een vervolging wegens witwassen.

107.2 Fasen

Over het algemeen wordt bij witwassen een drietal fasen onderkend:

1. Plaatsing/inbreng: waarbij het vermogensvoordeel (meestal onder de vorm van contant geld) voor het eerst in het financiële systeem wordt gebracht.
2. Versluiering/circulatie: waarbij een opeenvolging van soms complexe financiële transacties wordt uitgevoerd met als doel de oorsprong van het vermogen te verhullen.
3. Integratie/investering: waarbij het vermogen in de bovenwereld wordt geïnvesteerd, bijvoorbeeld door investering in onroerend goed. In deze fase is het vrijwel onmogelijk om de criminele herkomst te traceren. Antiwitwasmaatregelen richten zich dan ook voornamelijk op de eerste twee fasen.

107.3 Methodes

Bij het witwassen wordt een scala van methodes toegepast.

107.3.1 Via het buitenland

Iemand die een fortuin heeft verdiend met drugshandel zou de volgende methode kunnen toepassen:

- Hij richt een paar bedrijven op in een ver land met een gebrekkige controle en een vennootschap in het eigen land;
- Het geld wordt gestort en overgemaakt naar dat bedrijf in het buitenland, dat het investeert in weer een ander bedrijf (dat ook eigendom is van dezelfde persoon of van een stroman);
- Het eigen bedrijf leent het geld van het buitenlandse bedrijf en investeert het in gebouwen. De eigenaar kan nu gewoon winst maken met de opbrengst van de drugshandel, terwijl het voor de politie heel moeilijk is de herkomst van het geld te achterhalen;

Transacties die daarbij een rol spelen zijn:

- Geld wisselen van de ene valuta naar de andere;
- *Moneytransfers* - dat is een spoedzending van geld waarbij het contant wordt gestort en elders wordt opgenomen. Na het storten kan het geld soms al na een kwartier in het buitenlandse kantoor worden opgenomen;
- Het gebruik van een katvanger. Deze persoon ontvangt geld op zijn bankrekening dat hij vervolgens moet overboeken of opnemen en afgeven. In ruil hiervoor ontvangt hij een commissie. Uiteraard loopt de katvanger een zeer groot risico op juridische problemen want de bankrekening staat op zijn naam dus de pakkans is bijna 100%;
- Het gebruik van het hawala systeem, een informeel overboeksysteem in het Midden-Oosten en Azië. Na een paar keer overboeken is het geld vrijwel niet meer te traceren.

- Smurfen: het vervoeren of overboeken van kleinere hoeveelheden geld in meerdere malen om zo onder de meldingsgrens te blijven.

107.3.2 Via de eigen vennootschap

Een andere methode om geld wit te wassen en die weinig als dusdanig (h)erkend wordt is het misbruik/gebruik van de rechtspersoon (vennootschap) zelf. De (boekhoudkundige) structuren van de vennootschap kunnen worden gebruikt om wit te wassen geld te injecteren:

1. Via leningen toegestaan door aan de witwassers verwante bedrijven: dit is de *loan-backmethode* waarbij geld eerst via bijvoorbeeld fysiek transport naar een ander land (met minder strenge anti-witwasregels) wordt gebracht waar het op een rekening van een andere vennootschap (gecontroleerd door de witwassers) geplaatst wordt. Deze vennootschap verstrekt de eerste vennootschap een lening die niet teruggevorderd wordt en later de benaming “achtergestelde lening” verkrijgt.
2. Via het fictief verhogen van de omzet: in een vennootschap (bijvoorbeeld horeca- of marktbedrijven) waar contant geld als normaal betaalmiddel gebruikt wordt, wordt het wit te wassen geld ingebracht als normale omzet van een goed draaiend bedrijf. Dat over deze omzet belasting verschuldigd is, neemt men op de koop toe, gelet op het gemak waarmee kan worden witgewassen.
3. Het injecteren van wit te wassen geld via de rekening-courant: is een variatie op de *loan-back*methode maar hier wordt het wit te wassen geld rechtstreeks ingebracht via de rekening-courant van de zaakvoerder(s).

In de voorbeelden 1 en 3 moet vroeg of laat de zaak rechtgetrokken worden omdat deze lening of rekening-courant te zwaar doorweegt op de balans: naar de buitenwereld (via de gepubliceerde jaarrekening) geeft de vennootschap de indruk een (zeer) slechte betaler te zijn omdat de schulden (ogenschijnlijk) niet betaald worden. Meestal wordt overgegaan tot een kapitaalverhoging waarbij de “schuld” van de vennootschap aan de schuldeiser (meestal één der aandeelhouders) wordt omgezet in aandelen. Dergelijke kapitaalverhoging wordt (in België) beschouwd als “inbreng in natura” en maakt verplicht het voorwerp uit van een analyse door een bedrijfsrevisor. De kapitaalverhoging wordt vervolgens gepasseerd in een notariële akte en gepubliceerd.

Bij deze witwasmethoden ligt een grote verantwoordelijkheid bij professionals die betrokken zijn bij vennootschappen zoals revisoren, accountants en notarissen. Zij zijn verplicht vermoedens van witwassen te melden aan het centraal meldpunt (Financial Intelligence Unit - Nederland of Cel voor Financiële Informatieverwerking (CFI) in België). Dit levert niet veel op, afgaande op het (geringe) aantal meldingen van revisoren en accountants in de jaarverslagen van de CFI.

Het witwassen via een fictieve verhoging van de omzet is veel moeilijker te detecteren: dit vereist bijna een permanente vergelijking van het aantal klanten met het opgegeven aantal verkopen. Bedrijfstakken die hiermee vaak in verband worden gebracht, zijn belwinkels, gokautomatenenhallen en (in Nederland) de legale prostitutie.

107.3.3 Casino

Een methode die soms wordt gebruikt om geld wit te wassen, is het kopen en weer verzilveren van fiches in een casino. De bezitter van het geld verklaart dan dat hij het geld gewonnen heeft met gokken. Dit veronderstelt echter een verregaande naïviteit van de casino-uitbater of diens medeplichtigheid.

Zie ook het antiwitwasbeleid van Holland Casino.

107.3.4 Valse facturen

Ook kunnen valse facturen worden uitgeschreven. De ontvanger van het geld beweert daarvoor diensten of goederen te hebben geleverd, die in werkelijkheid nooit geleverd zijn.

107.4 Financiering van terrorisme

Financiering van terrorisme wordt vaak in een adem genoemd met witwassen omdat de methode vrijwel identiek is. Bij financiering van terrorisme wordt geld ingebracht in het financiële systeem en tracht men hiermee terroristische activiteiten te financieren zonder dat dit naar de oorspronkelijke eigenaars of inbrengers is terug te traceren. Ook hier kan men dezelfde fasen onderscheiden waarbij precies dezelfde methoden kunnen worden aangewend:

1. Plaatsing/inbreng: financiële middelen worden verkregen op legale (inzameling voor charitatieve doeleinden) dan wel illegale (afpersing, diefstal) wijze, en ingebracht in het financiële systeem.
2. Versluiering/circulatie: waarbij een opeenvolging van soms complexe financiële transacties wordt uitgevoerd met als doel de oorsprong (en uiteraard het uiteindelijke doel) van het vermogen te verhullen.
3. Integratie: Het geld wordt aangewend ter financiering van terroristische activiteiten.

107.5 Wettelijke regelingen

In de jaren '80 kwam internationale aandacht voor het witwasprobleem naar aanleiding van het witwassen van geld via internationale transacties door drugsbaronnen. Dit leidde tot een aantal VN-verdragen. De terroristische aanslagen van 11 september 2001 leidden eveneens tot een verhoogde aandacht voor financiering van terrorisme, hoewel hier al sinds 1999 een verdrag voor bestond. Ook in EU-verband zijn richtlijnen en verordeningen tegen witwassen uitgevaardigd.

De verdragen noemden criminalisering van witwassen, hetgeen vrijwel alle landen hebben overgenomen in een of andere vorm. Ook is er een trend tot strengere regels; aanvankelijk was slechts opzettelijk witwassen strafbaar, anno 2015 wordt vooral van de goede trouw uitgegaan: wat wist men en wat behoorde men te weten. Ook worden kleinere gevallen hard aangepakt.

Naast soevereine staten en de EU bestaan er ook organisaties die richtlijnen uitvaardigen, zoals de FATF en de Egmontgroep. Staten hebben internationale verdragen, standaarden en Europese wetgeving direct geïmplementeerd, of tot nationale wetgeving gemaakt. Daarnaast kan ook niet formele wetgeving worden uitgevaardigd. Deze regels leggen organisaties de verplichting op normen te implementeren die witwassen tegengaan. Een aantal van deze normen zijn:

- Het toepassen van Customer Due Diligence (KYC), waarbij klanten en hun aandeelhouders gescreend worden
- Het categoriseren van klanten naar risico
- Het niet accepteren van verdachte of te riskante aankomende klanten
- Het op de hoogte blijven van zwarte lijsten en hun updates, en deze vergelijken met het klantenbestand en (prospect)klanten.
- Het monitoren van klantgerelateerd risico
- Medewerking met de overheid, zowel passief (op initiatief van de overheid) als actief (op eigen initiatief bij verdenking)
- Het identificeren van PEPs (Politically Exposed Persons)
- Een deugdelijk systeem om alle informatie op te slaan en bij te houden
- Een interne compliance functie met aanvullende functies voor de interne auditor

107.5.1 België

In België is het witwassen van illegaal verworven vermogensvoordeel van alle misdrijven strafbaar volgens artikel 505, 1° lid 2-3-4 van het Strafwetboek.

In België moeten verdachte transacties gemeld worden aan de Cel voor Financiële Informatieverwerking (CFI). Het juridisch kader is de *Wet van 11 januari 1993 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme*.

Een heleboel meldingsplichtigen (praktisch iedereen die op een professionele manier met geld bezig is) (art. 2 van de Wet van 11 januari 1993) moeten verdachte transacties of andere zaken waarvan vermoed wordt dat ze te maken hebben met witwassen melden aan de CFI. Bepaalde bankverrichtingen, waarvan de omvang of frequentie aanzienlijk zijn, worden bijna ambtshalve doorgegeven aan de CFI.

De CFI onderzoekt de melding en indien de verdachte transactie of handeling kan gelinkt worden aan een misdrijf dat of strafbare gedraging die omschreven staat in een beperkte lijst (art. 3 van de Wet van 11 januari 1993) wordt een rapport overgemaakt aan de procureur des Konings.

Sedert 1 september 2007 geldt dat meldingsplichtigen (art. 2, 2bis en 2ter van de Wet van 11.1.1993), in die gevallen waarvan vermoed wordt dat het gaat om vermogensvoordelen afkomstig van fiscale fraude, enkel nog moeten melden indien het gaat om ernstige en georganiseerde fiscale fraude. Een apart Koninklijk Besluit heeft bepaald welke criteria deze fraude heeft. Indien één van deze criteria in een transactie gebruikt wordt moet de CFI ingelicht worden. Indien de meldingsplichtige meldt, geldt voor hem/haar een verschoningsgrond.

Nieuwe regelingen die witwassen in België moeten tegengaan zijn onder andere het voorschrift dat een transactie waarbij een handelaar betrokken is niet in contanten mag worden uitgevoerd wanneer het bedrag van de transactie gelijk of meer is dan € 15.000. In dat geval moet de transactie via girale weg verlopen. Deze beperking zal ook in EU verband gaan gelden.

Vanaf 2008 bestaan er geen effecten aan toonder meer zodat de werkelijke eigenaar steeds bekend zal zijn.

Ingevolge het Koninklijk Besluit (KB) van 5 oktober 2006 geldt vanaf 15 juni 2007 in België een “aangifteplicht”. Dit houdt in dat het " grensoverschrijdend vervoer van liquide middelen ter waarde van € 10.000 of meer” op verzoek van de bevoegde autoriteiten dient te worden aangegeven. Deze aangifteplicht geldt voor liquide middelen die vervoerd worden tussen België en een lidstaat van de Europese Gemeenschap of tussen deze lidstaat en België op de persoon, in de bagage of aan boord van een vervoermiddel hetzij op enige andere manier. Alle politiediensten en de douane zijn bevoegd om deze maatregel te controleren. Indien er aanwijzingen zijn dat het gaat om

mogelijk witwassen of financiering van illegale activiteiten (lees financiering van terrorisme) worden de liquide middelen in bewaring genomen gedurende maximaal 14 kalenderdagen onverminderd de mogelijkheid tot (voorlopige) inbeslagname door de gerechtelijke autoriteiten.

Dit KB is de Belgische implementatie van de EG-verordening 1889/2005 betreffende de controle van liquide middelen: ingevolge de strengere anti-witwasmaatregelen (voornamelijk in het Westen) is het voor witwassende criminelen moeilijker geworden om geld rechtstreeks te “injecteren” in het financieel stelsel. Daarom wordt er terecht van uitgegaan dat zij andere wegen en/of manieren zoeken om hun constante stroom van crimineel verworven geld wit te wassen of op een andere manier te gebruiken. Eén van deze wegen is het fysiek vervoer van geld (= liquide middelen) om het van een streng(er) gecontroleerd land te verplaatsen naar een land waar er minder anti-witwasmaatregelen zijn. Via de aangifteplicht, die in de ganse Europese Gemeenschap van kracht is/zal worden, wordt getracht het de criminelen moeilijker te maken om zo geld wit te wassen.

107.5.2 Nederland

Er is de Wet ter voorkoming van witwassen en financieren van terrorisme.

Hoofdstuk 108

ZigBee

ZigBee is een open standaard voor draadloze verbindingen tussen apparaten op korte afstand. Het is bedoeld als aanvulling op Bluetooth en wifi, het wordt gebruikt voor het doorsturen van sensorgegevens en voor (proces)besturing (monitoring & control), zoals de gezondheid van een patiënt of de veiligheid in uw huis controleren met behulp van sensoren.

108.1 Algemeen

ZigBee is de naam voor een standaard voor draadloze communicatie die ontworpen is vooral voor toepassingen in de industrie. ZigBee gaat bijvoorbeeld van afstandsbedieningen tot de communicatie tussen machines in een fabriek.

Praktisch voorbeeld van een thuissituatie met ZigBee:

- ZigBee Lamp controller: het licht bedienen op afstand
- Draagbare Panic button: mensen met een slechte gezondheid kunnen met een simpele druk op de knop de hulpdiensten verwittigen via de telefoonlijn
- Deur en raam beveiliging
- ZigBee Mailbox detector: detecteert of er post is geleverd in de brievenbus, handig tegen diefstal
- Computer met ZigBee Human Interface devices: toestellen met software waarmee je het huis kunt automatiseren

Het huis is geautomatiseerd: Het licht kan op afstand aangestoken worden, er is inbraakbeveiliging (bij inbraak wordt de politie ingelicht en gaat het licht aan), een panic button voor noodgevallen met de gezondheid en detectie van post. Alles wordt gelokaliseerd en geconfigureerd door de PAN coördinator. Dus de coördinator alarmeert de politie en de hulpdiensten.

ZigBee vindt zijn oorsprong in de IEEE-norm 802.15.4. De IEEE 802.15.4 voorziet 3 frequentiebanden waarin ZigBee kan werken: 868,3 MHz (Europa), 902-928 MHz (Amerika) en 2405-2480 MHz (wereldwijd). De transmissiesnelheid bedraagt maximaal 250 kbps met een bereik van 100 meter en ondersteunt een netwerk tot 65.000 apparaten.

ZigBee is een product van de ZigBee Alliance. De ZigBee alliantie is een associatie van bedrijven die samenwerken om (monitoring & control) producten aan te bieden gebaseerd op ZigBee. Deze producten hebben bepaalde eigenschappen: betrouwbaar, laag stroomverbruik, draadloos netwerk, goede prijs/kwaliteit. De alliantie heeft een aantal bekende promotors zoals Motorola, Philips, Samsung, Siemens…

108.2 Protocollen

ZigBee is gebaseerd op de IEEE 802.15.4 standaard (definieert de fysieke en MAC laag van het OSI-model). De lagen boven de specificatie van de 802.15.4 noemt men de ZigBee standaard, dus het is een uitbreiding op de 802.15.4 specificatie.

De fysieke laag is de laagste laag en bestaat uit 2 fysische lagen die werken op 2 aparte frequenties nl. 869/915 MHz en 2.4 GHz. Het gebruikt Direct Sequence Spread Spectrum (DSSS) om de verschillende frequentiebanden te verdelen in verschillende kanalen: 2.402-2.480 GHz in 16 kanalen, 915 MHz in 10 kanalen en 868 MHz in 1 kanaal. De fysieke laag voorziet 2 diensten: PHY data service en PHY management service. De PHY data service laat het zenden en ontvangen van PHY protocol data units (PPDU) toe over het radio kanaal. De eigenschappen van de fysieke laag zijn activatie en deactivatie van de radio tranceiver, energie detectie, kanaal selectie, link quality indication (LQI), verzenden en ontvangen van pakketten.

De MAC laag voorziet toegang tot het radio kanaal door gebruik te maken van Carrier Sense Multiple Access met Collision Avoidance mechanisme (CSMA/CA). De MAC laag voorziet ondersteuning voor het verzenden van beacon frames, netwerk synchronisatie en betrouwbare transmissie. De MAC laag voorziet 2 diensten: MAC data service en MAC management. De MAC data service laat het zenden en ontvangen toe van MAC protocol data units (MPDU) over de PHY data service. De eigenschap-

pen van de MAC laag zijn beacon management, kanaal toegang, GTS management, acknowledged frame delivery, association en disassociation.

De netwerklaag zorgt voor het zenden en ontvangen van data naar en van de applicatie laag. De netwerklaag is verantwoordelijk voor: opstarten van een netwerk, membership geven en ontnemen, configureren van een nieuw toestel, adressen toekennen aan toestellen die in het netwerk komen, synchronisatie, veiligheid toevoegen aan uitgaande frames en weghalen bij ontvangst en routing. Men kan met ZigBee 3 soorten netwerken opbouwen: cluster, ster en boomstructuur.

De applicatielaag bestaat uit 3 delen: Application Support Sublaag (APS), ZigBee Device Object (ZDO) en Application Framework (AF). De APS sub-laag is verantwoordelijk voor het bijhouden van tabellen voor 'binding', dit is nodig om 2 apparaten op elkaar af te stellen gebaseerd op hun diensten en behoeften, en het doorsturen van berichten tussen deze apparaten. Een andere taak van APS is discovery, dus het zoeken van andere apparaten in de nabijheid van een apparaat. ZDO is verantwoordelijk voor het definiëren van de rol van een apparaat in het netwerk en het opstellen van een veilige relatie tussen de netwerkapparaten.

108.3 ZigBee versus Bluetooth versus wifi

De transmissiesnelheid van Zigbee is stukken lager dan wifi en Bluetooth omdat het ontwikkeld is met als doel een laag stroomverbruik te hebben. ZigBee, Bluetooth en wifi zijn werkzaam in de industriële, wetenschappelijke en medische (ISM-)radiobanden. Een ZigBee netwerk kan uit veel apparaten bestaan, hierdoor wordt het bereik van het netwerk ook vergroot omdat de apparaten informatie aan elkaar doorgeven tot aan de coördinator.

108.4 Netwerkcomponenten

Een ZigBee netwerk wordt een PAN (Personal Area Network) genoemd en bestaat uit 1 coördinator, 1 of meerdere eindtoestellen en 1 of meerdere routers. Dus er zijn 3 verschillende ZigBeetoestellen:

- ZigBee coördinator (ZC): de coördinator vormt de wortel van de netwerkvertakking. Er is 1 ZigBee coördinator per netwerk en is verantwoordelijk voor de interne werking van het netwerk. De coördinator zet een netwerk op met een gegeven PAN-identifier.
- ZigBee Router (ZR): de router scant naar een netwerk om lid van te worden. Het kan ook gebruikt worden voor de coördinatie in het netwerk
- ZigBee End Device (ZED): een End Device moet berichten ontvangen en verzenden op de netwerklaag.

108.5 Externe links

- ZigBee Alliance
- IEEE 802.15.4 web site

Hoofdstuk 109

ZIP (bestandstype)

Een **zipbestand** of **zipfile** is een verliesvrij gecomprimeerd bestand waarin een of meer computerbestanden zijn ondergebracht.

109.1 Eigenschappen

Het ZIP-formaat kent vijf eigenschappen:

1. compressie: verkleinen van de ruimte die de gegevens in beslag nemen; het zipbestand is kleiner dan de oorspronkelijke bestanden. Hiervoor wordt een variant van het LZW-algoritme gebruikt.
2. Het archiveren: meerdere bestanden worden tezamen in één zipbestand gestoken, zo is het eenvoudiger te verspreiden zonder dat er essentiële onderdelen vergeten kunnen worden. Bovendien blijft de eventuele boomstructuur van bestanden en mappen behouden.
3. Het toevoegen van een controlemechanisme (CRC) om mogelijke gegevensfouten te detecteren.
4. Optionele encryptie van de data.
5. Optioneel kan een zipbestand worden opgedeeld in meerdere bestanden van gelijke grootte, zodat het bijvoorbeeld mogelijk wordt om een zipbestand verspreid over meerdere schijven (voorheen vooral diskettes) op te slaan. Het eerste deel krijgt de extensie .ZIP, de volgende delen .Z##, waarbij ## een oplopend nummer is.

109.2 Compressiemethode

Voor zipbestanden wordt meestal de deflate-compressiemethode gebruikt. In het verleden is er een groot aantal andere methoden gangbaar geweest die werden vervangen door betere opvolgers. Zipbestanden hebben doorgaans de extensie .ZIP maar er zijn ook zelfuitpakkende bestanden die de extensie .EXE hebben. Dit zijn programma's die een in het programma zelf opgenomen zipbestand kunnen uitpakken, zonder dat er een los uitpakprogramma nodig is.

109.3 Gebruik

Zipbestanden worden vooral gebruikt op het DOS- en Windows-platform. De bestandsformaten RAR en .7z zijn minder bekende formaten die beter comprimeren dan ZIP. In Unix en Unix-achtige besturingssystemen gebruikt men vooral de bestandsindeling gzip of bzip2 (voor de compressie) in combinatie met tar (voor de archivering). Het welbekende PKZIP van Phil Katz en WinZIP van Nico Mak bijvoorbeeld maken gebruik van de ZIP-compressiemethode.

Als meerdere kleine bestanden tezamen naar één zipbestand worden gecomprimeerd kunnen die kleine bestanden eerst samen genomen worden, en pas daarna gecomprimeerd worden. Hiermee wordt het uiteindelijke zipbestand kleiner, maar is daarmee geen standaard zipbestand meer. Een programma dat dit doet is bijvoorbeeld 7-zip, die daarmee een grotere compressie bereikt. Het uitpakken van zo'n bestand kan alleen maar met hetzelfde 7-zip.

109.4 Zippen

Het werkwoord "zippen" is afgeleid van de naam van dit bestandsformaat, maar wordt in algemene zin ook voor andere vormen van datacompressie en archivering gebruikt.

109.5 Programma's die ZIP-indeling ondersteunen

- Total Commander
- Krusader
- 7-Zip
- PeaZip
- PKZip
- WinRAR
- WinZip

- Stuffit
- ZipGenius

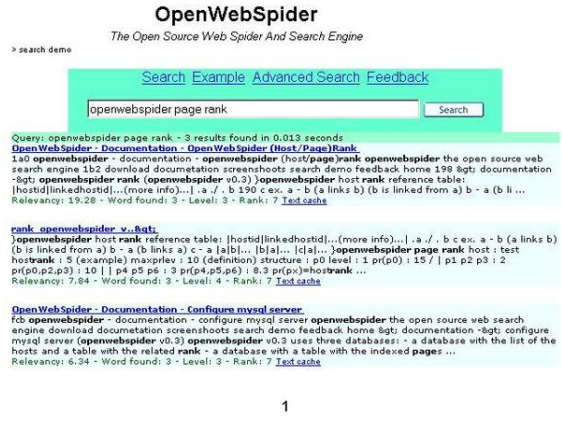
Vanaf Windows XP ondersteunt Microsoft Windows zip-bestanden zonder dat daar bijkomende software voor nodig is. Ze worden daar *gecomprimeerde mappen* genoemd.

109.6 Zie ook

- Datacompressie
- ARJ
- RAR
- JAR

Hoofdstuk 110

Zoekmachine



zoekresultaten van de opensource zoekmachine Openwebspider

Een **zoekmachine** is een computerprogramma waarmee men informatie kan zoeken in een bepaalde collectie; dit kan een bibliotheek, het internet, of een persoonlijke verzameling zijn.

Zonder nadere aanduiding bedoelt men tegenwoordig meestal een webdienst waarmee met behulp van vrije trefwoorden volledige tekst (*full text*) kan worden gezocht in het gehele *World Wide Web*.

In tegenstelling tot startpagina's of webgidsen is er geen of zeer weinig menselijke tussenkomst nodig; het bezoeken van de webpagina's en het sorteren van de rangschikkingen gebeurt met behulp van een algoritme.

Google is wereldwijd de meest gebruikte zoekmachine, andere populaire zoekmachines zijn Yahoo!, Bing en Baidu.

110.1 Technieken

Zoekmachines indexeren webpagina's geautomatiseerd door middel van robots/spiders. Dit zijn programma's die webpagina's scrapen en vervolgens nuttige informatie uit deze pagina's halen, zoals woorden en verwijzingen ("links") naar andere webpagina's. Deze links worden op hun beurt ook aan de spider gegeven om dan weer gedownload te worden. De gevonden woorden worden opgeslagen in een gigantische database.

De zoekmachines werken met verschillende technieken. Oorspronkelijk werkten de zoekmachines met de door de webmasters zelf opgegeven zoektermen (*keywords*), maar daar werd veel misbruik van gemaakt doordat de webmasters keywords gingen gebruiken die veel publiek trokken, maar geen verband hielden met de inhoud van de pagina, zoals het woord 'seks'.

Daarom werden diverse andere alternatieve technieken ontwikkeld. Zo werkt onder andere Google met de populariteit van de websites: het aantal malen dat een website op andere websites wordt vermeld. Op de websites van de zoekmachines is meestal wel informatie te vinden over hoe ze werken.

Het aantal spider-based-zoekmachines is beperkt. Grote internationale zoekmachines zijn Google, Teoma, Bing en Yahoo!. Bekende Nederlandse zoekmachines bedoeld om te zoeken naar Nederlandstalige pagina's zijn Kobala, Ilse en voorheen ook Track. Walhello is een in Nederland ontwikkelde internationale zoekmachine.

Er zijn ook metazoekmachines, zoekmachines die werken via de resultaten van andere zoekmachines. Voorbeelden zijn Metacrawler, Ixquick en Ez2Find. Nederland kent ook metazoekmachines zoals Zoeken.nl, Multizoeker, Metaspider.nl, Zoekal en Laquza.

Wolfram Alpha is een zoekmachine op internet, die niet zoekt naar pagina's (zoals Google doet), maar naar antwoorden op vragen, dat doet hij door te zoeken in een database van informatie

110.2 Gebieden

De meeste zoekmachines zijn bedoeld om iets op het web te vinden via het HTTP-protocol. Het gaat dan om informatie die ook met een browser bekeken kan worden. Daarnaast kunnen sommige zoekmachines ook informatie in nieuwsgroepen vinden. Bijvoorbeeld Google kopieert veel nieuwsgroepen naar de eigen servers, zodat daar in gezocht kan worden. Tot slot zijn er enkele zoekmachines die kunnen zoeken naar bestanden via het File Transfer Protocol.

110.3 Zoekmachine-marketing

Zoekmachine-marketing (*search engine marketing*) is het geheel aan activiteiten bedoeld om een webpagina hoog te laten scoren in de zoekresultaten van een zoekmachine, op voor de webpagina relevante trefwoorden of zoektermen. Zoekmachine-marketing bestaat uit twee onderdelen:

- Zoekmachineoptimalisatie en
- Zoekmachine-adverteren.

110.3.1 Adverteren bij zoekmachines

Een andere manier om 'hoog te scoren' bij zoekmachines is adverteren. Aanvankelijk kon er tegen betaling een plaats hoog in de ranking 'gekocht' worden als advertentie. Tegenwoordig is het bij bijna alle zoekmachines zo dat een dergelijke praktijk niet meer mogelijk is, omdat gebruikers het niet meer accepteren. In plaats daarvan worden er op een aparte plaats (vaak aan de rechterkant, soms ook bovenaan) zogenaamde 'gesponsorde koppelingen' getoond. Dit wordt door gebruikers als minder storend ervaren, omdat 'echte resultaten' en advertenties duidelijker te onderscheiden zijn.

De advertentieruimte bij de gesponsorde koppelingen wordt meestal 'verkocht' per opbod via het 'pay per click'-systeem. Bij bijvoorbeeld Google Adwords wordt de positie bij de gesponsorde koppelingen bepaald door het bod van de adverteerder te vermenigvuldigen met de Click-Through Rate.

110.4 Gespecialiseerde zoekmachines

Om de hegemonie van marktleiders als Google te ontlopen richten sommige zoekmachines zich op een bepaald specialisatiegebied. Zij worden ook wel verticale zoekmachines genoemd. Omdat zij speciaal zijn ontworpen om juist voor dit speciale gebied de beste resultaten naar boven te halen, denken zij het hier beter te doen dan algemene zoekmachines.

Een van die specialisatiegebieden is de academische wereld. Elsevier richt zich met Scopus op dit gat in de markt, waarmee zowel wetenschappelijk tijdschriften worden doorzocht, als wel de academische kennis op het Internet door gebruik te maken van Scirus. Web of Science (van Thompson Isi) is een concurrent die negenduizend tijdschriften en een krantenarchief van zestig jaar doorzoekt. Google probeert met Google Scholar zelf ook een speler in deze markt te worden. OAIster van de Universiteit van Michigan richt zich op wetenschappelijke informatie die door ruim duizend universiteiten en onderzoekscentra via Digital Academic Repositories beschikbaar wordt gemaakt. De MedischeZoekmachine.nl richt zich speciaal op medische zoektermen.

Een andere specialisatiegebied voor zoekmachines zijn diensten en consumentenproducten. Voor het vinden van op de Nederlandse markt huizen zijn Jaap.nl, HuizenZoeker.nl en Zuka.nl gespecialiseerd, in België kan je hiervoor terecht op Immoweb.be, Immoture.be en Hebbes.be. Voor vacatures Askjim.nl en Indeed, en voor auto's Gaspedaal.nl. Het Nederlandse El Cheapo heeft zich gespecialiseerd in het vergelijken van bepaalde producten bij verschillende aanbieders. Google doet hetzelfde met Froogle. Onderwijsinformatie is te vinden met Davindi. Een internationale boekenzoeksite is Addall.com.

110.5 Nadelen zoekmachines

Naast de vele voordelen van zoekmachines zoals Google, kleven er ook nadelen aan het gebruik van grote zoekmachines. Door de toename van data wordt het steeds moeilijker om gerichter te kunnen zoeken op een bepaald gebied, of in een andere taal dan het Engels. Vaak kun je op kleine, regionale zoekmachines, zoals hierboven staat beschreven, wel specifieke informatie krijgen in jouw taal, maar bij dit soort zoekmachines ontbreken de zoek– en analysekwaliteiten. Voor vele grote zoekmachines is het een uitdaging om ook deze kleine, regionale sites te betrekken in hun zoekresultaten.

Doordat zoekmachines heel het internet in kaart kunnen brengen vormen ze ook een probleem inzake privacy. Als privacygevoelige data eenmaal op internet zijn gepubliceerd zijn die data, zelfs als deze verwijderd zijn van de website waar zij stonden, vaak terug te vinden in de archieven van zoekmachines.

Bij Google uit zich dit in de mogelijkheid om de cache te kunnen bekijken. Daarnaast zou Google niet goed omgaan met de privacy van gebruikers van de zoekmachine. Zo zou Google de data niet-geanonimiseerd opslaan om aan de hand van de zoekgeschiedenis van de gebruiker beter passende advertenties te tonen.

De open source zoekmachine DuckDuckGo biedt een ongefilterd en privacyveilig alternatief.

110.6 Zoekfunctie

Een website, en een programma zoals een browser of reader, hebben vaak een zoekfunctie. Soms hebben deze opties zoals "alles markeren" en "hoofdlettergevoelig". Bij het zoeken in één document is er soms de optie "alles markeren" en kan men vaak de zoekrichting kiezen: vooruit of achteruit. Soms gaat men na het eind vanzelf weer verder vanaf het begin (en omgekeerd bij achteruit zoeken), soms stopt het zoeken bij het eind/begin. Soms onthoudt

het programma waar men met het zoeken begonnen is en stopt het na één cyclus.

110.7 Zie ook

- Lijst van zoekmachines

110.8 Literatuur

- Chung et al (2006) "SpidersRUs: Creating specialized search engines in multiple languages," *Decision Support Systems*,, nr. 42, pp. 1697-1714
- Chau et al (2007) "Supporting non-English Web searching: An experiment on the Spanish business and the Arabic medical intelligence portals," *Decision Support Systems*
- Hargittai, E. (2007) "The social, political, economic, and cultural dimensions of search engines: An introduction," *Journal of Computer-Mediated Communication*, nr. 12
- Guan, T en K. F. Wong (2003) "Nstar: an interactive tool for local web search," *Information & Management*, nr 41, pp. 213-225
- Braun-LaTour et al (2007) "Mood, information congruency, and overload," *Journal of Business Research*, nr. 60, pp. 1109-1116

W

110.9 Tekst-en beeldbronnen, medewerkers en licenties

110.9.1 Tekst

- **Achterdeurtje** *Bron:* https://nl.wikipedia.org/wiki/Achterdeurtje?oldid=40150746 *Bijdragers:* Advance, Danielm~nlwiki, Meneer, RobotQuistnix, LimoWreck, Freek Verkerk, Anorionil, Josq, SieBot, Thijs!bot, Aiko, Tukka, Heer van Robaais, JAnDbot, Rei-bot, DorganBot, TXiKiBoT, PipepBot, Zorrobot, B222, Alexbot, AbiBot, Astrion, Luckas-bot, Joris1919, Smile4ever, RomaineBot, EmausBot, Ward Moerman, DunjaP, MichèleD, Addbot en Anoniem: 2
- **Adware** *Bron:* https://nl.wikipedia.org/wiki/Adware?oldid=46891921 *Bijdragers:* HooftBot, Robbot, RobotE, Michiel1972, Meneer, MichielDMN, RobotMichiel1972, Lexw, RobotQuistnix, RoboRex, Vertrokken, Aergn, Chobot, YurikBot, FlaBot, SieBot, Thijs!bot, Escarbot, AlleborgoBot, VVVBot, GrouchoBot, Verboden, Alexbot, BOTarate, CarsracBot, Luckas-bot, Vini 17bot5, Manco Capac, Mathonius, Smile4ever, MondalorBot, ButkoBot, TobeBot, JurriaanH, EmausBot, Sjoerddebruin, Ripchip Bot, Martijnengler, Ward Moerman, AlbinS, MichèleD, Makecat-bot, Legobot, NielsAC en Anoniem: 9
- **Anoniem surfen** *Bron:* https://nl.wikipedia.org/wiki/Anoniem_surfen?oldid=45062960 *Bijdragers:* Robbot, Kattenkruid, Riki, The Banner, Mexicano, Hans Brenkman, Dqfn13, Pompidombot, Smile4ever, RomaineBot, ErikvanB, Joris0707, MexicanoBot, EmausBot, Nick.Robyn, Lexkol, Ward Moerman, Sander Van Durme, DunjaP, MichèleD, Brentjee, Addbot en Anoniem: 1
- **Antivirussoftware** *Bron:* https://nl.wikipedia.org/wiki/Antivirussoftware?oldid=47067906 *Bijdragers:* Bemoeial, Jeroen, Robbot, RobotE, Chris, Jupiler, MichielDMN, RobotQuistnix, LimoWreck, MADe, RobotJcb, RoboRex, YurikBot, Eve, FlaBot, Maniago, Kleuske, Zanaq, Gerbot, Berendvd, Peronista, Wikiklaas, .Koen, Jvhertum, SieBot, Thijs!bot, Aiko, Haarajot, JAnDbot, .anacondabot, Patrickvandervalk, Johan N, MoiraMoira, Encoder, YoshiDaSilva, VanBuren, Rudolphous, TXiKiBoT, VolkovBot, GijsvdL, BotMultichill, PolarBot, Jan.vanhaver, Groucho NL, PipepBot, GrouchoBot, KLBX, DragonBot, AlnoktaBOT, Filenox~nlwiki, Andorvb, SilvonenBot, ???? robot, JurgenNL, Emil76, CarsracBot, NjardarBot, Luckas-bot, MrBlueSky, ChenzwBot, Misi91, Timmieboy, XZeroBot, FoxBot, Kippenvlees1, SassoBot, Smile4ever, MrBlueBot, ErikvanB, Mozoa, EmausBot, HRoestBot, Waterfiets, WikitanvirBot, ChuispastonBot, Sjoerddebruin, Lotje, Piquedram, MerlIwBot, Tim-E-Veiligheid, Stef.kerkhofs, DunjaP, Manu De Pourcq, Pollej123, Grmbl76, Atrokov, Justincheng12345-bot, K1ngXSp3c1al, Legobot, Aggie2, Brentjee, Delphine Carlier, Tulp8, XXBlackburnXx, Stef Bryssinck, Kaj Sustronck, Thomas Lammens, Wikiwerner, DottyMcFear13 en Anoniem: 54
- **Avatar (computer)** *Bron:* https://nl.wikipedia.org/wiki/Avatar_(computer)?oldid=46331893 *Bijdragers:* Patrick, Falcongj, Robbot, Kattenkruid, RobotE, Sietske, Neovo.Geesink, Hardscarf, RobotMichiel1972, Pieter1, RobotQuistnix, Jelte, Gpvosbot, Algont, Riki, Servien, Christoffel K, Wenzeltjen, YurikBot, Eve, LeonardoRob0t, Gerbennn, Erwin, Gerbot, Wobuzowatsj, Dsjh, Simeon, BlackNight, .Koen, SieBot, Thijs!bot, Edwinb, NielsTriple, DimiTalen, Aiko, Casperinfo, Soulbot, JAnDbot, Elisabethsmit, Pelikana, Narayan, Shiv~nlwiki, TXiKiBoT, Handige Harrie, VolkovBot, AlleborgoBot, SlimmeHans, JebCee, Idioma-bot, Loveless, Ajo2106, Louperibot, PipepBot, BjornR, Zorrobot, GrouchoBot, Forrestjunky, Alexbot, Luckas-bot, MrBlueSky, ChenzwBot, ArthurBot, Eigenaar44, DéRaBot, Xqbot, Pompidombot, Lukasj16, RomaineBot, D'ohBot, Msj, RedBot, ErikvanB, Taalvos, EmausBot, Inge1993, JackieBot, EnricoKolk95, MichèleD, ~riley, Addbot, Tulp8 en Anoniem: 23
- **Backbone** *Bron:* https://nl.wikipedia.org/wiki/Backbone?oldid=47962665 *Bijdragers:* Romaine, Robbot, RobotE, Emvee, HetKantoor, RobotQuistnix, Rex, RoboRex, Zwobot, FlaBot, Kleuske, SieBot, Thijs!bot, MoiraMoira, Look Sharp!, VolkovBot, AlleborgoBot, Beany, AlnoktaBOT, PixelBot, RonnieV, Toth, De Wikischim, DumZiBoT, ErikvanB, EmausBot, Addbot, StroopwafelBot en Anoniem: 8
- **Internet** *Bron:* https://nl.wikipedia.org/wiki/Internet?oldid=47965455 *Bijdragers:* Andre Engels, Patrick, Amarant, Ap~nlwiki, Christian List, Pieter~nlwiki, Ellywa, Ludo~nlwiki, Rob Hooft, Rene Pijlman, Pven, Romaine, SanderSpek, Wilinckx, Hannes Karnoefel, Cicero~nlwiki, Guaka, LennartBolks, Willemdd, BenTels, Professor~nlwiki, Carol Fenijn, Garo~nlwiki, Ligtvoet, Muijz, Puckly, HooftBot, Advance, Robbot, Hashar, Kattenkruid, Oscar, Bezeh.nl, RobotE, Bob.v.R, Siebrand, Webkid~nlwiki, RonaldW, Edwtie, Quistnix, Kagaherk, Robotje, MichielDMN, RJB, Lexw, Pieter1, Yorian, Pjetter, Benneman, Ronn, Empoor, Tdevries, Tfa1964, Jcb, Fuss, Gpvos, Dolfy, RobotQuistnix, Nawi, Vitum, LimoWreck, Rex, Lucien D., Ed de Jonge, JeroenvB, Tomgreep, Venullian, Abnormaal, Joost, MADe, Edoderoo, Ucucha, Gpvosbot, Johjak, RoboRex, Riki, Erwin1990, Vertrokken, BotEmpoor, Peter b, Willemo, Wester2005, Christoffel K, Dartelaar, Jeroenbot, Obarskyr, Chobot, RonaldB, Aleichem, Zwobot, Dolledre, Jos-uit-boston, YurikBot, Eve, Troefkaart, Luna, Apdency, Maniago, Kleuske, Gerbennn, Ninane, Eskimbot, Fr33ke, Iggy~nlwiki, Kamphaus, SanderK, Josq, .marc., Bukowski, Sonty567, Tucker~nlwiki, MarcT, Adnergje, Clausule, Emmelie, Vincentsc, Berendvd, Mexicano, Gerritse, Simeon, Simon-sake, Kameraad Pjotr, Woudloper, EdBever, .Koen, Mbch331, Jvhertum, BerendBotje, SieBot, Thijs!bot, Edwinb, DimiTalen, AdnergjeBot, Erwin85Bot, Hajo, Rp, Basss, Escarbot, Magere Hein, BOT-Superzerocool, PHotoPower, Sindala, Bv, Paul B, Jahoe, Vis met 1 oog, JAnDbot, Machaerus, .anacondabot, A Duck, ReWinD, Waninge, JeroenvanVeen, BetBot~nlwiki, Johan N, MoiraMoira, CrazyPhunkbot, Joost 99, Pieter19, Simonbr, Po~nlwiki, Viking-nl, YoshiDaSilva, Look Sharp!, OekelWm, DodekBot, Edwin Zeelenberg, TXiKiBoT, Lymantria, VolkovBot, Candi, Le Fou, GijsvdL, BotMultichill, RenéV, ErikWarmelink, 3wisemen, Miho, Rmfloris, AlleborgoBot, Synthebot, Apocatequil, Sander1453, YonaBot, DieDubbelJoe, Idioma-bot, Loveless, Sswelm, Louperibot, Wutsje, Richardkiwi, Krisdedecker, PipepBot, BjornR, Vinvlugt, WDVLWD, GrouchoBot, Kthoelen, Dloohuis04, Iamthestig, DragonBot, Rrbb, Mleusink, Jarii94, Greenday2, RonnieV, Purbo T, ???? robot, Pieterpeeters13, Gijsisok, JurgenNL, MelancholieBot, CarsracBot, Plankje, Pompidom, Akoopal, Kwiki, Paisandes, Dqfn13, MrBlueSky, Goudsbloem, Japiobot, Jotterbot, Poepenmoslims, Marrakech, Edoderoobot, Hoopje, Peterson, ArthurBot, DSisyphBot, Mathonius, De Wikischim, FoxBot, Kippenvlees1, Xqbot, RibotBOT, Maasje, Olivier Bommel, Marganne, Spraakverwarring, Smile4ever, Hanssmellinckx, Trewal, RomaineBot, Comma~nlwiki, Trijnstel, Wiki13, TobeBot, TBloemink, JurriaanH, ErikvanB, KamikazeBot, TjBot, WinContro, Denkhenk, MexicanoBot, EmausBot, WikitanvirBot, ChuispastonBot, Eg-T2g, BakkertjeWouter, Smiba, Sjoerddebruin, ChrisN, Movses-bot, Dinosaur918, HanhilBot, Sikjes, Ripchip Bot, MerlIwBot, Wim Nobel, AvocatoBot, Malinka1, Jeroen Schrauwen, Grmbl76, Minsbot, Beatboxxer15, Nickjelle, Jennie1987, Maartenschrijft, Addbot, Laurannelanckmans, Tulp8, Salamander122, HexaCore, Kukkie, RotlinkBot, Robyvd, MatthijsWiki, Wwian1, StroopwafelBot, Moira Moira 368, Max greefhorst, DottyMcFear13, Oxygene7-13, WikiMeneer, Xxmarijnw en Anoniem: 332
- **Besturingssysteem** *Bron:* https://nl.wikipedia.org/wiki/Besturingssysteem?oldid=47940802 *Bijdragers:* Scipius, Andre Engels, Ap~nlwiki, Jcwf, Pieter~nlwiki, Ellywa, Pieter Suurmond, Rob Hooft, Arent, Fruggo, Bemoeial, Wilinckx, Guaka, BenTels, Streppel, Carol Fenijn, Rene~nlwiki, Joro~nlwiki, Kozmoz, HooftBot, Robbot, GerardM, Henricus, Nikai, Hashar, Riscysite, Willem vd Kletersteeg, PrisonerOfPain, Q-collective, Theo, RobotE, MartinD, Mwpnl, Michiel1972, HenkvD, Sherpa~nlwiki, Robotje, BenTheWikiMan, MichielDMN, RobotMichiel1972, Mdd, Koos Jol, Lexw, Emvee, Pjetter, Alex1, Mikenolte, Spearhead~nlwiki, RobotQuistnix, Ed de Jonge, Venullian, MADe, Gpvosbot, Robotpjetter, RoboRex, Riki, Gid, KokoBot, Translation Services Center, Annabel, Dartelaar, Tuvic, Obarskyr, Chobot, Takis~nlwiki, RonaldB, YurikBot, Eve, LeonardoRob0t, FlaBot, Maniago, Kleuske, Bruyninc, Waldo79, Sumurai8,

Chlewbot, RoboDick~nlwiki, Obi~nlwiki, Whizz, Mexicano, Simeon, Kameraad Pjotr, .Koen, Jvhertum, SieBot, Klootzakkie, Thijs!bot, Edwinb, AdnergjeBot, Bondgirl 2170, Obarskyr Bot, Escarbot, Madyno, Noescom, BOT-Superzerocool, Wolu, Paul B, JAnDbot, ZesZesZes, BetBot~nlwiki, MoiraMoira, YoshiDaSilva, Look Sharp!, WarddrBOT, TXiKiBoT, Lymantria, VolkovBot, BotMultichill, RenéV, AlleborgoBot, Vels, Synthebot, YonaBot, Idioma-bot, Gerakibot, Sswelm, Louperibot, PipepBot, BjornR, Kthoelen, DragonBot, PixelBot, MwpnlBot, Purbo T, BodhisattvaBot, AnokoBOT, Alecs.bot, JurgenNL, CarsracBot, Pompidom, EivindBot, LinkFA-Bot, LaaknorBot, Luckas-bot, MystBot, MrBlueSky, Ptbotgourou, Nallimbot, Jotterbot, JZ85, Marrakech, Hoopje, MauritsBot, ArthurBot, Mathonius, Diamant, Kippenvlees1, Xqbot, RibotBOT, Pompidombot, Theking2, Smile4ever, Woutb, RomaineBot, Wvanb, Trijnstel, Wiki13, MrBlueBot, TobeBot, Mattias.Campe, TBloemink, Dinamik-bot, ErikvanB, TjBot, MexicanoBot, EmausBot, ZéroBot, JhsBot, WikitanvirBot, ChuispastonBot, Eg-T2g, Lotje, Goingjulian, Grmbl76, SteenthIWbot, JoranCrabbé, Legobot, Addbot, Tulp8, Wenneke1981, Maxiebyte en Anoniem: 109

- **BIOS** *Bron:* https://nl.wikipedia.org/wiki/BIOS?oldid=47739540 *Bijdragers:* Andre Engels, Christian List, Erik Zachte, Ellywa, Arent, SanderSpek, Bemoeial, Wilinckx, BenTels, HooftBot, Robbot, RobotE, Michiel1972, Quistnix, A3, Robotje, W~nlwiki, RobotQuistnix, RoboRex, Vertrokken, Willemo, Palica, Dartelaar, Tuvic, Jeroen-91, Aleichem, YurikBot, FlaBot, Maniago, Eskimbot, RobotTbc, SanderK, Tobe Deprez, Whizz, Mexicano, Kameraad Pjotr, Mbch331, Jvhertum, SieBot, Thijs!bot, Edwinb, Erik Baas, Caenwyr, Wolu, Matthieu Mimpen, Virtlink, MoiraMoira, Grotezakpatat, Rei-bot, Look Sharp!, DodekBot, TXiKiBoT, Japiot, VolkovBot, BotMultichill, 3wisemen, Loveless, Zorrobot, WDVLWD, GrouchoBot, Vliegenmepper, Frank Geerlings, EjsBot, LaaknorBot, Luckas-bot, Gitaarman, ArthurBot, Je Eumaa, Rubinbot, Smile4ever, Wimbervoets, Egmontbot, RomaineBot, ReGA-pictures, Mattias.Campe, TBloemink, ErikvanB, Vazerth, EmausBot, Sjoerddebruin, MerlIwBot, AvocatoBot, Southparkfan, Nl maclean, YFdyh-bot, Legobot, Nietanoniem, StroopwafelBot en Anoniem: 41
- **Bluecasting** *Bron:* https://nl.wikipedia.org/wiki/Bluecasting?oldid=35583184 *Bijdragers:* Johjak, Havana1982, Aleichem, FlaBot, SieBot, Handige Harrie, Synthebot, Luckas-bot, Xqbot, EmausBot, Addbot en Anoniem: 2
- **Bluejacking** *Bron:* https://nl.wikipedia.org/wiki/Bluejacking?oldid=35502256 *Bijdragers:* Patrick, Puckly, HooftBot, Robbot, RobotE, Quistnix, MichielDMN, Gus (hernoemd), RobotQuistnix, RoboRex, Canp, Jvhertum, Thijs!bot, JAnDbot, CommonsDelinker, DodekBot, TXiKiBoT, Wutsje, PixelBot, DrJos, Luckas-bot, Goudsbloem, RudolphousBot, RomaineBot, MrBlueBot, MexicanoBot, Addbot en Anoniem: 3
- **Bluetooth** *Bron:* https://nl.wikipedia.org/wiki/Bluetooth?oldid=47720007 *Bijdragers:* Andre Engels, Patrick, Romaine, Jeroen, Willemdd, Carol Fenijn, Muijz, Puckly, HooftBot, Advance, Robbot, RonOnrust, Oscar, RobotE, Siebrand, Chris, MartinD, Taka, DaProx, Michiel1972, Quistnix, Svdmolen, Robotje, BenTheWikiMan, MichielDMN, Jan Duimel, Emvee, B kimmel, Pjetter, Joachim, Jurre, Jcb, RobotQuistnix, Marcieking, Abnormaal, Dryke, Gpvosbot, Algont, RoboRex, Riki, BotEmpoor, Willemo, Klaas1978, KokoBot, Yvesn, Dartelaar, RonaldB, Dolledre, YurikBot, Eve, Vdegroot, FlaBot, Maniago, Kleuske, WillBot, Eskimbot, RaMPo, Fontes, Gerbot, Bramdehaan, EdBever, SieBot, Thijs!bot, Tukka, Tkteun, RoboServien, Escarbot, Erik1980, JAnDbot, Mari1988, BotteHarry, CrazyPhunkbot, Rei-bot, Look Sharp!, DorganBot, WarddrBOT, TXiKiBoT, Lymantria, Ctxppc, Wegwezen, Mw007, GijsvdL, BotMultichill, Zwitser123, M. Renckens, Willemdeveertiende, Synthebot, Loveless, Mbsaerens, Luc everse, Vinvlugt, Vliegenmepper, AlnoktaBOT, Spoorjan, Tim van overtveldt, Stinos, Jarii94, Netraam, Alexbot, Emmenaar, BodhisattvaBot, Jeffzor, Toth, Cvnico, CarsracBot, Tymofyeyev pavlo, NjardarBot, MastiBot, Luckas-bot, MrBlueSky, Goudsbloem, Nallimbot, Hoopje, Peterson, ArthurBot, Jlthkoch, FoxBot, Xqbot, RibotBOT, Olivier Bommel, Spraakverwarring, Smile4ever, RomaineBot, RedBot, TobeBot, Jand12, Woumpousse, EmausBot, ZéroBot, LaurentI, JackieBot, Chielbuseyne, WikitanvirBot, Ebrambot, Rezabot, Janwillem1976, Legobot, StroopwafelBot, Xxmarijnw en Anoniem: 81
- **Bootloader** *Bron:* https://nl.wikipedia.org/wiki/Bootloader?oldid=45957633 *Bijdragers:* Snaily, Robotpjetter, Apdency, FlaBot, Mion, Jvhertum, PHouben, VanBuren, AnnabelsBot, Handige Harrie, Octogon, Smile4ever, RomaineBot, Wiki13, MrBlueBot, ErikvanB, Queeste, EmausBot, Eg-T2g, Addbot en Anoniem: 6
- **Bootsectorvirus** *Bron:* https://nl.wikipedia.org/wiki/Bootsectorvirus?oldid=37729535 *Bijdragers:* Bemoeial, Taka, HenkvD, MichielDMN, ArjenW, Ronaldvd, Fontes, Tvdm, Magere Hein, Zwitser123, Pompidombot, Heureka, Mattias.Campe, MaartenRijpkema en Anoniem: 7
- **Botnet** *Bron:* https://nl.wikipedia.org/wiki/Botnet?oldid=43539740 *Bijdragers:* Advance, Meneer, MichielDMN, B kimmel, Troefkaart, FlaBot, Maniago, Kleuske, Zanaq, Foxie001, Khx023, Mbch331, Aiko, Machaerus, 88scythe, Japiot, SAMnl, GrouchoBot, Iamthestig, Ewald, Luckas-bot, MrBlueSky, Ptbotgourou, ArthurBot, RomaineBot, Jeehaa, Wiki13, MondalorBot, Bartledoo, WinContro, EmausBot, ZéroBot, Mjbmrbot, Lotje, Ripchip Bot, MerlIwBot, Vagobot, MahdiBot, Addbot, Muzaffergul, StroopwafelBot, NielsVH en Anoniem: 11
- **Browserkaper** *Bron:* https://nl.wikipedia.org/wiki/Browserkaper?oldid=44861118 *Bijdragers:* CaAl, Wikiklaas, Sander1453, Arend41, EvilFreD, ErikvanB, Dinosaur918, Kloentje2, Ilie Cremers en Anoniem: 2
- **Brute force (methode)** *Bron:* https://nl.wikipedia.org/wiki/Brute_force_(methode)?oldid=46439463 *Bijdragers:* Muijz, Michiel1972, Dinx, Riki, Vertrokken, DéRahier, Maniago, Foxie001, Simeon, Jvhertum, Tukka, Vis met 1 oog, JAnDbot, Handige Harrie, VolkovBot, GijsvdL, Nipisiquit, Idioma-bot, Wutsje, GrouchoBot, Joost Herregodts, MelancholieBot, LaaknorBot, Luckas-bot, MrBlueSky, ArthurBot, RomaineBot, Wiki13, MrBlueBot, ErikvanB, Queeste, WikitanvirBot, ChuispastonBot, MerlIwBot, Rezabot, MichèleD, Rijndaal, Minsbot, Addbot, JP001, StroopwafelBot, Wikiwerner en Anoniem: 13
- **Bug (technologie)** *Bron:* https://nl.wikipedia.org/wiki/Bug_(technologie)?oldid=47747892 *Bijdragers:* KoenB, Carol Fenijn, Serassot, HooftBot, Robbot, Draconigena, Oscar, Danielm~nlwiki, Arrowman, Quistnix, Lexw, ThijsVermeir, IJzeren Jan, RobotQuistnix, Rex, Freek Verkerk, JeroenvB, Kiwix, Abcdefghjlmnopqrstuvyz, RoboRex, MoriBot, KokoBot, Ietskleiner, YurikBot, Apdency, Eskimbot, Rcoo, Trillian~nlwiki, SvGeloven, Mexicano, Simeon, Kameraad Pjotr, Maggy, SieBot, Thijs!bot, Escarbot, JAnDbot, DorganBot, Handige Harrie, Aibot, Gerakibot, GrouchoBot, Toth, Taketa, Pompidom, Common Good, Luckas-bot, Nallimbot, Edoderoobot, ArthurBot, RudolphousBot, Obersachsebot, Xqbot, Meerdervoort, Rubinbot, RomaineBot, BenzolBot, Atje222, Wiki13, RedBot, TobeBot, ErikvanB, EmausBot, ZéroBot, WikitanvirBot, ChuispastonBot, ChrisN, Minsbot, Kippenbot1, Legobot en Anoniem: 18
- **Cloud computing** *Bron:* https://nl.wikipedia.org/wiki/Cloud_computing?oldid=46699704 *Bijdragers:* Muijz, Robbot, Bob.v.R, Meneer, MichielDMN, Lexw, Galwaygirl, Wikix-oud, Tomgreep, MADe, Riki, Dartelaar, RonaldB, Jdoesburg, Maniago, Kleuske, Zanaq, .marc., Mexicano, Mbch331, SieBot, Joris, Magere Hein, Davin, Vis met 1 oog, Fjvelsen, MoiraMoira, Anneb, Look Sharp!, Wikibelgiaan, Qzagnix, TXiKiBoT, Japiot, VolkovBot, BotMultichill, Idioma-bot, Loveless, Jarune, GrouchoBot, Kthoelen, Voorthuizenr, DragonBot, Prlwytzkowsky, Tonkie, Darkicebot, SilvonenBot, Alecs.bot, MelancholieBot, Pompidom, Kwiki, Luckas-bot, Jayvd, Amirobot, MrBlueSky, JZ85, Hoopje, MauritsBot, ArthurBot, Tornado79, Everlind, De Wikischim, Xqbot, RibotBOT, DumZiBoT, Smile4ever, Mastadc, RomaineBot, Utrechtse, Trijnstel, D'ohBot, Wiki13, RedBot, TBloemink, Woodcutterty, Dinamik-bot, Bruno Pauwels, ErikvanB, TjBot, MexicanoBot, EmausBot, HRoestBot, JackieBot, Cloudforum, WikitanvirBot, Tm279905, Rienjo, Ripchip Bot, MerlIwBot, Ava157, Witsenburg.peter,

Jjk123, Remcojan, Rene.antenbrink, Grmbl76, Arvidfossen, Addbot, Tulp8, Phuijbers, 12345danNL, HAPPY1211, Wikiwerner, Clockfest, Swdevguy en Anoniem: 80

- **Computer** *Bron:* https://nl.wikipedia.org/wiki/Computer?oldid=47941208 *Bijdragers:* Scipius, Andre Engels, Walter, Amarant, Marza, ArthurKing, Mahjongg~nlwiki, Ellywa, Rob Hooft, Snoop, Rene Pijlman, Laurier, Romaine, SanderSpek, Fruggo, Bemoeial, Wilinckx, Hannes Karnoefel, Cicero~nlwiki, Guaka, LennartBolks, Jeroen, BenTels, Assies, Streppel, Falcongj, Carol Fenijn, Blukske, Eugene, Ligtvoet, Muijz, Waerth, HooftBot, Advance, Robbot, GerardM, Heli0s, Bartux, McDutchie, Hashar, Landriessen, Jintro, Hondeman, Kattenkruid, Oscar, Bezeh.nl, Theo, RobotE, Bob.v.R, Siebrand, Danielm~nlwiki, Chris, MartinD, Bernard van der Wees, Taka, DaProx, Michiel1972, Ano niem, HenkvD, Bean 19, A3, Hansv, Caseman, O E P~nlwiki, Robotje, BenTheWikiMan, Neovo.Geesink, Guanabot~nlwiki, MichielDMN, El barto, Andre.blum, Mdd, Koos Jol, Lexw, Ype, Pieter1, Yorian, JePe, Alex1, Arienh4, Emresys, Ronn, HetKantoor, MigGroningen, Drdefcom, Jcb, Rafvz, RobotQuistnix, LimoWreck, Rex, Freek Verkerk, Ed de Jonge, Valhallasw, T Houdijk, Joost, Neutraal, Dryke, Edoderoo, Gpvosbot, RoboRex, Riki, Servien, Vertrokken, BotEmpoor, Peter b, Frietmet, DJclaud, AlexP, Klaas1978, Titusvh, MoriBot, Translation Services Center, Tuvic, Obarskyr, Chobot, RonaldB, Aleichem, Dolledre, Moartn, DrBorka, Onno Zweers, Eve, ArjenW, Daka, FlaBot, Kalsermar, The Banner, Agowie, Ronaldvd, Maniago, Kleuske, Gerbennn, Ninane, SanderK, Josq, .marc., Flying DutchJan, Thomas-, Maarten1980, CedricD, Sonty567, Erwin, Edelhart, Hottestbrain, Robb, Adnergje, G.Lanting, Streep, Roelzzz, Vincentsc, Fontes, Hardloper, Johanna83, Yippie, Mexicano, Khx023, Måxïm, Simeon, Simon-sake, DennisPeeters, Kameraad Pjotr, EdBever, Imodium, Wikiklaas, .Koen, Jvhertum, Btalman, BerendBotje, SieBot, Thijs!bot, Edwinb, Erik Baas, Tukka, Jed, Coen1995, RoboServien, Stijnfolkers, Rygir, Escarbot, Ilias~nlwiki, ChristiaanPR, Erik1980, Foroa, Heer van Robaais, Magere Hein, BOT-Superzerocool, Paul B, Wtje, JAnDbot, .anacondabot, Calvero2, HandigeHarry, Johan N, MoiraMoira, Wimmel, Icedfire 800, Leopard, Fredknoks, SbJ, Ken123, YoshiDaSilva, IcedFire 008, Look Sharp!, Larzzz, WarddrBOT, Polaris~nlwiki, TXiKiBoT, Lymantria, Grashoofd, Aibot, VolkovBot, Ctxppc, R.schwab, Robin21496, GijsvdL, BotMultichill, RenéV, Silver Spoon, 3wisemen, LarzBot, AlleborgoBot, RubySS, Synthebot, Vacio, Lolsimon, YonaBot, Tleilax, Idioma-bot, Loveless, Gerakibot, Freaky Fries, Koektrommel, SAMnl, Louperibot, Butch, Ken123BOT, Wutsje, PipepBot, Vinvlugt, Makk1996, GrouchoBot, ArjanH, Kthoelen, DragonBot, Jarii94, Beachcomber, Apenkooi, Hans Kamp, DrJos, Forrestjunky, Alexbot, Greenday2, Nederlandse Leeuw, RonnieV, Kennyannydenny, Toth, Djmindscape, Dikkieeeeeeeeeeeeeee, JurgenNL, MelancholieBot, CarsracBot, Pompidom, Kwiki, Doc Brown, LinkFA-Bot, LaaknorBot, Jack Ver, MrBlueSky, Spock~nlwiki, Mezelf14, Halvar, Jotterbot, Kvdh, Hoopje, MauritsBot, Peterson, ArthurBot, Hslive, Mathonius, FoxBot, Xqbot, Almabot, SassoBot, RibotBOT, Spraakverwarring, Stier~nlwiki, Smile4ever, Mastadc, RomaineBot, Twiss~nlwiki, Trijnstel, Condor3d, Wiki13, Scorpi~nlwiki, TobeBot, FreakyBot, TBloemink, Woodcutterty, JurriaanH, Cgb~nlwiki, ErikvanB, KamikazeBot, Bartledoo, TjBot, WinContro, MexicanoBot, DixonDBot, EmausBot, Kadeike, ZéroBot, HRoestBot, JhsBot, Geniaal, Kulter20, Erik009, WikitanvirBot, Targaryen, ChuispastonBot, BakkertjeWouter, Mjbmrbot, HeinS5, Sjoerddebruin, ChrisN, TuurDS, Movses-bot, Goingjulian, Dinosaur918, Diablotje, Jixar2, Xxxlololxxx, Ripchip Bot, MerlIwBot, Markvasz, Vagobot, Glennznl, Malinka1, Grmbl76, Mitchproosten, Kloentje2, Dexbot, Legobot, Nietanoniem, Ppcool1, Addbot, Rillos, Tulp8, Kukkie, Wwian1, 12345danNL, StroopwafelBot, Seks gustavo, Lodewijk197, Wikiwerner, Popedijntje23, Edgoe, DottyMcFear13, Baarten en Anoniem: 422
- **Computercriminaliteit** *Bron:* https://nl.wikipedia.org/wiki/Computercriminaliteit?oldid=46237163 *Bijdragers:* Patrick, SanderSpek, Vexernl, Guaka, Jeroen, Carol Fenijn, Robbot, Michiel1972, Meneer, MichielDMN, Pjetter, RobotQuistnix, MADe, RoboRex, Karel Anthonissen, Tilanus, RonaldB, Aart, Maniago, Gerbot, Mexicano, Simeon, Jvhertum, Erwin85Bot, Benedict Wydooghe, JAnDbot, Machaerus, MoiraMoira, Rei-bot, Tschouten, Butch, Pompidom, HerculeBot, Luckas-bot, AStarBot, Cybercrime, Flurps, Edoderoobot, MauritsBot, ArthurBot, FoxBot, Xqbot, Smile4ever, Wiki13, MrBlueBot, ErikvanB, KamikazeBot, Opblaasmaat, EmausBot, ChuispastonBot, Sjoerddebruin, Lotje, MerlIwBot, AvocatoBot, Seine, Brdebu, Stef.kerkhofs, Tompie63, Ilse reeper, Makecat-bot, Legobot, Delphine Carlier, Ilie Cremers, Jonas7735, Ann-Sophie B, Nicolas.B, Emmelie2394, Kaj Sustronck, Joachim Sercu, Berdieke, Niels.Veryepe en Anoniem: 14
- **Computergeheugen** *Bron:* https://nl.wikipedia.org/wiki/Computergeheugen?oldid=45592195 *Bijdragers:* Ellywa, Pven, Bemoeial, Jeroen, Treenaks, Robbot, RobotE, Michiel1972, BenTheWikiMan, MichielDMN, Lexw, Bdijkstra, Alex1, RobotQuistnix, JeroenvB, Jan o b, RoboRex, BotEmpoor, MoriBot, Philip Bosma, WillBot, Josdorpjossie, Mion, Whizz, Mexicano, Simeon, Mbch331, Aiko, Madyno, Davin, JAnDbot, TXiKiBoT, Lymantria, Handige Harrie, SterkeBak, AbiBot, Karelflach, Luckas-bot, MrBlueSky, Xqbot, Pompidombot, Smile4ever, Degress, RomaineBot, ButkoBot, Savh, HRoestBot, Solidmetalme, Sjoerddebruin, MerlIwBot, Legobot, Nietanoniem, MatthijsWiki, Jos dekemmper, Neeroppie en Anoniem: 16
- **Computerkraker** *Bron:* https://nl.wikipedia.org/wiki/Computerkraker?oldid=47143184 *Bijdragers:* Romaine, Jeroen, Kattenkruid, Oscar, Danielm~nlwiki, Michiel1972, Meneer, Dlemckert, Robotje, MichielDMN, Rides, Edoderoo, RoboRex, Yvesn, Simeon, Jvhertum, Thijs!bot, Bbe, Tvdm, Magere Hein, Paul B, JAnDbot, YoshiDaSilva, Felix2036, Waldorfer, Skuipers, Timk70, Blueknight, Alecs.bot, FlippyFlink, HerculeBot, MrBlueSky, Hoopje, Mastadc, RomaineBot, MrBlueBot, Woodcutterty, ErikvanB, EmausBot, Lotje, MerlIwBot, AlbinS, Pieterjan E, Sander Van Durme, Vawa, DunjaP, Ilse reeper, Grmbl76, Kekkie123, Atrokov, Addbot, Nicolas.B, SouthparkfanBot, AxelleDejaeghere en Anoniem: 20
- **Computernetwerk** *Bron:* https://nl.wikipedia.org/wiki/Computernetwerk?oldid=47258802 *Bijdragers:* Andre Engels, Walter, Branko~nlwiki, Ellywa, Rob Hooft, Sjoerd, Rene Pijlman, Romaine, Wilinckx, Willemdd, BenTels, Carol Fenijn, Garo~nlwiki, HooftBot, Robbot, Hashar, PrisonerOfPain, Siebrand, Edwtie, Guanabot~nlwiki, MichielDMN, RobotMichiel1972, Lexw, Jan Duimel, Emvee, Ype, MADe, Edoderoo, Robotpjetter, RoboRex, Riki, Vertrokken, KokoBot, Yvesn, Bart l~nlwiki, CiceRobot~nlwiki, Maniago, Kleuske, Zanaq, SanderK, Dogmatica, Necromander, Mexicano, Simeon, Mbch331, SieBot, Ciell, JAnDbot, MoiraMoira, Iooryz, Look Sharp!, WarddrBOT, TXiKiBoT, BotMultichill, RubySS, Loveless, Louperibot, Beany, Vinvlugt, Zorrobot, GrouchoBot, Axhind, PixelBot, Alexbot, Alecs.bot, JurgenNL, MelancholieBot, CarsracBot, LinkFA-Bot, Naudefjbot, Luckas-bot, MystBot, MrBlueSky, Nallimbot, ARTol, Jotterbot, Zxabot, Edoderoobot, Hoopje, ArthurBot, TaBOT-zerem, FoxBot, Xqbot, Rubinbot, Smile4ever, RomaineBot, TobeBot, KamikazeBot, TjBot, WinContro, EmausBot, ZéroBot, WikitanvirBot, Eg-T2g, MerlIwBot, AvocatoBot, Statliner, Supercarwaar, Kippenbot1, Addbot, Tulp8, Ymnes, XXBlackburnXx, StroopwafelBot, Wikiwerner en Anoniem: 44
- **Computervirus** *Bron:* https://nl.wikipedia.org/wiki/Computervirus?oldid=46762042 *Bijdragers:* Andre Engels, Walter, KoenB, Ellywa, Evanherk, Pieter Suurmond, Lvg, Rene Pijlman, Pven, Jan Lapère, SanderSpek, Bemoeial, Roepers, Wilinckx, Jeroen, Willemdd, BenTels, Pieterse16, Ligtvoet, Muijz, Puckly, Advance, Robbot, Wim Hamhuis, Kattenkruid, R0n., Theo, RobotE, Siebrand, RonaldW, MartinD, Edwtie, Taka, Michiel1972, Meneer, Dolmonly, Robotje, Gpk481, MichielDMN, Lexw, Joep Zander, Pieter1, Pjetter, HetKantoor, Tdevries, Bartbilliet, Steinbach, RobotQuistnix, JeroenvB, MADe, Ucucha, Algont, RoboRex, Riki, Karel Anthonissen, Vertrokken, Willemo, Christoffel K, Paul-MD, DéRahier, Tuvic, Jeroenbot, Obarskyr, RonaldB, Aleichem, Zwobot, Dolledre, YurikBot, Eve, Troefkaart, Apdency, FlaBot, Kalsermar, Ronaldvd, Maniago, Kleuske, Eskimbot, HyperQuantum, Sumurai8, DirkHengst, Erwin, Robb, Sebazzz, Xopotl, WiebeVanDerWorp, Bazzo9, Peter200, PatrickKik, Dsjh, Khx023, Simeon, DennisPeeters, Canp, Yugioh, Ugur Basak Bot~nlwiki, EdBever, .Koen, Mbch331, Jvhertum, Ischa1, Btalman, SieBot, Thijs!bot, Hajo, Texke, Erik1980, Vis met 1 oog, LeChuck, Kanman,

JAnDbot, Patrickvandervalk, MoiraMoira, Jonas, CrazyPhunkbot, TARBOT, Leopard, Enormekever, Rembert Andy, Rei-bot, Xyzzy, Look Sharp!, Jan Terpstra, Kemical, Bo W, TXiKiBoT, Lymantria, Handige Harrie, Japiot, VolkovBot, RenéV, AlleborgoBot, YonaBot, Tleilax, SAMnl, Richardkiwi, PipepBot, GrouchoBot, Kthoelen, AlnoktaBOT, PixelBot, MwpnlBot, GameMaker, Alexbot, BOTarate, Erik1100, Toth, Taketa, Alecs.bot, ???? robot, EvilFreD, CarsracBot, Pompidom, Akoopal, Kwiki, JRB, Ralf Roletschek, Naudefjbot, WikiDreamer Bot, MrBlueSky, La Corona, Jotterbot, JZ85, Hoopje, Peterson, ArthurBot, Henny1972P, Mathonius, FoxBot, Xqbot, Wittekind, Rubinbot, Olivier Bommel, Pompidombot, Smile4ever, Mastadc, RomaineBot, Ebrokken, Wiki13, Heureka, RedBot, Mattias.Campe, Dinamik-bot, JurriaanH, ErikvanB, KamikazeBot, Vahnstad, Artemis29, EmausBot, ZéroBot, HRoestBot, AlexW~nlwiki, ChuispastonBot, ChrisN, DirkVE, Ripchip Bot, MerlIwBot, AvicBot, AvocatoBot, Rezabot, Pieterjan E, Tine26, Nielsja123, Grmbl76, WePisto, Zerp~nlwiki, Michiel TM, Dexbot, WOLF LΛMBERT, Makecat-bot, Legobot, Jelle619, Tulp8, Nununu~nlwiki, Leklekleklekklek, Anoniem2206, DottyMcFear13, Wikidevnl, Ronnie PG en Anoniem: 176

- **Computervredebreuk** *Bron:* https://nl.wikipedia.org/wiki/Computervredebreuk?oldid=47141082 *Bijdragers:* Patrick, Oscar, Josv, Bajoro, AlexP, Apdency, BotOx, Sonty567, Klavertwee, Jvhertum, Davin, T.roffel, Framhein, Smile4ever, MrBlueBot, ErikvanB, Kulter20, Seine, Addbot, AxelleDejaeghere en Anoniem: 11
- **Computerworm** *Bron:* https://nl.wikipedia.org/wiki/Computerworm?oldid=46261042 *Bijdragers:* SanderSpek, BenTels, Puckly, HooftBot, Robbot, Michiel1972, Meneer, MichielDMN, RobotQuistnix, JeroenvB, RoboRex, Riki, Palica, Errabee, YurikBot, The Banner, Kleuske, Eskimbot, Zanaq, Xopotl, Gerbot, Mexicano, Mbch331, SieBot, Thijs!bot, JAnDbot, MoiraMoira, CrazyPhunkbot, Look Sharp!, Grashoofd, Handige Harrie, BotMultichill, RenéV, AlleborgoBot, YonaBot, Idioma-bot, Zorrobot, WDVLWD, KB72, Gerrit Van Gelder, BOTarate, BotSottile, JurgenNL, MelancholieBot, Pompidom, JRB, Amirobot, MrBlueSky, Nallimbot, MauritsBot, ArthurBot, Mathonius, Rrdoomernik, Xqbot, Rubinbot, RibotBOT, RomaineBot, D'ohBot, EmausBot, Chielbuseyne, ChuispastonBot, BakkertjeWouter, MrSokPop, Sander Van Durme, Stef.kerkhofs, Stijn.Berghmans, MichèleD, Dexbot, Legobot, Tulp8, Tack.thibaut, RallyBot en Anoniem: 28
- **Contentmanagementsysteem** *Bron:* https://nl.wikipedia.org/wiki/Contentmanagementsysteem?oldid=43840914 *Bijdragers:* Andre Engels, Romaine, Stonehead~nlwiki, Robbot, IMFJ, MartinD, Taka, Michiel1972, Meneer, Omegium, O E P~nlwiki, Sietske, Pe7er, Lexw, Bthv, Ype, Frikimenia, Yorian, Ronn, MigGroningen, Empoor, Tdevries, Gpvos, RobotQuistnix, Bert76, Dryke, Kiwix, Edoderoo, RoboRex, Riki, Eros, Vertrokken, BotEmpoor, Wester2005, Annabel, Yvesn, Christoffel K, Xaviervd, Jeroenbot, Obarskyr, RonaldB, Zwobot, Dolledre, RS Jelle, Ladon~nlwiki, YurikBot, Woe, Eve, JimTer, MarQ, Vdegroot, Maniago, Kleuske, BesselDekker, Eskimbot, Salomo, Murfy, Niels, Zanaq, Sumurai8, Tom-NL, Localhost~nlwiki, Poldiri~nlwiki, Cerberus™, Ajoman, Pveijden, Brinkie, Hardloper, Rob zomerdijk, Mexicano, Simeon, RubenLubbes, RichardTuin, EdBever, Yoda~nlwiki, .Koen, Djubbels, Christophelambrechts, Mintro, Jvhertum, SieBot, Joris, MRiedijk, George4, Erik Baas, Lester112, Yash, PRLamers, Brimz, Erik1980, JSKuipers, Sustructu, Markapeldoorn, Adil Gunaslan, Overbosch, BenBox, Jverveer, Pbaan, Cvevander~nlwiki, Apollo~nlwiki, MoiraMoira, Mediajargo, Schoninr, Elaine Fuente, Woudenberg, Wikit~nlwiki, Soulseeker, Look Sharp!, CentraalDH, Vincentegt, TXiKiBoT, Lymantria, CCI, VolkovBot, Bkruiswijk, Blooming Bizz Management, LVX, Basz, GijsvdL, BotMultichill, Rtbrouwer, Mrkasper, Sarah Franco, Heiner~nlwiki, Lolsimon, Tengu~nlwiki, Sswelm, Wutsje, Zorrobot, Xanland, GrouchoBot, Gientjes, Ron.schoningh, Rvonk, Purbo T, BodhisattvaBot, Roywasse, Hardworks~nlwiki, AdvertBanner.com, Pompidom, FiriBot, Justschim, HerculeBot, Monkey2356, Durk de Vries, Bs137510, Nallimbot, JZ85, ArthurBot, DSisyphBot, Maarten.klanderman, Mathonius, Mikevandijk, Criskruijff, Xqbot, RibotBOT, Smile4ever, Woutb, RomaineBot, Annepleun, MSTONE666, EmausBot, Weverp, HRoestBot, Wikiredactie, RedactieITC, Statiic~nlwiki, Boberwt, WikitanvirBot, ChuispastonBot, Fiammybe, Isadesign, Movses-bot, MerlIwBot, YFdyh-bot, Roland Tjardo, BertAir, Legobot, Espaan, Michielklonhammer, DelaMeuse, NielsAC en Anoniem: 191
- **Cookie (internet)** *Bron:* https://nl.wikipedia.org/wiki/Cookie_(internet)?oldid=47902979 *Bijdragers:* Andre Engels, Patrick, Ellywa, Pven, Romaine, BenTels, Streppel, Advance, Robbot, Kattenkruid, Oscar, Taka, Michiel1972, Robotje, MichielDMN, Snaily, RobotQuistnix, Justhg, Tomgreep, Gpvosbot, RoboRex, Riki, Servien, Knuga, Eve, Maniago, RobotTbc, Niels, Bw, Emmelie, Warddr, Mexicano, Mbch331, Jvhertum, BerendBotje, SieBot, Thijs!bot, Adam P, JAnDbot, Johan N, MoiraMoira, Ajakkes, CrazyPhunkbot, Rei-bot, Albeda van Blommesteynweg, Ken123, Look Sharp!, Skywalkr, DodekBot, AnnabelsBot, TXiKiBoT, VolkovBot, Zwitser123, AlleborgoBot, Freaky Fries, Wutsje, Vinvlugt, Zorrobot, Alexbot, BOTarate, Purbo T, Toth, EvilFreD, MelancholieBot, CarsracBot, LinkFA-Bot, MrBlueSky, Nallimbot, ArthurBot, FoxBot, Xqbot, Wittekind, RibotBOT, Schilders, Pompidombot, Spraakverwarring, Smile4ever, Mastadc, RomaineBot, Wiki13, ErikvanB, EmausBot, Savh, De Jaren, JeroenDeConinck, Oudehampsink, Dominique.devriese, Gammo123, Michielderoo, Lotje, Dinosaur918, Ripchip Bot, MerlIwBot, Malinka1, AlbinS, Grmbl76, Und, Dexbot, Natuur12, Smoetsj, Legobot, Lloydje33, KehppKukkieBot, Ronnie PG en Anoniem: 65
- **Cyberoorlog** *Bron:* https://nl.wikipedia.org/wiki/Cyberoorlog?oldid=47728211 *Bijdragers:* Romaine, Robbot, MichielDMN, Chobot, RonaldB, Alankomaat, Kleuske, Hansmuller, Wikiklaas, Jvhertum, Benedict Wydooghe, Rikipedia, CommonsDelinker, Japiot, Paul2, Jarune, Capaccio, Luckas-bot, MrBlueSky, Japiobot, Emelha, Pompidombot, Gooper20, Smile4ever, RomaineBot, RedBot, ErikvanB, Reinaart-Bot, TjBot, Bermond, Rezabot, Pieterjan E, Nick Dbvr, Markro, Borvo, Addbot, Delphine Carlier, Jonas7735, Ann-Sophie B, 12345dan-NL, Iwein Janssens, Tack.thibaut, BlauweVis, Kaj Sustronck, Archerskull, Stiem22, Wicoby, Wikiwerner, Perudotes, RallyBot, PMat26 en Anoniem: 7
- **Cyberpesten** *Bron:* https://nl.wikipedia.org/wiki/Cyberpesten?oldid=47776253 *Bijdragers:* Romaine, Advance, Kattenkruid, MichielDMN, Lexw, Rides, RobotQuistnix, MADe, Edoderoo, Just a member, Chobot, LHO, RonaldB, Dolledre, Eve, Maniago, Kleuske, Ninane, Zanaq, Melsaran, Adnergje, Peti me, Foxie001, Roelzzz, Scoub, Halandinh, Mexicano, Canp, EdBever, .Koen, Mbch331, Lionel~nlwiki, Joris, Rozemarijn vL, Tvdm, Madyno, Maiella, Magere Hein, Ciell, Paul B, MoiraMoira, CommonsDelinker, Iooryz, Ken123, YoshiDaSilva, Look Sharp!, Chaemera, Felix2036, Primaxyes, Dunken~nlwiki, Narayan, Lymantria, Grashoofd, Jansch, RenéV, 3wisemen, Sander1453, Bouwmaar, Aclypson, GrouchoBot, CategorieBot, Kthoelen, DustSpinner, JetzzDG, Vliegenmepper, Beachcomber, Forrestjunky, Alexbot, LikeKarma, JurgenNL, Ivo Goedhart, JanB46, MastiBot, Luckas-bot, MrBlueSky, ArthurBot, Mathonius, De Wikischim, Xqbot, Smile4ever, RomaineBot, Trijnstel, Babylonboy, Wiki13, Stdx, RedBot, TBloemink, Woodcutterty, JurriaanH, ErikvanB, TjBot, EmausBot, ZéroBot, Elco12, Sa.devries, Kulter20, Chielbuseyne, WikitanvirBot, Lotje, ChrisN, AvocatoBot, RobkeDel, Marie.Vroman, PVG-44, Vawa, Stef.kerkhofs, Daffe, Stijn.Berghmans, MichèleD, Grmbl76, Makecat-bot, YFdyh-bot, Maartenschrijft, Nietanoniem, WillemBK, Addbot, Joost51, Tulp8, Niels-Bru, GuppieB52, KendryDV, HannaBMV, Archerskull, Joachim Sercu, SimonD.M, Junnes113, Best Towel, Shoarma2005 en Anoniem: 105
- **Cyberspace** *Bron:* https://nl.wikipedia.org/wiki/Cyberspace?oldid=47669766 *Bijdragers:* Hannes Karnoefel, Jeroen, MichielDMN, Riki, Maniago, SieBot, Thijs!bot, Hajo, Escarbot, TOM, Obitwan, DodekBot, VolkovBot, BotMultichill, Loveless, Gerakibot, Zorrobot, GrouchoBot, BodhisattvaBot, Toth, Luckas-bot, Ptbotgourou, DumZiBoT, BenzolBot, MrBlueBot, KamikazeBot, DixonDBot, JackieBot, Mentibot, WikitanvirBot, ChuispastonBot, MerlIwBot, AvocatoBot, DunjaP, Addbot, StroopwafelBot, BlauweVis, Niels.Veryepe en Anoniem: 4

- **Dialer** *Bron:* https://nl.wikipedia.org/wiki/Dialer?oldid=39398579 *Bijdragers:* Pjetter, YurikBot, Troefkaart, ArjenW, Jandeboer, SieBot, Thijs!bot, Moonieb, Tvdm, BetBot~nlwiki, BotMultichill, Loveless, GrouchoBot, RudolphousBot, ErikvanB, EmausBot, Addbot en Anoniem: 1

- **Distributed denial-of-service** *Bron:* https://nl.wikipedia.org/wiki/Distributed_denial-of-service?oldid=47785136 *Bijdragers:* Andre Engels, Arent, Carol Fenijn, Robbot, Bontenbal, Theo, RobotE, Meneer, MichielDMN, Rides, JePe, Tdevries, Snaily, RobotQuistnix, Henna, RoboRex, Riki, RonaldB, Zwobot, YurikBot, FlaBot, Maniago, Kleuske, Eskimbot, Sumurai8, Mion, JrPol, Harry S., Khx023, Simeon, Jvhertum, SieBot, Thijs!bot, Joris, George4, Benedict Wydooghe, Escarbot, Maiella, JAnDbot, MoiraMoira, CommonsDelinker, Rei-bot, Look Sharp!, DodekBot, DorganBot, Rudolphous, TXiKiBoT, Lymantria, Grashoofd, Japiot, VolkovBot, BotMultichill, Velorian, Halimk~nlwiki, Sander1453, YonaBot, VVVBot, Mar(c), Davv69, GrouchoBot, SvenDK, DragonBot, Blueknight, SilvonenBot, JurgenNL, CarsracBot, MastiBot, Muro Bot, Luckas-bot, MrBlueSky, Ptbotgourou, Spock~nlwiki, AStarBot, ChenzwBot, ArthurBot, FoxBot, Xqbot, Aqua21, Smile4ever, Erik Wannee, Voortman, Wiki13, Heureka, RedBot, TobeBot, Dinamik-bot, ErikvanB, ReinaartBot, EmausBot, WikitanvirBot, Lotje, Manubot, MerlIwBot, Vagobot, Liverpolle, Kwuekn, Nick Dbvr, Dreadtania, Addbot, Johnd12, Jonas7735, Thalita Temmerman, T123E, Dalukasio, Jepz11 en Anoniem: 49

- **Domain Name System** *Bron:* https://nl.wikipedia.org/wiki/Domain_Name_System?oldid=46549297 *Bijdragers:* Branko~nlwiki, SoTTo, Ellywa, Rob Hooft, Sjoerd, Romaine, BenTels, Carol Fenijn, Serassot, Panthouse, HooftBot, Advance, Robbot, GerardM, Siebrand, Michiel1972, GWirken, Robotje, Guanabot~nlwiki, Ronn, RobotQuistnix, LimoWreck, Gpvosbot, Robotpjetter, Algont, RoboRex, Riki, Obarskyr, Dz, RonaldB, Aleichem, Zwobot, Diogenes, YurikBot, LeonardoRob0t, Maniago, Kleuske, Eskimbot, Josq, Chlewbot, Zaheer12a, Vincentsc, Mexicano, Khx023, Simeon, Kameraad Pjotr, .Koen, SieBot, Thijs!bot, Tukka, Rp, Peter142, Erik1980, Davin, ErikRomijn, Hafkensite, Migiloviz, Soulbot, Waninge, MoiraMoira, BotteHarry, YoshiDaSilva, Look Sharp!, DodekBot, DorganBot, TXiKiBoT, Handige Harrie, VolkovBot, Synthebot, Idioma-bot, Loveless, Freaky Fries, Mdavids, BjornR, Zabot, GrouchoBot, Tonkie, Alecs.bot, Kuba, Huisman88, MelancholieBot, MastiBot, Wikirace, Nafets~nlwiki, Luckas-bot, Ptbotgourou, ChenzwBot, Hoopje, MauritsBot, Peterson, Coradriaan, Enschedem, FoxBot, Rubinbot, Krinkle, LucienBOT, Trewal, RomaineBot, ButkoBot, Innv, RedBot, TBloemink, ErikvanB, EmausBot, Tjibbe I, Kulter20, WikitanvirBot, Dilic, ChuispastonBot, Lotje, Movses-bot, Maash, Bodhost, Leifnsn, MerlIwBot, Minsbot, Kippenbot1, Legobot, Thomas Lammens, Oskardebot en Anoniem: 54

- **Domeinnaam** *Bron:* https://nl.wikipedia.org/wiki/Domeinnaam?oldid=46925547 *Bijdragers:* Patrick, Rob Hooft, Romaine, Robin~nlwiki, Wilinckx, BenTels, Pieterse16, Streppel, Carol Fenijn, Muijz, HooftBot, Advance, Robbot, Johan Lont, Buttonfreak, Webkid~nlwiki, Taka, Michiel1972, Bean 19, A3, GWirken, Robotje, MichielDMN, Tbeernot, Ilse(a), JimmyShelter, RobotQuistnix, LimoWreck, Rex, AlbertWaninge, Galwaygirl, Joost, MADe, Gpvosbot, RoboRex, Riki, Lander, Willemo, Wixnl, CyeZ, Tuvic, Obarskyr, Chobot, Naz~nlwiki, Corriebert, Aleichem, YurikBot, Test-tools~nlwiki, Cyberdots, Robert einar, Kleuske, Ninane, Eskimbot, RobotTbc, Lifeforms, SanderK, Sonty567, Legbatterij-Argonautica, Nieuw, JFD~nlwiki, Fontes, Mexicano, Simeon, EdBever, Wikiklaas, Mbch331, SieBot, Thijs!bot, Edwinb, Escarbot, Madyno, BOT-Superzerocool, ErikRomijn, LeChuck, JAnDbot, WeiaR, Richardb2, Wimmel, Look Sharp!, Chaemera, TXiKiBoT, Japiot, VolkovBot, GijsvdL, Silver Spoon, Zwitser123, Robert schekelmek, DavidD, Idioma-bot, Loveless, Gerakibot, Freaky Fries, Dekaptein, Louperibot, Avbentem, Mdavids, Pieterhendriks, Wutsje, BjornR, Zorrobot, GrouchoBot, DragonBot, Darkicebot, MelancholieBot, CarsracBot, NjardarBot, SusBot, Dqfn13, Amirobot, MrBlueSky, Nallimbot, Japiobot, Coradriaan, De Wikischim, FoxBot, Xqbot, MerlLinkBot, Smile4ever, RedBot, Dinamik-bot, ErikvanB, KamikazeBot, DixonDBot, Crmtd, Richard112, Delay, MerlIwBot, Jelmr, Jhoop, TBM, ZeaForUs, W.G.J., Internetpedianl, Youbuntu, Legobot, Thomas Lammens, Kathleenbuffels, TatotobiasT en Anoniem: 49

- **Dynamic Host Configuration Protocol** *Bron:* https://nl.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol?oldid=47741244 *Bijdragers:* Andre Engels, Erik Zachte, Rob Hooft, Fruggo, Bemoeial, Wilinckx, Guaka, BenTels, Rene~nlwiki, Panthouse, HooftBot, Robbot, Hondeman, RobotE, Bob.v.R, Michiel1972, Quistnix, Caseman, O E P~nlwiki, RobotMichiel1972, Koos Jol, Emvee, Fuss, RobotQuistnix, RoboRex, Riki, Dartelaar, RonaldB, YurikBot, LeonardoRob0t, FlaBot, Kleuske, Eskimbot, Fr33ke, RobotTbc, Zanaq, .marc., Bbredewold, Robb, Emmelie, Mexicano, Simeon, DennisPeeters, Bergen2, Woudloper, SieBot, Morax, Thijs!bot, Joris, Escarbot, Tvdm, JAnDbot, .anacondabot, Pieterd, Nbobe, MoiraMoira, Rei-bot, Look Sharp!, Waldorfer, Rudolphous, TXiKiBoT, ARVER, AlleborgoBot, DaBot~nlwiki, Louperibot, Zorrobot, GrouchoBot, DustSpinner, AlnoktaBOT, Gamut, Alexbot, SilvonenBot, Luckas-bot, Jotterbot, MartinLommers, TaBOT-zerem, Basvbbot, Everlind, FoxBot, Xqbot, RomaineBot, BenzolBot, Dustwellow, ButkoBot, KamikazeBot, Martoost, EmausBot, Whaledad, Bernhardegen, Dinux, Erik009, WikitanvirBot, ChuispastonBot, Ed Lane, Legobot, JP001, GuppieB52, KehppKukkieBot, Wikidatist en Anoniem: 45

- **E-mail** *Bron:* https://nl.wikipedia.org/wiki/E-mail?oldid=47770918 *Bijdragers:* Patrick, KoenB, Ellywa, Rob Hooft, Rene Pijlman, Pven, Inca, Mtcv, Jan Lapère, Xastor, Romaine, SanderSpek, Cicero~nlwiki, BenTels, Carol Fenijn, Garo~nlwiki, Puckly, Ben~nlwiki, HooftBot, Robbot, David Eerdmans, RobotE, Siebrand, NeoGeo-x, Bernard van der Wees, Michiel1972, Ano niem, Jupiler, BenTheWikiMan, Gpk481, MichielDMN, RobotMichiel1972, Mdd, RJB, Martinus, HetKantoor, Sixtus, Dolfy, JimmyShelter, RobotQuistnix, Rex, Gwyrrdin, Justhg, JeroenvB, IIVQ, Edoderoo, Algont, RoboRex, Riki, Servien, KokoBot, Paul-MD, Tuvic, Jeroenbot, Chobot, Aleichem, Zwobot, Errabee, Jos-uit-boston, YurikBot, Eve, Wasily, Kleuske, Eskimbot, Fr33ke, BranMoviC, SanderK, Pieter Verrips, Melsaran, BlackCat, Chlewbot, Adnergje, Eto, Staarink, Xfinx, Whizz, Mexicano, Simeon, Sgeraedts, BlackNight, .Koen, Zointer, BerendBotje, SieBot, Thijs!bot, Erwin85Bot, Erik Baas, Ropo, RoboServien, Casperinfo, Erik1980, Maiella, BOT-Superzerocool, Matthieu Mimpen, Paul B, JAnDbot, A Duck, Bor Komorovski, Rembert Andy, Ken123, YoshiDaSilva, Calvinturbo, Frankkie12345, PAvdK, DodekBot, James02, TXiKiBoT, Lymantria, Handige Harrie, Iek, Aibot, VolkovBot, AndreeHollander, Le Fou, BotMultichill, ErikWarmelink, Zwitser123, AlleborgoBot, Koos Dijkstra, Rietvogel, Gerakibot, Louperibot, Ken123BOT, PipepBot, BasvanPelt, Zabot, GrouchoBot, Kthoelen, DragonBot, AlnoktaBOT, BOTarate, Blueknight, SilvonenBot, Toth, EjsBot, FlippyFlink, CarsracBot, Pompidom, Kwiki, Kenobot, Luckas-bot, MrBlueSky, BotMultichillT, Jotterbot, JanDeFietser, Obersachsebot, Xqbot, SassoBot, Krinkle, Smile4ever, RomaineBot, Wiki13, RedBot, TobeBot, NormanB, JurriaanH, ErikvanB, WinContro, MexicanoBot, EmausBot, Savh, HRoestBot, ScalaDiSeta, ChuispastonBot, Rolfkleef, MerlIwBot, Scholier, Ilse reeper, Phah7x, Legobot, Steven-wostijn en Anoniem: 74

- **Emoticon** *Bron:* https://nl.wikipedia.org/wiki/Emoticon?oldid=47762029 *Bijdragers:* Andre Engels, Greco, Snoop, Advance, Robbot, Hashar, RobotE, Michiel1972, EJR, Bean 19, Kagaherk, Guusvonscheven, MichielDMN, Lexw, Joep Zander, B kimmel, Pieter1, Pjetter, JePe, Empoor, Steinbach, RobotQuistnix, LimoWreck, Ed de Jonge, Jelte, RoboRex, Richardw, Servien, MoriBot, Annabel, Christoffel K, Paul-MD, Tuvic, Chobot, Aleichem, Witger, Dolledre, YurikBot, Wasily, Maniago, Kleuske, BesselDekker, Tom 1992, Gerbennn, Joël, Zanaq, Verrekijker, Melsaran, BlackCat, W4rr10r, Al, Scoub, Simeon, Kameraad Pjotr, EdBever, Randyyy, SieBot, Thijs!bot, Joris, Erwin85Bot, Erik Baas, Thor NL, Sint Aldegonde, Balko Kabo, JAnDbot, Toreddo, A Duck, MoiraMoira, Gabadubo~nlwiki, Rembert Andy, Ajox, Ken123, Florrat, Look Sharp!, VanBuren, Knijntje143, Kyuuseishu, TXiKiBoT, GijsvdL, Mork, Synthebot, Loveless, Gerakibot, Bant diet, GLOatWP, Davv69, Richardkiwi, Vinvlugt, Zorrobot, Helanhuaren, Dh3201, Tekstman, BOTarate, SterkeBak, SJdeBest, Capaccio,

SilvonenBot, JurgenNL, PeHa, CarsracBot, Pompidom, Laloeka, Luckas-bot, MrBlueSky, Goudsbloem, Jotterbot, Xqbot, Rubinbot, RibotBOT, Spraakverwarring, Smile4ever, RomaineBot, Wiki13, JurriaanH, ErikvanB, TjBot, EmausBot, Kulter20, Olnnu, TuurDS, MerlIwBot, Scholier, AvocatoBot, Dnamic, Danuta, WOLF LΛMBERT, Southparkfan, Makecat-bot, Addbot, Tulp8, JP001, Iesvoagel, Triiiiing, MatthijsWiki, Tony Bloem, Justine Raadt, Thomas Lammens, Iemandyolo, Xxmarijnw en Anoniem: 133

- **Encryptie** *Bron:* https://nl.wikipedia.org/wiki/Encryptie?oldid=46936203 *Bijdragers:* Andre Engels, Patrick, TeunSpaans, Ellywa, Evanherk, Rob Hooft, Ezel, Falcongj, Carol Fenijn, Jan Arkesteijn, Panthouse, HooftBot, Advance, Robbot, Rick van Rein, Oscar, Bob.v.R, Joachim, Drdefcom, Gus (hernoemd), RobotQuistnix, RoboRex, Dolledre, YurikBot, Aart, Ninane, Warddr, Mexicano, Khx023, Simeon, Thijs!bot, Erik Baas, JAnDbot, HandigeHarry, MoiraMoira, Koentje115, Philia~nlwiki, Look Sharp!, Handige Harrie, Roestje, Den Hieperboree, Wutsje, SilvonenBot, Pompidom, Marrakech, RudolphousBot, RibotBOT, Emelha, RomaineBot, Wiki13, Havanafreestone, JanKanis, Legobot, BonstraGeert en Anoniem: 22
- **Faker** *Bron:* https://nl.wikipedia.org/wiki/Faker?oldid=47077736 *Bijdragers:* Patrick, Advance, Mexicano, Mbch331, Erik1980, Maiella, FakirNL, Bor Komorovski, MoiraMoira, Handige Harrie, GrouchoBot, Kwik, Kwiki, DéRaBot, Pompidombot, Smile4ever, RomaineBot, Heureka, ErikvanB, Dennyboy1997, MexicanoBot, Nietanoniem, RosaliaA, Stef Bryssinck, R0457167, KayleeClaeys, Tasia Pleune, Archerskull, Joachim Sercu, Berdieke, Thomas Lammens en Anoniem: 4
- **File Transfer Protocol** *Bron:* https://nl.wikipedia.org/wiki/File_Transfer_Protocol?oldid=44633690 *Bijdragers:* Andre Engels, Patrick, Ellywa, Rob Hooft, Snoop, Youandme, Romaine, Fruggo, Wilinckx, BenTels, Garo~nlwiki, HooftBot, Robbot, Chris, DaProx, Fleprick, Michiel1972, Alicey, Yorian, Ronn, MigGroningen, Fuss, RobotQuistnix, LimoWreck, Rex, Galwaygirl, Marcieking, RoboRex, Riki, Vertrokken, Knuga, Christoffel K, Tuvic, Obarskyr, Chobot, Ron.de.groot, YurikBot, FlaBot, Eskimbot, Loek037, Gerbot, Q300r bc2, Whizz, Mexicano, Simeon, .Koen, BerendBotje, SieBot, Thijs!bot, Aiko, Escarbot, Wolu, JAnDbot, Johan N, MoiraMoira, BotteHarry, Osmium~nlwiki, VanBuren, DodekBot, TXiKiBoT, Aibot, VolkovBot, BotMultichill, AlleborgoBot, Synthebot, Apocatequil, Koektrommel, SAMnl, Caber, BjornR, GrouchoBot, Bb22, AlnoktaBOT, SterkeBak, SilvonenBot, CarsracBot, EivindBot, Luckas-bot, MrBlueSky, BlackBot (hernoemd), Mathonius, Xqbot, SassoBot, Rubinbot, RibotBOT, Smile4ever, RomaineBot, BenzolBot, TobeBot, Dinamik-bot, EmausBot, HRoestBot, Dinux, ChuispastonBot, MerlIwBot, Kippenbot1, Makecat-bot, Addbot, Wikiwerner en Anoniem: 41
- **Firewall** *Bron:* https://nl.wikipedia.org/wiki/Firewall?oldid=47588041 *Bijdragers:* Ellywa, Rob Hooft, Nick~nlwiki, Wilinckx, Jeroen, BenTels, Carol Fenijn, Advance, Robbot, RobotE, Chris, Arnie, Taka, DaProx, Mwpnl, Meneer, O E P~nlwiki, Gpk481, FoekeNoppert, MichielDMN, Lexw, Johannes49, Emvee, Tbc, Rixnet, Dolfy, KlaasZ4usV, RobotQuistnix, Joost, Algont, RoboRex, Hverbiesen, Annabel, Tuvic, Obarskyr, Tubantia, Chobot, RonaldB, YurikBot, Daka, JörgenMoorlag, Kleuske, Eskimbot, SanderK, Melsaran, Chlewbot, Mexicano, Simeon, Ugur Basak Bot~nlwiki, SieBot, Thijs!bot, Joris, Edwinb, Tukka, Escarbot, Erik1980, Magere Hein, Davin, JAnDbot, Hstuivenberg, Huzzlet the bot, Look Sharp!, Chaemera, Rubenkon, Rudolphous, TXiKiBoT, Lymantria, VolkovBot, GijsvdL, BotMultichill, Elconomeno, AlleborgoBot, Sander1453, YonaBot, Idioma-bot, Loveless, Zabot, GrouchoBot, DragonBot, AlnoktaBOT, Bimpens, BOTarate, Fantom008, Alecs.bot, Justin.ere, EvilFreD, Pompidom, Luckas-bot, Amirobot, MrBlueSky, Halvar, Flurps, ArthurBot, Obersachsebot, Xqbot, RibotBOT, RomaineBot, Heureka, S.collet, TobeBot, Ver-bot, ErikvanB, MexicanoBot, EmausBot, Savh, ZéroBot, HRoestBot, Ruudje76, Gammo123, WikitanvirBot, Ebrambot, Sjoerddebruin, MerlIwBot, Pieterjan E, Sander Van Durme, Tompie63, Dexbot, TheDragonhunter, Addbot, MatthijsWiki, StroopwafelBot, Thomas Lammens en Anoniem: 70
- **Gebruikersaccountbeheer** *Bron:* https://nl.wikipedia.org/wiki/Gebruikersaccountbeheer?oldid=47111589 *Bijdragers:* JoJan, Alex1, Simeon, SPQRobin, SieBot, Basvb, Johan N, Calvinturbo, TXiKiBoT, GrouchoBot, DragonBot, Toth, MelancholieBot, Smile4ever, RomaineBot, RedBot, ErikvanB, KamikazeBot, Beezlebub~nlwiki, WinContro, EmausBot, Addbot, Hatoka en Anoniem: 5
- **Geldezel** *Bron:* https://nl.wikipedia.org/wiki/Geldezel?oldid=47500296 *Bijdragers:* Kattenkruid, Jvhertum, Bor Komorovski, Erwin85TBot, Dqfn13, MrBlueSky, Olivier67, RomaineBot, ErikvanB, Eg-T2g, Dutchbesttyper, Malinka1, JP001, Toyo Mojito en Anoniem: 2
- **Grooming (pedofilie)** *Bron:* https://nl.wikipedia.org/wiki/Grooming_(pedofilie)?oldid=47532216 *Bijdragers:* Patrick, MichielDMN, Bor Komorovski, Dqfn13, Woodcutterty, Queeste, BrackezMassimo, PMat26 en Jonas Vandeplassche
- **Hacker** *Bron:* https://nl.wikipedia.org/wiki/Hacker?oldid=47649712 *Bijdragers:* Andre Engels, Patrick, Branko~nlwiki, Rob Hooft, SanderSpek, Wilinckx, BenTels, HooftBot, Robbot, Dersonlwd, Kattenkruid, Chris, Olivier~nlwiki, Michiel1972, Meneer, Alicey, Dlemckert, A3, GWirken, MichielDMN, Pjetter, RobotQuistnix, Qwertyus, Wikix-oud, Edoderoo, RoboRex, Vertrokken, Yvesn, RonaldB, Maniago, Kleuske, Ninane, RobotTbc, SanderK, Wybe, Sonty567, Schildpadje, Mexicano, Simeon, Simon-sake, Mbch331, Jvhertum, SieBot, Thijs!bot, Joris, Hajo, Benedict Wydooghe, Kfvd, Paul B, MSBOT, M0, JAnDbot, Machaerus, MoiraMoira, TARBOT, Ken123, Look Sharp!, Wouterjanss, DodekBot, AnnabelsBot, WarddrBOT, TXiKiBoT, VolkovBot, OxyDrokz, GijsvdL, BotMultichill, ARVER, Zwitser123, Lolsimon, Loveless, Gerakibot, Louperibot, Beany, Jarune, Zorrobot, GrouchoBot, Vliegenmepper, Nelux, Forrestjunky, Blueknight, SilvonenBot, FlippyFlink, Kwiki, MrBlueSky, Galoubet, Marnixked, Pipolol, Hoopje, BKannen, Mathonius, Saschaporsche, Rubinbot, RibotBOT, Bazkie botsauto, Wiki13, MrBlueBot, TBloemink, ErikvanB, WinContro, Woohoo, EmausBot, Kulter20, MerlIwBot, Terzo, KevStyle, Waflix, Malinka1, AlbinS, Pieterjan E, RobkeDel, Tompie63, Stijn.Berghmans, Grmbl76, SKooij, Legobot, Desmet dave, Delphine Carlier, Tulp8, Ilie Cremers, Nicolas.B, SkyOfTheHell, HMMuller, Bowero, Vidjgz, DaanDeleye, Kaj Sustronck, KayleeClaeys, Berdieke, Carol Fenijn (merge), Niels.Veryepe, Wicoby, Grasmat, Oxygene7-13 en Anoniem: 96
- **Harde schijf** *Bron:* https://nl.wikipedia.org/wiki/Harde_schijf?oldid=47713006 *Bijdragers:* Andre Engels, Ellywa, Evanherk, Rob Hooft, Pven, SanderSpek, Bemoeial, Wilinckx, Jeroen, BenTels, Jeanpaulmars, Carol Fenijn, Ligtvoet, Muijz, HooftBot, Advance, Robbot, Henricus, Bartux, Oscar, Kilo~nlwiki, Andries, RobotE, Johan Lont, Danielm~nlwiki, Rasbak, MartinD, Edwtie, Henk van Haandel, Hjvannes, Michiel1972, Tdw~nlwiki, Omegium, A3, Caseman, Nijdam, Robotje, BenTheWikiMan, MichielDMN, Stropdas, Lexw, Ype, Pieter1, Ziggyziggyziggy, JePe, MigGroningen, Lieven Smits, Klever, RobotQuistnix, Ed de Jonge, Marcieking, Joost, Dryke, Gpvosbot, RoboRex, Kamu, Riki, Magalhães, Vertrokken, Husky, BotEmpoor, Wixnl, Titusvh, Palica, MoriBot, Yvesn, Obarskyr, Xenan, Zwobot, Dolledre, YurikBot, Eve, BotOx, Maniago, Kleuske, BesselDekker, Arend041, Ninane, Eskimbot, KittenKlub~nlwiki, Snowflake~nlwiki, SanderK, .marc., Thomas-, Erwin, Chingon, Roelzzz, Bkoop, JrPol, Whizz, Simeon, Kameraad Pjotr, Imodium, .Koen, SieBot, Morax, Thijs!bot, AdnergjeBot, Erik Baas, Van der Hoorn, JurgenG, Asantoe, Caenwyr, Escarbot, Ciell, Davin, JAnDbot, Freestyle, A Duck, BliepToet, JeroenvanVeen, MoiraMoira, Fireblade 92, YoshiDaSilva, Look Sharp!, OekelWm, Wouterjanss, VanBuren, TXiKiBoT, Lymantria, Handige Harrie, Japiot, VolkovBot, RenéV, AlleborgoBot, Synthebot, Sander1453, YonaBot, Mar(c), Loveless, Emiel.molenaar, Freaky Fries, Nsolisa, GrouchoBot, Kthoelen, Axhind, DragonBot, Tjako, Berrre, Alexbot, RonnieV, BodhisattvaBot, Hobbema, MelancholieBot, Pompidom, NjardarBot, PauloCalipari, Luckas-bot, CarlaHoek, MrBlueSky, Ptbotgourou, Nallimbot, Japiobot, Jotterbot, JZ85, Yonidebot, Hoopje, Peterson, Janboonen, Daniël Slenders, Siem Weel, CyrielK, FredTC, FoxBot, Xqbot, RibotBOT, Moretus69, Pompidombot, RomaineBot, Trijnstel, Wiki13, RedBot, ErikvanB, Verdel, Jorn.stifter, KamikazeBot, Queeste, Bigbang990, MexicanoBot, EmausBot, JackieBot, Arjen42, Kulter20, BanaanExpert, Maslol, ChuispastonBot, Sjoerddebruin, CocuBot, Movses-bot, Vagobot, AlbinS, ElfjeTwaalfje, Heikens, Dexbot, Legobot, Hilliebill, Kukkie, Wikiwerner en Anoniem: 179

- **Hashfunctie** *Bron:* https://nl.wikipedia.org/wiki/Hashfunctie?oldid=47411359 *Bijdragers:* KoenB, Meneer, RobotQuistnix, LimoWreck, RoboRex, Riki, Chobot, YurikBot, Apdency, Maniago, .marc., Chlewbot, Simeon, Mbch331, SieBot, Magere Hein, JAnDbot, TXiKiBoT, Aibot, VolkovBot, Loveless, Alexbot, MelancholieBot, FlippyFlink, CarsracBot, LaaknorBot, Luckas-bot, MrBlueSky, Nallimbot, Marrakech, ArthurBot, Xqbot, Bart Demeyere, RibotBOT, RomaineBot, Dinamik-bot, JurriaanH, ErikvanB, Bartledoo, EmausBot, MerlIwBot, MadamIamadam, JanKanis, Addbot en Anoniem: 6
- **Honeypot (informatica)** *Bron:* https://nl.wikipedia.org/wiki/Honeypot_(informatica)?oldid=37966938 *Bijdragers:* RobotE, Emiel, BrightSide, Jvhertum, SieBot, Thijs!bot, VanBuren, Grashoofd, Quarantainenet, Alexbot, LaaknorBot, Luckas-bot, Amirobot, MrBlueSky, Smile4ever, RedBot, EmausBot, AvatarTeam, Simon tally, Brdebu, Addbot en Nicolas.B
- **Hyperlink** *Bron:* https://nl.wikipedia.org/wiki/Hyperlink?oldid=47601188 *Bijdragers:* Andre Engels, Romaine, Bemoeial, BenTels, Carol Fenijn, Serassot, HooftBot, Robbot, MartinD, Michiel1972, Svdmolen, A3, DennisExtr, LimoWreck, Rex, IIVQ, Abnormaal, RoboRex, Door de wol geverfd, Vertrokken, Willemo, RonaldB, Vdegroot, Maniago, Kleuske, Zanaq, Melsaran, Kawouter, Eagle00789, Mexicano, Simeon, DennisPeeters, .Koen, Jvhertum, SieBot, Thijs!bot, Rp, Basss, Magere Hein, Vis met 1 oog, JAnDbot, MoiraMoira, AnnabelsBot, VolkovBot, RenéV, F-j123, Muntje35, Velocitas, Naudefj, Japiobot, ArthurBot, FoxBot, Xqbot, Maasje, Wiki13, ErikvanB, KamikazeBot, TjBot, Lexcy11, EmausBot, HRoestBot, ChrisN, MerlIwBot, Bernard Ladenthin, JYBot, Addbot, Hvanl en Anoniem: 25
- **Identiteitsfraude** *Bron:* https://nl.wikipedia.org/wiki/Identiteitsfraude?oldid=46308948 *Bijdragers:* Advance, Robbot, Meneer, MichielDMN, RobotMichiel1972, RobotQuistnix, IIVQ, Edoderoo, Algont, Vertrokken, DéRahier, Apdency, Jvhertum, SieBot, Thijs!bot, JurgenG, Rozemarijn vL, Bbe, Maiella, Bor Komorovski, Rei-bot, AnnabelsBot, Skuipers, Grashoofd, GijsvdL, Wutsje, Richardkiwi, Zorrobot, Peter Tenbult, Stuffie, DragonBot, AGL, Ilse Winter, Mpieterse, Taketa, Stijnvanerp, Luckas-bot, Amirobot, MrBlueSky, Ptbotgourou, Halvar, MauritsBot, DéRaBot, DSisyphBot, Obersachsebot, Saschaporsche, Pompidombot, RomaineBot, MondalorBot, Woodcutterty, Mcapdevila, ErikvanB, EmausBot, ZéroBot, Ripchip Bot, Aad aad, Stevina58, Tine26, Kwuekn, Ilse reeper, Minsbot, Nabetaro, Addbot en Anoniem: 15
- **Internet der dingen** *Bron:* https://nl.wikipedia.org/wiki/Internet_der_dingen?oldid=47803468 *Bijdragers:* Bob.v.R, MichielDMN, The Banner, Kameraad Pjotr, Wikiklaas, Sambo, Basvb, Rens ten Hagen, Grieg, Sander1453, Nederduivel, Taketa, Willieworte1007, De Wikischim, RomaineBot, Whaledad, Gewild, KafiRobot, Kukkie, Amity Oak, Wikiwerner, DutchRonin, RonBo, PMat26 en Anoniem: 4
- **Internet protocol spoofing** *Bron:* https://nl.wikipedia.org/wiki/Internet_protocol_spoofing?oldid=47213860 *Bijdragers:* Jeroen, BenTels, Michiel1972, Meneer, O E P~nlwiki, Lexw, RobotQuistnix, Galwaygirl, RoboRex, Riki, LeonardoRob0t, FlaBot, Thijs!bot, AceT, Maiella, YoshiDaSilva, Alexbot, CarsracBot, MrBlueSky, ArthurBot, RudolphousBot, DumZiBoT, Marcel van b, MrBlueBot, EmausBot, WikitanvirBot, Lotje, Joopwikibot, Ward Moerman, Kwuekn, Makecat-bot, Addbot, Wikiwerner en Anoniem: 10
- **Internetbankieren** *Bron:* https://nl.wikipedia.org/wiki/Internetbankieren?oldid=47429906 *Bijdragers:* Patrick, Pven, Puckly, Advance, Robbot, Johan Lont, Siebrand, Michiel1972, Svdmolen, Bee, Dolfy, RobotQuistnix, MADe, Edoderoo, RoboRex, Riki, YurikBot, Maniago, Waldo79, Eto, Wenceslas, Uncle Istvan, SieBot, Erwin85Bot, RoboServien, ChristiaanPR, Paul B, JAnDbot, Mpm, Pelikana, Duijker, Rei-bot, Look Sharp!, DodekBot, TXiKiBoT, Handige Harrie, VolkovBot, Louperibot, GrouchoBot, DragonBot, Xxl filip, Alexbot, Luckas-bot, MrBlueSky, ArthurBot, HHahn, Pentachlorphenol, Xqbot, Nick141, Erik Wannee, ButkoBot, Mooi is de wereld, ErikvanB, Denkhenk, EmausBot, ZéroBot, WikitanvirBot, ChuispastonBot, Lotje, Flagman11235, Ripchip Bot, MerlIwBot, Scholier, Minsbot, Addbot, QuintenMassijs, DiamantBot, Kulterine20, Wwian1, Sofia Lindberg en Anoniem: 23
- **Internetcensuur** *Bron:* https://nl.wikipedia.org/wiki/Internetcensuur?oldid=47695969 *Bijdragers:* Andre Engels, MichielDMN, RonaldB, Maniago, Foxie001, Davin, Shinieono, Luckas-bot, Amirobot, EdgeNavidad, Halvar, DéRaBot, Mathonius, Xqbot, Smile4ever, RomaineBot, Raast, Wiki13, RedBot, Edinwiki, WinContro, EmausBot, ZéroBot, JackieBot, BakkertjeWouter, Joeykapi, MerlIwBot, Campanile, Lennart97, LymaBot, Karmakolle, Ijscoman, Addbot, Annemichielsens, MatthijsWiki, Rdoroshenko, Wikiwerner en Anoniem: 9
- **Internetfraude** *Bron:* https://nl.wikipedia.org/wiki/Internetfraude?oldid=46562184 *Bijdragers:* Romaine, Robbot, MichielDMN, Ronn, Tdevries, RobotQuistnix, Algont, Husky, Christoffel K, Dolledre, YurikBot, Troefkaart, Maniago, Gouwenaar, SieBot, Ciell, Vis met 1 oog, Raimon, Bor Komorovski, MoiraMoira, Repeater, AGL, Gwiki~nlwiki, SilvonenBot, Toth, MelancholieBot, Manon72, Mathonius, SassoBot, Heureka, Hereticus obstinatus, JurriaanH, ErikvanB, MexicanoBot, Whaledad, ZéroBot, Antoine.01, MerlIwBot, Stef.kerkhofs, Kwuekn, Supercarwaar, Kippenbot1, Nietanoniem, Addbot, Tulp8, Ann-Sophie B, MalysseT, Cromanty, Emmelie2394, DaanDeleye, Niels.Veryepe, Stiem22, Rubenvanbrug en Anoniem: 9
- **Internetprovider** *Bron:* https://nl.wikipedia.org/wiki/Internetprovider?oldid=47272119 *Bijdragers:* Andre Engels, Patrick, TeunSpaans, Branko~nlwiki, Rob Hooft, Pven, Jammers, SanderSpek, Bemoeial, Wilinckx, Jeroen, BenTels, Jeanpaulmars, Rene~nlwiki, Puckly, Advance, Robbot, Oscar, RobotE, Edwtie, Ano niem, O E P~nlwiki, Robotje, MichielDMN, Lexw, IJzeren Jan, Dolfy, Ilario, KlaasZ4usV, RobotQuistnix, Rex, Edoderoo, Stijn Calle, RoboRex, IvarSnaaijer, Riki, Xaviervd, Jeroenbot, Chobot, Jos-uit-boston, YurikBot, Eve, Sonett72~nlwiki, Apdency, FlaBot, Snakes, Danny Mekic, Ninane, Eskimbot, Verrekijker, .marc., Melsaran, Legbatterij-Argonautica, Mion, Eto, Pveijden, Knowledge, BraveNewWorld, Mexicano, Mbch331, SieBot, Thijs!bot, AdnergjeBot, Wouterke89, Bram wouda, Escarbot, Maiella, Heer van Robaais, Mrk~nlwiki, Paul B, JAnDbot, Basvb, MoiraMoira, BotteHarry, Po~nlwiki, Look Sharp!, Airflow, Handige Harrie, VolkovBot, Pachango, Inconnu~nlwiki, BotMultichill, AlleborgoBot, Vels, Loveless, Koektrommel, Richardkiwi, PipepBot, Dloohuis04, DragonBot, Carsrac, Lord Utopia, Alecs.bot, Maurits, Tim009, CarsracBot, MastiBot, Luckas-bot, Mrpraline, Amirobot, MrBlueSky, Ptbotgourou, ArthurBot, Xqbot, Rubinbot, Trickstudents, Smile4ever, D'ohBot, ButkoBot, RedBot, TobeBot, ErikvanB, EmausBot, HRoestBot, WikitanvirBot, Basd82, Eg-T2g, Joopwikibot, CocuBot, Ripchip Bot, MerlIwBot, Bottleneck, Webbyo, Minsbot, Toonzetter, Legobot, MatthijsWiki, Wikiwerner, Grasmat en Anoniem: 55
- **IP-adres** *Bron:* https://nl.wikipedia.org/wiki/IP-adres?oldid=47698168 *Bijdragers:* Andre Engels, Walter, Patrick, Ellywa, Romaine, Bemoeial, BenTels, Pieterse16, Falcongj, Carol Fenijn, Garo~nlwiki, Puckly, Advance, Robbot, RobotE, Bob.v.R, Buttonfreak, Danielm~nlwiki, Mwpnl, Michiel1972, Quistnix, Robotje, MichielDMN, Lexw, Pjetter, Alex1, HetKantoor, Tdevries, Fuss, RobotQuistnix, Galwaygirl, Abnormaal, Joost, Dryke, Edoderoo, Ucucha, Just a member, RoboRex, Richardw, Riki, EdY, Vertrokken, Willemo, Vanelburg, Christoffel K, Dartelaar, Chobot, RonaldB, Aleichem, Dolledre, Bart l~nlwiki, Sonett72~nlwiki, Luna, Maniago, Kleuske, Purodha, Zanaq, SanderK, .marc., Ramoonus, Thomas-, Joshua~nlwiki, Zonix, Erwin, Warddr, Mexicano, EdBever, .Koen, Mbch331, Jvhertum, SieBot, Thijs!bot, Joris, Edwinb, Erik Baas, Wvw, Madyno, Erik1980, Magere Hein, Ciell, JAnDbot, ReWinD, MoiraMoira, Janus28, Erwin85, Rei-bot, Ken123, Look Sharp!, DorganBot, TXiKiBoT, Handige Harrie, VolkovBot, Mtthshksm, GijsvdL, Silver Spoon, Prlwytzkofski, Erwin85TBot, AlleborgoBot, Schwarz productions, RubySS, Synthebot, Sander1453, Idioma-bot, Loveless, Koektrommel, Louperibot, P3t0r, Wutsje, Kyle the bot, GrouchoBot, Kthoelen, DragonBot, Rjkasteel, Bigboss57, Timantha102938, SilvonenBot, EvilFreD, JurgenNL, Pompidom, Access, JRB, MrBlueSky, Ptbotgourou, Nallimbot, Johan 9090, Diamant, FoxBot, Kippenvlees1, Xqbot, Rubinbot, Smile4ever, RomaineBot, BenzolBot, Wiki13, TobeBot, Dinamik-bot, ErikvanB, Denkhenk, EmausBot, Tjibbe I, Kulter20, BioPupil, WittePrins, Gossesol, Movses-bot, Sikjes, MerlIwBot, Groenrood23, Minsbot, Kloentje2, YFdyh-bot, Nietanoniem, Addbot, Tulp8, Higger, Robyvd, Hidde7271, StroopwafelBot, 3FR0STY4, Wikiwerner, Joskedekakbosse, Kakatje en Anoniem: 147

- **IRC-bot** *Bron:* https://nl.wikipedia.org/wiki/IRC-bot?oldid=36524414 *Bijdragers:* Kattenkruid, Annabel, UFO~nlwiki, Mexicano, Simeon, Jvhertum, JAnDbot, MoehMan, WarddrBOT, Japiot, Kakarot6, Alexbot, Kwiki, ChrisiPK, MrBlueSky, LolsimonBot, Smile4ever, EmausBot, Double07, Brentjee, Addbot en Anoniem: 3
- **Keylogger** *Bron:* https://nl.wikipedia.org/wiki/Keylogger?oldid=46841624 *Bijdragers:* Fruggo, Kattenkruid, RobotE, Michiel1972, Bean 19, MichielDMN, Mdd, RobotQuistnix, Jelte, Dryke, Edoderoo, RoboRex, Annabel, Christoffel K, Obarskyr, RonaldB, YurikBot, FlaBot, Kleuske, Erwin, Mexicano, Simeon, EdBever, SieBot, Thijs!bot, Erik Baas, Tukka, Rozemarijn vL, Erik1980, Markapeldoorn, JAnDbot, A Duck, ArnaudH, Johan N, Look Sharp!, OekelWm, Narayan, TXiKiBoT, Handige Harrie, Aibot, VolkovBot, Silver Spoon, Loveless, Wutsje, Vinvlugt, Seowebsites, GrouchoBot, Alexbot, RobbertS, RonnieV, Alecs.bot, FlippyFlink, Luckas-bot, MrBlueSky, ChenzwBot, Yonidebot, Xqbot, Maasje, Trijnstel, MrBlueBot, EmausBot, Batterybird, TomDeBuyser, Lotje, Sreejithk2000, Ilse reeper, Calorshear, Nietanoniem, Addbot, Robyvd, Michael Dave, Wikiwerner en Anoniem: 43
- **Klikfraude** *Bron:* https://nl.wikipedia.org/wiki/Klikfraude?oldid=46660127 *Bijdragers:* SanderSpek, Robbot, Joachim, RobotQuistnix, Wikix-oud, MADe, RobotTbc, SieBot, Freestyle, Chtit draco, Rudolphous, Silver Spoon Sokpop, Fwtrader, AGL, LaaknorBot, Luckas-bot, MystBot, Edoderoobot, Smile4ever, Trijnstel, ErikvanB, WikitanvirBot, Ebrambot, ChuispastonBot, Lotje, Ripchip Bot, YFdyh-bot, Addbot en Anoniem: 8
- **Linux** *Bron:* https://nl.wikipedia.org/wiki/Linux?oldid=47775634 *Bijdragers:* Andre Engels, Walter, Patrick, Pieter Suurmond, Rob Hooft, Rene Pijlman, SanderSpek, Wilinckx, Guaka, Jeroen, Justacat, SigmundFreud, Bart~nlwiki, Mac Cain13, Domie, Garo~nlwiki, Puckly, HooftBot, Robbot, Gidonb, GerardM, Bramschnmkrs, Nikai, McDutchie, Laudaka, Flok, Oski, Dick Bos, Q-collective, RobotE, Siebrand, Michiel1972, Meneer, Bean 19, A3, Robotje, BenTheWikiMan, MichielDMN, Jognet, Doitashimashite, Emvee, Yorian, Pjetter, Jcb, Fuss, RobotQuistnix, LimoWreck, Rex, Qwertyus, JeroenvB, Venullian, PPP, Gpvosbot, Robotpjetter, Algont, RoboRex, Riki, P.H. Louw, Vertrokken, Eriq~nlwiki, BotEmpoor, Willemo, Letinon, Jeroenbot, Jeroen-91, RonaldB, Tobislav, Eve, Pval, Wbsoft, Kleuske, Fr33ke, Zanaq, Kwoot, Josq, Erwin, G.P.~nlwiki, Robb, Lennart, Marc-André Aßbrock, Ytrecq, Mexicano, Simeon, Rhandor, Kameraad Pjotr, .Koen, SieBot, Bouwe Brouwer, ErikJanVens, Edwinb, Erwin85Bot, George4, Tukka, Escarbot, Erik1980, Noescom, Wolu, Paul B, LeChuck, Robert Buzink, JAnDbot, Freestyle, BetBot~nlwiki, Xfactor, MoiraMoira, CrazyPhunkbot, Look Sharp!, SanderVG, Larzzz, AnnabelsBot, WarddrBOT, TXiKiBoT, Aibot, VolkovBot, Titania, Zuliani, GijsvdL, Erwin85TBot, LarzBot, Die vandaal, DokterT, Synthebot, Idioma-bot, Zbisasimone~nlwiki, Mdavids, MTrBot, BjornR, Kthoelen, DragonBot, Ledux, DrJos, Zed~nlwiki, Forrestjunky, Gamut, Alexbot, Klungel~nlwiki, Purbo T, AnokoBOT, SilvonenBot, Toth, JurgenNL, MelancholieBot, CarsracBot, Pompidom, LinkFABot, Luckas-bot, MrBlueSky, Ke~nlwiki, Nallimbot, Japiobot, Galoubet, Jotterbot, Hileak, Hoopje, MauritsBot, ArthurBot, Puckipedia, JanDeFietser, De Wikischim, FoxBot, Xqbot, GhalyBot, SassoBot, Jashaj, Emelha, Smile4ever, RomaineBot, Wvanb, Sanderd17, Wiki13, BokimBot, RedBot, TobeBot, ErikvanB, Queeste, MexicanoBot, EmausBot, ZéroBot, WikitanvirBot, ChuispastonBot, Eg-T2g, MerlIwBot, Terzo, Nummer 12, Vagobot, AlbinS, Ajv39, Dexbot, Natuur12, Addbot, S078, Tulp8, KevinVorstermans, XXBlackburnXx, KehppKukkieBot, Wikiwerner, Oskardebot, CoatThese en Anoniem: 135
- **Live-cd** *Bron:* https://nl.wikipedia.org/wiki/Live-cd?oldid=45957365 *Bijdragers:* Guaka, Jeroen, HooftBot, Robbot, Nikai, Pimvantend, Johan Lont, A3, Spinal83, BenTheWikiMan, MichielDMN, RobotMichiel1972, Doitashimashite, Elwikipedista~nlwiki, RobotQuistnix, LimoWreck, Rex, RoboRex, BotEmpoor, MoriBot, Jeroen-91, Tobislav, Typhoner, YurikBot, FlaBot, Eskimbot, Ramoonus, NewMikey, Peti me, Whizz, Dr. F.C. Turner, SieBot, Thijs!bot, Escarbot, JAnDbot, Whollabilla, TXiKiBoT, VolkovBot, GijsvdL, BotMultichill, AlleborgoBot, Hxhbot, Jeroenverhulst, Alexbot, BOTarate, SilvonenBot, Emil76, CarsracBot, Pompidom, SpBot, Mercy, LaaknorBot, SF007, ArthurBot, Kippenvlees1, Xqbot, RibotBOT, Pompidombot, Smile4ever, MondalorBot, TobeBot, Dinamik-bot, MexicanoBot, EmausBot, ZéroBot, WikitanvirBot, ChuispastonBot, Eg-T2g, Ripchip Bot, Legobot en Anoniem: 20
- **MacOS** *Bron:* https://nl.wikipedia.org/wiki/MacOS?oldid=47768712 *Bijdragers:* TeunSpaans, Greco, Ronald, Hannes Karnoefel, Guaka, Jeroen, BenTels, Jeanpaulmars, Carol Fenijn, Christiaan~nlwiki, Muijz, HooftBot, Robbot, Johnny~nlwiki, Bontenbal, Nikai, Oscar, RobotE, Buttonfreak, RonaldW, Taka, Mwpnl, A3, Peter Haas, Gpk481, MichielDMN, RobotMichiel1972, Lexw, Doitashimashite, JePe, Bries, Rabarberski, Empoor, Evil berry, RobotQuistnix, LimoWreck, Guyvago, Tobiasvanderwal, Goingin~nlwiki, Dryke, Johjak, RoboRex, Richardw, Riki, Vertrokken, BotEmpoor, MoriBot, Paul-MD, Jeroenbot, Obarskyr, Chobot, RonaldB, Typhoner, Dolledre, YurikBot, Manuel Claeys Bouuaert, MysteryQuest, Troefkaart, Vincent Jacobs, BotOx, RobotTbc, MwM, Kvitske, Marcelkennis, LucVerhelst, À la Mac, Lennart, Ivory, Gerbot, Mexicano, Paulstar, .Koen, Jvhertum, SieBot, Juvarra, Thijs!bot, David12345, Escarbot, DJPeugeot~nlwiki, Magere Hein, Ciell, BotChristophe, MSBOT, JAnDbot, Eddyspeeder, NOOBnl, Whollabilla, MoiraMoira, CommonsDelinker, Jochem V, Macosxnews, Evilonline, Nomadcowboy, Paulverhoeven, Ken123, Look Sharp!, Webplanet, Wouterjanss, Stephanvk, VanBuren, DodekBot, Gamie, Bo W, TXiKiBoT, Grashoofd, VolkovBot, Ief2, BotMultichill, Silver Spoon, 3wisemen, Lennartgoosens, M. Renckens, Synthebot, Victor LP, Gileba, Tleilax, Gerakibot, Tomtom137, Avbentem, Alwetendheid alom, Richardkiwi, Psebok, Sanpiper800, Zippo^, DragonBot, AlnoktaBOT, Abiboe, Roxxy~nlwiki, Excel20, PieterDeBruijn, Prlwytzkowsky, Alexbot, BOTarate, AnokoBOT, Toth, Alecs.bot, EvilFreD, LaaknorBot, SuperDutchGuy, Luckas-bot, MystBot, MrBlueSky, Ptbotgourou, Xeranos, Cx1213, Nallimbot, Jotterbot, Tommy Kronkvist, Edoderoobot, Hoopje, MauritsBot, Totie, GrashoofdBot, XZeroBot, Obersachsebot, FoxBot, Kippenvlees1, Xqbot, RibotBOT, Krinkle, Emelha, Pompidombot, Smile4ever, RomaineBot, BenzolBot, T-bo, Trijnstel, Wiki13, Gastonw, RedBot, Dutchgabber, TobeBot, Woodcutterty, LilyKitty, JurriaanH, ErikvanB, Verdel, KamikazeBot, TjBot, Sal~nlwiki, WinContro, Haheti, Rikvolvo, MexicanoBot, Jpk.hakvoort, EmausBot, Rik007, BakkertjeWouter, Sjoerddebruin, CocuBot, YannickFran, Dinosaur918, DirkVE, Ripchip Bot, MerlIwBot, SunKeeper, IlxWrite, AvocatoBot, Brbotnl, Rezabot, Dijsburger, Mijco, KafiRobot, I-am-will, Rico515, MGTroost, EnzaiBot, Kippenbot1, Jzn123, Legobot, Trichtenaar, S078, Snippex, KevinVorstermans, MatthijsWiki, XXBlackburnXx, KehppKukkieBot, DJLaurens11, ILUUUK, Djlaurens12, 1989, Wikiwerner, Sandrabloemenhoff, Schrijveryas, NielsAC, Jordi2830 en Anoniem: 170
- **Mailserver** *Bron:* https://nl.wikipedia.org/wiki/Mailserver?oldid=46345166 *Bijdragers:* Serassot, Robbot, RobotE, JePe, Patrick79~nlwiki, RobotQuistnix, Rex, JeroenvB, Stormshadownl, RoboRex, Riki, Dolledre, Troefkaart, FlaBot, Kleuske, Willem ter Haar, Eskimbot, Mexicano, SieBot, Erik Baas, JAnDbot, Look Sharp!, TXiKiBoT, Michaelkmd, Loveless, PipepBot, Zabot, SpBot, Kwiki, PauloCalipari, MastiBot, Luckas-bot, MrBlueSky, Ronaldo Aves, Japiobot, BKannen, Smile4ever, RedBot, ErikvanB, EmausBot, MerlIwBot, Addbot, Ahappylittletree, Jonathan.bakker en Anoniem: 21
- **Man-in-the-middle-aanval** *Bron:* https://nl.wikipedia.org/wiki/Man-in-the-middle-aanval?oldid=45295624 *Bijdragers:* Streppel, Carol Fenijn, Robbot, Oscar, RobotMichiel1972, Dolfy, Egs, MADe, Jeroenbot, YurikBot, FlaBot, Simeon, SieBot, Erwin85Bot, Heer van Robaais, JAnDbot, Look Sharp!, DodekBot, VolkovBot, Gerakibot, JanTurin, Louperibot, GrouchoBot, Joost Herregodts, SilvonenBot, JanB46, Luckas-bot, ArthurBot, TaBOT-zerem, SassoBot, Woodcutterty, Dinamik-bot, ErikvanB, MexicanoBot, EmausBot, WikitanvirBot, Rezabot, MichèleD, Justincheng12345-bot, Legobot, Joachim Sercu en Anoniem: 2
- **Moederbord** *Bron:* https://nl.wikipedia.org/wiki/Moederbord?oldid=47476964 *Bijdragers:* Andre Engels, Walter, Pven, Arent, Bemoeial, BenTels, Carol Fenijn, Rene~nlwiki, Puckly, Robbot, Willem vd Kletersteeg, Siebrand, Danielm~nlwiki, HenkvD, Robotje, MichielDMN,

CaAl, Lexw, Milliped, RobotQuistnix, LimoWreck, T Houdijk, Tomgreep, Abnormaal, Joost, RoboRex, Riki, Willemo, Kweetal, Christoffel K, Obarskyr, Eve, Kleuske, Ninane, RobotTbc, SanderK, .marc., Emmelie, Whizz, Mexicano, EdBever, Royvdmaas, SieBot, Thijs!bot, Tukka, Escarbot, Magere Hein, JAnDbot, MoiraMoira, CommonsDelinker, Look Sharp!, DodekBot, TXiKiBoT, Lymantria, VolkovBot, BotMultichill, Jmp98251, AlleborgoBot, Kamustra, Gerakibot, Emiel.molenaar, GrouchoBot, DragonBot, Jarii94, Alexbot, Capaccio, SilvonenBot, Alecs.bot, JurgenNL, NjardarBot, Elektriciteit, Luckas-bot, Jotterbot, ChenzwBot, MauritsBot, Xqbot, Meerdervoort, Rubinbot, RibotBOT, Pompidombot, Smile4ever, Wiki13, Mattias.Campe, TBloemink, EmausBot, HRoestBot, JackieBot, WikitanvirBot, Eg-T2g, CocuBot, MerlIwBot, Vagobot, AvocatoBot, Kloentje2, FireKikker, Legobot, Nietanoniem, Tulp8, Fresmaro, DottyMcFear13 en Anoniem: 90

- **Nettiquette** *Bron:* https://nl.wikipedia.org/wiki/Nettiquette?oldid=48052119 *Bijdragers:* Andre Engels, Walter, Pieter~nlwiki, Evanherk, Arent, Romaine, Bemoeial, BenTels, Puckly, HooftBot, Robbot, Nikai, Bob.v.R, Jupiler, Guanabot~nlwiki, Laban, MichielDMN, RobotMichiel1972, Rides, Bthv, MigGroningen, Jcb, RobotQuistnix, Vitum, Rex, Qwertyus, Gpvosbot, Robotpjetter, RoboRex, Riki, Vertrokken, Dartelaar, Chobot, Aleichem, Dolledre, YurikBot, Eve, Hans M., Kleuske, Eskimbot, Sumurai8, PeterPan, Mexicano, Berkoet, Jvhertum, SieBot, Thijs!bot, Quasar, Sustructu, JAnDbot, A Duck, MoiraMoira, Hulten, Look Sharp!, VolkovBot, BotMultichill, VanBeem, AlleborgoBot, Synthebot, Mofrikaantje, Loveless, Wutsje, GrouchoBot, PixelBot, Alexbot, BodhisattvaBot, Taketa, JurgenNL, Pompidom, MrBlueSky, Marrakech, Peterson, Xqbot, Smile4ever, Erik Wannee, RomaineBot, Wiki13, TobeBot, ErikvanB, Bourdon16, Denkhenk, EmausBot, ZéroBot, WikitanvirBot, MerlIwBot, Tine26, DunjaP, Grmbl76, Extinguished Fire, Nietanoniem, Addbot, Kukkie, Kehpp, Benniedom, FactoryText en Anoniem: 43
- **Nieuwsgroep** *Bron:* https://nl.wikipedia.org/wiki/Nieuwsgroep?oldid=39260842 *Bijdragers:* Walter, SanderSpek, BenTels, Puckly, Robbot, Oscar, A3, Caseman, Lexw, Arienh4, Jcb, Dolfy, Rex, Bert76, Johjak, RoboRex, Kwibus, Jeroenbot, Chobot, RonaldB, Jkransen, ArjenW, Fr33ke, Lampje, Ivory, Whizz, Simeon, SieBot, Ken123, Look Sharp!, GijsvdL, Wimpus, Hitnieuws, Palaemon, GrouchoBot, APrometheus, RonnieV, Darthvader2008, MrBlueSky, MerlIwBot, Legobot en Anoniem: 21
- **Nigeriaanse oplichting** *Bron:* https://nl.wikipedia.org/wiki/Nigeriaanse_oplichting?oldid=46502554 *Bijdragers:* Muijz, Advance, Johnny~nlwiki, Caseman, MichielDMN, RobotMichiel1972, Martinus, Ronn, MigGroningen, Dolfy, RobotQuistnix, Wikix-oud, MADe, Algont, Riki, AlexP, Wester2005, DéRahier, Jeroenbot, Aleichem, Ninane, Vanzetti, Foxie001, Jvhertum, WikiFB2, SieBot, Thijs!bot, Erwin85Bot, Van der Hoorn, Erik1980, Maiella, BOT-Superzerocool, Bor Komorovski, MoiraMoira, Narayan, Skuipers, TXiKiBoT, Handige Harrie, VolkovBot, Paul K., Louperibot, Zabot, GrouchoBot, SlamPamper, Velocitas, SilvonenBot, Pompidom, FvdL, Veerle.troch, MrBlueSky, Goudsbloem, Edoderoobot, SteinUmStein, BKannen, Xqbot, Saschaporsche, Meerdervoort, RibotBOT, Smile4ever, Erik Wannee, RomaineBot, TobeBot, ErikvanB, MexicanoBot, EmausBot, Whaledad, Lotje, Stoereavatar, Sikjes, Youbuntu, Addbot, Wwikix, Janaa D, Stef Bryssinck, Kaj Sustronck, Joachim Sercu, Berdieke, Wicoby, Wikiwerner en Anoniem: 21
- **Online betalen** *Bron:* https://nl.wikipedia.org/wiki/Online_betalen?oldid=47429911 *Bijdragers:* Riki, Kleuske, BrightSide, Waldo79, Skuipers, Josroos, MrBlueSky, Edoderoobot, RomaineBot, Félix, Woodcutterty en Niels-Bru
- **PayPal** *Bron:* https://nl.wikipedia.org/wiki/PayPal?oldid=47430183 *Bijdragers:* Andre Engels, Walter, Streppel, Robbot, Bontenbal, RobotE, Michiel1972, O E P~nlwiki, MichielDMN, RobotMichiel1972, Sybren, Rides, Ronn, MigGroningen, Steinbach, JimmyShelter, RobotQuistnix, MADe, Riki, DéRahier, MagalhaesBot, RonaldB, Writeroscar, Asbak, FlaBot, Kleuske, JD, Zanaq, Waldo79, Chlewbot, Sonty567, Martijnvg, JFD~nlwiki, Sjonnie, Simeon, EdBever, CrazyPhunk, SieBot, Thijs!bot, Edwinb, DimiTalen, Tukka, Dennisgoedegebuure, FakirNL, Sindala, JAnDbot, Janmarques, Janssenfrank, Mpm, Bor Komorovski, MoiraMoira, Rei-bot, Skuipers, TXiKiBoT, VolkovBot, Le Fou, BotMultichill, Idioma-bot, Gerakibot, Freaky Fries, DreamWearl, Veendorp, Wutsje, Jarune, Zorrobot, GrouchoBot, Jarii94, Kwiki, Kagee, Glatisant, Naudefjbot, Luckas-bot, MrBlueSky, Peterson, ArthurBot, HHahn, PaulP, Byeboer, Xqbot, RibotBOT, Sokkertop, LucienBOT, Pompidombot, Smile4ever, Erik Wannee, RomaineBot, Félix, Wiki13, ButkoBot, TBloemink, ErikvanB, ReinaartBot, KamikazeBot, EmausBot, ZéroBot, Sopkok, ChuispastonBot, Mjbmrbot, PayPalNL, MariekeB, Taalverslaafde, Joopwikibot, Ripchip Bot, MerlIwBot, Kashmiri, JYBot, Kippenbot1, Legobot, Lucasio98, Bramverk, NFKnaap, MatthijsWiki, Stef Bryssinck, Tasia Pleune, ToonVA, Wicoby, Eustratiou, Ronnie PG en Anoniem: 66
- **Pharming (internet)** *Bron:* https://nl.wikipedia.org/wiki/Pharming_(internet)?oldid=46611013 *Bijdragers:* Oski, RobotE, Barbarossa~nlwiki, MichielDMN, Demophon, RobotQuistnix, RoboRex, Riki, Zwobot, Meijers, MarQ, FlaBot, RaMPo, Jvhertum, SieBot, Thijs!bot, Tasja, Escarbot, Bbe, Iooryz, TXiKiBoT, VolkovBot, AgentX, Zorrobot, PixelBot, Ballie19, Smile4ever, EmausBot, Ripchip Bot, MerlIwBot, Stijn.Berghmans, Dexbot, Addbot, Stef Bryssinck, Berdieke, Larsb99, Wikiwerner, Perudotes en Anoniem: 2
- **Phishing** *Bron:* https://nl.wikipedia.org/wiki/Phishing?oldid=47552325 *Bijdragers:* Patrick, Ellywa, Bemoeial, Robbot, Pantalone, Siebrand, MartinD, Meneer, Barbarossa~nlwiki, Bean 19, MichielDMN, RobotMichiel1972, Lexw, ESanders, Pjetter, Sixtus, RobotQuistnix, Galwaygirl, Wikix-oud, Abnormaal, Stormshadownl, MADe, RoboRex, Riki, Klaas1978, KokoBot, Chobot, RonaldB, Zwobot, Dolledre, YurikBot, Eve, Troefkaart, FlaBot, Kleuske, Eskimbot, RaMPo, Melsaran, Chlewbot, Vincentsc, Lost, Warddr, Jvhertum, Spankeronie, SieBot, Thijs!bot, Tasja, Rozemarijn vL, Bbe, Maiella, JAnDbot, MoiraMoira, CommonsDelinker, CrazyPhunkbot, Pieter19, Thijshuberts, Rei-bot, Look Sharp!, DodekBot, DorganBot, TXiKiBoT, Lymantria, VolkovBot, Repeater, Mingoes, Loveless, Beany, GrouchoBot, Kwik, MelancholieBot, Pompidom, SpBot, JanB46, LinkFA-Bot, Luckas-bot, Ptbotgourou, MauritsBot, ArthurBot, Mathonius, Xqbot, Spraakverwarring, Smile4ever, Félix, Trijnstel, Woeterman 94, RedBot, ErikvanB, MexicanoBot, EmausBot, AäronVerachtert, TuHan-Bot, WikitanvirBot, Eg-T2g, Lotje, BijsG, Manubot, DunjaP, Ilse reeper, MichèleD, Grmbl76, Dexbot, Aggie2, Brentjee, Addbot, Ann-Sophie B, Amity Oak, Rolf Kemp., Stef Bryssinck, DaanDeleye, Tina3104, Kaj Sustronck, Maarten Ceunen, Tasia Pleune, Thomas Lammens, BrackezMassimo, Xxmarijnw en Anoniem: 51
- **Portaal (internet)** *Bron:* https://nl.wikipedia.org/wiki/Portaal_(internet)?oldid=46939743 *Bijdragers:* Romaine, Fruggo, Cicero~nlwiki, Jerroleth, RobotMichiel1972, RobotQuistnix, RonaldB, Ronaldvd, Maniago, Emiel, Non Plus Ultra, SieBot, Escarbot, JAnDbot, MoiraMoira, Ken123, YoshiDaSilva, Look Sharp!, Rudolphous, TXiKiBoT, Grashoofd, Aibot, BotMultichill, Maghiel, AlleborgoBot, Loveless, Koektrommel, RolfTZ, GrouchoBot, PixelBot, Darkicebot, Mike.lifeguard, SilvonenBot, LaaknorBot, Luckas-bot, MystBot, MrBlueSky, Nallimbot, ArthurBot, Dienast, Xqbot, RibotBOT, RedBot, EmausBot, Kadeike, WikitanvirBot, ChuispastonBot, Movses-bot, Ripchip Bot, MerlIwBot, Rezabot, HiW-Bot, Kasymbot, Addbot, Wikiwerner en Anoniem: 8
- **Pretty Good Privacy** *Bron:* https://nl.wikipedia.org/wiki/Pretty_Good_Privacy?oldid=46396342 *Bijdragers:* Walter, Puckly, Panthouse, Robbot, RobotE, Michiel1972, Robotje, Hardscarf, RobotQuistnix, MADe, RoboRex, Jeroenbot, Jorisv, YurikBot, FlaBot, Odo~nlwiki, Pimm, Marc-André Aßbrock, Gerbot, Mexicano, Red15, Simeon, SieBot, Dtech, FakirNL, Handige Harrie, Japiot, VolkovBot, KKoolstra, BotMultichill, Loveless, JanTurin, Louperibot, Tucquero, Zorrobot, GrouchoBot, AlnoktaBOT, Marijnvdzaag, Westerlaken, Alexbot, Darkicebot, S0516759, Luckas-bot, MrBlueSky, Edoderoobot, TaBOT-zerem, Xqbot, Pompidombot, Smile4ever, RedBot, ErikvanB, EmausBot, MerlIwBot, Legobot en Anoniem: 16

- **Proxyserver** *Bron:* https://nl.wikipedia.org/wiki/Proxyserver?oldid=47713783 *Bijdragers:* Walter, Marza, Ellywa, Rob Hooft, Bemoeial, Willemdd, BenTels, Carol Fenijn, HooftBot, Robbot, Paul Hermans, GerardM, Kattenkruid, RobotE, Chris, MartinD, Alicey, Bean 19, Jupiler, Robotje, Laban, Lexw, Ype, Bios, RobotQuistnix, Robotpjetter, RoboRex, Riki, China Crisis, KokoBot, Annabel, Dartelaar, Jeroenbot, Chobot, RonaldB, Aleichem, Dolledre, The Banner, Maniago, Kleuske, Eskimbot, Fr33ke, RobotTbc, RaMPo, Niels, Verrekijker, .marc., Robb, Gio, Gerbot, Mexicano, Rmoorlag, BerendBotje, SieBot, Thijs!bot, Edwinb, Erik Baas, Tukka, Van der Hoorn, Escarbot, Davin, JAnDbot, Machaerus, .anacondabot, MoiraMoira, Rei-bot, SbJ, Po0ky, DorganBot, TXiKiBoT, Toffguy, VolkovBot, Repeater, GijsvdL, ARVER, Lolsimon, Loveless, Louperibot, Wutsje, Richardkiwi, BjornR, Zabot, DragonBot, AlnoktaBOT, PieterJanR, Alexbot, RonnieV, BodhisattvaBot, Alecs.bot, Pompidom, LinkFA-Bot, MastiBot, LaaknorBot, Luckas-bot, Tim Auke Kools, MrBlueSky, JZ85, ChenzwBot, Coradriaan, Xqbot, Oskkar, LucienBOT, Pompidombot, Wiki13, MrBlueBot, ErikvanB, MexicanoBot, EmausBot, Whaledad, Lievelavens, Tjibbe I, WikitanvirBot, Dilic, DirkVE, Ilse reeper, YFdyh-bot, Legobot, XXBlackburnXx, Appelsenperenenzo en Anoniem: 92

- **Ransomware** *Bron:* https://nl.wikipedia.org/wiki/Ransomware?oldid=47532963 *Bijdragers:* Kattenkruid, RobotE, Ynst, Michiel1972, MichielDMN, Bdijkstra, Ype, Vertrokken, Klaas1978, Kleuske, Eskimbot, Robb, LeeGer, Thijs!bot, CommonsDelinker, VolkovBot, BotMultichill, M. Renckens, PixelBot, Luckas-bot, Manon72, Hoopje, Smile4ever, EmausBot, ZéroBot, Michielderoo, Lotje, Joopwikibot, Fab301, DeGilian, MerlIwBot, Sandra1983, JYBot, Michiel TM, Dexbot, Trancelot, Addbot, AxelleDejaeghere, Berdieke en Anoniem: 12

- **Recht om vergeten te worden** *Bron:* https://nl.wikipedia.org/wiki/Recht_om_vergeten_te_worden?oldid=47192484 *Bijdragers:* Aiko, Pompidom, Joostik, Mooi is de wereld, ErikvanB, Sikjes, SaskiaHutten, WesJa, White Canvas en Anoniem: 1

- **Scriptkiddie** *Bron:* https://nl.wikipedia.org/wiki/Scriptkiddie?oldid=47684156 *Bijdragers:* Rob Hooft, Bontenbal, RobotE, Puc conDoin, MichielDMN, Lexw, RobotQuistnix, Gwyrrdin, China Crisis, YurikBot, FlaBot, Kleuske, Sumurai8, Chlewbot, Necromander, Mexicano, Simeon, Jvhertum, Havelaar, SieBot, Thijs!bot, Vis met 1 oog, Ken123, Look Sharp!, TXiKiBoT, VolkovBot, Wimpus, DrJos, Blueknight, Taketa, LaaknorBot, MrBlueSky, Flurps, Edoderoobot, ArthurBot, Mathonius, Jackie, Xqbot, Pompidombot, MrBlueBot, RedBot, PieterDP, EmausBot, WikitanvirBot, AlbinS, Pieterjan E, DunjaP, ZeaForUs, Addbot, Nicolas.B, AxelleDejaeghere, Jellelimpens en Anoniem: 11

- **Server** *Bron:* https://nl.wikipedia.org/wiki/Server?oldid=45316739 *Bijdragers:* Pven, Cicero~nlwiki, Jeroen, BenTels, Jeanpaulmars, Carol Fenijn, Rene~nlwiki, Serassot, HooftBot, Robbot, RobotE, RonaldW, RobotMichiel1972, HetKantoor, JimmyShelter, RobotQuistnix, JeroenvB, IIVQ, MADe, RoboRex, Peter b, Willemo, Hverbiesen, Obarskyr, Chobot, Dolledre, YurikBot, Troefkaart, FlaBot, Testtools~nlwiki, Kleuske, Eskimbot, Zanaq, Mexicano, Khx023, Kameraad Pjotr, SPQRobin, Mbch331, SieBot, Thijs!bot, Tukka, Escarbot, MaEr, Erik1980, JAnDbot, MoiraMoira, TARBOT, NLmarcel, Ken123, Look Sharp!, Wouterjanss, DodekBot, TXiKiBoT, Lymantria, VolkovBot, BotMultichill, Synthebot, Idioma-bot, Loveless, BjornR, GrouchoBot, LA2-bot, BodhisattvaBot, Basdej, Nio17, LaaknorBot, Luckas-bot, Amirobot, MrBlueSky, Ptbotgourou, Boemannek, ChristopheS, ChenzwBot, TaBOT-zerem, Mathonius, FoxBot, Xqbot, RibotBOT, Lizatjeah, Wiki13, RedBot, Vermijn, Mattias.Campe, EmausBot, WikitanvirBot, Smiba, Mjbmrbot, Sjoerddebruin, MerlIwBot, Vagobot, Ed Lane, Legobot, Damianpsp, Tulp8, StroopwafelBot en Anoniem: 40

- **Social engineering (informatica)** *Bron:* https://nl.wikipedia.org/wiki/Social_engineering_(informatica)?oldid=47359392 *Bijdragers:* Patrick, DXL, Hjvannes, Meneer, Gpvos, RobotQuistnix, Algont, YurikBot, DiedX, Fontes, Jvhertum, SieBot, Thijs!bot, TXiKi, MoiraMoira, PAvdK, WarddrBOT, TXiKiBoT, BotMultichill, YonaBot, Zabot, Alexbot, CarsracBot, Pompidom, Kwiki, Luckas-bot, MrBlueSky, ArthurBot, Xqbot, RibotBOT, Trijnstel, RedBot, Woodcutterty, ErikvanB, EmausBot, JackieBot, ChuispastonBot, MerlIwBot, Tine26, DarafshBot, Nietanoniem, Addbot, 12345danNL, AxelleDejaeghere, Perudotes en Anoniem: 18

- **Software** *Bron:* https://nl.wikipedia.org/wiki/Software?oldid=47418674 *Bijdragers:* Scipius, Evanherk, Rob Hooft, Snoop, Rene Pijlman, SanderSpek, Cicero~nlwiki, Jeroen, BenTels, HooftBot, Robbot, Ubes, RonOnrust, Oscar, RobotE, Jhenyal, Siebrand, MartinD, Hjvannes, Meneer, A3, O E P~nlwiki, Robotje, MichielDMN, Mdd, Nlmark, JimmyShelter, LimoWreck, Rex, Freek Verkerk, Justhg, Qwertyus, Tomgreep, Bert76, Dryke, Kiwix, Edoderoo, Johjak, RoboRex, Riki, Vertrokken, BotEmpoor, Annabel, RonaldB, BotOx, Ronaldvd, Maniago, Kleuske, Ninane, SdeVries, SanderK, Mion, Essea02 wikipedia, Simeon, Woudloper, Jvhertum, BerendBotje, SieBot, Edwinb, Tvdm, Heer van Robaais, R.A.N. Hilderink, JAnDbot, A Duck, MoiraMoira, BotteHarry, Gabadubo~nlwiki, Theyoung, Calvinturbo, VanBuren, CentraalDH, YewBowman, TXiKiBoT, Lymantria, BertS, Handige Harrie, VolkovBot, RenéV, 3wisemen, Zwitser123, Rietvogel, Synthebot, Idioma-bot, Gerakibot, JanTurin, Tjschijf, GrouchoBot, Eiland, Timvanderzande, Fenke, Voorthuizenr, DragonBot, LA2-bot, WezyBot, Beachcomber, SilvonenBot, Jmeverts, Wikijens, Luckas-bot, MrBlueSky, Ptbotgourou, Jotterbot, ChristopheS, MauritsBot, ArthurBot, DSisyphBot, FoxBot, Xqbot, Saschaporsche, RibotBOT, Smile4ever, RomaineBot, ButkoBot, RedBot, JeanLuc hooglugt, Dinamik-bot, JurriaanH, ErikvanB, ReinaartBot, KamikazeBot, WinContro, Wester, MexicanoBot, DixonDBot, EmausBot, HRoestBot, Eg-T2g, Sjoerddebruin, MerlIwBot, Moddereter, Vinco0o, Legobot, Addbot, KehppKukkieBot, NielsAC en Anoniem: 65

- **Solid state drive** *Bron:* https://nl.wikipedia.org/wiki/Solid_state_drive?oldid=47714972 *Bijdragers:* Andre Engels, Romaine, Bemoeial, Advance, Robbot, Kattenkruid, DaProx, MichielDMN, Bdijkstra, RobotQuistnix, MADe, Just a member, Richardw, Riki, Paul-MD, Dartelaar, Chobot, RonaldB, FlaBot, Maniago, Kleuske, Mexicano, SieBot, Thijs!bot, David12345, Brimz, ChristiaanPR, Tjeerdomaat, Xfactor, MoiraMoira, Look Sharp!, VanBuren, CyFo, TXiKiBoT, Lymantria, Handige Harrie, VolkovBot, Jonathan.slenders, Mausy5043, Bic, GijsvdL, BotMultichill, 3wisemen, AlleborgoBot, Loveless, GrouchoBot, DragonBot, PixelBot, Hans Kamp, Capaccio, BotSottile, Difool, Coman~nlwiki, JurgenNL, MelancholieBot, Broadbot, Pompidom, Nio17, Dqfn13, LaaknorBot, Ralf Roletschek, Luckas-bot, MrBlueSky, Xeranos, MauritsBot, ArthurBot, Redwodka, Obersachsebot, Jlthkoch, Xqbot, RibotBOT, Maasje, WikiRAM, Theking2, Smile4ever, RomaineBot, MrBlueBot, RedBot, ErikvanB, Verdel, EmausBot, MaximHuyghelier, O0Rollo0o, Chielbuseyne, WikitanvirBot, ChuispastonBot, RT13, DeGilian, Ripchip Bot, MerlIwBot, AlterBerg, SunKeeper, Dexbot, Addbot, Accountplz en Anoniem: 67

- **Spam (post)** *Bron:* https://nl.wikipedia.org/wiki/Spam_(post)?oldid=47620726 *Bijdragers:* Andre Engels, Walter, Ellywa, Rob Hooft, Ronald, Rene Pijlman, Romaine, SanderSpek, Bemoeial, Wilinckx, Cicero~nlwiki, LennartBolks, BenTels, Argus~nlwiki, Muijz, Puckly, HooftBot, Robbot, Wim Hamhuis, Hashar, Casper, Siebrand, RonaldW, Arrowman, MartinD, Mwpnl, Michiel1972, Allesbehalve, O E P~nlwiki, Dolmonly, Jeroenr, MichielDMN, Itsme, Lexw, Bdijkstra, Martinus, Pjetter, JePe, Tdevries, Jcb, Capivara, RobotQuistnix, Rex, Qwertyus, Joost, MADe, Edoderoo, SanderSpekBot, Robotpjetter, RoboRex, Riki, Eros, Servien, Vertrokken, UcuchaBot, BotEmpoor, Willemo, Wester2005, Klaas1978, Palica, Christoffel K, Tuvic, Jeroenbot, Chobot, RonaldB, Aleichem, Adrdui, Dolledre, Ime~nlwiki, YurikBot, Eve, Troefkaart, Luna, Daka, FlaBot, Kleuske, Gerbennn, Ninane, RobotTbc, Observer~nlwiki, Zanaq, Qampina, Thomas-, Erwin, Marco Langbroek, Vincentsc, Berendvd, Mexicano, Khx023, Kameraad Pjotr, .Koen, Mbch331, Jvhertum, SieBot, Thijs!bot, Joris, John Braun~nlwiki, Escarbot, Knelis, Ciell, Paul B, Vis met 1 oog, Antigluut, Raimon, Kanman, JAnDbot, Ilonamay, Toon Macharis, .anacondabot, Mpm, HandigeHarry, Waninge, BetBot~nlwiki, MoiraMoira, Luctor, CommonsDelinker, Jochem V, Enormekever, Jmember,

Flevotrekkie, Look Sharp!, Narayan, TottyBot, TXiKiBoT, Lymantria, Handige Harrie, Japiot, CyHe, Kosty~nlwiki, Klas3b, BotMultichill, RenéV, ErikWarmelink, 3wisemen, Lollimewirewiki, Dan008, Piratelol, Synthebot, Den Hieperboree, BjornR, Zorrobot, JohanKnol, GrouchoBot, ArjanH, Harrryberg, Tonkie, Ilse Winter, Filmfreak1, Toth, Svessum, BertJanWolfs, JurgenNL, Pompidom, Glatisant, Luckas-bot, Amirobot, MrBlueSky, Spock~nlwiki, Japiobot, JZ85, AStarBot, Turkhero~nlwiki, Marrakech, Hoopje, MauritsBot, Theobald Tiger, Mathonius, Xqbot, Saschaporsche, Rubinbot, Maasje, Pompidombot, Phasker, Smile4ever, RomaineBot, Wiki13, TBloemink, ErikvanB, MexicanoBot, EmausBot, ZéroBot, HRoestBot, The Nut, Lotje, Pipke20, Hijisk, MerlIwBot, EZ~nlwiki, DunjaP, Bj.schoenmakers, Grmbl76, Don Kedero, EnzaiBot, Dexbot, Legobot, Tulp8, MatthijsWiki, Wwian1, AxelleDejaeghere, Emmelie2394, Kaj Sustronck, KayleeClaeys, Baba2k14, Niels.Veryepe, ToonVA, Stiem22, Wicoby, Wikiwerner, DottyMcFear13, Bas1010209 en Anoniem: 106

- **Spamfilter** *Bron:* https://nl.wikipedia.org/wiki/Spamfilter?oldid=45883808 *Bijdragers:* SanderSpek, Bemoeial, RobotE, Emvee, Bdijkstra, Klever, RonaldB, YurikBot, FlaBot, Kleuske, Gerbot, Simeon, Jvhertum, Thijs!bot, Elensar87, Gertjan2, Patrickvandervalk, CommonsDelinker, Handige Harrie, VolkovBot, BotMultichill, Sswelm, Zabot, PixelBot, Luckas-bot, MrBlueSky, Saschaporsche, SassoBot, Jashaj, Smile4ever, RomaineBot, DutchDude007, Brentjee, Addbot, Wikiwerner en Anoniem: 7
- **Spoofing** *Bron:* https://nl.wikipedia.org/wiki/Spoofing?oldid=45055541 *Bijdragers:* TeunSpaans, Bemoeial, Cicero~nlwiki, Falcongj, Advance, Robbot, Theo, RobotE, Michiel1972, Dolmonly, Robotje, MichielDMN, Bdijkstra, Tomgreep, Algont, Vrijwerker, Kalsermar, Markmark~nlwiki, Emmelie, Khx023, Kameraad Pjotr, Jvhertum, SieBot, Thijs!bot, Van der Hoorn, Vis met 1 oog, EcheLoN, Loveless, JaFFoG, MattSl, Markkkje, Luckas-bot, Japiobot, MauritsBot, Mathonius, LucienBOT, Smile4ever, MrBlueBot, Bordewolf, ErikvanB, EmausBot, ZéroBot, WikitanvirBot, Iwein Janssens, AxelleDejaeghere, Perudotes en Anoniem: 14
- **Spyware** *Bron:* https://nl.wikipedia.org/wiki/Spyware?oldid=46770929 *Bijdragers:* Andre Engels, Ellywa, SanderSpek, Fruggo, Wilinckx, Cicero~nlwiki, Jeroen, BenTels, Rm, Falcongj, Puckly, Robbot, Torero, Oscar, DXL, Arnie, Taka, Michiel1972, Meneer, Jupiler, AartTeun, BenTheWikiMan, Laban, MichielDMN, Lexw, Martinus, Pjetter, JePe, Jcb, RobotQuistnix, Rex, Justhg, Ed de Jonge, Venullian, Jan o b, MADe, Ucucha, Gpvosbot, RoboRex, Riki, Vertrokken, Peter b, DJclaud, RonaldB, Dolledre, YurikBot, Troefkaart, FlaBot, Mstegeman, Maniago, Eskimbot, Op.mijn.werk, Emmelie, ElKonquistador, Funkyman~nlwiki, Mexicano, .Koen, SieBot, Thijs!bot, Metz~nlwiki, Tukka, Escarbot, JAnDbot, .anacondabot, Lambo1404, Basvb, BetBot~nlwiki, Johan N, MoiraMoira, Wetenschapsfreak, Rei-bot, YoshiDaSilva, VanBuren, AnnabelsBot, TXiKiBoT, Lymantria, VolkovBot, BotMultichill, AlleborgoBot, Sander1453, Loveless, Tgeorgescu, Wutsje, ArjanH, MwpnlBot, BOTarate, SilvonenBot, Luckas-bot, MrBlueSky, Vinnie665, XZeroBot, Mathonius, Smile4ever, Dinamikbot, ErikvanB, KamikazeBot, EmausBot, Kulter20, ChrisN, Cas8919, Sander Van Durme, MichèleD, Troedeboer, Dexbot, Legobot, Nietanoniem, Desmet dave, Robyvd, Arch, Stef Bryssinck, Kaj Sustronck, Berdieke en Anoniem: 70
- **SQL-injectie** *Bron:* https://nl.wikipedia.org/wiki/SQL-injectie?oldid=47602162 *Bijdragers:* Taka, MichielDMN, RobotQuistnix, Teunie, MADe, Riki, Chobot, Kleuske, Hansmuller, Mbch331, SieBot, Thijs!bot, Magere Hein, JAnDbot, Fogeltje, MoiraMoira, Multichill, Look Sharp!, VolkovBot, BotMultichill, Rietvogel, Sboden, DeJaVu3, DaBot~nlwiki, GrouchoBot, PixelBot, Alexbot, SilvonenBot, MastiBot, LaaknorBot, Luckas-bot, MrBlueSky, DirlBot, Xqbot, Rubinbot, Olivier Bommel, Smile4ever, Wiki13, Patrick-98, TBloemink, Woodcutterty, ErikvanB, WinContro, MexicanoBot, EmausBot, JackieBot, Manubot, Dexbot, Southparkfan, Addbot, ElodieBlancke en Anoniem: 20
- **Streaming media** *Bron:* https://nl.wikipedia.org/wiki/Streaming_media?oldid=47699743 *Bijdragers:* Patrick, Ellywa, Romaine, Bemoeial, Cicero~nlwiki, Guaka, Falcongj, Robbot, Oscar, Chris, JoJan, Mwpnl, Michiel1972, Bean 19, A3, Caseman, Jupiler, Robotje, Laban, MichielDMN, Sonuwe, Ype, Pjetter, JePe, Tdevries, Karoma, Jcb, Effeietsanders, Bajoro, Galwaygirl, T Houdijk, MADe, Robotpjetter, Johjak, RoboRex, BotEmpoor, Willemo, Annabel, Tuvic, Jeroenbot, Obarskyr, Chobot, RonaldB, Aleichem, Dolledre, Daka, Vdegroot, FlaBot, Migdejong, Geograaf, BotOx, Maniago, Kleuske, WillBot, Ninane, Zanaq, PJB~nlwiki, Erwin, Robb, Lordmarchmain, Mexicano, Jvhertum, SieBot, Bouwe Brouwer, Cyrre, Thijs!bot, Edwinb, Valhallasw-botje, Obarskyr Bot, Verstreken, WouterDevolder, JAnDbot, MoiraMoira, Look Sharp!, Grashoofd, VolkovBot, Titusn, Wimpus, Tenth Plague, Loveless, Groucho NL, GrouchoBot, AlnoktaBOT, WezyBot, MwpnlBot, Alexbot, SilvonenBot, LaaknorBot, Luckas-bot, MrBlueSky, Nfef, Japiobot, ArthurBot, RudolphousBot, Diamant, Xqbot, Pompidombot, Smile4ever, RomaineBot, MrBlueBot, ErikvanB, Raphaella~nlwiki, Queeste, MexicanoBot, EmausBot, ZéroBot, WikitanvirBot, Ebrambot, Sjoerddebruin, MerlIwBot, Malinka1, Timelezz, BobDijs, Addbot, Firstonetop1, Tulp8, Wikiwerner, Oskardebot en Anoniem: 74
- **TCP/IP** *Bron:* https://nl.wikipedia.org/wiki/TCP/IP?oldid=47834305 *Bijdragers:* Walter, TeunSpaans, Ellywa, Snoop, Romaine, Bemoeial, Puckly, Robbot, GerardM, RobotE, Bob.v.R, Danielm~nlwiki, Reinouts, DaProx, Tr606, A3, Caseman, O E P~nlwiki, GWirken, MichielDMN, El barto, Sawims, Emvee, JePe, Snaily, Ilario, Rex, Galwaygirl, T Houdijk, Joost, Algont, RoboRex, Riki, Xaviervd, DéRahier, Dartelaar, Jeroenbot, Zwobot, JörgenMoorlag, Kleuske, Gerbennn, Lavachequirit, Niels, Dogmatica, Adnergje, Whizz, Mexicano, Khx023, SieBot, Thijs!bot, Edwinb, Erik Baas, BOT-Superzerocool, JAnDbot, BetBot~nlwiki, MoiraMoira, YoshiDaSilva, Look Sharp!, Bo W, TXiKiBoT, VolkovBot, GijsvdL, Zwitser123, AlleborgoBot, Vels, Gerakibot, Den Hieperboree, Mmeerman, Groucho NL, GrouchoBot, DustSpinner, DragonBot, BodhisattvaBot, JurgenNL, Luckas-bot, MrBlueSky, Jotterbot, TaBOT-zerem, Xqbot, SassoBot, RibotBOT, Smile4ever, RomaineBot, Wiki13, RedBot, Woodcutterty, Vrpvillerius, WinContro, EmausBot, HRoestBot, Eg-T2g, MerlIwBot, Wildcat38, AvocatoBot, Grmbl76, Youbuntu, JYBot, Kippenbot1, Legobot, Tack.thibaut, Grasmat en Anoniem: 83
- **Tor (netwerk)** *Bron:* https://nl.wikipedia.org/wiki/Tor_(netwerk)?oldid=47959582 *Bijdragers:* Carol Fenijn, Jan Arkesteijn, Robbot, RobotMichiel1972, Lexw, Bios, Riki, Jos-uit-boston, YurikBot, FlaBot, JörgenMoorlag, Kleuske, Eskimbot, Verrekijker, Erwin, WiebeVanDerWorp, Vincentsc, Simeon, Woudloper, SieBot, Thijs!bot, DimiTalen, Aiko, AdnergjeBot, Erik Baas, Wammes Waggel, Basvb, EuRobert, Rei-bot, Look Sharp!, Narayan, Lymantria, Japiot, VolkovBot, 3wisemen, AlleborgoBot, GrouchoBot, Brabo SD, Westerlaken, Alexbot, SterkeBak, Toth, EvilFreD, JurgenNL, CarsracBot, LaaknorBot, Luckas-bot, Amirobot, MrBlueSky, Donny nl, Flurps, Xqbot, Smile4ever, Erik Wannee, D'ohBot, MrBlueBot, RedBot, Woodcutterty, ErikvanB, Asimov, EmausBot, ZéroBot, S0214828, Sparhawk, WikitanvirBot, Eg-T2g, Mjbmrbot, Lotje, MerlIwBot, Rezabot, Grmbl76, Altapedia, JYBot, DS21, Tsuruya, TweePassen, Addbot, Jonas7735, Meiræ, ElodieBlancke, Thejustaguy, VakoNoway, Alice2Alice, Appelsenperenenzo en Anoniem: 29
- **Trojaans paard (computers)** *Bron:* https://nl.wikipedia.org/wiki/Trojaans_paard_(computers)?oldid=46497113 *Bijdragers:* Ellywa, Lvg, Muijz, Puckly, Robbot, Känsterle, Meneer, Quistnix, MichielDMN, Lexw, Rex, Höyhens, MADe, Edoderoo, Robotpjetter, RoboRex, Riki, Vertrokken, Kwibus, DéRahier, Tuvic, Obarskyr, Chobot, RonaldB, Dolledre, Troefkaart, ArjenW, Kleuske, RobotTbc, Emiel, SanderK, .marc., Chlewbot, Adnergje, Brinkie, Gerbot, Berendvd, Mexicano, Khx023, Simeon, Mbch331, SieBot, Thijs!bot, Edwinb, Aiko, Escarbot, Robert Buzink, JAnDbot, Slipknol, MoiraMoira, SbJ, Calvinturbo, Look Sharp!, OekelWm, TXiKiBoT, Lymantria, VolkovBot, Repeater, GijsvdL, BotMultichill, 3wisemen, Zwitser123, AlleborgoBot, DaBot~nlwiki, Loveless, Freaky Fries, Nielswitte, GrouchoBot, Menke, Kthoelen, Jarii94, Beachcomber, Hans Kamp, Alexbot, EvilFreD, JurgenNL, MelancholieBot, LaaknorBot, Annaoldenhave, MrBlueSky, Ptbotgourou, Nallimbot, Flurps, RudolphousBot, Mathonius, De Wikischim, Xqbot, SassoBot, RibotBOT, Maasje, Pompidombot, Smile4ever, Wiki13, Woodcutterty, Dinamik-bot, ErikvanB, EmausBot, Bib-lost, WittePrins, Sjoerddebruin, ChrisN, MerlIwBot, AvocatoBot, Rezabot, AlbinS, Niekbuitbe, Younes1020, Qwertyasdfg~nlwiki, Addbot, Tulp8, MatthijsWiki, Tack.thibaut en Anoniem: 93

- **Uitgebreid gevalideerd SSL-certificaat** *Bron:* https://nl.wikipedia.org/wiki/Uitgebreid_gevalideerd_SSL-certificaat?oldid=44712943 *Bijdragers:* Romaine, Den Hieperboree, Smile4ever, Kloentje2, KLBot2 en Anoniem: 2
- **Update (software)** *Bron:* https://nl.wikipedia.org/wiki/Update_(software)?oldid=44358260 *Bijdragers:* Romaine, Jeroen, Wim Hamhuis, Thijs!, MichielDMN, Emvee, Ype, Ed de Jonge, Jan o b, Algont, Vertrokken, Herazio, BotOx, Ch@ss, Simeon, EdBever, Xfactor, Leopard, VanBuren, AnnabelsBot, Siskus, MrBlueSky, Edoderoobot, Smile4ever, Eg-T2g, Wenneke1981 en Anoniem: 5
- **Valse beveiligingssoftware** *Bron:* https://nl.wikipedia.org/wiki/Valse_beveiligingssoftware?oldid=47195517 *Bijdragers:* Kattenkruid, Maniago, VolkovBot, ErikvanB, Mcstabberd, MerlIwBot, Pieterjan E, Tine26, Danuta, Gamefreak23, Addbot, DiamantBot en Anoniem: 2
- **Videokaart** *Bron:* https://nl.wikipedia.org/wiki/Videokaart?oldid=47794195 *Bijdragers:* Andre Engels, Ellywa, Romaine, Wilinckx, BenTels, Garo~nlwiki, Muijz, HooftBot, Advance, Robbot, Hashar, Andries, RobotE, Chris, Taka, Quistnix, Kagaherk, Robotje, BenTheWikiMan, MichielDMN, Speur, RJB, Lexw, Yorian, JePe, Fuss, RobotQuistnix, LimoWreck, Ed de Jonge, JeroenvB, Tomgreep, Venullian, Marcieking, Abnormaal, Joost, Edoderoo, Gadget~nlwiki, RoboRex, DaPowerBoy, Kheowkul, Vertrokken, Palica, Yvesn, Obarskyr, RonaldB, Dolledre, Sdomburg, YurikBot, Eve, Geograaf, Ronaldvd, Gerbennn, Eskimbot, Fr33ke, Quasar3D, SanderK, Robb, Simeon, Vesennas, SieBot, Thijs!bot, Rein N., Yoong, Magere Hein, Davin, Paul B, JAnDbot, Hniep57, BetBot~nlwiki, Johan N, MoiraMoira, CommonsDelinker, Duijker, Look Sharp!, Felix2036, DodekBot, TXiKiBoT, Lymantria, Handige Harrie, VolkovBot, BotMultichill, Marc84, Rmfloris, MichaelBoogaard, DaBot~nlwiki, Emiel.molenaar, UIC2, Louperibot, Erik Joling, Den Hieperboree, Wutsje, Richardkiwi, Zorrobot, SilvonenBot, Toth, CaseModder, MelancholieBot, D-virus, DrFO.Tn.Bot~nlwiki, Luckas-bot, MystBot, MrBlueSky, Gelu92, Xeranos, Chosen1~nlwiki, Japiobot, Megabeat, MauritsBot, Hans Hoogglans, Xqbot, RibotBOT, Pompidombot, RomaineBot, Twiss~nlwiki, Wiki13, JurriaanH, ReinaartBot, Fnator, Later42, EmausBot, HRoestBot, O0Rollo0o, Erik009, ChuispastonBot, MerlIwBot, Rezabot, Grmbl76, Natuur12, Maartenschrijft, Legobot, Selime, Kukkie, MatthijsWiki, Wikiwerner, Oxygene7-13, Ronnie PG en Anoniem: 116
- **Virtueel Particulier Netwerk** *Bron:* https://nl.wikipedia.org/wiki/Virtueel_Particulier_Netwerk?oldid=47775795 *Bijdragers:* Patrick, Evanherk, Bemoeial, Carol Fenijn, HooftBot, Robbot, RonOnrust, Vvim~nlwiki, Robotje, RobotQuistnix, Rex, RoboRex, Riki, China Crisis, YurikBot, LeonardoRob0t, FlaBot, Maniago, Kleuske, Rickpastoor, Zanaq, Verrekijker, RoboDick~nlwiki, Caudex Rax, Chingon, Street011, Gerbot, Mexicano, Simeon, Jvhertum, SieBot, Thijs!bot, Escarbot, Maiella, MoiraMoira, Iooryz, Rei-bot, AnnabelsBot, TXiKiBoT, Lymantria, Benlan, Japiot, VolkovBot, AlleborgoBot, Sander1453, Ibbeltje, Loveless, Louperibot, Ken123BOT, Jarune, Richardkiwi, BjornR, Zorrobot, GrouchoBot, Philippe Belet, AlnoktaBOT, Carsrac, Tonkie, Alexbot, Mike.lifeguard, CarsracBot, Mercy, Luckas-bot, MystBot, Ptbotgourou, ArthurBot, RudolphousBot, DirlBot, MagnusA.Bot, Mathonius, Xqbot, Rubinbot, Pompidombot, RomaineBot, D'ohBot, S.collet, ErikvanB, Queeste, Wester, EleferenBot, EmausBot, Onzichtbaar, MerlIwBot, Djbranco, Legobot, StroopwafelBot, Edehaan en Anoniem: 48
- **Virtuele gemeenschap** *Bron:* https://nl.wikipedia.org/wiki/Virtuele_gemeenschap?oldid=46642983 *Bijdragers:* SanderSpek, Jeroen, Robbot, Siebrand, RobotMichiel1972, Fuss, Dedalus, Vertrokken, RonaldB, YurikBot, Apdency, BotOx, Maniago, Amenophis, Mexicano, SieBot, Thijs!bot, FakirNL, Davin, JAnDbot, Pelikana, DodekBot, Handige Harrie, VolkovBot, BotMultichill, Zwitser123, Gerakibot, GrouchoBot, PixelBot, AnokoBOT, Alexanderziegler, Waltervos84, Luckas-bot, MrBlueSky, ArthurBot, De Wikischim, Diamant, Xqbot, Pompidombot, Smile4ever, Kees.haverkamp, ErikvanB, Bubbly, EmausBot, ChuispastonBot, MerlIwBot, Tine26, Vawa, Kwuekn, Nielsja123, Manu De Pourcq, Ilse reeper, Danuta, Legobot, Addbot, Finishing Touch, Niels.Veryepe en Anoniem: 16
- **Wachtwoord** *Bron:* https://nl.wikipedia.org/wiki/Wachtwoord?oldid=46980521 *Bijdragers:* Ellywa, Carol Fenijn, Muijz, Siebrand, Taka, Meneer, MichielDMN, Fuss, RobotQuistnix, JeroenvB, Joost, MADe, Kiwix, RoboRex, Door de wol geverfd, Vertrokken, Yvesn, Dé-Rahier, Dake~nlwiki, YurikBot, Kleuske, Fr33ke, BranMoviC, Melsaran, Erwin, Bb, Foxie001, Paulus 2, Halandinh, Warddr, Mexicano, Khx023, Simeon, .Koen, SieBot, Thijs!bot, Erwin85Bot, Davin, JAnDbot, VanBuren, WarddrBOT, TXiKiBoT, Grashoofd, Handige Harrie, VolkovBot, BotMultichill, RenéV, AlleborgoBot, Dgregoire, Mar(c), Timk70, Alexbot, Friedricheins, FlippyFlink, MastiBot, Luckasbot, Amirobot, Donny nl, Flurps, ArthurBot, Xqbot, Olivier Bommel, DickOZ, Erik Wannee, RomaineBot, RedBot, Mattias.Campe, EmausBot, ZéroBot, HRoestBot, ChuispastonBot, Lotje, ChrisN, EZ~nlwiki, Vagobot, Rezabot, Rvaneerde, Stijn.Berghmans, Addbot, Kukkie, 12345danNL, Dick99999, KehppKukkieBot en Anoniem: 19
- **Webbrowser** *Bron:* https://nl.wikipedia.org/wiki/Webbrowser?oldid=46721533 *Bijdragers:* Andre Engels, TeunSpaans, Christian List, Youssefsan, Rob Hooft, Rene Pijlman, Jammers, Frenzie, Romaine, Glenn, Wilinckx, Jeroen, BenTels, Christiaan~nlwiki, HooftBot, Robbot, Nikai, RobotE, Johi, Danielm~nlwiki, Reinouts, Wietse Venema, Taka, DaProx, Omegium, A3, O E P~nlwiki, Robotje, MartV, Guanabot~nlwiki, MichielDMN, Lexw, Joris Gillis, Fuss, JimmyShelter, RobotQuistnix, -Lars-, LimoWreck, Freek Verkerk, Bert76, Neutraal, MADe, Kiwix, Robotpjetter, RoboRex, Klemen Kocjancic, Riki, Willemo, Klaas1978, Christoffel K, Jeroenbot, RonaldB, Zwobot, Dolledre, BertK, YurikBot, Cepheus, FlaBot, Maniago, Kleuske, Gerbennn, Eskimbot, RobotTbc, Golradir, RoboDick~nlwiki, Hermanberghuis, Fontes, Flying Dutchman, Whizz, Simeon, .Koen, Jvhertum, SieBot, Thijs!bot, Erwin85Bot, Erik Baas, Hajo, Escarbot, Erik1980, Heer van Robaais, PJ Geest, BOT-Superzerocool, JAnDbot, MoiraMoira, Rei-bot, RobIII, AnnabelsBot, TXiKiBoT, VolkovBot, BotMultichill, RenéV, AlleborgoBot, Synthebot, Tleilax, Idioma-bot, Mar(c), Loveless, Arend41, TahR78, PipepBot, Zorrobot, GrouchoBot, Kroose, DragonBot, AlnoktaBOT, Darkicebot, Capaccio, AnokoBOT, SilvonenBot, Alecs.bot, MelancholieBot, Pjkoning, Pompidom, Kwiki, PauloCalipari, LaaknorBot, Luckas-bot, MrBlueSky, Nallimbot, Jotterbot, Peterson, ArthurBot, FoxBot, Xqbot, Rubinbot, LucienBOT, Smile4ever, Rik van Doorn, Stero~nlwiki, Reallyniceandstuff, ButkoBot, RedBot, Mooi is de wereld, TobeBot, Camoka4, WinContro, MexicanoBot, EmausBot, HRoestBot, 1Veertje, WikitanvirBot, MerlIwBot, DutchHoratius, Kloentje2, Legobot, DhrLorenzo, NielsAC en Anoniem: 54
- **Weblog** *Bron:* https://nl.wikipedia.org/wiki/Weblog?oldid=47902416 *Bijdragers:* Andre Engels, Walter, Patrick, Dimi15, Marza, Ellywa, Rob Hooft, Youandme, Frenzie, Fruggo, Bemoeial, Guaka, Jeroen, Marijke, BenTels, Falcongj, Stonehead~nlwiki, Puckly, Waerth, Serassot, Ben~nlwiki, HooftBot, Advance, Robbot, DarkHorse, Stafhorst, Kattenkruid, Oscar, RobotE, Siebrand, IMFJ, Känsterle, Ciciban, RonaldW, Mwpnl, Michiel1972, Meneer, Martijnvanes, Bean 19, Robotje, BenTheWikiMan, Laban, Hardscarf, Lexw, Pieter1, Pjetter, JePe, Ronn, MigGroningen, Arvid, Tdevries, Karoma, Bstorm~nlwiki, Apampakai, Gpvos, Dolfy, RobotQuistnix, Vitum, Siegbru, Effeietsanders, Rex, Justhg, Qwertyus, Wikix-oud, Kevin P Kelly~nlwiki, Venullian, Bert76, Joost, Nevargmij, MADe, Edoderoo, Ucucha, Just a member, Robotpjetter, Algont, RoboRex, Vertrokken, Husky, Willemo, DJclaud, AlexP, Christoffel K, Tuvic, Obarskyr, Tubantia, Chobot, RonaldB, Ietskleiner, Aleichem, Dolledre, YurikBot, Joop1234, Eve, MarQ, FlaBot, Geograaf, Maniago, Kleuske, BesselDekker, Ukkie, Ninane, Eskimbot, Fr33ke, Mel~nlwiki, GeeJee, Zanaq, SanderK, .marc., Melsaran, Qampina, Kassia~nlwiki, Thomas-, Quis, Ericos~nlwiki, Studiosus.nl, Antonie, Gorhendad, JorisvS, MasterAb, DrsYell, Warddr, Verbaljam, Mexicano, Simeon, Simon-sake, Indeed (hernoemd), Kameraad Pjotr, Hansmuller, EdBever, Amor~nlwiki, Spafu, .Koen, Jvhertum, CrazyPhunk, SieBot, Thijs!bot, Joris, Edwinb, Aiko, AdnergjeBot, Axel Molit, Tukka, Shovel~nlwiki, Casperinfo, Sobaka, Erik1980, TTS, BOT-Superzerocool, Davin, Arie b, Devlas, Machaerus, Tachtiger, Rohtop, A Duck, Yosephus, ErikEngerd, BetBot~nlwiki, Lenos, MoiraMoira, CrazyPhunkbot, Freaky, Leopard,

Agora, Getty, SbJ, Felix2036, Jm~nlwiki, MoehMan, Waldorfer, WarddrBOT, Oldname154, TXiKiBoT, Cutepoison, RNts, VolkovBot, Erik2007~nlwiki, Henniew, Le Fou, LVX, Merrin, GijsvdL, BotMultichill, Rob621123, 3wisemen, Die vandaal, AlleborgoBot, Vels, Synthebot, Sander1453, Bloghier.nl, Loveless, Freaky Fries, Sswelm, Byrialbot, A.a.dehaan, Wutsje, PieterJansegers, GrouchoBot, Kthoelen, AlnoktaBOT, PieterJanR, Dln, Alexbot, Robhaesn, SilvonenBot, Toth, MelancholieBot, Pompidom, Kwiki, Luckas-bot, MrBlueSky, Italrob, Galoubet, Edoderoobot, Hoopje, ArthurBot, TaBOT-zerem, Flinus, Durdane, FoxBot, Xqbot, Saschaporsche, RibotBOT, Maasje, Stahert, Pompidombot, Smile4ever, RomaineBot, Raast, Wiki13, ButkoBot, Heureka, TobeBot, Dinamik-bot, ErikvanB, Blackpen, DixonDBot, Tyneverum, EmausBot, Whaledad, YNhuis, ZéroBot, HRoestBot, VR-Land, DieED, Erik009, WikitanvirBot, Spco-mark, Lotje, ChrisN, Dinosaur918, Sikjes, Bvlg, MerlIwBot, Bertmeert, Nummer 12, AvocatoBot, Rezabot, HiW-Bot, Tine26, Neanderen, Grmbl76, Extinguished Fire, WOLF LΛMBERT, Jaap K, Maudmaudmaud, TheDragonhunter, Addbot, Maartje Boshuizen, Ymnes, Kukkie, Aronprins, Annick2000, MatthijsWiki, Kaj Sustronck, SimonD.M, Popo johan, EtienneRozenblad, Joyce van de Pas en Anoniem: 265

- **Website** *Bron:* https://nl.wikipedia.org/wiki/Website?oldid=46470489 *Bijdragers:* Andre Engels, Patrick, Erik Zachte, Evanherk, Rob Hooft, Wilinckx, Pieterse16, Streppel, Puckly, Serassot, HooftBot, Advance, Robbot, PrisonerOfPain, RobotE, Johan Lont, AlfonsVH, MartinD, Taka, Wurblzap~nlwiki, Michiel1972, Guanabot~nlwiki, MichielDMN, Lexw, Ronn, Tdevries, LimoWreck, Freek Verkerk, Edelwater, Abnormaal, RoboRex, Theun, Door de wol geverfd, Riki, Servien, Vertrokken, Husky, Klaas1978, Tilanus, Tuvic, RonaldB, Corriebert, Moartn, Dkamm~nlwiki, Apdency, Cyberdots, Charles de Vilder~nlwiki, Maniago, Kleuske, BesselDekker, WillBot, SanderK, Thomas-, Sumurai8, Sonty567, Erwin, Mion, Robb, Adnergje, Thijs nl, Berendvd, Mexicano, Simeon, EdBever, .Koen, CrazyPhunk, SieBot, Edwinb, George4, Tukka, Escarbot, Madyno, Heer van Robaais, John2, Paul B, Wtje, JAnDbot, Machaerus, Jan Storms~nlwiki, Clockwork Orange, Johan N, MoiraMoira, Kruidnagel, CrazyPhunkbot, Ken123, Look Sharp!, OekelWm, AnnabelsBot, WarddrBOT, Rudolphous, Lymantria, VolkovBot, Andries Van den Abeele, Hajo1972, GijsvdL, RenéV, Jjbroekema, Synthebot, Lolsimon, Idioma-bot, Loveless, Freaky Fries, Thomas Desmet, GyoTo, Richardkiwi, Zorrobot, Ilse.vermeulen01, GrouchoBot, Julesp~nlwiki, Koenieboy97, EvilFreD, CarsracBot, Pompidom, Richy987, Kwiki, Naudefj, Luckas-bot, MystBot, Amirobot, MrBlueSky, Goudsbloem, Galoubet, AStarBot, Edoderoobot, Vdkdaan, Mathonius, FoxBot, Xqbot, Saschaporsche, Rubinbot, Elkan, Pompidombot, Smile4ever, RomaineBot, Mpvdm, Wiki13, RedBot, Huhbakker, JurriaanH, ErikvanB, KamikazeBot, TjBot, Wester, Maximmaster, EmausBot, Savh, ZéroBot, WikitanvirBot, Delay, Sjoerddebruin, Lotje, ChrisN, Clearminds, Vagobot, Malinka1, KafiRobot, Grmbl76, Minsbot, Extinguished Fire, Steinsplitter, Legobot, Nietanoniem, Tulp8, Arch, MatthijsWiki, ElodieBlancke, Yolo-Brian en Anoniem: 96
- **Whois** *Bron:* https://nl.wikipedia.org/wiki/Whois?oldid=42697438 *Bijdragers:* SanderSpek, Bontenbal, Bartux, PrisonerOfPain, RobotE, Danielm~nlwiki, Chris, Sam Hocevar, Alicey, GWirken, RobotMichiel1972, Henks, RobotQuistnix, MADe, Robotpjetter, RoboRex, Willemo, Christoffel K, DéRahier, YurikBot, Sonett72~nlwiki, FlaBot, Diagraph01, Kleuske, Eskimbot, Mexicano, .Koen, Thijs!bot, Cadezo, ErikRomijn, JAnDbot, BotMultichill, AlleborgoBot, RubySS, Mdavids, GrouchoBot, DragonBot, Tonkie, Broadbot, Pompidom, Luckas-bot, Ptbotgourou, Xqbot, RibotBOT, Pompidombot, Smile4ever, Ida Shaw, Dinamik-bot, ZéroBot, Dilic, Legobot, Casperw93 en Anoniem: 23
- **Wi-Fi** *Bron:* https://nl.wikipedia.org/wiki/Wi-Fi?oldid=47275757 *Bijdragers:* Rob Hooft, Ronald, Rene Pijlman, Math1985, Guaka, Jeroen, BenTels, Pieterse16, Carol Fenijn, Serassot, Panthouse, Advance, Robbot, RonOnrust, Bontenbal, GerardM, Stafhorst, Towgun, Truckerruud, Edwtie, Michiel1972, Quistnix, Martijn, Ewoudhuysmans, MichielDMN, Andre.blum, Lexw, Emvee, Pieter1, JePe, Tdevries, Tenthije, Elreteipos, Gpvos, RobotQuistnix, Galwaygirl, Joost, MADe, Edoderoo, RoboRex, Riki, BotEmpoor, Willemo, Christoffel K, Enschede, Dolfijn, Tuvic, Geertivp, RonaldB, Daniel575, Dolledre, Bart l~nlwiki, Jos-uit-boston, Job Bouwman, Troefkaart, Apdency, FlaBot, Maniago, Kleuske, Ninane, SanderK, Verrekijker, Sumurai8, Chlewbot, Roel Schreurs, Jandeboer, Vincentsc, Fontes, Flying Dutchman, Mexicano, Simeon, .Koen, SieBot, Thijs!bot, Joris, Edwinb, Aiko, Tukka, Bram wouda, Valhallasw-botje, FakirNL, Jverveer, Schuf06, Hweerman, Fjvelsen, JAnDbot, Igor.passchier, JeroenvanVeen, MoiraMoira, BotteHarry, Look Sharp!, TXiKiBoT, Jerin, San jose0, BotMultichill, Silver Spoon, TaalVerbeteraar~nlwiki, Ctm, 3wisemen, Sander1453, Louperibot, Butch, GrouchoBot, Kthoelen, Gohan71, Phsmit, Spoorjan, Kbrouwer, Tim van overtveldt, D.boerlage, Wouter Demonie, Rjkasteel, Gwiki~nlwiki, Toth, Pompidom, Akoopal, Kwiki, Huubsch, Luckas-bot, MrBlueSky, Japiobot, Antennebureau, ArthurBot, TaBOT-zerem, Mathonius, De Wikischim, Obersachsebot, FoxBot, Pompidombot, Spraakverwarring, Phasker, Smile4ever, RomaineBot, Jgamleus, Danuss, Wiki13, Ida Shaw, Dinamik-bot, JurriaanH, ErikvanB, TWHIT, EmausBot, HRoestBot, T'Phon, WikitanvirBot, Eg-T2g, Delay, Lotje, DeGilian, MerlIwBot, Xatr2, Can't buy me lunch, Timelezz, Supercarwaar, Kippenbot1, Legobot, Amorada2012, Lucashub, Tulp8, StroopwafelBot, Wikiwerner, Oxygene7-13, Hpted, Wikidevnl, Ronnie PG, Brave zebra en Anoniem: 144
- **Witwassen** *Bron:* https://nl.wikipedia.org/wiki/Witwassen?oldid=47459036 *Bijdragers:* Andre Engels, Patrick, Robbot, Johan Lont, Bob.v.R, Michiel1972, Ype, RobotQuistnix, T Houdijk, Gpvosbot, RoboRex, Riki, Vertrokken, AlexP, DéRahier, WebBot, YurikBot, Apdency, Isopokelil, Maniago, Kleuske, SanderK, Gerbot, Kameraad Pjotr, Mbch331, Jvhertum, SieBot, Thijs!bot, Jvbq, Maiella, Sint Aldegonde, LuRobby, Johan N, MoiraMoira, Wimmel, VanBuren, Endorf, TXiKiBoT, Lymantria, Aibot, VolkovBot, Phenoss, Idioma-bot, Louperibot, Zorrobot, GrouchoBot, AGL, BodhisattvaBot, SilvonenBot, Toth, JurgenNL, Pompidom, Astrion, Luckas-bot, MystBot, Ptbotgourou, Nallimbot, Hoopje, Xqbot, Rubinbot, DumZiBoT, Pompidombot, TBloemink, Dinamik-bot, ReinaartBot, MexicanoBot, DixonDBot, EmausBot, ZéroBot, WikitanvirBot, Mjbmrbot, Danielnl, ZeaForUs, Garant, Legobot, Tulp8, Oxygene7-13 en Anoniem: 42
- **ZigBee** *Bron:* https://nl.wikipedia.org/wiki/ZigBee?oldid=46561091 *Bijdragers:* Robbot, Stefan Mensink, MichielDMN, Chobot, MoiraMoira, Rudolphous, TXiKiBoT, JacobH, BotMultichill, GrouchoBot, Cocco Bill, Tim van overtveldt, Jeroendoggen, Alexbot, FRvanderVeen, BodhisattvaBot, Pompidom, LaaknorBot, Xqbot, RomaineBot, EmausBot, ZéroBot, Woutifier, Minsbot, Addbot, JP001, StroopwafelBot en Anoniem: 12
- **ZIP (bestandstype)** *Bron:* https://nl.wikipedia.org/wiki/ZIP_(bestandstype)?oldid=47787189 *Bijdragers:* Andre Engels, Amarant, Evanherk, Ezel, Bemoeial, Wilinckx, BenTels, Ben~nlwiki, Kozmoz, HooftBot, Robbot, Siebrand, Michiel1972, Quistnix, Jouke Witteveen, Robotje, BenTheWikiMan, Laban, MichielDMN, Emvee, Henks, RobotQuistnix, LimoWreck, Ed de Jonge, RoboRex, Richardw, Riki, TuvicBot, YurikBot, FlaBot, Willemvanbeirendonck, WillBot, Ninane, RobotTbc, Simeon, EdBever, .Koen, SieBot, Madyno, JAnDbot, Rei-bot, Look Sharp!, Rudolphous, TXiKiBoT, VolkovBot, GijsvdL, BotMultichill, Zwitser123, AylaAsperger, AlleborgoBot, Luc everse, GrouchoBot, DragonBot, PixelBot, AbiBot, LaaknorBot, Luckas-bot, MystBot, Hans Hoogglans, RudolphousBot, Xqbot, Smile4ever, RedBot, Blackpen, EmausBot, Dexbot, Legobot, Wikiwerner en Anoniem: 19
- **Zoekmachine** *Bron:* https://nl.wikipedia.org/wiki/Zoekmachine?oldid=47403463 *Bijdragers:* Andre Engels, Walter, Patrick, Greco, Ellywa, Evanherk, Frenzie, Romaine, SanderSpek, Bemoeial, Wilinckx, BenTels, HooftBot, Advance, Robbot, Homeros, RobotE, Rasbak, Arrowman, O E P~nlwiki, Guusvonscheven, Robotje, BenTheWikiMan, MichielDMN, CaAl, Hardscarf, RobotMichiel1972, Mdd, Pjetter, Bee, Evil berry, RobotQuistnix, Effeietsanders, LimoWreck, Justhg, Henna, T Houdijk, MADe, RoboRex, Riki, AlexP, China Crisis, Christoffel K, Tuvic, Obarskyr, Chobot, RonaldB, Dolledre, YurikBot, FlaBot, JörgenMoorlag, Ronaldvd, Kleuske, Eskimbot, KittenKlub~nlwiki, Zanaq, SanderK, Thomas-, Mion, Robb, LeeGer, Foxie001, Mmeulens, Gerbot, Lodewijk123, Berkoet, Simeon, Ugur Basak Bot~nlwiki, EdBever, .Koen, SieBot, Thijs!bot, AdnergjeBot, Hajo, Daimanta, Tvdm, Erik1980, Magere Hein, Ciell, Rikipedia,

Peter@vdgraaf.info, Ariekers, JAnDbot, Machaerus, Freestyle, BeMe~nlwiki, MoiraMoira, Crazyhouses, Ken123, Corné van Dorp, Look Sharp!, StefanKroon, AnnabelsBot, Rudolphous, Libr~nlwiki, YewBowman, TXiKiBoT, VolkovBot, BotMultichill, Erasmus123, RenéV, 3wisemen, AlleborgoBot, Synthebot, Idioma-bot, Koektrommel, Groucho NL, PipepBot, Zorrobot, GrouchoBot, Jaap7, BOTarate, Zwaja, Species8473~nlwiki, Alex&Sjeel, Wim van Ingen, C01der, Jaakdeneve, PeHa, Pompidom, Glatisant, MrBlueSky, Hoopje, MauritsBot, ArthurBot, FoxBot, Xqbot, Muism4t, DumZiBoT, Pompidombot, RomaineBot, Wiki13, RedBot, TobeBot, JurriaanH, ErikvanB, EmausBot, HRoestBot, FeyBart, Lotje, Scholier, AvocatoBot, TBM, LodeBogaert, Southparkfan, Legobot, Benniedom, Sinterklaasismaao, Wikiwerner, Anneke de non, Svenius85 en Anoniem: 86

110.9.2 Afbeeldingen

- **Bestand:14-06-11-ssd-RalfR-N3S_7886-03.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/e/e9/14-06-11-ssd-RalfR-N3S_7886-03.jpg *Licentie:* GFDL 1.2 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Ralf Roletschek
- **Bestand:2008_Intel_Developer_Forum_Taiwan_Day2_Showcase_Intel_SSD_Prototype.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/8/80/2008_Intel_Developer_Forum_Taiwan_Day2_Showcase_Intel_SSD_Prototype.jpg *Licentie:* CC BY-SA 4.0-3.0-2.5-2.0-1.0 *Bijdragers:* Rico Shen *Oorspronkelijke artiest:* Rico Shen
- **Bestand:Aanmelden_Wikipedia.PNG** *Bron:* https://upload.wikimedia.org/wikipedia/commons/6/61/Aanmelden_Wikipedia.PNG *Licentie:* CC BY-SA 3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* MADe
- **Bestand:Abit-kt7-large.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/a/a6/Abit-kt7-large.jpg *Licentie:* CC0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Gary Houston
- **Bestand:Aeroporto_Porto_11.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/5/59/Aeroporto_Porto_11.jpg *Licentie:* CC BY-SA 3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Manuel de Sousa
- **Bestand:African_american_male_selfie.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/0/00/African_american_male_selfie.jpg *Licentie:* CC BY-SA 3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* User:Frassman
- **Bestand:An_example_of_theoretical_DNS_recursion-nl.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/8/86/An_example_of_theoretical_DNS_recursion-nl.svg *Licentie:* Public domain *Bijdragers:* Eigen werk + Image:An example of theoretical DNS recursion.svg *Oorspronkelijke artiest:* GWirken op de Nederlandstalige Wikipedia
- **Bestand:Angry.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/5/5c/Angry.png *Licentie:* CC-BY-SA-3.0 *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:Apple2.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/7/74/Apple2.jpg *Licentie:* CC-BY-SA-3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Rolf Schmidt (RolfS)
- **Bestand:Bluetooth_logo_on_mouse_from_aside.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/1/1a/Bluetooth_logo_on_mouse_from_aside.jpg *Licentie:* CC BY-SA 3.0 *Bijdragers:* eigene Arbeit – own work *Oorspronkelijke artiest:* Standardizer
- **Bestand:Blush.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/3/36/Blush.png *Licentie:* CC-BY-SA-3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Piolinfax
- **Bestand:BusNetwerk.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/a/a3/BusNetwerk.png *Licentie:* CC-BY-SA-3.0 *Bijdragers:* Originally from nl.wikipedia; description page is/was here. *Oorspronkelijke artiest:* Original uploader was PrisonerOfPain at nl.wikipedia Later versions were uploaded by Edwtie at nl.wikipedia.
- **Bestand:Chip-antenne.JPG** *Bron:* https://upload.wikimedia.org/wikipedia/commons/8/80/Chip-antenne.JPG *Licentie:* CC BY 3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* TestAccount1234
- **Bestand:Chips.JPG** *Bron:* https://upload.wikimedia.org/wikipedia/commons/6/6a/Chips.JPG *Licentie:* CC BY-SA 3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Sterkebak
- **Bestand:Cisco_router_WPS_button.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/3/3d/Cisco_router_WPS_button.jpg *Licentie:* CC BY-SA 3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* ArnoldReinhold
- **Bestand:ClamWin_0.90_Scan_Screen.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/d/d2/ClamWin_0.90_Scan_Screen.png *Licentie:* GPL *Bijdragers:* Screenshot *Oorspronkelijke artiest:* ClamWin team
- **Bestand:Cloud_computing_nl.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/9/92/Cloud_computing_nl.svg *Licentie:* CC BY-SA 3.0 *Bijdragers:* File:Cloud computing.svg / Translation: Eigen werk *Oorspronkelijke artiest:* Icons:Tango!-Project / Layout:Sam Johnston / Translation: Wikibelgiaan
- **Bestand:Commons-logo.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/4/4a/Commons-logo.svg *Licentie:* Public domain *Bijdragers:* This version created by Pumbaa, using a proper partial circle and SVG geometry features. (Former versions used to be slightly warped.) *Oorspronkelijke artiest:* SVG version was created by User:Grunt and cleaned up by 3247, based on the earlier PNG version, created by Reidab.
- **Bestand:Confused.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/6/68/Confused.png *Licentie:* Artistic 2.0 *Bijdragers:* kde-look.org *Oorspronkelijke artiest:* kborrey
- **Bestand:Cry.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/d/d8/Cry.png *Licentie:* Artistic 2.0 *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:DHCP-lease-voorbeeld.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/5/54/DHCP-lease-voorbeeld.png *Licentie:* CC0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Endaargaanweweer
- **Bestand:DHCPDORA.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/0/0d/DHCPDORA.png *Licentie:* CC0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Endaargaanweweer
- **Bestand:DNS-names-ru.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/c/cb/DNS-names-ru.svg *Licentie:* CC BY-SA 1.0 *Bijdragers:* File:Dns-raum.svg *Oorspronkelijke artiest:* George Shuklin, based on work of User:Hank van Helvete
- **Bestand:Embedded_World_2014_SSD.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/6/65/Embedded_World_2014_SSD.jpg *Licentie:* CC0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Ordercrazy

- **Bestand:Emoticons_Puck_1881.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/5/59/Emoticons_Puck_1881.png *Licentie:* Public domain *Bijdragers:* Cropped from Image:Puck No212 p64f.png. Originally published in *Puck* no. 212, p. 65. *Oorspronkelijke artiest:* Unknown typesetter/author of *Puck*
- **Bestand:Extendedvalidation.PNG** *Bron:* https://upload.wikimedia.org/wikipedia/commons/7/74/Extendedvalidation.PNG *Licentie:* MPL 1.1 *Bijdragers:* Transferred from en.wikipedia to Commons by User:Sreejithk2000 using CommonsHelper. *Oorspronkelijke artiest:* Thompson.matthew at en.wikipedia
- **Bestand:Face-grin.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/b/bc/Face-grin.svg *Licentie:* Public domain *Bijdragers:* The Tango! Desktop Project *Oorspronkelijke artiest:* The people from the Tango! project
- **Bestand:Face-plain.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/d/df/Face-plain.svg *Licentie:* Public domain *Bijdragers:* The Tango! Desktop Project *Oorspronkelijke artiest:* The people from the Tango! project
- **Bestand:Firefox_Cookie_Manager.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/6/6e/Firefox_Cookie_Manager.png *Licentie:* MPL 1.1 *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:Flag_of_Australia.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/b/b9/Flag_of_Australia.svg *Licentie:* Public domain *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Ian Fieggen
- **Bestand:Flag_of_Bahrain.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/2/2c/Flag_of_Bahrain.svg *Licentie:* Public domain *Bijdragers:* http://www.moci.gov.bh/en/KingdomofBahrain/BahrainFlag/ *Oorspronkelijke artiest:* Source: Drawn by User:SKopp, rewritten by User:Zscout370
- **Bestand:Flag_of_Belarus.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/8/85/Flag_of_Belarus.svg *Licentie:* Public domain *Bijdragers:* http://www.tnpa.by/ViewFileText.php?UrlRid=52178&UrlOnd=%D1%D2%C1%20911-2008 *Oorspronkelijke artiest:* Zscout370
- **Bestand:Flag_of_Cuba.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/b/bd/Flag_of_Cuba.svg *Licentie:* Public domain *Bijdragers:* Drawn by User:Madden *Oorspronkelijke artiest:* see below
- **Bestand:Flag_of_Egypt.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/f/fe/Flag_of_Egypt.svg *Licentie:* CC0 *Bijdragers:* From the Open Clip Art website. *Oorspronkelijke artiest:* Open Clip Art
- **Bestand:Flag_of_Eritrea.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/2/29/Flag_of_Eritrea.svg *Licentie:* CC0 *Bijdragers:* From the Open Clip Art website. *Oorspronkelijke artiest:* [[user:]]
- **Bestand:Flag_of_France.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/c/c3/Flag_of_France.svg *Licentie:* Public domain *Bijdragers:* http://web.archive.org/web/*/http://www.diplomatie.gouv.fr/de/frankreich_3/frankreich-entdecken_244/portrat-frankreichs_247/die-symbole-der-franzosischen-republik_260/trikolore-die-nationalfahne_114.html *Oorspronkelijke artiest:* This graphic was drawn by SKopp.
- **Bestand:Flag_of_Iran.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/c/ca/Flag_of_Iran.svg *Licentie:* Public domain *Bijdragers:* URL http://www.isiri.org/portal/files/std/1.htm and an English translation / interpretation at URL http://flagspot.net/flags/ir'.html *Oorspronkelijke artiest:* Various
- **Bestand:Flag_of_Libya.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/0/05/Flag_of_Libya.svg *Licentie:* Public domain *Bijdragers:* File:Flag of Libya (1951).svg *Oorspronkelijke artiest:* De broncode van dit SVG-bestand is deugdelijk.
- **Bestand:Flag_of_Malaysia.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/6/66/Flag_of_Malaysia.svg *Licentie:* Public domain *Bijdragers:* Create based on the Malaysian Government Website (archive version)
Oorspronkelijke artiest: SKopp, Zscout370 and Ranking Update

- **Bestand:Flag_of_Myanmar.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/8/8c/Flag_of_Myanmar.svg *Licentie:* CC0 *Bijdragers:* Open Clip Art *Oorspronkelijke artiest:* Onbekend
- **Bestand:Flag_of_North_Korea.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/5/51/Flag_of_North_Korea.svg *Licentie:* Public domain *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Zscout370
- **Bestand:Flag_of_Russia.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/f/f3/Flag_of_Russia.svg *Licentie:* Public domain *Bijdragers:* Государственный флаг Российской Федерации. Цвета флага: (Blue - Pantone 286 C, Red - Pantone 485 C) взяты из [1][2][3][4] *Oorspronkelijke artiest:* Zscout370
- **Bestand:Flag_of_Saudi_Arabia.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/0/0d/Flag_of_Saudi_Arabia.svg *Licentie:* CC0 *Bijdragers:* the actual flag *Oorspronkelijke artiest:* Onbekend
- **Bestand:Flag_of_South_Korea.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/0/09/Flag_of_South_Korea.svg *Licentie:* Public domain *Bijdragers:* Ordinance Act of the Law concerning the National Flag of the Republic of Korea, Construction and color guidelines (Russian/English) *Oorspronkelijke artiest:* Various
- **Bestand:Flag_of_Sri_Lanka.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/1/11/Flag_of_Sri_Lanka.svg *Licentie:* Public domain *Bijdragers:* SLS 693 - National flag of Sri Lanka *Oorspronkelijke artiest:* Zscout370
- **Bestand:Flag_of_Syria.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/5/53/Flag_of_Syria.svg *Licentie:* Public domain *Bijdragers:* see below *Oorspronkelijke artiest:* see below
- **Bestand:Flag_of_Thailand.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/a/a9/Flag_of_Thailand.svg *Licentie:* Public domain *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Zscout370

- **Bestand:Flag_of_Tunisia.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/c/ce/Flag_of_Tunisia.svg *Licentie:* Public domain *Bijdragers:* http://www.w3.org/ *Oorspronkelijke artiest:* entraîneur: BEN KHALIFA WISSAM
- **Bestand:Flag_of_Turkey.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/b/b4/Flag_of_Turkey.svg *Licentie:* Public domain *Bijdragers:* Turkish Flag Law (Türk Bayrağı Kanunu), Law nr. 2893 of 22 September 1983. Text (in Turkish) at the website of the Turkish Historical Society (Türk Tarih Kurumu) *Oorspronkelijke artiest:* David Benbennick (original author)
- **Bestand:Flag_of_Turkmenistan.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/1/1b/Flag_of_Turkmenistan.svg *Licentie:* Public domain *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:Flag_of_Uzbekistan.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/8/84/Flag_of_Uzbekistan.svg *Licentie:* Public domain *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* O'zbekiston Respublikasining Davlat bayrog'i. The officially defined colours are Pantone 313C for blue and 361C for green (source: [1], [2]). Drawn by User:Zscout370.
- **Bestand:Flag_of_Venezuela.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/0/06/Flag_of_Venezuela.svg *Licentie:* Public domain *Bijdragers:* official websites *Oorspronkelijke artiest:* Zscout370
- **Bestand:Flag_of_Vietnam.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/2/21/Flag_of_Vietnam.svg *Licentie:* Public domain *Bijdragers:* http://vbqppl.moj.gov.vn/law/vi/1951_to_1960/1955/195511/195511300001 http://vbqppl.moj.gov.vn/vbpq/Lists/Vn%20bn%20php%20lut/View_Detail.aspx?ItemID=820 *Oorspronkelijke artiest:* Lưu Ly vẽ lại theo nguồn trên
- **Bestand:Flag_of_the_People'{}s_Republic_of_China.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/f/fa/Flag_of_the_People%27s_Republic_of_China.svg *Licentie:* Public domain *Bijdragers:* Eigen werk, http://www.protocol.gov.hk/flags/eng/n_flag/design.html *Oorspronkelijke artiest:* Drawn by User:SKopp, redrawn by User:Denelson83 and User:Zscout370
- **Bestand:Flag_of_the_United_Arab_Emirates.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/c/cb/Flag_of_the_United_Arab_Emirates.svg *Licentie:* Public domain *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:Flag_of_the_United_States.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/a/a4/Flag_of_the_United_States.svg *Licentie:* Public domain *Bijdragers:* SVG implementation of U. S. Code: Title 4, Chapter 1, Section 1 [1] (the United States Federal "Flag Law"). *Oorspronkelijke artiest:* Dbenbenn, Zscout370, Jacobolus, Indolences, Technion.
- **Bestand:Fotothek_df_n-35_0000073_Facharbeiter_für_Satztechnik.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/d/d8/Fotothek_df_n-35_0000073_Facharbeiter_f%C3%BCr_Satztechnik.jpg *Licentie:* CC BY-SA 3.0 de *Bijdragers:* Deutsche Fotothek *Oorspronkelijke artiest:* Eugen Nosko
- **Bestand:FragmentationDefragmentation.gif** *Bron:* https://upload.wikimedia.org/wikipedia/commons/d/d0/FragmentationDefragmentation.gif *Licentie:* CC BY-SA 3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* XZise
- **Bestand:Ftp_(terminalprogram).png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/7/7e/Ftp_%28terminalprogram%29.png *Licentie:* Public domain *Bijdragers:* selfmade with Gimp *Oorspronkelijke artiest:* This file was made by **User:Sven**
- **Bestand:Gateway_firewall.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/e/eb/Gateway_firewall.svg *Licentie:* CC-BY-SA-3.0 *Bijdragers:* selbst erstellt mithilfe von xfig und der xfig-libaries. *Oorspronkelijke artiest:* Harald Mühlböck
- **Bestand:Glider.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/4/45/Glider.svg *Licentie:* Public domain *Bijdragers:* Hacker Emblem *Oorspronkelijke artiest:* Eric S. Raymond
- **Bestand:Google_add.JPG** *Bron:* https://upload.wikimedia.org/wikipedia/commons/b/bc/Google_add.JPG *Licentie:* CC-BY-SA-3.0 *Bijdragers:* Originally from nl.wikipedia; description page is/was here. *Oorspronkelijke artiest:* Original uploader was Freestyle at nl.wikipedia Later versions were uploaded by Erik Baas at nl.wikipedia.
- **Bestand:H96566k.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/8/8a/H96566k.jpg *Licentie:* Public domain *Bijdragers:* U.S. Naval Historical Center Online Library Photograph NH 96566-KN *Oorspronkelijke artiest:* Courtesy of the Naval Surface Warfare Center, Dahlgren, VA., 1988.
- **Bestand:HardDisk1.ogg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/c/cf/HardDisk1.ogg *Licentie:* CC BY 3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Peter Potrowl
- **Bestand:Hard_drive-en.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/5/52/Hard_drive-en.svg *Licentie:* CC-BY-SA-3.0 *Bijdragers:* Own work, based on the public domain image Image:Hdd od srodka.jpg. Image renamed from Image:Hard drive.svg *Oorspronkelijke artiest:* Surachit
- **Bestand:Hoe_e-mail_werkt.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/1/17/Hoe_e-mail_werkt.svg *Licentie:* CC-BY-SA-3.0 *Bijdragers:* Image:Wie E-Mail funktioniert.svg (which sources Image:Cómo funciona el e-mail.svg) *Oorspronkelijke artiest:* Tijmen Stam = IIVQ
- **Bestand:Hyperlink-Wikipedia.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/d/d5/Hyperlink-Wikipedia.svg *Licentie:* CC0 *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:IBM_350_RAMAC_disk_mechanism.agr.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/1/11/IBM_350_RAMAC_disk_mechanism.agr.jpg *Licentie:* CC BY-SA 3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* ArnoldReinhold
- **Bestand:IDE_cable_40_pin_&_80_pin.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/6/61/IDE_cable_40_pin_%26_80_pin.jpg *Licentie:* CC BY-SA 2.0 de *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* User Smial on de.wikipedia
- **Bestand:IP_stack_connections.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/c/c4/IP_stack_connections.svg *Licentie:* CC-BY-SA-3.0 *Bijdragers:* Prior Wikipedia artwork by en:User:Cburnett *Oorspronkelijke artiest:* en:User:Kbrose
- **Bestand:Innansicht_Festplatte_512_MB_von_Quantum.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/3/30/Innansicht_Festplatte_512_MB_von_Quantum.jpg *Licentie:* CC-BY-SA-3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* SPBer
- **Bestand:Internet_Banking-01_(xndr).JPG** *Bron:* https://upload.wikimedia.org/wikipedia/commons/6/6c/Internet_Banking-01_%28xndr%29.JPG *Licentie:* CC BY 2.5 *Bijdragers:* No machine-readable source provided. Own work assumed (based on copyright claims). *Oorspronkelijke artiest:* No machine-readable author provided. Svdmolen assumed (based on copyright claims).
- **Bestand:Internet_blackholes.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/9/9e/Internet_blackholes.svg *Licentie:* CC BY-SA 3.0 *Bijdragers:* Internet_blackholes_en7.png
http://en.rsf.org/ *Oorspronkelijke artiest:* Internet_blackholes_en7.png: 23prootie

- **Bestand:Internet_of_Things.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/a/ab/Internet_of_Things.jpg *Licentie:* CC BY 2.0 *Bijdragers:* Cropped and sign removed from Internet of things signed by the author.jpg *Oorspronkelijke artiest:* Wilgengebroed on Flickr
- **Bestand:Internet_users_en_2007.PNG** *Bron:* https://upload.wikimedia.org/wikipedia/commons/3/32/Internet_users_en_2007.PNG *Licentie:* Public domain *Bijdragers:* Verplaatst vanaf en.wikipedia naar Commons door Liftarn met behulp van CommonsHelper. *Oorspronkelijke artiest:* Mm11 op de Engelstalige Wikipedia
- **Bestand:Internetbos.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/7/74/Internetbos.jpg *Licentie:* Public domain *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Apdency
- **Bestand:Ironie.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/a/ae/Ironie.png *Licentie:* Public domain *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* self
- **Bestand:K600i_Bluejacked.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/c/c3/K600i_Bluejacked.jpg *Licentie:* Public domain *Bijdragers:* Verplaatst vanaf en.wikipedia naar Commons. *Oorspronkelijke artiest:* De originele uploader was Kallemax op de Engelstalige Wikipedia
- **Bestand:Keylogger-hardware-PS2-example-connected.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/d/dc/Keylogger-hardware-PS2-example-connected.jpg *Licentie:* GFDL *Bijdragers:* http://www.weboctopus.nl/webshop/img/p/59-430-large.jpg *Oorspronkelijke artiest:* http://www.weboctopus.nl
- **Bestand:Keylogger-hardware-PS2.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/1/11/Keylogger-hardware-PS2.jpg *Licentie:* Copyrighted free use *Bijdragers:* http://www.keylogger-keyloggers.nl/images/keylogger_company_keylogger_hardware_PS2.jpg *Oorspronkelijke artiest:* www.keylogger-keyloggers.nl
- **Bestand:Keylogger-screen-capture-example.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/2/22/Keylogger-screen-capture-example.png *Licentie:* MPL 1.1 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* own work
- **Bestand:Keylogger-software-logfile-example.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/c/c4/Keylogger-software-logfile-example.jpg *Licentie:* GPL *Bijdragers:* Own work in combination with the keylogger program http://pykeylogger.sourceforge.net/ and the text editor http://notepad-plus.sourceforge.net/ *Oorspronkelijke artiest:* Own work
- **Bestand:Linus_Torvalds_talking.jpeg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/2/2f/Linus_Torvalds_talking.jpeg *Licentie:* CC-BY-SA-3.0 *Bijdragers:* Linuxmag.com *Oorspronkelijke artiest:* kuvaaja
- **Bestand:Morris_Worm.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/b/b6/Morris_Worm.jpg *Licentie:* CC BY-SA 2.0 *Bijdragers:* Museum of Science - Morris Internet Worm *Oorspronkelijke artiest:* Go Card USA from Boston, USA
- **Bestand:Mozilla_Firefox_2.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/2/2d/Mozilla_Firefox_2.png *Licentie:* CC BY-SA 3.0 *Bijdragers:* Transferred from nl.wikipedia *Oorspronkelijke artiest:* Original uploader was Golradir at nl.wikipedia
- **Bestand:NL_Cookie.ogg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/a/a9/NL_Cookie.ogg *Licentie:* CC BY-SA 4.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Oudehampsink
- **Bestand:NigerianScam.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/7/71/NigerianScam.jpg *Licentie:* CC BY-SA 3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Morburre
- **Bestand:Nl-Computer-article.ogg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/f/f1/Nl-Computer-article.ogg *Licentie:* CC-BY-SA-3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Jcb
- **Bestand:Nl-Internet-article.ogg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/d/d6/Nl-Internet-article.ogg *Licentie:* CC BY-SA 3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Plankje
- **Bestand:Nl-Linux-article.ogg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/d/df/Nl-Linux-article.ogg *Licentie:* CC BY-SA 3.0 *Bijdragers:*
- Afgeleid van Linux *Oorspronkelijke artiest:* **Spreker:** Jcb
  Auteurs van het artikel
- **Bestand:Nuvola_single_chevron_right.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/e/ee/1rightarrow_blue.svg *Licentie:* LGPL *Bijdragers:* 1rightarrow.png: *Oorspronkelijke artiest:* en:David Vignoni, User:Stannered
- **Bestand:Nvidia7600GS_TOP.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/a/ab/Nvidia7600GS_TOP.jpg *Licentie:* CC BY-SA 3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* CaseModder
- **Bestand:OSX-logo-latest.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/2/26/OSX-logo-latest.png *Licentie:* CC BY-SA 4.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Jordi2830
- **Bestand:OpenOffice.org_Writer.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/8/85/OpenOffice.org_Writer.png *Licentie:* LGPL *Bijdragers:* http://hacktolive.org/images *Oorspronkelijke artiest:* http://hacktolive.org/
- **Bestand:Openwebspider_search_engine.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/c/c0/Openwebspider_search_engine.jpg *Licentie:* CC-BY-SA-3.0 *Bijdragers:* http://www.openwebspider.org/ *Oorspronkelijke artiest:* Stefano Alimonti
- **Bestand:PayPal.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/b/b5/PayPal.svg *Licentie:* Public domain *Bijdragers:* PayPal Press Center *Oorspronkelijke artiest:* PayPal
- **Bestand:Perpendicular_Recording_Diagram.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/8/8a/Perpendicular_Recording_Diagram.svg *Licentie:* Public domain *Bijdragers:* http://commons.wikimedia.org/w/index.php?title=File:Perpendicular-eng.jpg *Oorspronkelijke artiest:* TyIzaeL
- **Bestand:PhishingTrustedBank.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/d/d0/PhishingTrustedBank.png *Licentie:* Public domain *Bijdragers:* en:Image:PhishingTrustedBank.png *Oorspronkelijke artiest:* Andrew Levine
- **Bestand:Phoenix_bios.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/2/23/Phoenix_bios.jpg *Licentie:* CC-BY-SA-3.0 *Bijdragers:* No machine-readable source provided. Own work assumed (based on copyright claims). *Oorspronkelijke artiest:* No machine-readable author provided. Audriusa assumed (based on copyright claims).

- **Bestand:Physical_Token_Ring_Wiring.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/4/48/Physical_Token_Ring_Wiring.jpg *Licentie:* CC BY-SA 4.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* ARTol
- **Bestand:Portal.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/c/c9/Portal.svg *Licentie:* CC BY 2.5 *Bijdragers:*
  - Portal.svg

  Oorspronkelijke artiest: Portal.svg: Pepetps
- **Bestand:Proxy2.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/c/c4/Proxy2.jpg *Licentie:* Public domain *Bijdragers:* Originally from nl.wikipedia; description page is/was here. *Oorspronkelijke artiest:* Original uploader was Repeater at nl.wikipedia
- **Bestand:Question_mark_alternate.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/f/f8/Question_mark_alternate.svg *Licentie:* Public domain *Bijdragers:* Image:Question mark alternate.png *Oorspronkelijke artiest:* User:Stannered
- **Bestand:Random-readers.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/6/62/Random-readers.jpg *Licentie:* CC BY-SA 3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Aloxe
- **Bestand:Ransomware_voorbeeld.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/4/4b/Ransomware_voorbeeld.png *Licentie:* CC BY-SA 3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Fab301
- **Bestand:Ring_topology.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/3/38/Ring_topology.png *Licentie:* GPL *Bijdragers:* http://eo.wikipedia.org/wiki/Dosiero:Ringreta%C4%B5o.png *Oorspronkelijke artiest:* Yannickv
- **Bestand:Rir.gif** *Bron:* https://upload.wikimedia.org/wikipedia/commons/d/d0/Rir.gif *Licentie:* CC BY-SA 2.5 *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:RomanW-01.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/4/4a/RomanW-01.png *Licentie:* CC-BY-SA-3.0 *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:SATA_Data_Cable.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/e/ef/SATA_Data_Cable.jpg *Licentie:* CC-BY-SA-3.0 *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:SMirC-rolleyes.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/6/66/SMirC-rolleyes.svg *Licentie:* CC-BY-SA-3.0 *Bijdragers:* Eigen werk (Originele tekst: *own design*) *Oorspronkelijke artiest:* chris
- **Bestand:SMirC-wtf.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/8/8b/SMirC-wtf.svg *Licentie:* CC-BY-SA-3.0 *Bijdragers:* Eigen werk (Originele tekst: *own design*) *Oorspronkelijke artiest:* chris
- **Bestand:SNA_segment.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/c/c7/SNA_segment.png *Licentie:* CC BY 3.0 *Bijdragers:* Screenshot of free software GUESS, derivative work of File:Sna large.png, uncropped version *Oorspronkelijke artiest:* Screenshot taken by User:DarwinPeacock
- **Bestand:Sad.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/d/d8/Sad.png *Licentie:* Artistic 2.0 *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:Shade.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/d/dc/Shade.png *Licentie:* Artistic 2.0 *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:Siemens_M75_Bluejacking.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/b/b0/Siemens_M75_Bluejacking.jpg *Licentie:* Public domain *Bijdragers:* Verplaatst vanaf en.wikipedia naar Commons. *Oorspronkelijke artiest:* De originele uploader was Kallemax op de Engelstalige Wikipedia
- **Bestand:Smile.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/2/26/Smile.png *Licentie:* Artistic 2.0 *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:Spamfilter.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/b/ba/Spamfilter.jpg *Licentie:* CC BY-SA 2.5 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Peter Eich (www.bodenseepeter.de)
- **Bestand:Spammed-mail-folder.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/5/56/Spammed-mail-folder.png *Licentie:* GPL *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:Stachledraht_DDos_Attack.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/3/3f/Stachledraht_DDos_Attack.svg *Licentie:* LGPL *Bijdragers:* All Crystal icons were posted by the author as LGPL on kde-look *Oorspronkelijke artiest:* Everaldo Coelho and YellowIcon
- **Bestand:Star_topology.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/c/c9/Star_topology.png *Licentie:* GPL *Bijdragers:* http://eo.wikipedia.org/wiki/Dosiero:Stelreta%C4%B5o.png *Oorspronkelijke artiest:* Yannickv
- **Bestand:Teeth.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/7/72/Teeth.png *Licentie:* Artistic 2.0 *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:Tongue.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/c/c4/Tongue.png *Licentie:* Artistic 2.0 *Bijdragers:* kde-look.org *Oorspronkelijke artiest:* kborrey
- **Bestand:Tor-logo-2011-flat.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/1/15/Tor-logo-2011-flat.svg *Licentie:* CC BY 3.0 us *Bijdragers:* https://media.torproject.org/image/official-images/2011-tor-logo-flat.svg *Oorspronkelijke artiest:* The Tor Project, Inc.
- **Bestand:Tux.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/3/35/Tux.svg *Licentie:* CC0 *Bijdragers:* [1], garrett/Tux on GitHub *Oorspronkelijke artiest:* Larry Ewing, Simon Budig, Garrett LeSage
- **Bestand:Ubuntu_8.04_Live_CD.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/f/f7/Ubuntu_8.04_Live_CD.png *Licentie:* GPL *Bijdragers:* http://hacktolive.org/images *Oorspronkelijke artiest:* http://hacktolive.org/
- **Bestand:Usage_share_of_web_browsers_(Source_StatCounter).svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/8/86/Usage_share_of_web_browsers_%28Source_StatCounter%29.svg *Licentie:* CC BY 3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Usage share of web browsers (Source Net Applications).svg: arichnad, Daniel.Cardenas, Litehacker
- **Bestand:VPN_remote.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/a/a4/VPN_remote.jpg *Licentie:* Public domain *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Philippe Belet op de Nederlandstalige Wikipedia

- **Bestand:VPN_site-to-site.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/0/0f/VPN_site-to-site.jpg *Licentie:* Public domain *Bijdragers:* Transfered from nl.wikipedia *Oorspronkelijke artiest:* Philippe Belet at nl.wikipedia
- **Bestand:VPN_topologie.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/7/77/VPN_topologie.jpg *Licentie:* Public domain *Bijdragers:* Transfered from nl.wikipedia
  Oorspronkelijke artiest: Original uploader was Philippe Belet at nl.wikipedia
- **Bestand:Vabariigi_aastapaev_Tartu_Anne_kanalis_24-02-2013_06.JPG** *Bron:* https://upload.wikimedia.org/wikipedia/commons/4/40/Vabariigi_aastapaev_Tartu_Anne_kanalis_24-02-2013_06.JPG *Licentie:* CC BY-SA 3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Sigita Matulevičienė
- **Bestand:Virtual_girl_in_petticoat.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/9/9d/Virtual_girl_in_petticoat.jpg *Licentie:* CC BY 2.0 *Bijdragers:* http://www.flickr.com/photos/briannaberesford/6015350847/sizes/o/in/photostream/ *Oorspronkelijke artiest:* Brianna Beresford
- **Bestand:Vista-kmixdocked.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/2/22/Vista-kmixdocked.png *Licentie:* GPL *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:WWDC_2011_Moscone_West_Interior.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/8/83/WWDC_2011_Moscone_West_Interior.jpg *Licentie:* CC BY 2.0 *Bijdragers:* IMG_1639.JPG *Oorspronkelijke artiest:* Ben Miller
- **Bestand:Wat_is_PGP_(Pretty_Good_Privacy)?.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/2/2a/Wat_is_PGP_%28Pretty_Good_Privacy%29%3F.png *Licentie:* CC BY-SA 3.0 *Bijdragers:* https://www.bof.nl/ons-werk/internetvrijheid-toolbox/ *Oorspronkelijke artiest:* Bits of Freedom
- **Bestand:Wat_is_Tor_(The_onion_routing)?.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/1/14/Wat_is_Tor_%28The_onion_routing%29%3F.png *Licentie:* CC BY-SA 3.0 *Bijdragers:* https://www.bof.nl/ons-werk/internetvrijheid-toolbox/ *Oorspronkelijke artiest:* Bits of Freedom
- **Bestand:Web_browser_usage_share.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/0/04/Web_browser_usage_share.svg *Licentie:* Public domain *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:Werking_Anoniem_Surfen.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/e/eb/Werking_Anoniem_Surfen.jpg *Licentie:* CC0 *Bijdragers:* Gecreëerd door Nick Robyn m.b.v. Visio *Oorspronkelijke artiest:* Nick.Robyn
- **Bestand:WiFi-detector.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/d/d0/WiFi-detector.jpg *Licentie:* Public domain *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Raysonho @ Open Grid Scheduler / Grid Engine
- **Bestand:Wikibooks-logo.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/f/fa/Wikibooks-logo.svg *Licentie:* CC BY-SA 3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* User:Bastique, User:Ramac et al.
- **Bestand:Wikimedia-servers.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/7/79/Wikimedia-servers.png *Licentie:* CC-BY-SA-3.0 *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Jimbo Wales
- **Bestand:Wikipedia_spamfilter.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/b/b8/Wikipedia_spamfilter.png *Licentie:* CC BY-SA 3.0 *Bijdragers:* nl.wikipedia.org *Oorspronkelijke artiest:* De originele uploader was Johan Lont op de Nederlandstalige Wikipedia
- **Bestand:Wikiquote-logo.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/f/fa/Wikiquote-logo.svg *Licentie:* Public domain *Bijdragers:* Eigen werk *Oorspronkelijke artiest:* Rei-artur
- **Bestand:Wiktfavicon_en.svg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/c/c3/Wiktfavicon_en.svg *Licentie:* CC BY-SA 3.0 *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:Wink.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/9/9a/Wink.png *Licentie:* Artistic 2.0 *Bijdragers:* ? *Oorspronkelijke artiest:* ?
- **Bestand:Www.wikipedia.org_screenshot_2013.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/e/e9/Www.wikipedia.org_screenshot_2013.png *Licentie:* CC BY-SA 3.0 *Bijdragers:* www.wikipedia.org *Oorspronkelijke artiest:* This page layout was originally designed by User:CatherineMunro and User:AlanBarrett, with many contributions by other users. Talk:Www.wikipedia.org portal/Catherine.
- **Bestand:Zenda1_Gibson.jpg** *Bron:* https://upload.wikimedia.org/wikipedia/commons/a/aa/Zenda1_Gibson.jpg *Licentie:* Public domain *Bijdragers:* http://www.silverwhistle.co.uk/ruritania/bookillustrations.html *Oorspronkelijke artiest:* Charles Dana Gibson
- **Bestand:Zombie-process.png** *Bron:* https://upload.wikimedia.org/wikipedia/commons/f/fe/Zombie-process.png *Licentie:* CC-BY-SA-3.0 *Bijdragers:* ? *Oorspronkelijke artiest:* ?

110.9.3 Inhoudslicentie