De toekomst van cybersecurity

Waarom organisaties hun securitystrategie herzien

kpn. Het netwerk van Nederland

Inhoud

Even vooraf

Digitalisering verandert je organisatie ingrijpend. Je werkt met steeds meer data en applicaties, die verspreid zijn over een groeiend aantal plekken. Vanaf verschillende locaties zoeken medewerkers, leveranciers, klanten, apparaten en sensoren verbinding met je infrastructuur. Met AI als katalysator ontstaat een snel uitdijend ICT-landschap – en dus potentieel meer zwakke plekken. En criminelen? Die worden ondertussen professioneler. Natuurlijk, als CISO, CIO of security-professional sta je ook niet stil, maar het kost veel tijd en energie om criminelen voor te blijven. Tijd en energie die bovendien schaarser wordt door een tekort aan securityprofessionals.

Om in dat groeiende en kwetsbaarder wordende ICT-landschap mensen en organisaties goed te beschermen, komt vanuit Den Haag en Brussel nieuwe securitywet- en regelgeving. En dat maakt de zaken er niet eenvoudiger op. Het goede nieuws? Organisaties die hun security in al die turbulentie goed weten te organiseren – buitenshuis en binnenshuis – hebben een streepje voor. Om het vertrouwen van klanten, medewerkers of partners te vergroten bijvoorbeeld, de samenwerking te verbeteren of nieuwe opdrachten binnen te halen. De Rijksoverheid heeft dit al in beleid gegoten: in een quickguide adviseert de NCTV om securityrisico's bij aanbestedingen te minimaliseren door organisaties te weren die een securityrisico vormen[1]. In dit eBook helpen we je op weg om je security effectief te organiseren, zodat jij dat streepje voor hebt en houdt. Inclusief een blik bij ons achter de schermen.

1 Quickguide 'Samenvatting van de handvatten risicomitigatie', uitgegeven door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

5 security-uitdagingen

Als CISO, CIO of securityprofessional ben je continu in de weer om je organisatie veilig te houden. En dat is een taak die er niet lichter op wordt. Dat komt door de verhoogde security-dreigingen – zeker nu criminelen ook AI inzetten –, de toenemende wet- en regelgeving en de groeiende werkdruk vanwege het tekort aan security-professionals. Wat het weer lastiger maakt om te voldoen aan nieuwe securityeisen en -verplichtingen van de wetgever, klanten en leveranciers. Hoe doorbreek je die vicieuze cirkel en profiteer je van alle nieuwe mogelijk-heden die ontstaan wanneer je je security wél goed op orde hebt?

Van een groter ICT-landschap – dat bovendien complexer en diverser wordt – tot steeds professioneler opererende criminelen: we nemen je hier mee langs de 5 grootste security-uitdagingen voor CISO's, CIO's en securityprofessionals.

Per uitdaging laten we zien hoe je die kunt ondervangen en in je voordeel kunt ombuigen. Zo doorbreek je stap voor stap de vicieuze cirkel en breng je de security effectief op orde.

'Securitydreigingen groeien niet meer lineair, maar exponentieel.'
-Vladimir Cibic, CISO KPN

1 Groter ICT-landschap, grotere aanvalsoppervlakte

Organisaties gebruiken steeds meer applicaties – bij grote organisaties loopt dat al snel in de honderden.[2] Soms heeft de centrale ICT-afdeling al die applicaties netjes in beheer, vaak is het schaduw-ICT: applicaties die medewerkers inzetten zonder dat je ICT-team er zicht op heeft. Via API's kunnen tech-savvy medewerkers de koppeling maken met andere applicaties of databronnen, wat het aantal zwakke plekken verder vergroot. Overigens kunnen ook de 'gewone' applicaties, die dus wel vanuit de centrale ICT-afdeling komen, een zwakke plek vormen. Zo zijn in gangbare applicaties die organisaties wereldwijd gebruiken, recent meer dan 25.000 kwetsbaarheden gevonden.[3]

Risico: verschillende omgevingen naast elkaar

Een groeiend aantal data en applicaties gaat naar of staat in de cloud, terwijl een deel achterblijft in een datacenter – op een eigen locatie of van een andere partij. Data en applicaties verspreiden zich dus over datacenters en verschillende cloudomgevingen: publiek, privaat en SaaS. En dat blijft niet onopgemerkt. Zo wordt een nieuwe internet-facing server binnen enkele seconden al gescand op zwakheden. Dat overkwam ook Ticketcounter, waar een medewerker gegevens plaatste in een Microsoft Azure-container. In een mum van tijd waren privacygevoelige gegevens van honderdduizenden klanten gestolen.

Zo minimaliseer je dit risico

Start met een heldere strategie voor je data en applicaties. Bepaal welke applicaties je in je datacenter(s) houdt, welke je naar de publieke cloud wilt brengen en welke je – vanwege gevoeligheid, betrouwbaarheid of beschikbaarheid – liever in een private cloud plaatst. Dat combineer je met goede basishygiëne, zoals patchmanagement, segmentatie en een immutable back-up.

Dat vul je onder meer aan met deze tools en methodes:

- Data Loss Prevention (DLP)
- Cloud Access Security Broker (CASB)
- Cloud Security Posture Management (CSPM)
- Zero Trust Network Access (ZTNA)
- Identity and Access Management (IAM)
- Netwerksecurity en private networks
- Logfilemanagement (LFM)

2 Dit blijkt uit de applicatiescans die we uitvoeren bij klanten. Bij grotere organisaties gaat het om 300 tot 1500 (web)applicaties.
3 State of Application Security 2024, Datadog

Risico: thuis- en onderweg werken

Een groeiend aantal medewerkers werkt vanaf verschillende locaties, thuis en onderweg, op wisselende tijden. Ook buiten kantooruren en in het weekend. Dat brengt risico's met zich mee. Wanneer de medewerker een thuisnetwerk gebruikt waarop ook een slimme deurbel of wasmachine zit, bijvoorbeeld. En wanneer de credentials van een medewerker gestolen zijn, is het lastiger te controleren of de 'identiteit' die inlogt, werkelijk degene is die het zegt te zijn.

Zo minimaliseer je dit risico

Voor de beveiliging van endpoints en identiteiten kun je Multifactor authenticatie (MFA) inzetten, werken met een Virtual Private Network (VPN) of Zero Trust Network Access (ZTNA) en met gegevensversleuteling. Daarnaast zijn ook niet-technische oplossingen belangrijk, zoals het verhogen van het bewustzijn van cyberrisico's door trainingen.

Risico: meer én nieuwe endpoints in IT- en OT-omgevingen

Van de kantoorvloer tot de fabriekshal: we gebruiken steeds meer IT- én OT-apparatuur. Endpoints dus. In de IT gaat het om een groeiend aantal laptops, mobieltjes en tablets, vaak unmanaged. Daar komen tal van sensoren bij, in apparatuur als kopieermachines, koelinstallaties of medische instrumenten. Elk aangesloten op een applicatie waarvan niet altijd even duidelijk is of deze kwetsbaarheden kent. In de OT – de operationele technologie in fabrieken, ziekenhuizen, (lucht)havens, energiecentrales of distributiecentra – staan de endpoints vaak los van internetgekoppelde netwerken. Omdat een goed overzicht van het aantal endpoints en/of applicaties vaak ontbreekt, weten organisaties vaak niet of er vulnerabilities zijn. Daarnaast gaat de integratie van IT en OT-omgevingen wel steeds sneller – en groeien dus ook de risico's. Veel OT-systemen en -infrastructuren die kritische processen aansturen, zijn namelijk verouderd. Patchen van applicaties of machines is lastig of onmogelijk. Ze barsten daardoor van de zwakke plekken. Zo wisten aanvallers een Amerikaans bedrijf binnen te komen via een temperatuurmeter in een aquarium.

Zo minimaliseer je dit risico
Allereerst zijn er goede tools waarmee je alle endpoints in kaart kunt brengen. Daarnaast kun je de integratie van IT en OT aanwenden om de security waar mogelijk te integreren en zo kosten te besparen.

Verbeter de security van de endpoints met onder meer:

- Endpoint Protection en XDR
- Logfilemanagement van applicaties: verzamel logdata op één centrale plek, dit versnelt (security)incident response
- Eén SIEM-oplossing voor het loggen en analyseren van verdachte patronen
- Intrusion Detection en Prevention Systems (IDS/IPS)
- Airgapped (niet aangesloten op internet) en gesegmenteerde netwerken met firewalls
- Datadiodes waar alleen een signaal uit kan (en niet terug erin)
- Data-encryptie, monitoring en anti-malware
- Goed patchmanagement en, als dat niet kan virtueel patchmanagement in een firewall

Risico: langere ketens en intensievere ketensamenwerking

Samenwerking in ketens helpt je organisatie efficiënter te werken en sneller in te spelen op dat wat de markt van je vraagt. Het levert ook nieuwe securityrisico's en kwetsbaarheden: ketensamenwerking kan niet zonder uitwisseling van data of koppeling van applicaties. Third party-risicomanagement wordt dus steeds belangrijker. Zo lagen vorig jaar persoons-gegevens van klanten van verschillende grote bedrijven op straat door een securitylek in de software van softwareleverancier Nebu, toeleverancier van onderzoeksbureau Blauw. Werk je samen in ketens, dan wil je veilig data uit kunnen wisselen – dus zonder het risico van besmetting met malware of verlies van controle over je data.

Zo minimaliseer je dit risico
Start met een eenduidig securitybeleid waar alle toeleveranciers zich aan kunnen houden. Zorg voor basishygiëne, zoals goed patchmanagement. Neem daarnaast aanvullende technische maatregelen, zoals:

- Gebruik een intelligente firewall en netwerksegmentatie, zodat leveranciers maar bij een beperkt deel van je netwerk kunnen komen
- Gebruik tooling om broncode die bij leveranciers vandaan komt, te valideren
- Voorkom dataverlies door een data-exchangeoplossing te gebruiken. Daarmee gaat je data niet daadwerkelijk naar de server van een andere partij
- Verzamel de logs van de diverse systemen die gebruikt worden, zoals bijvoorbeeld logs van events, servers, syslogs en autorisatie en access logs op 1 centrale plek. Dit voorkomt een vendor lock-in en creëert 1 omgeving waarin IT en OT data samen gebruikt kan worden voor performance- en security monitorring

2 Snelle professionalisering criminaliteit

Op de grotere aanvalsoppervlakte met meer zwakke plekken, bewegen zich steeds professioneler georganiseerde criminelen. Van solitaire techneuten zijn het goed geoliede machines geworden, in efficiënt gestructureerde organisaties waar gespecialiseerde teams nauw samenwerken. Zo zijn er teams die aanvallerssoftware ontwikkelen en andere teams die de aanvallen uitvoeren. Technische kennis is voor dat laatste nauwelijks meer nodig: er zijn inmiddels duizenden gebruiksvriendelijke ransomwarefamilies, met bekende namen als Petya en REvil. En dat aantal blijft groeien. Je kunt op het dark web Hacking-as-a-Service (HaaS) en Ransomware-as-a-Service (RaaS) afnemen, inclusief SLA-afspraken, DDos-aanvallen kopen voor enkele tientjes of een aanvalsabonnement afnemen tegen een vast maandelijks tarief.

Risico: laagdrempelige aanvalssoftware

De inzet van aanvalssoftware verandert door die laagdrempeligheid. Zo kunnen nieuwe groepen, ook zonder al te veel technische kennis, aanvallen uitvoeren. Bovendien is de pakkans klein. Het aantal succesvolle aanvallen groeit daardoor explosief. Ook worden aanvallen soms alleen ingezet om schade aan te richten. Of als een afleidingsmanoeuvre. In andere gevallen gebruiken landen – of exacter geformuleerd: 'statelijke actoren' – de software in een oorlog. Hier waarschuwt de AIVD al langer voor[4].

Met de instrumenten van cybercriminelen verzamelen statelijke actoren inlichtingen en ontregelen ze hele landen. Vanuit de oorlogskassen gaan daardoor aanzienlijke bedragen richting cybercriminelen, wat de professionalisering van de toeleverings-industrie verder vergroot. Inclusief illegale marktplaatsen voor de verkoop van gestolen gegevens, het witwassen van geld of uitwisselen van exploits. Je vindt er zelfs online cursussen en handleidingen.

Zo minimaliseer je dit risico

Tegen de HaaS- en RaaS-aanvallen helpt maar 1 ding: je security goed op orde brengen (zie vorige adviezen). Tegen DDoS-aanvallen bestaan wel extra maatregelen. Zo kun je al het verkeer door 'een wasstraat' in de cloud leiden: een infrastructuur die buiten je eigen organisatie om, speciaal ontworpen is om kwaadaardig verkeer te filteren en legitiem verkeer door te laten. Een ander soort ontwikkeling is de intensivering van samenwerking tussen CISO's. Ze wisselen wereldwijd threat intelligence uit, herkennen potentiële aanvallers en nieuwe technieken eerder, waarschuwen elkaar en voorkomen zo dat criminelen schade aan kunnen richten. Maak gebruik van marktleidende fabrikanten. Zij hebben een grote footprint en analyseren van al hun devices de nieuwe dreigingen en stellen die vervolgens beschikbaar als threat intelligence.

4 Dreigingsbeeld Statelijke Actoren 2 (2022)

3 Artificiële Intelligentie (AI): extra versnelling

Een groter wordende aanvalsoppervlakte plus de professionalisering van criminelen is – bij elkaar opgeteld – al een forse uitdaging. Daar komt AI nog eens bij, als een extra versnelling. Bijna de helft van alle securityspecialisten, zo'n 45%, verwacht dat vooral criminelen gaan profiteren van AI.[5] Met AI kunnen zij hun aanvallen namelijk steeds geavanceerder opzetten, aanvallen automatiseren en ervoor zorgen dat ze moeilijker te detecteren zijn. Daarnaast gebruiken ze Large Language Modellen (LLM) en deepfakes om phishing-tactieken te ontwikkelen die het amateuristische niveau ontstijgen en griezelig echt zijn. Zo maakte een medewerker van een multinational in Hong Kong begin dit jaar 25 miljoen dollar over naar aanvallers die de medewerker met een deepfake videocall om de tuin leidden.[6]

Risico: geautomatiseerde aanvallen

De Anti-Phishing Work Group (APWG) stelt dat vorig jaar hét jaar voor phishing was in Nederland, met bijna 5 miljoen phishing-aanvallen. Aanvallen die blijven groeien in volume, frequentie en complexiteit.[7]
En met generatieve AI genereren criminelen geautomatiseerde content die nog overtuigender en geloofwaardiger is. Inmiddels is er ook zelflerende en 'polyforme' malware. Dit is malware die zichzelf automatisch aanpast aan de verdedigingssystemen die het tegenkomt, waardoor detectie en succesvolle bestrijding nog lastiger wordt.

Zo minimaliseer je dit risico

AI biedt gelukkig ook kansen voor security-professionals. Denk aan de inzet van algoritmes die helpen bij het analyseren van logdata.
En al vraagt het extra kennis en training van securityprofessionals om de tools goed te doorgronden, het levert ook veel op. Zo kunnen LLM's helpen om aanvallen te interpreteren en zijn ze een vraagbaak voor junior analisten.

5 Splunk: The State of Security 2024 – The Race to Harness AI
6 'Financieel-medewerker in Hongkong betaalt 24 miljoen na videogesprek met deepfake', Volkskrant Tech (2024)
7 'Generatieve ai maakt opkomst in cyberaanvallen', Computable (2024)

4 Wet- en regelgeving

Natuurlijk, wet- en regelgeving is er om ons te beschermen. Tegelijk legt het ook extra druk op je organisatie. Dat geldt vooral voor compliance-, security- en ICT-medewerkers. Zij moeten op de hoogte blijven van veranderingen, de nieuwste vereisten kennen, zichzelf en hun team trainen, systemen en processen aanpassen én zorgen voor naleving. Belangrijk werk. Want voldoet je organisatie niet aan wet- en regelgeving, dan loop je forse risico's. Denk aan boetes of reputatieschade. In sommige gevallen zijn bestuurders zelfs hoofdelijk aansprakelijk. Dat zie je bijvoorbeeld in NIS2.

De scope: om deze wetgeving kun je niet heen

Algemene wetgeving die over security gaat of het securitybeleid raakt, zijn onder meer de AVG, NIS2 en de AI-act. Daarnaast is er veel sectorspecifieke wet- en regelgeving. Denk aan NEN7510 voor de zorg, de BIO voor de overheid of DORA voor financiële instellingen. Er zijn diverse standaarden waarvan je moet aantonen dat je eraan voldoet, zoals ISAE, SOC2 en ISO. Tal van initiatieven geven bovendien security-aanbevelingen, zoals eIDAS, het EU cybersecurity certification scheme on Cloud services (EUCS) en de European Data Protection Board. Die aanbevelingen gaan onder meer over beveiliging, de omgang met persoonsgegevens in de cloud en datasoevereiniteit.

Al die wetten, regels, normen, standaarden en aanbevelingen vinden hun weg ook naar aanbestedingstrajecten en pitches. Opdrachtgevers uit allerlei sectoren willen bijvoorbeeld hard bewijs dat je als leverancier of partner voldoet aan securityvereisten. In de introductie noemden we al even de quickguide van het NCTV (pagina 3). Maar de overheid ontwikkelt nu ook de ABRO: de algemene beveiligingseisen voor rijksoverheidsopdrachten.

Risico: NIS2 richtlijn tijdig implementeren.

NIS2 is een richtlijn die impact heeft op veel organisaties. Deze richtlijn zal eerst in de Nederlandse wetgeving worden geïmplementeerd, waarna de daarin opgenomen (extra) verplichtingen voor organisaties gaan gelden. Dit zal naar verwachting niet eerder dan medio 2025 zijn. Vergeleken met NIS1, de richtlijn die in Nederland is uitgewerkt in de Wet beveiliging netwerk- en informatiesystemen (Wbni), geldt NIS2 voor een veel grotere groep organisaties. Ook is de nieuwe wet indirect van toepassing op leveranciers, omdat een organisatie die onder de NIS2 komt te vallen, verplicht is die eisen door te vertalen naar haar leveranciers. Als CISO of CIO heb je dus ineens een veel grotere verantwoordelijkheid. De eisen waar je aan moet voldoen, bestaan onder meer uit het implementeren van een reeks technische en organisatorische maatregelen om securityrisico's van je netwerk- en informatiesystemen te beheren, inclusief aandacht voor securitybewustzijn, encryptiebeleid, incidentafhandeling en meer.

Meer weten over NIS2?
Lees hier meer.

Zo minimaliseer je dit risico

Gelukkig biedt NIS2 ook veel kansen om het securitybeleid in je organisatie te moderniseren. Zo is het de eerste regelgeving waarin concrete maatregelen en methodes als MFA en Zero Trust worden genoemd. NIS2 biedt zelfs handvatten voor een integraal security- en complianceplan om Zero Trust structureel in de organisatie te 'embedden'. Een security-expert van KPN gaat graag met je in gesprek om een logische roadmap op te stellen.

5 Tekort aan securityprofessionals

Niet alleen in Nederland, overal ter wereld is een tekort aan securityprofessionals, zo blijkt uit Amerikaans onderzoek: 89% van de aan het onderzoek deelnemende organisaties heeft moeite met het vinden van goede security-mensen[8]. De 4 hierboven genoemde uitdagingen vergroten de werkdruk al, het tekort aan mensen legt extra druk. Doordat aanvallen 24/7 plaatsvinden en veel securityexperts dag en nacht klaar moeten staan, is de werkbelasting zwaar.

Risico: werkstress en groot verloop

Ondertussen verandert het gewenste profiel van de securityprofessional. Ging het meestal om technische mensen met diepgaande kennis van systemen en inrichting van securitybeleid, nu zijn mensen met een breed scala aan vaardigheden nodig. Denk aan netwerkbeheer, forensisch onderzoek, malware-analyse, communicatie of leiderschap. Professionals hebben bovendien vaak meerdere rollen en verantwoordelijkheden, iets waar de IT-opleidingen ze onvoldoende op voorbereiden. Daardoor stijgt de werkdruk en werkstress van securityprofessionals. Onderzoeksbureau Gartner verwacht dat de komende jaren 25% op zoek gaat naar ander werk, ook omdat ze zich onvoldoende gesteund voelen door hun organisatie. ‘Het elimineren van stress is een onrealistisch doel’, schrijft Gartner, ‘maar mensen kunnen ongelooflijk uitdagende en stressvolle banen aan in culturen waarin ze goed worden ondersteund.’

Als organisatie kun je daarom het best een heldere keuze maken. Of je doet de security volledig zelf óf je besteedt het uit. Kies je ervoor om het zelf te doen, realiseer je dan dat investeren in het opbouwen van specifieke securitykennis gedurende een langere tijd erbij hoort. Om de juiste mensen te behouden, is het belangrijk een cultuur te scheppen waarin zij zich gehoord en gesteund voelen. Bedrijven concurreren hevig om het beschikbare talent, wat de salarissen en andere arbeidsvoorwaarden omhoog stuwt. Dit kan het voor sommige organisaties moeilijker maken om gekwalificeerd personeel met voldoende kennis aan te trekken.

Zo minimaliseer je dit risico

Omdat het lastiger wordt om de juiste securityprofessionals en -kennis in huis te halen én te houden, kiezen steeds meer organisaties om alle security uit te besteden. Zij richten zich op het verbeteren van de ICT in hun kritische processen, omdat de ICT-budgetten daar van meer toegevoegde waarde zijn. Wel is het verstandig om het securitybeleid samen met je securitypartner op te stellen en minimale basiskennis in huis te houden. Als organisatie blijf je immers zelf verantwoordelijk.

8 Uitgevoerd door Vanson Bourne, in opdracht van Check Point.

Zo organiseren wij onze security zelf

Net als veel andere organisaties in Nederland hebben ook wij te maken met de 5 grote security-uitdagingen. Omdat wij zorgen voor de vitale infrastructuur van Nederland, hebben we een extra grote securityverantwoordelijkheid. Dat we onze ervaring en expertise delen, vinden we daarom eigenlijk niet meer dan normaal. Alleen al omdat we zo samen Nederland nóg veiliger kunnen maken. En als land voorop kunnen blijven lopen in innovatie en toepassing van nieuwe technologie.

Security First: onze strategie
Iedereen die bij KPN werkt, kent onze security-strategie: Security First. Wat we ook doen, waar we ook aan werken: security komt first. Dat is de afgelopen jaren deel van onze mindset geworden. Security First betekent ook dat we de blik op de buitenwereld richten. Op de meest actuele risico's en de nieuwste dreigingen. We zijn realistisch en onderkennen dat de groei van criminaliteit niet langer lineair is, maar exponentieel. Criminelen professionaliseren snel – aan ons de taak nog sneller en beter voorbereid te zijn.

'Hoe belangrijker security voor je organisatie wordt, hoe minder je het je kunt veroorloven de security er, zeg maar, doorheen te duwen,'
- Vladimir Cibic,
CISO KPN

Lees verder

Van traditionele security naar Security First: zo veranderden we

Om de securitydreigingen het hoofd te kunnen bieden, zien we veel organisaties hun security-strategie aanpassen. Wij maakten zelf ook zo'n verandering door. Van directief naar samen-werkend, van puur aansturend naar begeleidend. Zo werkten we toe naar onze huidige strategie: Security First'

Onze strategie

De strategie hebben we samengevat in 4 A's

Our strategy

Adaptive	We anticiperen op onzekerheden en securityrisico's
Automate	We maken veiligheid onderdeel van alle bedrijfsprocessen
Aware	We trainen alle medewerkers op risicobewustzijn
Assure	We zorgen dat beveiliging aantoonbaar geïmplementeerd is

1. Adaptive: we anticiperen op onzekerheden en risico's

Deze eerste A staat voor ons vermogen om ons snel aan te passen aan een veranderende omgeving. Aan de veranderende risico's en dreigingen, maar ook aan de toenemende en striktere wet- en regelgeving. Inclusief de normen, standaarden en aanbevelingen – sectorspecifiek en algemeen – die we in het hoofdstuk hiervoor noemden. Onder Adaptive vallen o.a. 3 disciplines: Business Continuity Management (BCM), het Blue team en het Red team.

BCM: continu klaarstaan om te reageren

De mensen van BCM zorgen ervoor dat we als organisatie continu klaarstaan – respons ready – en voorbereid zijn op incidenten. En als er toch iets gebeurt, dat we als heel KPN door kunnen en de primaire processen geen of minimale hinder ondervinden. Daarvoor brengt BCM al onze assets en processen goed in kaart en ontwikkelt maatregelen en beleid voor de continuïteit van al die assets. Voorbeelden zijn redundantie in bekabeling, extra stroomvoorziening in datacenters, beleid bij een dijkdoorbraak én cybersecuritymaatregelen. Voor gevoelige data bijvoorbeeld, die vragen om datasoevereiniteit – die blijven in onze eigen datacenters op Nederlands grondgebied, vallend onder Nederlandse wet- en regelgeving. Daarnaast zorg je met BCM dat er draaiboeken zijn en er is nagedacht over het Major Incident Management (MIM)-proces.

'We hebben niet alleen een plan B, maar ook een plan C en D. En verandert onze omgeving, dan stellen we alle plannen weer bij.'

- Jos Oostdam,
Security en BCM-advisor

Lees verder

Blue team: houdt KPN veilig met nieuwe verdedigingstechnologie

Ons Blue team, waar ons CERT onderdeel van is, bewaakt al onze assets. En dat zijn er veel. Zo verwerken we alleen al dagelijks zo'n 40 miljard events in ons eigen SIEM. Een event is overigens een logging van een activiteit en dus doorgaans iets onschuldigs, zoals bijvoorbeeld een medewerker die inlogt. Maar al die events zul je wel moeten analyseren op afwijkingen die kúnnen duiden op securitybedreigingen. Want het Blue team grijpt ook in als ze onregelmatigheden of een dreiging detecteren. Vanwege de grote hoeveelheid events, hebben ze het werk geautomatiseerd met onder meer detectieregels, usecases en de AI-tool Copilot. Daarnaast zetten ze threat intelligence in voor detectie.

In communities als The Circle of Trust werken de mensen van het Blue team samen met securityspecialisten van andere partijen en delen ze onderling informatie die helpt bij het detecteren van indringers. Denk aan tools, procedures of IP-reeksen waarvan ze weten dat criminelen die gebruiken. Vinden ze een indringer, dan isoleren ze de dreiging en doen ze er alles aan om schade te beperken. De threat intelligence van zo'n incident delen ze met andere partijen zodat ook die tijdig aanvallen waarnemen en kunnen stoppen.

'Wat wij als Blue team beschermen, is onvergelijkbaar met andere bedrijven – het gaat niet alleen om het verdedigen van onszelf, maar om heel Nederland.'

- Coen de Jong,

teamlead Blue team en Computer Emergency Response Team

Lees verder

Red team: ethical hackers op zoek naar kwetsbaarheden

Ons Red team test al onze producten en diensten, op zoek naar de zwakste schakel, open poorten of andere kwetsbaarheden. Van router tot core netwerk, in de hele keten. Worden de juiste meldingen getriggerd, zijn de maatregelen afdoende? Als ethical hackers onderzoeken ze zwakke plekken en wat er gebeurt als een aanval plaatsvindt.

Daarvoor gebruikt het Red team allerlei verschillende soorten technologie. Social engineering bijvoorbeeld, met phishing-tactieken. Puur technisch, door open poorten of fouten in de code te zoeken. En door de fysieke kwetsbaarheden te testen, zoals gebouwen. Daarbinnen doorlopen ze verschillende routes. Zoals die van supplychains en leveranciers, maar ook insider threats – dus bedreigingen van binnenuit. Denk aan diefstal van credentials. Samen met het Blue team testen ze verschillende scenario's. Het Red team valt aan, het Blue team verdedigt. Als Purple team komen ze bij elkaar om oplossingen te ontwikkelen en verbeteringen aan te brengen.

'We gebruiken de nieuwste aanvalstechnologie om onze simulaties uit te voeren. Soms ontwikkelen we de software zelf. Zo blijven we criminelen een stap voor.'

- Mark de Groot,

teamlead Red team en ethical hacker

Lees verder

2. Automate: we maken veiligheid onderdeel van alle bedrijfsprocessen

We hebben ongelooflijk veel assets bij KPN. Zoveel, dat we de bescherming ervan wel moeten automatiseren. Niet alleen automatiseren in de technische zin van het woord, maar ook automatiseren in de zin van security tot een gewoonte maken. Voor iedereen, in elke rol. Zo maken we ons securitywerk schaalbaar, wat ook wel moet om de werkdruk op een aanvaardbaar niveau te houden.

Onze securityafdeling stelt het securitybeleid op en bepaalt de securityprocessen, voor de invulling ervan zorgt onze hele organisatie. En dat doen we echt samen – onze securityafdeling dicteert niet, maar investeert in een cultuur van vertrouwen en overleg. Met het programma Shift left hebben zij de afgelopen jaren bovendien geïnvesteerd in een werkwijze waarbij developers van meet af aan security in hun werkprocessen integreren: de DevSecOps-methode.
De decentrale securitymedewerkers zorgen voor uniforme securityprocessen, overal in onze organisatie. Dat maakt het automatiseren van onze security mogelijk.

We doen het samen

Onze securityafdeling met onze CISO aan het hoofd: een ‘partner in crime’ voor onze organisatie

Van ...

- CISO
- Centrale organisatie
- Focus op beleid uitstippelen en operationaliseren
- Minimale proces- en controlframeworks
- Dicteerde wat de organisatie moest doen

... naar

- CISO
- Federatieve organisatie
- Focus op organisatie begeleiden en controle van securityprocessen
- Sterke security- en operationele monitoring
- Helpt de organisatie te doen

3. Awareness: we trainen alle medewerkers op risicobewustzijn

Bij KPN werken ruim 10.000 collega's. We willen dat elke collega niet alleen bewust is van het belang van veiligheid, maar daar ook naar handelt. Onze CISO en de securityafdeling zijn accountable, iedereen bij KPN is responsible. We spreken daarom ook wel over onze 'menselijke firewall' als de eerste linie van verdediging. En dat maakt bewustzijn van de risico's en kennis een belangrijk wapen. Hacks beginnen namelijk vaak met het ontfutselen van credentials als gevolg van een menselijke fout.

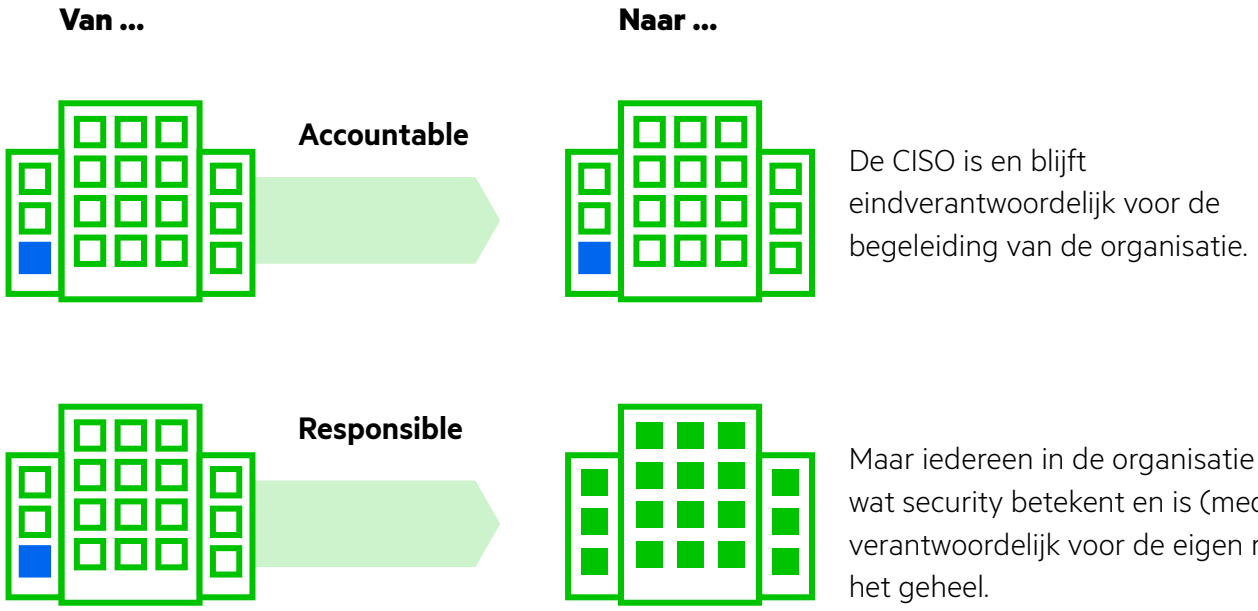
Met trainingen, online informatie en gezamenlijke sessies versterken we onze eerste verdedigingslinie. Dat vraagt wel om een veranderend profiel van securitycollega's. Zo is het steeds belangrijker dat ze naast zeer technische kennis, ook communicatieve, advies- en leiderschapsvaardigheden hebben. Natuurlijk, we hebben nog steeds zeer technische mensen nodig, maar óók mensen die het securitydenken goed uit kunnen dragen.

'Het belang van een waterdicht securitybeleid is groter dan ooit. Security First is een mindset, een persoonlijke opdracht voor ons allemaal: we zetten de veiligheid van onze netwerken en systemen, de digitale veiligheid van onze klanten en die van onze collega's altijd op één.'

- Vladimir Cibic, CISO KPN

Veranderde mindset

iedereen op de eigen manier verantwoordelijk voor onze security



4. Assure: We zorgen dat beveiliging aantoonbaar geïmplementeerd is

Wet- en regelgeving heeft veel impact op ons. Overheid, toezichthouders, klanten: we worden goed in de gaten gehouden. Zo hebben we geregeld te maken met audits en inspecties. Logisch, want het is ook heel belangrijk dat ons netwerk en onze diensten en producten aantoonbaar goed beveiligd zijn. Controleren is de methode om daar zekerheid over te creëren. Dat maakt helder ingerichte security- en complianceprocessen zo belangrijk. Onze KPN Security Policy geeft ons het noodzakelijke houvast.

Security Watchtower: realtime zicht op securitystatus

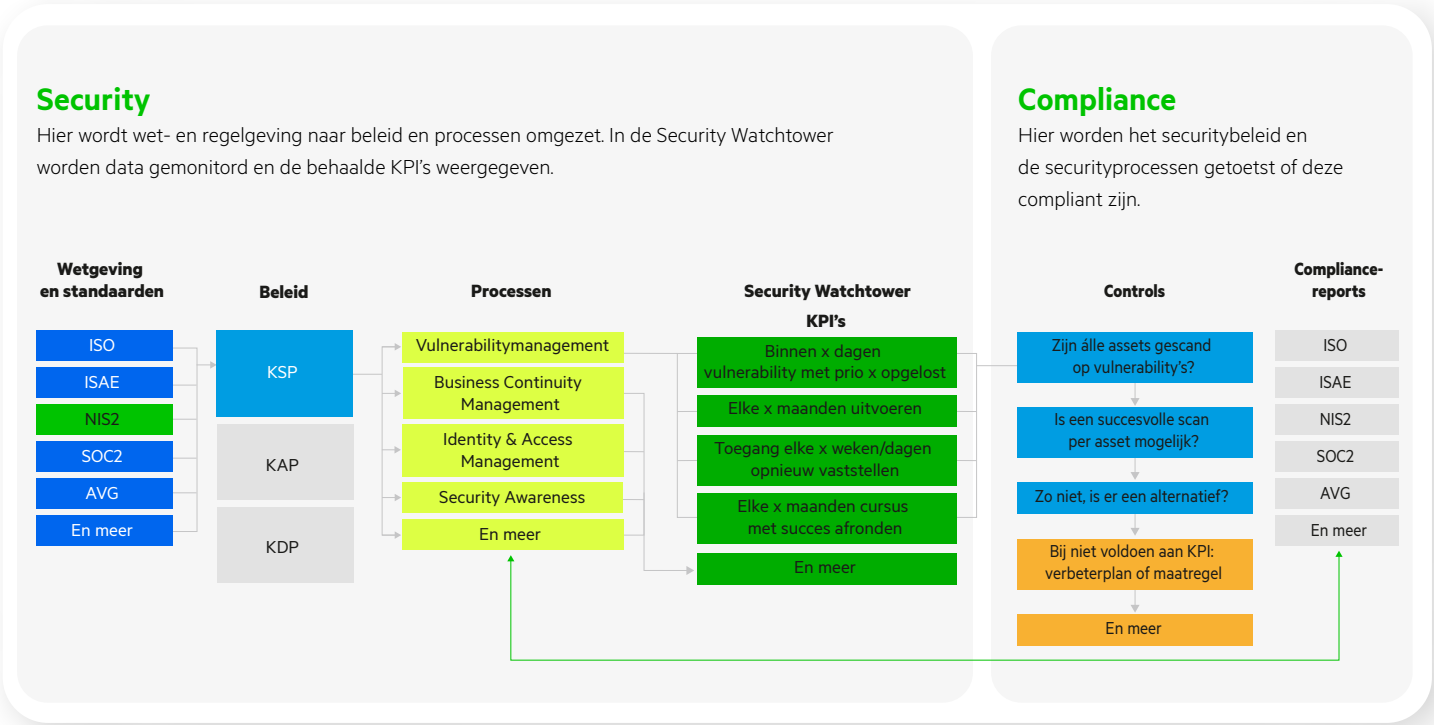
Met data gedreven security in gedachten ontwikkelden we de KPN Security Watchtower: een aanpak waarmee we op elk moment inzicht hebben in de securitystatus van al onze assets. Hoeveel kwetsbaarheden zijn er opgelost, zijn er end point protection agents geïnstalleerd – zelfs of medewerkers succesvol zijn getraind. De Watchtower biedt heel KPN, van Raad van Bestuur tot teamleads, inzicht in de status van de veiligheid van onze organisatie. Daarnaast werken we al veel langer met een security- en complianceplatform waarmee we onze security- en complianceprocessen kunnen monitoren.

‘Als je niet weet wat je hebt, kun je het ook niet beveiligen. En hoe veilig zijn we nou werkelijk? Op basis van data blijven we de security verbeteren.’

- Ernst Doornebosch,

teamlead monitoring en reporting

Lees verder



Security First: KPN Security Policy (KSP) als houvast

In ons securitybeleid combineren we wereldwijde standaarden met een eigen Nederlandse aanpak. Die combinatie hebben we vertaald naar onze KPN Security Policy (KSP), dat iedere dag weer ruim 10.000 KPN'ers én duizenden medewerkers van andere organisaties houvast geeft. Met onze KSP doen we meer dan dat wat strikt wettelijk verplicht is. Hierin staan alle maatregelen en vereisten waaraan onze organisatie en leveranciers in de dagelijkse praktijk moeten voldoen. Die maatregelen gelden voor alle assets: systemen, platformen, netwerken, toepassingen, documenten en apparaten.

Zelfs voor de medewerkers die met die assets werken. De KSP zelf hebben we grotendeels openbaar toegankelijk gemaakt, zodat al onze klanten – feitelijk heel Nederland – zelf kunnen beoordelen of en hoe hun diensten beveiligd zijn. Je leest erin wat onze maatregelen zijn op het gebied van fysieke beveiliging, informatiebeveiliging, business continuity en privacy. En je kunt de structuur en opzet als een best practice gebruiken voor je eigen securitybeleid.

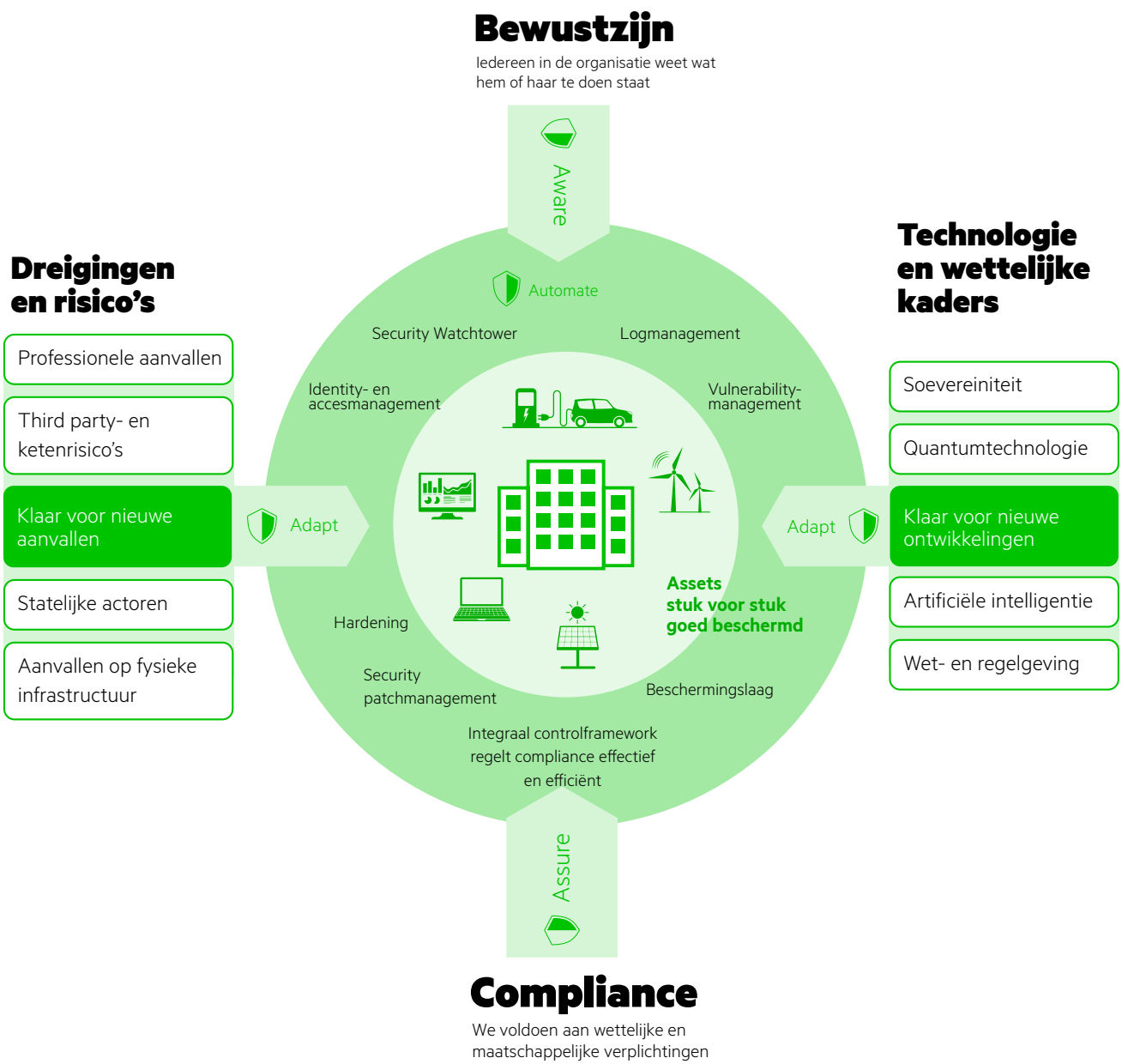
Aanvullend beleid, normen en regelgeving

Naast de KSP hebben we de KPN Assurance Policy (KAP) en de KPN Data Policy (KDP), waarin je leest hoe we verantwoord omgaan met AI en data. Daarnaast voldoen we aan:

- alle relevante ISO-certificeringen, zoals ISO27001, ISO22301, ISO9001. Jaarlijks wordt dit onafhankelijk ge-audit.
- de internationale ISAE 3000-standaard, met de focus op assurance. Daarvoor auditen we onze beheerprocessen jaarlijks.
- de jaarlijkse audit van een externe partij op ons business continuity management, een randvoorwaarde voor onze ISO- en ISAE-certificering.
- alle relevante NEN-certificeringen, zoals NEN7510, NEN7512, NEN7513.

Security First: Zero Trust als basisprincipe

De 4a's vormen de basis voor alles wat we doen op securitygebied. Ze zijn het uitgangspunt voor ons controle framework warrmee we aan kunnen tonen dat onze assets veilig zijn in een veranderende omgeving.



Over Zero Trust

Met Zero Trust ga je ervanuit dat het gevaar niet meer alleen van buitenaf komt, maar ook van binnenuit kan komen. Medewerkers kunnen namelijk bewust of onbewust datalekken veroorzaken of poorten open zetten. Denk maar aan de GGD-medewerker die tijdens corona persoonsgegevens verzamelde en deze op het darkweb verkocht.

Zero Trust bestaat uit 3 elementen:

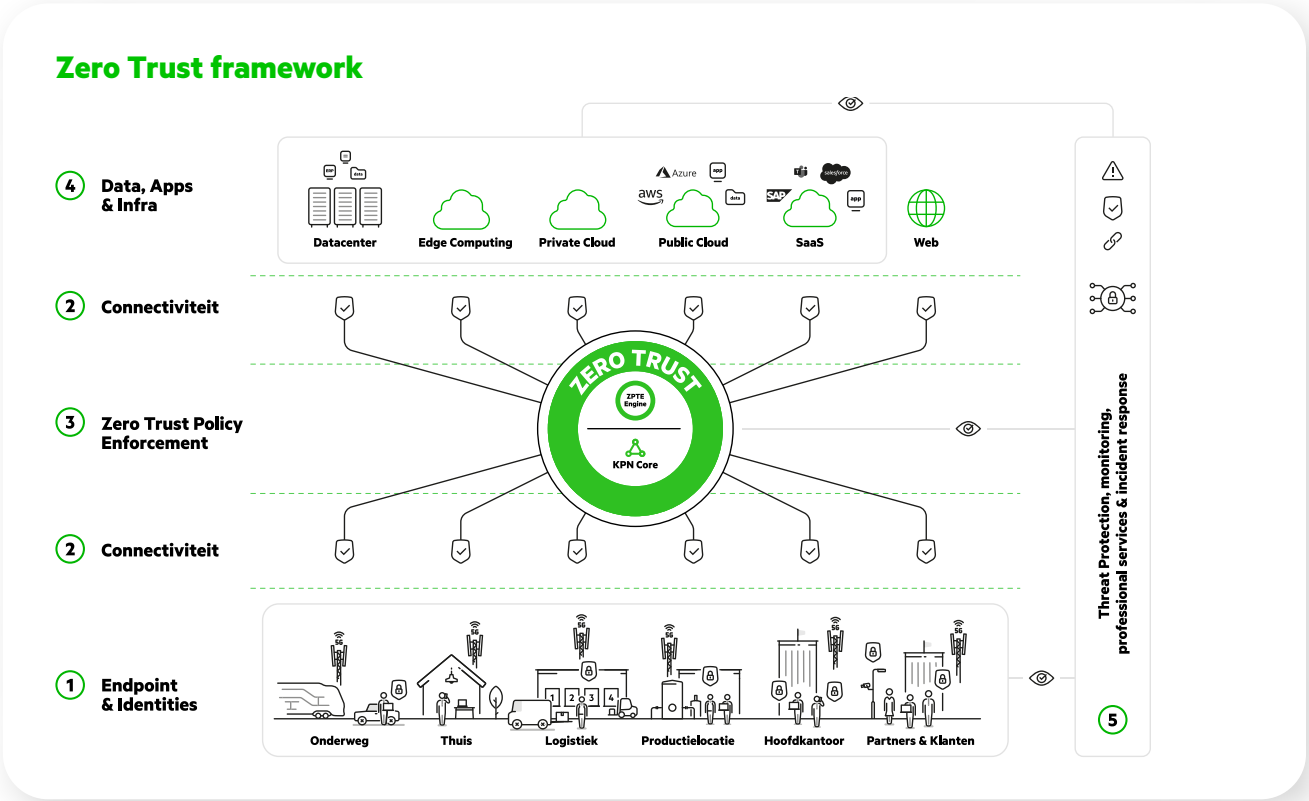
- Authenticatie: alle 'identiteiten' – mensen en apparaten – moeten steeds opnieuw aantonen dat ze zijn wie ze zeggen dat ze zijn.
- (Micro)segmentatie: ze krijgen minimale toegang, precies genoeg om hun werk goed te kunnen doen.
- Monitoring: alle activiteiten worden gemonitord én er wordt geverifieerd of een identiteit een activiteit mag uitvoeren.

In het volgende hoofdstuk ontdek je hoe Zero Trust als basisfilosofie terugkomt in de manier waarop we onze dienstverlening aanbieden. Zowel onze generieke diensten als onze specifieke securitydiensten.

Hoe kunnen we jouw organisatie helpen

Met de ervaring die we in onze eigen organisatie opdoen, verrijken we continu ons aanbod aan securitydiensten en -producten. Natuurlijk, onze reguliere diensten zijn al secure by design. Wat betekent dat je, als je onze diensten gebruikt, sowieso al een solide basisniveau aan security hebt. Maar dat alleen is niet toereikend. Daarom bieden we je een scala aan securitydiensten waarmee je jullie security op het gewenste niveau brengt.

De 5 elementen van het Zero Trust-framework
Ons aanbod aan securitydiensten hebben we georganiseerd in een Zero Trust-framework. Vanuit dit framework kun je heel gericht toewerken naar een solide Zero Trust-architectuur. Het framework bestaat uit 5 elementen. De invulling van elk element kan per organisatie overigens nog flink verschillen. Afhankelijk van bijvoorbeeld je sector, ambities of omvang. Wij helpen je er graag bij.



1. Endpoints en identities

Endpoints, zoals laptops, sensoren, machines en andere apparaten, zijn hét toegangsmiddel tot je infrastructuur, data en applicaties. Deze bescherm je dus goed tegen aanvallen. Daarvoor bieden we je endpointsecurity.
Met identity- en access managementsecurity (IAM) krijgen medewerkers, externe partijen of apparaten bepaalde rechten op een apparaat, applicatie of netwerk. Dan is het wel belangrijk te controleren of een persoon daadwerkelijk is wie hij zegt dat hij is. Dat kan bijvoorbeeld met multifactor authenticatie (MFA).
Voor IAM- en endpointsecurity bieden we diverse diensten, zodat partners en klanten altijd veilig je netwerk kunnen gebruiken. Daarnaast bieden we een secure dataexchange voor veilige data-uitwisseling met ketenpartners, waarbij je data op je eigen servers blijven.

2. Connectiviteit

Vanuit je endpoints start de verbinding met je data en applicaties. Belangrijk dus dat je deze verbindingen veilig opzet. We adviseren om daarvoor verschillende topologieën te gebruiken, via diverse netwerk- en netwerksecurity-oplossingen. Zo kun je in een OT-omgeving kiezen voor een lokaal draaiend private 5G-netwerk dat verbonden is met data en applicaties die on premise of in de edge staan. In een IT-omgeving kun je een SDWAN-netwerk kiezen voor de verbinding met je applicaties. Die verbindingen kun je het best via een controle bij het ZTPE (zie 3) laten lopen.

We bieden VPN- en SDWAN-verbindingen met je eigen datacenter en edge. Ook bieden we oplossingen om private en public clouds direct te bereiken. En we maken het mogelijk om SaaS-applicaties onzichtbaar voor anderen – en daarmee 'afgesloten' van het publieke internet – te bereiken. Op het gebied van netwerksecurity bestaan diverse mogelijkheden varierend zoals Anti-DDoS, Network Access Control (NAC), diverse Firewall-functionaliteiten waaronder sandboxing, IDS, IPS en meer.

3. Zero Trust Policy Enforcement (ZTPE)

Zero Trust Policy Enforcement (ZTPE) is de technologie die bepaalt of je op basis van je identiteit en de context voldoet aan de regels om bij de gevraagde data en applicaties te komen. Die context kan slaan op je apparaat, de vertrouwelijkheid van data, je locatie, het tijdstip, etc.. Zo kun je een zeer fijnmazig security- en toegangsbeleid toepassen.
ZTPE is een samenwerking tussen de gekozen ZTPE-engine en de segmentatie in je netwerk. Toepassingen als Cloud Security Posture Management (CSPM), Data Loss Prevention (DLP) en meer kun je vanuit ZTPE inzetten.

4. Data, applicaties en infrastructuur

Data, applicaties en infrastructuur staan verspreid over steeds meer locaties. In publieke en private cloudomgevingen, in SaaS-applicaties, in het eigen datacenter – soms alleen bereikbaar via internet, soms alleen via het eigen bedrijfsnetwerk. De keuze voor de juiste locaties maak je weloverwogen. Zo kunnen data en applicaties technisch minder geschikt zijn of té kritisch voor de cloud, en houd je ze daarom on premise of in een private cloud. Maar ook daar hebben ze beveiliging nodig – net als de infrastructuur, zoals containers en servers, waar ze op draaien. Belangrijk is het daarom om alle data te classificeren en op basis daarvan je keuzes te maken. Dat geldt ook voor je applicaties, inclusief je schaduw-ICT. Die classificatie kunnen we voor je automatiseren.

Backups van je data, applicaties en infrastructuur zijn natuurlijk onmisbaar in een compleet en modern securitybeleid. We helpen je graag met een immutable backup: een backup in de cloud die niet aangepast kan worden door aanvallers. Inclusief adequate beveiliging ervan.

5. Threat protection, monitoring, professional services en incident repsonse

Met threat protection controleer je de eerste 4 elementen continu op afwijkingen die kúnnen duiden op een security-incident. Voorbeelden van threat protection die we je kunnen bieden zijn een SOC/SIEM-oplossing of XDR, wat staat voor uitgebreide detectie en respons. Ontdek je een mogelijk incident dat niet meer automatisch gestopt kan worden, dan kun je terugvallen op incident response.

Met Logfilemanagement (LFM) verkrijg je inzichten en verminder je de afhankelijkheid van leveranciers door logbestanden centraal te verbinden, samen te voegen en op te slaan. Deze logs kunnen gebruikt worden voor performance monitorring, maar vaker nog als waardevolle input voor threat protection en incident response.

Professional services

Naast al deze veilige diensten en specifieke securitydiensten die bijdragen aan je Zero Trust-architectuur, kunnen we je ook ondersteunen met professional services. Denk aan hulp bij de ontwikkeling van je securitybeleid, awareness trainingen of de inrichting en invulling van verschillende verantwoordelijkheden.

Benieuwd naar je mogelijkheden?

Neem dan contact op met je accountmanager bij KPN. Die schakelt vrijblijvend één van onze securityspecialisten voor je in.

In de praktijk

Klantverhalen over cybersecurity

CIBG: extra beveiliging van privileged accounts

Uitvoeringsorganisatie Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG) verwerkt véél persoonsgegevens. Ook heel gevoelige. Deze zijn opgeslagen in registers als het Donorregister, het BIG-register en het UZI-register. Voor het beheer ervan zijn er accounts met verhoogde rechten in gebruik, de zogenaamde privileged accounts. Het CIBG beschermt deze accounts met onze Privileged Access Management (PAM)-oplossing.

Zo'n PAM-oplossing beveiligt de toegang tot privileged accounts en monitort het gebruik ervan om afwijkingen snel te detecteren. Noodzakelijk, want cybercriminelen kennen de waarde van deze privileged accounts. Uit onderzoek blijkt dat de meeste cyberaanvallen plaatsvinden door misbruik van gestolen privileged accounts. Met PAM organiseer je het centraal beheer van deze accounts, inclusief het maken, beheren en verwijderen ervan, plus het toewijzen van specifieke privileges.

Lees het hele verhaal van het CIBG

Security bij Spaarnelanden: veilig je auto of fiets parkeren

Een fijne leefomgeving, dat belooft Spaarnelanden haar inwoners, ondernemers en bezoekers. In opdracht van de gemeente Haarlem zorgt zij onder meer voor de openbare parkeervoorzieningen. Spaarnelanden heeft 7 gemeentelijke parkeergarages in beheer en een viertal bewonersparkeerarages, met in totaal bijna 4.000 parkeerplekken. Ook worden straatparkeerautomaten beheerd en onderhouden. Plus een aantal grote fietsstallingen die ruimte bieden aan zo'n 8.000 fietsen.
Van een goed beveiligde connectie met het parkeermanagementsysteem in de cloud hangt dus nogal wat af.

Met de parkeergarages en stallingen in Haarlem zorgt Spaarnelanden ervoor dat bezoekers en inwoners makkelijk hun auto of fiets kwijt kunnen en dat ondernemers goed bereikbaar zijn. Onmisbaar in een prettig leefbare gemeente. Ook dragen de parkeergarages bij aan de begroting van de gemeente zodat belangrijke gemeentelijke voorzieningen kunnen worden betaald.
Een storing betekent dus niet alleen reputatieschade, maar drukt direct op de financiering van voorzieningen voor de inwoners. Een hack kan zelfs regelrecht gevaarlijk zijn – de grootste nachtmerrie van een beheerder is dat persoonlijke en/of financiële gegevens van parkeerders buit gemaakt worden. Of dat iemand op afstand de slagbomen kan overnemen.

KPN helpt Spaarnelanden met securityadvies en een MPLS-netwerk Ook maken ze gebruik van een firewall vanuit onze datacenters en Elastic Interconnect (trusted internetverbinding) die redundant zijn uitgevoerd voor extra betrouwbaarheid.

Lees het hele verhaal van Spaarnelanden

Security bij VWS: Welzijn en hart van álle Nederlanders veilig houden

Een departementaal team van bijna 100 securityspecialisten verdeeld over agentschappen, diensten, de inspectie, een planbureau en zelfstandige bestuursorganen (zbo's), soms wel enkele tientallen mensen groot. Het is nogal een club die CISO Oscar Koeroo bij het ministerie van Volksgezondheid, Welzijn en Sport (VWS) onder zich heeft. De data en systemen die zij moeten beschermen zijn eveneens indrukwekkend: van kostbare medicijninformatie tot politiek bepalende bevolkingsonderzoeken. Dichterbij het welzijn en het hart van Nederlanders kun je eigenlijk niet komen.

Natuurlijk, ze hebben niet zoveel staatsgeheimen in huis als de buren van Justitie en Veiligheid, lacht Oscar, maar de informatie die VWS in huis heeft is ook niet mals. Het gaat om informatie die direct raakt aan het welzijn, de gezondheid en het hart van álle Nederlanders. Nogal privacygevoelig dus. En dan heeft hij het nog niet eens over de informatie en systemen van organisaties die onder het departement vallen: het RIVM, het SCP, de NZa – ga maar door. Uiteindelijk zijn hij en zijn team verantwoordelijk voor de continuïteit van de dienstverlening van zowel het hele ambtenarenapparaat op het departement als van de vele organisaties en zbo's die eronder vallen, plus voor het veilig houden van alle gegevens.

VWS kiest voor KPN als leverancier van Identity- en accesmanagement (IAM), Datacenterdiensten (private cloud, Datacenterfaciliteiten voor belangrijke registers, advies bij soevereiniteitsvraagstukken

Lees het hele verhaal van VWS

Daarom KPN

Hier doen we het voor

We zetten alles op alles om iedereen in Nederland te verbinden met een duurzame toekomst. We geloven in de kracht van verbinding. In de kracht van een veilige en betrouwbare verbinding, zodat je altijd goed beschermd bent. Zonder dat je daar veel tijd en energie in hoeft te steken, wat het doel of de omvang van je organisatie ook is. Daar werken wij dag en nacht keihard aan.

Daarom KPN

Vertrouw op het netwerk van Nederland.
Wij hanteren de hoogste betrouwbaarheidsstandaarden. Dat moet ook wel als je verantwoordelijk bent voor dé vitale ICT-infrastructuur in ons land. En daar profiteren al onze klanten van mee.

Wij geloven in partnerschap.
Onze klanten willen meegenomen worden in nieuwe technologische ontwikkelingen. Zien wat het hen oplevert. Niet eenmalig, maar blijvend. Dat zie je aan de manier waarop we onze diensten inrichten: als managed services.

Veiligheid staat bij ons voorop.
Natuurlijk omdat we onze eigen netwerken 24/7 beschermen, maar ook omdat wij zelf veiligheidsdiensten leveren. We voldoen aan alle relevante ISO-normen, aangevuld met streng eigen securitybeleid.

Eén van de duurzaamste providers ter wereld.
We investeren in duurzaamheid van onszelf en onze keten. Ondanks het explosief gestegen dataverkeer daalt ons energieverbruik daardoor jaarlijks én staan we al jaren bovenaan de internationale sustainability-index.

Maak een afspraak
Wil je weten hoe we jouw organisatie vooruit kunnen helpen? Maak een afspraak met je accountmanager of vul vrijblijvend het contactformulier in.

Contactformulier

AD-21513/10-24/KRE