NL SECURE [ID]

CYBER »2022

SECURITY PERSPECTIVES

Samen maken we Nederland veiliger

“Het wordt tijd dat we security-bewustzijn vertalen naar actie”

Marieke Snoep,
Chief Business Market KPN

kpn Security

NL SECURE [ID]

LET'S TALK ABOUT IT

Voorwoord

kpn Security

» De digitale transformatie van de bv Nederland is in volle gang. Steeds meer bedrijven benutten de voordelen van onder andere hybride werken, de cloud en het Internet of Things. Een positieve ontwikkeling. Tegelijkertijd groeit de afhankelijkheid van digitale technologie. We moeten ons ervan bewust zijn dat dit ons ook kwetsbaar maakt voor cyberaanvallen en digitale verstoringen."

Cyber-security is relevanter dan ooit

Cybercriminaliteit is volgens onderzoek uitgegroeid tot de grootste bedreiging voor bedrijven. Een goede IT-beveiliging is dan ook belangrijker dan ooit. Niet alleen om ons te beschermen tegen (statelijke) actoren, maar juist ook als fundament waar nieuwe innovaties op kunnen landen. Laten we zorgen dat we maximaal voorbereid zijn.

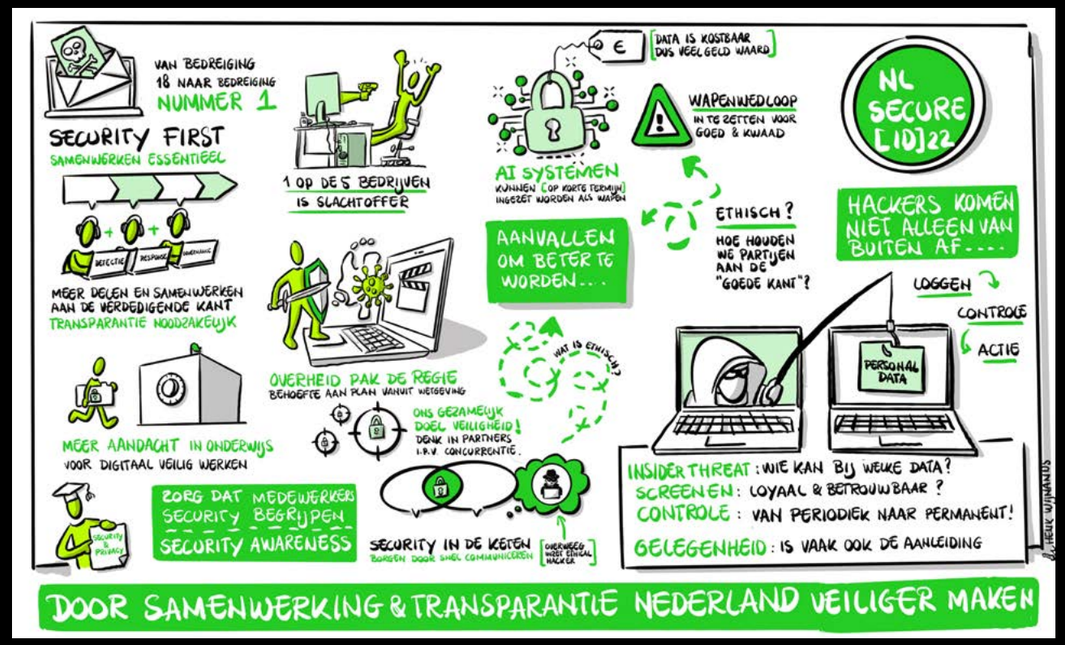
Elke organisatie en werknemer heeft hierin zijn eigen verantwoordelijkheid. Want cybersecurity doe je uiteindelijk echt samen. Dat geldt ook voor de bv Nederland en zelfs daarbuiten. Security houdt niet op bij de grenzen van een land. Ons beste antwoord op de groeiende risico's is nog meer inzetten op kennisdeling en samenwerking op alle niveaus. Security hoort thuis in ons DNA.

Met het magazine Cyber Security Perspectives stimuleert KPN Security deze informatie-uitwisseling binnen de securitycommunity. Toonaangevende experts delen hun visie op informatiebeveiliging in 2022. Niet omdat ze daar een commercieel belang bij hebben, maar omdat ze willen bijdragen aan de digitale weerbaarheid van Nederland.

De inzichten uit dit magazine zijn ook toepasbaar op uw organisatie. Het is de hoogste tijd voor actie. Veiligheid is een basisvoorwaarde voor verdere innovatie, digitalisering en economische groei en vooruitgang. Security first, samen voor een veiliger Nederland. Join us!

Lisette Oosterbroek
Executive Vice President KPN Security

NL SECURE [ID]



LET'S TALK ABOUT IT

kpn Security

Inhoud

» De ransomware-aanval op de Universiteit Maastricht was een wake-upcall voor het Nederlandse onderwijs. Ook bij hogeschool Saxion kwam security nog hoger op de agenda te staan. “Ons team werd fors uitgebreid en we kregen meer budget voor maatregelen”, zegt Henry Meutstege, CISO van Saxion. Toch blijft hij waakzaam. “Cybercriminelen hebben maar één gaatje nodig om binnen te komen.”

Een hogeschool is geen kasteel, maar een open tuin

Henry Meutstege
CISO, hogeschool Saxion

Met ruim 26.000 leerlingen behoort Saxion tot de grotere hogescholen van Nederland. Vanuit vestigingen in Enschede, Deventer en Apeldoorn biedt Saxion een breed scala aan opleidingen aan, verdeeld over dertien academies. Meutstege werkt sinds januari 2020 bij Saxion, eerst nog als securityofficer. Hij kwam binnen op een spannend moment. De Universiteit Maastricht was zojuist het slachtoffer geworden van een ransomware-aanval. De universiteit zag geen andere uitweg dan het betalen van ongeveer 200.000 euro in bitcoins.

Meer budget voor security
Het incident zette de onderwijssector op scherp. “Informatiebeveiliging en privacy waren al belangrijke aandachtspunten binnen Saxion”, benadrukt Meutstege. “Maar we vroegen ons wel af: kan dit ons ook overkomen? Het antwoord daarop was: jazeker.” Het college van bestuur trof dan ook direct aanvullende maatregelen. Zo werd er budget vrijgemaakt voor extra capaciteit. “Voor de aanval had de CISO één privacyofficer en één securityofficer onder zich. Nu zijn dat er elk drie.”

Daarnaast besloot Saxion werk te maken van twee grote verbetertrajecten die al gepland stonden. “De toenmalige CISO wilde Saxion aansluiten bij SURFsoc. Dit is het gezamenlijke Security Operations Centre (SOC) van SURF, een coöperatie van Nederlandse onderwijs- en onderzoeksinstellingen.

Dat traject werd versneld in gang gezet. Ook lag er een plan om de werkplekinfrastructuur te vernieuwen, waarbij we de werkplekken beter onder beheer wilden brengen. Beide projecten kregen door ‘Maastricht’ een flinke boost.”

Nieuw beleid voor privacy en security
Meutstege werd op 1 juli 2021 aangesteld als CISO. Hij is onder meer verantwoordelijk voor het informatiebeveiligingsbeleid. “Ons beleid is volledig geactualiseerd, met een model van SURF als uitgangspunt.” Dit model bestaat uit zes privacy- en vijf informatiebeveiligingsprincipes. Het privacybeleid is gestoeld op de Algemene verordening gegevensbescherming (AVG). “Denk hierbij aan AVG-principes als rechtmatigheid, doelbinding, transparantie en minimalisatie van verwerking. Deze principes hebben wij vertaald naar beleid.”

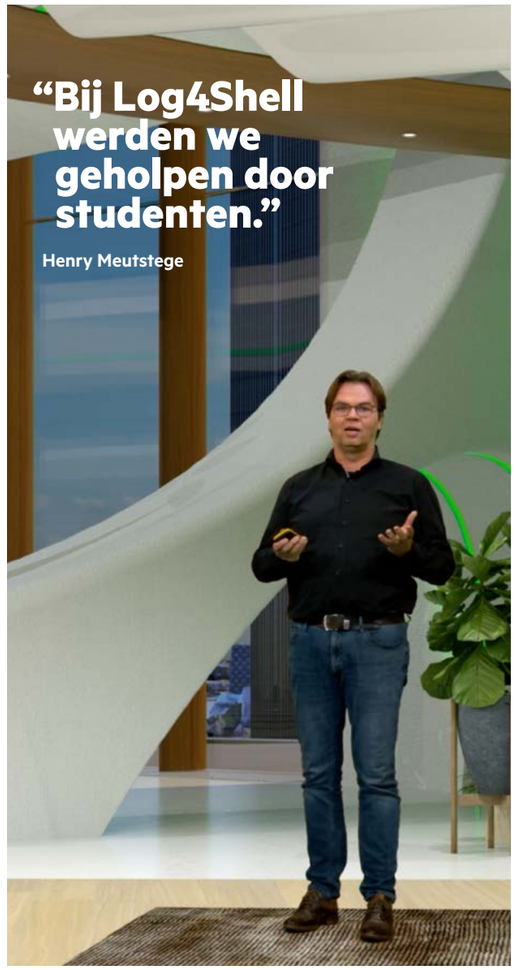
De informatiebeveiligingsprincipes schrijven voor hoe Saxion in de praktijk omgaat met informatiebeveiliging. “We maken keuzes op basis van de risico’s. Een medewerker krijgt precies de toegang die nodig is om zijn werk te doen: niet meer en niet minder. We passen beveiliging en privacy vanaf het begin toe, dus bij elk nieuw initiatief denken we na over de risico’s. En we hanteren een continu verbeterproces voor security. De dreigingen en risico’s verschuiven ook, dus we blijven de boel aanscherpen.”

MFA voorkomt hacks
Een voorbeeld van zo’n verbetering is het aanzetten van multifactorauthenticatie (MFA) voor alle medewerkers en studenten. “Dat heeft bij ons al een aantal grote hacks voorkomen”, vertelt de CISO. “In het afgelopen jaar werd er met diverse accounts opeens vanuit het buitenland ingelogd, terwijl de betreffende studenten gewoon in Nederland zaten. Dankzij MFA mislukten de inlogpogingen, konden de studenten hun account resetten en was er niks aan de hand. MFA is voor ons een waardevolle maatregel die ik elke organisatie zou aanbevelen.”

Ook de logging en monitoring zijn naar een hoger niveau getild. “We gebruiken nu een SIEM-oplossing die per dag 90 gigabyte analyseert. Daardoor halen we nu de juiste inzichten naar boven en kunnen we hierop acteren.” Een andere verbetering is de transitie naar risicogebaseerd werken. “We gaan met de academies in gesprek over de risico’s. Soms accepteren we bewust een risico. Zo experimenteren sommige opleidingen met technologieën als robotisering. Dan zoeken we naar manieren om het risico te verkleinen.”

Wapenwedloop met cybercriminelen
Toch maakt Meutstege zich geen illusies. “Een schoolomgeving is geen kasteel dat je dicht kunt timmeren, maar een open tuin waar iedereen naar binnen kan wandelen. Het is bijzonder lastig om cybercriminelen buiten de deur te houden. Zeker omdat zij hun aanvalsmethoden continu verfijnen. Daar vindt veel innovatie plaats. Bij de Universiteit Maastricht werd bijvoorbeeld de virusscanner uitgezet. Daarom hebben we binnen het SOC afgesproken dat er een alarm afgaat als dat gebeurt. Zo proberen we te anticiperen op aanvallen.”

Ransomware is niet het enige waar de CISO zich zorgen over maakt. “Wij hebben een grote onderzoeksafdeling met veel intellectueel eigendom. Zijn die data goed genoeg beveiligd? Ook datalekken zijn een serieus risico. Bij diverse onderwijsinstellingen is een database met gegevens van studenten en medewerkers gestolen, waarna de hackers deze online probeerden te verkopen. Zo’n hack begint meestal bij een phishingmail. Daarom besteden we extra aandacht aan awareness en organiseren we trainingen voor het personeel.”



Soms moet Meutstege lastige keuzes maken.
“Een onderwijsinstelling heeft geen onbeperkt budget voor informatiebeveiliging. We kunnen niet alle studenten meenemen in een phishingtest, of alle 500 applicaties optimaal beveiligen. Daarom focussen we ons op de grootste risico’s. Onze medewerkers, de gebruikers met de meeste rechten, worden wél onderworpen aan een phishingtest. En we geven prioriteit aan de beveiliging van de kernapplicaties, zoals de studentenadministratie, de cijferadministratie en de roostering.”

“MFA heeft al een aantal grote hacks voorkomen.”

Henry Meutstege

Studenten springen bij
Werken als CISO van een hogeschool heeft ook zo zijn voordelen, vertelt Meutstege. “Log4Shell leverde ons een enorme bak werk op. We moesten honderden leveranciers afbellen om te bepalen welke applicaties de component bevatten. Na een paar telefoontjes werd ons duidelijk dat we dit met een klein team nooit op korte termijn voor elkaar zouden krijgen. Toen ontstond het idee om studenten van de opleiding Security Management in te schakelen. Elke dag werden we geholpen door een groepje van zes tot tien man.”

De studenten kregen een lijst met vragen die ze aan de leveranciers moesten stellen. “We instrueerden ze om goed door te vragen, want een leverancier zegt al snel dat er geen probleem is. Dankzij de studenten wisten we binnen een paar weken precies welke applicaties een risico vormden.
Ook konden we de juiste maatregelen nemen, zoals het achter een beveiligde verbinding plaatsen of zelfs uitschakelen van bepaalde applicaties. Voor de studenten was dit een leerzame ervaring. Zonder hun hulp was het ons nooit gelukt.”

Zo’n creatieve oplossing is volgens de CISO kenmerkend voor het onderwijs. “Ik heb jarenlang in de financiële sector gewerkt. Daar is veel meer budget voor securitymaatregelen. Onderwijsinstellingen moeten selectiever zijn: welke maatregelen hebben we nu écht nodig? Wij gaan efficiënter om met de beschikbare middelen. Daar kan het bedrijfsleven nog wat van leren.”

Henry Meutstege is sinds januari 2020 de CISO van hogeschool Saxion. Hij heeft meer dan 20 jaar ervaring als securityexpert. In het verleden was Meutstege onder andere werkzaam bij Achmea, Delta Lloyd en het Kadaster.

» Cybercriminelen verfijnen hun aanvalstechnieken voortdurend, en gaan steeds vaker stapsgewijs op hun doel af. “Een combinatie van verschillende incidenten kan erop duiden dat er een aanval aan de gang is”, zegt Pieter Molen, Technical Director Benelux bij securityleverancier Trend Micro. “Dan moet je het verband tussen die verschillende incidenten wel kunnen leggen.”

Gebrek aan inzicht is de basis voor bijna elke aanval

Pieter Molen
Technical Director Benelux, Trend Micro

Slachtoffers krijgen het vaak pas door dat ze bijvoorbeeld met ransomware te maken hebben als het te laat is en de aanvaller het losgeld opeist. “Maar dat is natuurlijk nooit de eerste stap in een aanval”, stelt Molen. “Aan het losgeldbriefje gaan heel wat stappen vooraf, zoals een gebruiker die op een phishinglink klikt waarna er sprake is van verdacht gedrag en communicatie met een verdachte bestemming.”

Een op zichzelf staand incident hoeft volgens Molen nog geen reden te zijn tot zorgen. “Het gaat om de combinatie van incidenten. Die combinatie kan duiden op een bepaald type aanval, waardoor je weet welke acties je moet ondernemen. Heb je geen inzicht in wat er allemaal in de aanvalsketen gebeurt, dan zie je niet het hele verhaal van een aanval en weet je niet hoe je moet handelen. Een gebrek aan inzicht is de basis voor bijna elke aanval die niet succesvol gestopt kon worden.”

Marathon
“Sommige typen aanvallen kun je niet meer stoppen met alleen detectie op je endpoints of je servers. Het is niet ‘dit is kwaadaardig, dit stoppen we, en klaar’”, vervolgt de Technical Director Benelux van Trend Micro. Mogelijk zit de aanvaller al lang binnen, te wachten op het juiste moment om toe te slaan. “Eén keer per week in je securitydata kijken, is dan niet voldoende. Je moet continu inzicht hebben in wat er binnen je IT-omgevingen gebeurt. 24 uur per dag, 7 dagen per week.” Verslappen is geen optie.

De dreiging die uitgaat van de kwetsbaarheden in Log4j die eind 2021 aan het licht kwamen, bewijst dat wel. Mede door het snelle handelen van veel organisaties lijkt de eerste schade mee te vallen. Het is echter niet uit te sluiten dat aanvallers alsnog toeslaan, bijvoorbeeld door kwetsbare systemen aan te vallen die organisaties tijdens het patchen over het hoofd hebben

gezien. Of misschien waren ze op het moment van patchen al binnen. Het Nationaal Cyber Security Centrum (NCSC) heeft het dan ook over ‘een marathon waarvan je van tevoren niet weet hoe lang deze is en wanneer je wordt gevraagd om te sprinten’.

Sneller reageren
Met het juiste inzicht is het verloop van een marathon echter wel beter te voorspellen, en weten de deelnemers wat ze moeten doen. Of zoals Molen het omschrijft: “Als je meer ziet, kun je ook sneller reageren.” Deze drie uitgangspunten zijn daarbij volgens hem van belang:

1. Maak de hele IT-infrastructuur inzichtelijk
“Voor het volledige verhaal moet je om te beginnen weten welke assets je binnen je IT-infrastructuur hebt, anders kun je die componenten niet beveiligen. Alle desktops, servers, netwerken, public cloudomgevingen en SaaS-applicaties moeten in kaart worden gebracht, maar ook de IoT-omgevingen die aan het TCP/IP-domein worden gekoppeld.”

“De volgende vraag is: wat is de status van die componenten? Voldoen ze aan de policy’s?”, aldus Molen. “Welke software-versies zijn in gebruik, en zitten daar kwetsbaarheden in? En welke modules roepen applicaties aan? Weet je bijvoorbeeld dat Log4j wordt gebruikt voor logging?” De antwoorden op deze vragen helpen bij het vaststellen van een risicoprofiel voor bijvoorbeeld applicaties en servers.

Ook moet er inzicht zijn in de verschillende aanvalstechnieken waarmee cybercriminelen het aanvalsoppervlak kunnen bestoken. “Het is cruciaal om over de juiste threat intelligence te beschikken.”

“Je moet continu inzicht hebben in wat er binnen je IT-omgevingen gebeurt.”

Pieter Molen

2. Breng alles samen op één centrale plaats
De data die afkomstig zijn van al deze componenten moeten vervolgens op één centrale plaats worden neergezet. Dit om een ‘alert overload’ te voorkomen. Uit onderzoek van Trend Micro blijkt dat organisaties wereldwijd gemiddeld 29 oplossingen voor securitymonitoring gebruiken. Dit maakt het voor securityteams lastig om alerts te prioriteren en cyberrisico’s efficiënt te beheren. “Het niet kunnen prioriteren van waarschuwingen kan de organisatie blootstellen aan cyberaanvallen”, waarschuwt Molen.

Het verkrijgen van een gecentraliseerd inzicht kan volgens Molen op meerdere manieren. “Organisaties staan voor de keuze: make, or buy.” ‘Make’ houdt in dat ze zelf een Security Information & Event Management (SIEM)-systeem inrichten en daar alle IT-componenten en dreigingsmodellen op aansluiten. “Dat kan een goede oplossing zijn, maar bedenk wel dat je een SIEM-systeem continu moet bijhouden. Voeg je nieuwe onderdelen toe aan de IT-infrastructuur? Dan moet je ook weer zorgen voor de integraties met het SIEM-systeem en de dreigingsmodellen aanpassen.”

Organisaties die daar niet de middelen voor hebben, kunnen beter een platform gebruiken dat voorziet in de integraties en de dreigingsinformatie. Hiermee is inzicht en respons vanaf één enkele console mogelijk. “Zo kan de security-afdeling sneller reageren en remediëren en focussen op wat belangrijk is. Trend Micro helpt door acties te automatiseren en stappen te adviseren.”

3. Zorg voor de juiste kennis
Zonder de juiste kennis leidt het verzamelen van data nog niet tot inzicht. “Vergelijk het met een foto of schilderij: vaak ga je dingen pas zien als je er tekst en uitleg bij krijgt.” Zo werkt het volgens Molen ook bij securitydata. Zonder de juiste kennis van aanvalspatronen is het lastig om hier aanvalspatronen in te ontdekken. “Je moet verschillende data-elementen met elkaar kunnen combineren. Pas dan herken je patronen en kun je die bijvoorbeeld koppelen aan een hackersgroep en een ransomwarefamilie.”
Daarbij is het wel belangrijk dat die kennis actueel blijft. Dat is voor veel organisaties een hele opgave, als ze al aan de juiste mensen kunnen komen. “Dat is ook de reden dat steeds meer organisaties ervoor kiezen om detectie en response uit te besteden”, weet Molen.

Driepoot
“Je hebt inzicht in de hele infrastructuur nodig, de data die je daarmee vergaart moet je op een goede manier samenbrengen en je moet de juiste kennis in huis hebben voor het analyseren van de data”, vat Molen samen. Deze drie uitgangspunten zijn volgens hem allemaal even belangrijk. “Vergelijk het met een krukje met drie poten. Als één poot afbreekt, valt het krukje om en lig je op de grond.”

Pieter Molen is al zijn hele carrière actief binnen de IT-sector en bekleedde meerdere functies op het gebied van informatie- en cybersecurity. Vanaf 1 januari 2020 vervult hij bij Trend Micro de functie van Technical Director Benelux.

LET'S TALK ABOUT IT

» Paul Slootmaker en Dimitri van Zantvliet leerden elkaar in 2003 kennen. Bijna twintig jaar later hebben ze allebei ervaring als CISO van een groot Nederlands bedrijf: KPN en NS. Samen maken ze de balans op. Hoe is informatiebeveiliging door de jaren heen veranderd? En welke securityuitdagingen zijn tijdloos?"

De consequenties van een cyberaanval zijn nu vele malen heftiger

Dimitri van Zantvliet & **Paul Slootmaker**
CISO, NS & KPN

Slootmaker denkt met plezier terug aan de eerste kennismaking. "Als relatief onervaren consultant bij KPMG werd ik ingeschakeld door leasemaatschappij Athlon. Dimitri was als CIO mijn opdrachtgever. Athlon had behoefte aan ondersteuning op het gebied van Business Continuity Management. Ik had vooral gewerkt voor grote bedrijven. Dimitri gaf meteen aan dat het er bij Athlon wat praktischer aan toe ging. 'We zitten niet te wachten op academisch gewauwel', zei hij."

Anderhalf jaar lang werkten de twee intensief met elkaar samen. "We waren bij Athlon bezig met de implementatie van een aantal frameworks, waaronder de code-Tabaksblat", vertelt Van Zantvliet. "Paul kon als consultant heel goed luisteren en bracht veel praktisch toepasbare kennis mee. De opdracht werd steeds groter. We pakten zelfs een stuk cybersecurity samen op. Zo hebben we de BS 7799-standaard uit Engeland gehaald en vertaald naar beleid."

Na deze opdracht gingen beiden hun eigen weg. Toch bleven ze contact houden. Jaren later kwamen de carrières van Slootmaker en Van Zantvliet op een vergelijkbaar punt uit. Eerstgenoemde was tot voor kort de CISO van KPN en houdt zich nu bezig met Cybersecurity Risk Monitoring & Reporting, terwijl Van Zantvliet sinds augustus 2021 werkzaam is als CISO van NS. "Vakinhoudelijk zijn we dichter naar elkaar toegegroeid, dat is grappig om te zien", zegt Slootmaker.

Cybercriminaliteit nu grootste risico
Hun vakgebied is in twintig jaar tijd radicaal veranderd. Van Zantvliet: "Informatiebeveiliging was vroeger veel minder zichtbaar. Cybersecurity was slechts een onderdeel van het takenpakket van de CIO en geen zelfstandige functie. Nu ziet het bedrijfsleven cybercriminaliteit als grootste risico. Tien jaar geleden stond dit risico nog op de achttiende plek. Het onderwerp is veel relevanter geworden. Niet alleen in directiekamers, maar ook in de samenleving."

Slootmaker beaamt dat. “Het dreigingslandschap is compleet veranderd. Ransomware is uitgegroeid tot een miljardenindustrie. Twintig jaar geleden vond er wel digitale criminaliteit plaats, maar het was van een totaal andere orde dan nu. We waren toen vooral bezig met beleid, risicoanalyses en het vastleggen van preventieve beveiligingsmaatregelen, zodat je kon aantonen dat je een plan had. Er was veel minder aandacht voor detectie, respons en recovery.”

“Door de digitalisering is alles anders geworden”, vult Van Zantvliet aan. “De wereld is nu hyperconnected door bedrijven zoals KPN. De consequenties van een cyberaanval zijn vele malen heftiger dan vroeger, en ze lopen over in het fysieke domein. Een ransomware-aanval op een ziekenhuis kan zomaar levens kosten. Ook de securitytechnologieën zijn enorm veranderd. De cyberfunctie wordt nu in toenemende mate geautomatiseerd met behulp van AI en machine learning. Dat laatste geldt overigens ook voor de aanvallers.”

Basishygiëne blijft een uitdaging

Toch zijn er volgens de twee experts ook overeenkomsten tussen vroeger en nu. “Security begint nog steeds bij de basishygiëne”, stelt Slootmaker. “Zo moeten het asset-management en patchmanagement op orde zijn. Deze basismaatregelen zijn natuurlijk niet voldoende om veilig te zijn, maar zo voorkom je wel 80 procent van de incidenten. Op dit punt ging het vroeger al mis, en dit blijft een uitdaging.”

Van Zantvliet noemt ook het menselijk gedrag als overeenkomst tussen toen en nu. “De menselijke firewall is niet per se beter geworden. Ons gedrag verandert niet, maar komt op een andere manier tot uiting.” Dat geldt volgens de CISO van de NS ook voor crimineel gedrag. “Vroeger probeerden we met een zilverpapiertje gratis te bellen in een telefooncel. Nu zijn er scriptkiddies die het wifinetwerk in de treinen proberen te misbruiken.”

Hoge werkdruk

De twee constateren allebei dat het werk van securityprofessionals er niet makkelijker op is geworden. Slootmaker: “Onze netwerken worden steeds complexer en een aanvaller hoeft maar één zwakke plek in je verdediging te vinden. Statelijke actoren en ransomwarebendes hebben bijna oneindige middelen. Securityexperts staan onder hoge druk om hier een adequate verdediging tegenover te stellen, vaak met beperkte middelen. Het is een ongelijke strijd.”

Die druk eist soms zijn tol. “Een topsporter heeft na een topprestatie tijd om bij te komen, maar een securityprofessional niet. Na een aantal incidenten kort achter elkaar worden mensen moe en gefrustreerd.” Ook Slootmaker zelf vond de CISO-rol af en toe zwaar. “Ik begon twee jaar geleden met het Citrix-lek en eindigde met Log4Shell. Je staat altijd aan. Nu ik een nieuwe opdracht heb gekregen, is er wel een last van mijn schouders gevallen.”

Paul Slootmaker werkt al sinds 2009 in verschillende functies bij KPN. Van eind 2019 tot eind 2021 vervulde hij de rol van CISO. Momenteel is Slootmaker verantwoordelijk voor Cybersecurity Risk Monitoring & Reporting binnen KPN.

Van Zantvliet herkent dat. “Het is een infinite game waarbij je altijd maar bezig bent om die hyperconnected omgeving dicht te houden. Soms heb je het idee dat je nooit kunt winnen van de hackers. Ook binnen onze teams bestaat het risico op burn-out. Als CISO probeer je te zorgen voor een positieve mentaliteit. We gaan de strijd misschien nooit winnen, maar we proberen wel elk jaar beter te worden. De ene keer slaan we een aanval af, de andere keer worden we wellicht gehackt en leren we ervan.”

Securitykennis is schaars

KPN en de NS opereren in een andere sector, maar er zijn ook gelijkenissen. Zo zijn beide Nederlandse bedrijven onderdeel van de vitale infrastructuur. Daarmee staan ze voor vergelijkbare securityuitdagingen: de continuïteit van hun dienstverlening moet te allen tijde gewaarborgd zijn. Slootmaker en Van Zantvliet zien het aantrekken van securitykennis daarbij als de grootste uitdaging voor hun organisatie.

Slootmaker: “We kunnen niet zonder goede securityprofessionals: van ethical hackers en netwerkexperts tot incident-responders en consultants. Nu ben ik bijvoorbeeld betrokken bij de implementatie van nieuwe regelgeving voor telecomoperators om de veiligheid van het netwerk te vergroten. Voor zo’n klus heb je allerlei soorten expertise nodig. Die mensen zijn niet makkelijk te vinden.”

“In het algemeen is het heel lastig om de juiste kennis en kunde binnen te halen”, erkent ook Van Zantvliet.

“Het aanbod is zeer beperkt, zeker als je ervaring zoekt. NS biedt ook niet de hoge salarissen uit het bedrijfsleven, dus je mikt op de mensen die maatschappelijke relevantie zien in het werk. Dat is voor mij ook de reden waarom ik bij de NS ben gaan werken. Ik wil bijdragen aan de digitale weerbaarheid van mobiel Nederland.”

Minimale eisen aan security

Slootmaker en Van Zantvliet hebben op dat vlak nog wel een advies voor de regering. Zij pleiten voor wettelijke minimale eisen aan security. “Ik vind het redelijk asociaal dat sommige bedrijven wel volop mee willen in de digitalisering, maar weigeren te investeren in cybersecurity”, aldus Van Zantvliet. Slootmaker wijst erop dat cyberaanvallen steeds vaker via de supplychain lopen. “We moeten de gehele keten beter beveiligen. Blijkbaar lukt dat alleen met regelgeving.”

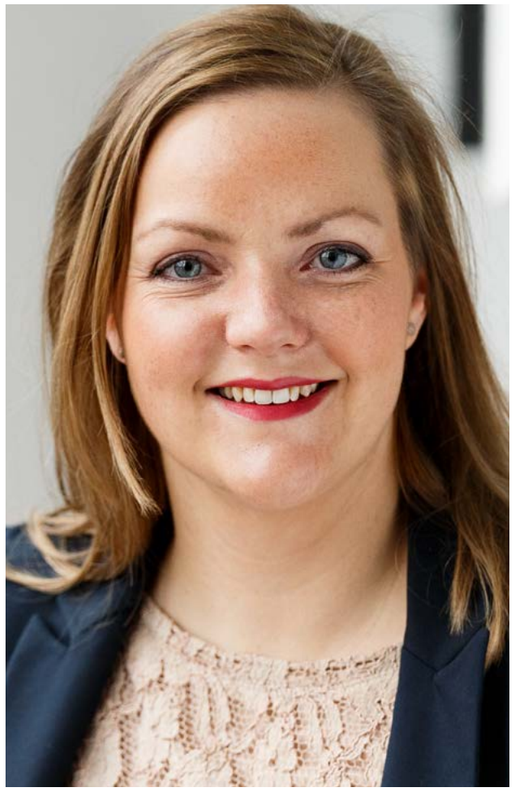
De twee sluiten af met een advies aan medesecurity-professionals. “Blijf jezelf ontwikkelen”, zegt de CISO van NS. “Op professioneel gebied, maar ook op menselijk gebied. Neem geen genoegen met stilstand.” Slootmaker: “En blijf oefenen. Zorg dat je voorbereid bent op een cyberaanval, want ondanks alle preventieve maatregelen weet je dat het een keer misgaat.”

Dimitri van Zantvliet heeft dertig jaar IT-ervaring. Sinds augustus 2021 is hij de CISO van NS. Hij houdt zich onder meer bezig met cyberrisicomanagement op het gebied van IT, OT en IoT en met Europese spoorwegprojecten.

» Slimme apparaten moeten vanaf 1 augustus 2024 voldoen aan minimale cyberveiligheidseisen. Fabrikanten hebben dus nog twee jaar de tijd om hun producten te laten testen en certificeren. “Maar wacht daar niet te lang mee”, waarschuwt Sabyne van Mourik, Business Development Manager bij Kiwa Nederland. “Het gaat om enorme aantallen IoT-producten.”

Maak haast met certificering IoT-producten

Sabyne van Mourik,
Business Development Manager, Kiwa Nederland



Consumenten moeten erop kunnen vertrouwen dat aangeschafte producten veilig zijn voor gebruik. Zo geeft een CE-markering bij elektrische apparaten aan dat de fabrikant of importeur verklaart dat het product voldoet aan de geldende eisen en hier verantwoording voor neemt. Eisen aan elektrische apparaten zijn dat ze getest zijn op aspecten zoals brandveiligheid en elektromagnetische compatibiliteit.

Dit vertrouwen willen ze eveneens hebben bij de aanschaf van connected apparaten, of het nu een slimme koelkast, deurbel of misschien zelfs wel een wc-pot is. “Daar komen consumenten echter bedrogen uit”, zegt Van Mourik. “Voor producten die zijn verbonden met het Internet of Things is de cyberveiligheid gewoon nog helemaal niet aantoonbaar ingeregeld of zijn er überhaupt geen wettelijke eisen. En dat terwijl het aantal security-incidenten met slimme apparaten de afgelopen jaren snel toeneemt.”

Certificering relevanter dan ooit
“Certificering van met het internet verbonden producten is relevanter dan ooit”, stelt Van Mourik. Zonder een certificaat moeten consumenten zelf maar inschatten hoe cyberveilig een IoT-device is, en dat wordt volgens de Business Development Manager van Kiwa Nederland steeds lastiger. “Zeker als je ziet hoe tegenwoordig alles met elkaar is verbonden. De keten wordt steeds complexer.”

Als voorbeeld geeft ze de slimme wc-pot die aan de hand van uitwerpselen de gezondheid van de gebruiker meet. “Deze closetpot herkent de gebruiker en zorgt ervoor dat meetgegevens automatisch in een elektronisch patiëntendossier in de cloud worden opgeslagen. Indien nodig kan de huisarts dan aan de bel trekken.” Bij dit concept zijn veel partijen betrokken, van de leveranciers van de closetpot, de sensoren en de software tot de cloudprovider waar de gegevens worden opgeslagen. Het is dan voor de consument of een inkoper lastig om te achterhalen of al die partijen de techniek, processen en mensen op orde hebben, en of persoonsgegevens veilig zijn en blijven. “Een certificaat zorgt voor transparantie en laat zien dat de toiletpot aan de minimale veiligheidseisen voldoet.”

“Ga zo snel mogelijk met een Notified Body om de tafel zitten.”

Sabyne van Mourik

De fabrikant van in dit voorbeeld de wc-pot is eveneens gebaat bij die transparantie. “Traditionele fabrikanten die nu slimme producten op de markt brengen, krijgen met allerlei nieuwe vraagstukken te maken. Hoe weet je dat de geselecteerde software secure by design is? En hoe weet je dat de cloudinfrastructuur en de data die daar worden neergezet veilig zijn? Door de complexiteit van de keten ziet een fabrikant het vaak zelf niet meer. Een certificering biedt ook de fabrikant inzicht in de cyberveiligheid van zijn product.

Radio Equipment Directive
Vanaf 1 augustus 2024 moeten slimme apparaten in Europa bovendien voldoen aan de cybersecurity-eisen uit de Radio Equipment Directive (RED). Zo worden er eisen gesteld aan het wachtwoordgebruik, het updaten van de software en het beheren en beschermen van persoonlijke data. De fabrikant mag geen CE-markering aanbrengen op IoT-producten die hier niet aan voldoen. Deze mogen dus niet op de Europese markt worden verkocht.

Compliance met de RED kan bijvoorbeeld worden aangetoond door producten te toetsen aan de ETSI EN 303 645-standaard die eisen en procedures bevat voor de cyberveiligheid van IoT-apparaten. “Er is nog geen geharmoniseerde standaard waartegen een leverancier zelf de betreffende IoT-producten kan testen of ze aan de security-eisen voldoen”, legt Van Mourik uit. Alle producten moeten dus voor een onafhankelijke beoordeling worden aangeboden bij een Notified Body zoals Kiwa, zolang er geen geharmoniseerde standaard beschikbaar is. Deze instantie stelt aan de hand van een assessment vast of het product aan de eisen voldoet. Hierdoor komt het product in aanmerking voor een certificaat en kan het product met CE worden gemarkeerd.

Zoek de samenwerking
“Wacht niet te lang met het laten certificeren van je IoT-producten”, zo drukt Van Mourik fabrikanten op het hart. “Het gaat om enorme aantallen producten die moeten worden gecertificeerd. Veel fabrikanten hebben al snel zo’n 150 IoT-producten in het portfolio. Denk daarom al in een vroegtijdig stadium na over wat de impact van de nieuwe wetgeving is op je eigen portfolio. Zorg dat je de risico-analyse op orde hebt en denk na over welke budgetten je vrijmaakt voor certificering.”

“Ga bovendien zo snel mogelijk met een Notified Body om de tafel zitten”, vervolgt de Business Development Manager van Kiwa Nederland. “Zoek daarbij de samenwerking op. Zodat we samen na kunnen denken over hoe certificeren behapbaar kan worden gemaakt en kunnen bepalen hoe het testplan eruitziet. Zorg er bijvoorbeeld voor dat er tijdens de tests iemand beschikbaar is voor het beantwoorden van vragen. Certificeringsinstellingen kunnen nog wel eens gezien worden als een black box waar je iets naartoe stuurt en waar dan misschien een keer een resultaat uitkomt. Wij willen hierin echter het tegendeel bewijzen. Wij willen er juist samen met de klant voor zorgen dat een certificeringstraject zo snel mogelijk wordt afgerond.”

Volgens Van Mourik hebben ook inkopende partijen een rol in het versnellen van de certificeringstrajecten. “Richt je inkoopbeleid nu al in conform de RED en bedenk welke eisen je moet stellen aan de cyberveiligheid van de producten die je inkoopt. Op die manier creëer je een push richting de markt. En waarom zou je wachten met de inkoop van veilige producten?”

Testlab KPN Security
Kiwa Nederland heeft zelf het nodige gedaan om certificeringstrajecten te versnellen. Zo biedt de instantie een ‘pre-compliance check’. Van Mourik: “We bekijken de producten, bepalen welke scope van toepassing is, helpen bij het opstellen van een testplan en maken een voorzichtige inschatting of een product de test wel of niet doorstaat. Hiermee kan de leverancier onderbouwd een afweging maken welke producten als eerste worden aangeboden voor certificering, en welke producten eerst nog aanpassingen nodig hebben.”

Voor het daadwerkelijk testen van consumentenproducten heeft Kiwa een overeenkomst gesloten met KPN Security. Binnen de overeenkomst toetst KPN Security in zijn hoogwaardige testfaciliteiten of IoT-producten voldoen aan de ETSI EN 303 645-standaard en dus in de basis voldoende cyberveilig zijn. De testfaciliteiten worden door Kiwa als onafhankelijke toetsende instelling gemonitord. Kwaliteit, onafhankelijkheid en onpartijdigheid blijven op die manier gewaarborgd. Kiwa kan daardoor de testresultaten – in combinatie met de resultaten van door Kiwa uitgevoerde aanvullende tests – accepteren voor het uitgeven van een productcertificaat.

“Voor fabrikanten zijn korte doorlooptijden belangrijk. Zij willen gewoon zo snel mogelijk met een product naar de markt”, aldus Van Mourik. “KPN beschikt over een state-of-the-art testlab met de capaciteit die nodig is voor het op grote schaal testen van IoT-producten. Binnen de labomgeving van KPN Security kunnen wij klanten snel helpen.”

Label in ontwikkeling

Kiwa ontwikkelt bovendien een label voor gecertificeerde cyberveilige IoT-producten. “Daarmee laat je als fabrikant in aanloop naar 1 augustus 2024 al zien dat je producten onafhankelijk zijn getest door een Notified Body.”

“Dat label zullen we ook na deze deadline verder ontwikkelen, zodat aan het label is te zien aan welke zaken bovenop de minimale veiligheidseisen nog meer wordt voldaan”, besluit Van Mourik. “Dit ontwikkelen we in samenwerking met marktpartijen, het moet immers toegevoegde waarde bieden voor de marktpartijen.”

Sabyne van Mourik heeft ruim twintig jaar ervaring op het gebied van brandveiligheid en security. Bij Kiwa Nederland was ze onder andere manager van de Fire Safety & Security-products business unit. Sinds januari 2021 is ze als Business Development Manager werkzaam bij Kiwa Nederland en met name verantwoordelijk voor de ontwikkeling van cybersecurity test- en certificeringsdiensten voor IoT-producten.

NL SECURE [ID]

» Het klassieke advies van veel securityprofessionals? Begin bij het begin. Inventariseer de assets, de kroonjuwelen, de risico's. Om vervolgens met die informatie passende maatregelen te nemen. Volgens Oscar Koeroo, CISO van het ministerie van Volksgezondheid, Welzijn en Sport (VWS) is die strategie aan herziening toe. Hij pleit voor het benaderen van security als een verzameling van doolhofjes. "En doolhofjes los je sneller op van achter naar voren."

Benader security achterstevoren

Oscar Koeroo
CISO, het ministerie van VWS

Koeroo baseert zijn inzicht op een jeugdherinnering: het oplossen van doolhofjes in de Donald Duck. "Ik kwam er als kind al snel achter dat je deze sneller van achter naar voren oplost. Je komt dan veel minder keuzepaden tegen." Zo werkt het volgens hem ook voor security. "Je moet eerst heel goed bedenken naar welke situatie je toe wilt, of welk probleem je wilt tackelen. Je moet dat einddoel niet vaag houden, maar heel scherp definiëren. Vervolgens ga je terugredeneren. Hoe kom ik daar zo goed en zo efficiënt mogelijk? Het doel bepaalt de missie, en niet andersom."

Deze manier van denken kwam hemzelf goed van pas toen hij vorig jaar startte in zijn functie als CISO Concern van het ministerie van VWS. "Mijn angst was dat er in mijn beginperiode een hack zou plaatsvinden, terwijl ik nog niet goed wist hoe de organisatie in elkaar stak. Ik ben er toen van uitgegaan dat er al een hacker binnen was. Een die bovendien elk moment kon toeslaan."

Assume breach
Vanuit dat 'assume breach'-uitgangspunt is hij terug gaan redeneren. "Wat moet ik als eerste doen? Dat zijn de juiste mensen informeren en een crisisteam samenstellen. Daar heb ik contactinformatie voor nodig. Ik moet weten wie waarvoor verantwoordelijk is. Hoe ik die personen kan bereiken. Wie de lead neemt in een respons.

Die informatie moet je paraat hebben voor een crisis losbarst. Niets is zo vervelend als moeten rondbellen en -appen tot je de juiste mensen te pakken hebt, terwijl een hacker alles aan het slopen is."

Deze benadering is op allerlei deelgebieden toepasbaar. Bijvoorbeeld op het stoppen van de aanval op het moment dat deze plaatsvindt. "In plaats van alle mogelijke securityoplossingen nagaan die een aanval kunnen stoppen, kun je ook inventariseren welke middelen een aanvaller nodig heeft. En hoe, wanneer en onder welke omstandigheden het onschadelijk maken van die middelen effectief is. Een hacker heeft bijvoorbeeld altijd een werkende netwerkverbinding nodig. Misschien kun je al een aanval afslaan door simpelweg de netwerkkabel eruit te trekken."

kpn Security

Stay out of my territory
Een stapje verder terug is het voorkomen dat hackers überhaupt binnenkomen. Volgens Koeroo is het hiervoor belangrijk dat je je eigen omgeving nauwkeurig onder de loep neemt. "Het belangrijkste is dat je aanvalsoppervlak zo klein mogelijk blijft. Daarvoor moet je weten welke apparaten er op je bedrijfsnetwerk zijn. Scan je bedrijfsnetwerk, doe een pentest, en doe wat met die informatie. Het is belangrijk dat je precies weet wat je tegenstander al heeft kunnen ontdekken over jouw infrastructuur."

Belangrijk is volgens Koeroo dat je genoeg barrières opwerpt. "Het is onzinnig om daarvoor te investeren in een enorme hoeveelheid securityoplossingen", merkt hij op. "Het toepassen van bijvoorbeeld multifactorauthenticatie voor alle belangrijke accounts kan voor hackers al genoeg reden zijn om jouw organisatie over te slaan. Ze gaan namelijk liever voor laaghangend fruit. Dat kost hen minder geld en middelen." In plaats van het installeren van zoveel mogelijk technische securityoplossingen kun je volgens hem beter focussen op het definiëren van de juiste einddoelen. Mensen zijn in dat proces onmisbaar. "Zoek de juiste mensen bij je plannen en laat hen meedenken, of zelfs meebeslissen. Nodig die netwerk- of systeembeheerder uit in de boardroom als er beslissingen vallen over zijn vakgebied. Daar zit waardevolle kennis. Het is belangrijk dat de mensen vanaf het begin bij je einddoelen betrokken zijn. Dat vergroot hun betrokkenheid." Ook niet-technisch personeel is daarin cruciaal. "Wil je succes boeken, dan moet je iedereen meenemen in je plannen. Ook, of misschien wel vooral diegenen die in hun dagelijks werk ver van het onderwerp afstaan."

Gratis winst
Veel 'gratis' winst valt volgens Koeroo te behalen bij het ontwikkelteam. "Ga eens praten met de mensen in je developer-teams over de CI/CD-straten. Daar kun je zoveel kwaliteitszaken in borgen dat er voor hackers maar weinig overblijft om te misbruiken. En hoe gaaf is het als je developerteam naar jou toekomt en situaties schetst waarin hackers misbruik van de software kunnen maken. Dat gebeurt alleen als je hen meeneemt in je einddoel en hen stimuleert om informatie terug te geven."

"Bereid elkaar voor op een crisis."
Oscar Koeroo

Ook bij de uitrol van het securitybeleid in de hele organisatie is de focus op het einddoel weer onmisbaar. "Je moet het uiteindelijke doel van het beleid altijd uitleggen. Zeker ook aan digibeten", merkt hij op. "Leg hen uit wat je van plan bent, en wat zij kunnen doen om een cyberaanval te voorkomen.Maar ook waarom bepaalde beleidsregels daartoe bijdragen. Dat waarom is cruciaal.

Oscar Koeroo is CISO Concern bij het ministerie van Volksgezondheid, Welzijn en Sport (VWS). Daarvoor was hij onder andere actief in de CISO-afdeling van KPN in het team Strategy & Policy. Zijn expertises liggen onder andere bij identitymanagement, toegepaste cryptografie, systeembeveiliging en netwerkbeveiliging.

Neem hen mee in jouw omgekeerde route door het doolhof. Maak duidelijk waarom je vanuit het vastgestelde doel terugwerkt, en hoe het beleid en de securitymiddelen daaraan bijdragen. Niet met technisch securityjargon, maar gewoon in jip-en-janneketaal. Als je die waarom-vraag niet kan beantwoorden, ben je in mijn optiek af."

Trainingen: voorbij compliance

Een goede manier om het begrip van technisch en niet-technische medewerkers en de betrokkenheid bij security te vergroten, is volgens Koeroo via trainingen. Maar ook hier geldt de omgekeerde route door het doolhof. Want ook trainingen kun je volgens hem beter achterstevoren benaderen. "Ik zie veel bedrijven trainingen afwerken voor een compliance-vinkje. Doodzonde. Bedenk eerst wat nu eigenlijk het doel van je training is. Zo kun je een training veel beter inrichten."

Daarbij mag je de doelgroep niet uit het oog verliezen, merkt hij op. "Trainingen lijken vaak wel bedoeld voor mensen die technische informatica gestudeerd hebben. Onderschat niet wat de emotionele reactie is van mensen die een training volgen die ze niet begrijpen. 'Dit lukt mij nooit, een hacker is altijd slimmer dan ik.' Met die aanpak verzwak je mensen, in plaats van dat je ze in hun kracht zet. Dat kan nooit de bedoeling zijn."

"Je moet je einddoelen scherp definiëren."

Oscar Koeroo

» Cybersecurity moet hoger op de nationale agenda komen te staan. Dat vindt Irma Jepma, directeur Strategy, Sourcing, Cybersecurity & Change bij Coöperatie VGZ. Ook pleit Jepma voor het breed delen van cybersecurity-informatie. "Zorgverzekeraars hebben een cruciale rol in het Nederlandse zorgstelsel. Zij zijn erbij gebaat dat beschikbare informatie snel wordt gedeeld."

Zo belangrijk vindt de regering cybersecurity blijkbaar nog niet

Irma Jepma
Coöperatie, VGZ

Met ruim vier miljoen leden is Coöperatie VGZ een van de grootste zorgverzekeraars van Nederland. Jepma is onder andere verantwoordelijk voor het securitybeleid. Haar primaire taak: het beschermen van de gegevens van de leden. "Dat zijn onze kroonjuwelen. Wij moeten garanderen dat deze bij ons in veilige handen zijn. Een datalek zou enorme consequenties hebben, zowel voor onze leden als voor Coöperatie VGZ zelf."

Focus op awareness

Coöperatie VGZ doet er dan ook alles aan om klantgegevens te beschermen. "We beveiligen onze endpoints extra goed en doen controles op de toegang tot gegevens", geeft Jepma als voorbeeld. "Ook security-awareness is een belangrijk aandachtspunt. We trainen het personeel in gevaarherkenning en houden periodiek phishingsimulaties. Dit houdt onze medewerkers scherp en alert. Zij zijn immers onze first line of defence. Verder worden al onze mensen gescreend en zorgen we dat ze alleen toegang hebben tot de gegevens die nodig zijn voor hun werk."

Ondanks alle maatregelen sluit Jepma niet uit dat een slimme cybercrimineel binnen kan komen bij bedrijven via bijvoorbeeld een phishingaanval. “Zelfs een ervaren securityprofessional kan in een phishingmail trappen. Sommige aanvallers zijn zo gewiekst dat berichten niet van echt zijn te onderscheiden. Er worden zelfs hele websites nagemaakt. Je moet veel alerter zijn dan je denkt.”

“Cybersecurity verdient een eigen ministerie.”

Irma Jepma

Continu DDoS-aanvallen
Phishing is slechts een van de digitale gevaren waarmee de zorgverzekeraar te maken heeft. “Op DDoS-aanvallen en gerichte aanvallen op applicaties zijn we ook alert”, vertelt Jepma. “Onze security-oplossingen kunnen gelukkig veel aanvallen al bij de voordeur herkennen en stoppen.” Coöperatie VGZ is eveneens beducht op ransomware. “Ransomware brengt de continuïteit van onze dienstverlening in gevaar, net als een DDoS-aanval. Dat is dan niet alleen vervelend voor onze leden als zij bijvoorbeeld geen declaraties kunnen indienen, maar ook voor de zorgaanbieders. Zij hebben de betalingen van zorgverzekeraars nodig om aan hun financiële verplichtingen te voldoen.”

Dreigingsinformatie delen
Volgens Jepma hebben zorgverzekeraars een systeemfunctie in het Nederlandse zorgstelsel. Toch worden zij nog niet tot de vitale infrastructuur gerekend. Zorgverzekeraars ontvangen dus ook geen dreigingsinformatie van het NCSC. Wel kunnen zij een beroep doen op de kennis van het Digital Trust Center. “Informatie over digitale bedreigingen is net zo relevant voor de vitale infrastructuur als voor de rest van het bedrijfsleven. Ik zou graag zien dat relevante cybersecurity-informatie vanuit één punt breed wordt gedeeld. Waarom is dit geen generieke voorziening in Nederland?”

“Nederland is een klein land dat feitelijk één groot ecosysteem vormt. Alles is met elkaar verweven. Als één cruciale schakel getroffen wordt door een cyberaanval, hebben we daar allemaal last van. Ik snap wel dat het NCSC voorzichtig is met het delen van vertrouwelijke informatie, maar daar zijn oplossingen voor. Zo kun je als NCSC bedrijven uitvoerig screenen, of je deelt de informatie via CERT’s. Nu valt een aantal cruciale organisaties nog steeds buiten de boot.”

Recht op redteaming
Daarmee stipt Jepma nog een belangrijk onderwerp aan: security in de keten. Een aanval op één bedrijf kan talloze ketenpartners raken. Hoe wapent Coöperatie VGZ zich hiertegen? “Elke IT-leverancier die wij contracteren, dient de beveiliging op orde te hebben. Als wij geen eisen stellen aan security, introduceren wij een potentiële kwetsbaarheid voor Coöperatie VGZ. Wij willen dus weten hoe veilig een leverancier is. Dan kan bijvoorbeeld via een assurance-verklaring. Maar zo’n verklaring zegt zeker niet alles.”

“In onze contracten nemen we mede daarom het recht op redteaming mee. Soms wordt dit door leveranciers ter discussie gesteld. Dan ben je toch geneigd te denken dat ze iets te verbergen hebben, al realiseer ik me dat dat te kort door de bocht is. Ik zie redteaming als een hele mooie kans om te verbeteren en de cyberweerbaarheid nog verder te vergroten.”

Digitale veiligheid
“Het is de verantwoordelijkheid van Coöperatie VGZ om de persoonsgegevens van miljoenen Nederlandse burgers te beschermen. Deze taak nemen wij uiterst serieus”, zegt de bevlogen directeur. “Dat zou elke organisatie moeten doen. Ik maak me soms wel zorgen over hoe wij in Nederland met informatiebeveiliging omgaan. Ik realiseer me echter ook heel goed dat iedereen slachtoffer kan worden en dat één foutje grote gevolgen kan hebben.”

Volgens Jepma heeft de overheid een belangrijke taak als het gaat om het waarborgen van de veiligheid van de Nederlanders. “Niet alleen fysiek, maar vooral ook digitaal. De financiële sector staat onder toezicht van De Nederlandsche Bank. Wij moeten aan strikte eisen voldoen op het gebied van cybersecurity. Hoe is het toezicht geregeld voor de vele andere organisaties die grote hoeveelheden gevoelige gegevens van burgers verwerken?”

“Een aanval op één bedrijf kan grote gevolgen hebben voor velen.”

Irma Jepma

Urgentie niet aanwezig
Een oplossing zou volgens haar kunnen zijn dat de regering minimale securityeisen definieert, controleert én handhaaft. Maar of dat nu ook gaat gebeuren? “Cybersecurity verdient een eigen ministerie. In plaats daarvan hebben we nu een staatssecretaris voor Koninkrijksrelaties en Digitalisering. Zo belangrijk vindt de regering het blijkbaar nog niet.”

“De urgentie van het probleem wordt niet ingezien”, stelt Jepma. “In het regeerakkoord staat dat het kabinet met een meerjarige securityaanpak komt. Een aanpak is één, maar het komt aan op de implementatie. Wie gaat dat doen? En hoe precies? Ons land heeft geen geweldig trackrecord als het gaat om grootschalige ICT-projecten. Ik vraag me af wie uit het kabinet dit in goede banen kan leiden. Ik zie die mensen niet en daar maak ik mij grote zorgen om.” Zou zij zelf minister van Digitalisering en Cybersecurity willen worden? “Als Mark of Sigrid mij had gevraagd, was ik wel gekomen.”

Irma Jepma heeft ruim 30 jaar IT-ervaring. Sinds 2019 is ze directeur Strategy, Sourcing, Cybersecurity & Change Bij Coöperatie VGZ. Daarvoor vervulde ze diverse functies op het gebied van IT-infrastructuur, SLA- en businessmanagement.

» Als een hacker écht binnen wil komen, dan lukt dat meestal ook. Er zit altijd wel een zwakke plek in de beveiliging. “Ik ken geen enkel bedrijf dat 100 procent secure is”, zegt Mark de Groot, Team Lead van het KPN REDteam. Volgens De Groot is het doel van cybersecurity om daar zo dicht mogelijk bij in de buurt te komen. “Dat begint bij een goed inzicht in je data en assets.”

Een aanvaller staat altijd met 1-0 voor

Mark de Groot
Team Lead, KPN REDteam

Een IT-omgeving kan op papier uitstekend beveiligd zijn. Maar hoe effectief zijn de securitymaatregelen in de praktijk? Een redteamingactie geeft antwoord op deze vraag. Redteamers zoals De Groot en zijn collega’s kruipen in de huid van een cybercrimineel. Ze zoeken een manier om binnen te komen, en tonen bijvoorbeeld aan dat het mogelijk is om waardevolle informatie te stelen. Vervolgens geven ze gericht advies om echte cybercriminelen buiten de deur te houden.

De Groot weet dan ook precies hoe cybercriminelen te werk gaan. “Een cyberaanval bestaat uit meerdere fasen: de cyber kill chain. In de verkenningsfase probeert de aanvaller zoveel mogelijk informatie over het bedrijf te verzamelen. Wie werken er? Wat is hun functie? Met wie hebben ze zakelijk en privé contact? Wat zijn hun hobby’s? Wie zijn bevoegd om betalingen te voldoen? Wie zijn hun leveranciers? Ook wordt op het darkweb gezocht naar bruikbare informatie, zoals lijsten met e-mailadressen en wachtwoorddumps.”

Emotionele trigger
Als de aanvaller een goed beeld van het doelwit heeft, breekt de weaponization-fase aan. “Vaak kiest de cybercrimineel in deze fase een scenario met een emotionele trigger waar werknemers gevoelig voor zijn. Stel dat het doelwit een bedrijf in de binnenstad van Amsterdam is. Dan kun je bijvoorbeeld inspelen op het parkeerprobleem. Je maakt een phishingmail over een herziening van het parkeerbeleid: mensen moeten zich snel aanmelden voor een parkeerplaats. Zoiets is heel effectief.”
Het versturen van de e-mail valt onder de delivery-fase. De Groot noemt nog twee voorbeelden van weaponization en delivery. “Naar een zorginstelling kun je bijvoorbeeld een phishingmail sturen over een gratis Dopper-waterfles voor alle medewerkers. ‘We zijn aan het inventariseren hoeveel flessen we naar elke vestiging moeten sturen. En wil je een dagblad hacken? Dan gooi je een envelop met een usb-stick door de brievenbus bij een journalist. Dat wekt meteen interesse, zeker als er een politielogo op staat.”

Controle over assets
In de exploitation-fase wordt meestal een actie van een gebruiker geïnitieerd. “De medewerker opent de malafide bijlage en downloadt een stukje malware. Of de journalist steekt de usb-stick in zijn pc. Dan komen we aan bij de installation-fase: de aanvaller nestelt zich in het systeem. Het geïnfecteerde systeem maakt vervolgens verbinding met een command & control (C&C)-server en wacht op nieuwe instructies (de command & controle-fase). Op deze manier krijgt de aanvaller controle over assets binnen de organisatie.”

Nu kan de cybercrimineel zijn doelstelling realiseren (actions on objective). “Bijvoorbeeld het stelen van intellectueel eigendom, persoonsgegevens of financiële gegevens. Daarmee is de cyber kill chain voltooid.” De Groot plaatst wel een kanttekening bij dit model. “Dit zijn de basisstappen, maar een aanvaller doet nog veel meer. Hij kan een gecompromitteerd systeem bijvoorbeeld ook patchen zodat de systeembeheerder dat niet hoeft te doen. Dit verkleint het risico op detectie en het lek kan niet door een andere hacker misbruikt worden.”

Detectie voorkomen
Er zijn nog veel meer trucjes om onder de radar te blijven. “Als je ’s nachts inlogt op systemen terwijl alle werknemers dat alleen overdag doen, valt het meteen op. Een slimme aanvaller bootst het gedrag van de gebruikers na en logt op dezelfde tijd in. Een hacker kan ook de virusscanner uitzetten. Soms werkt dat averechts, omdat er dan juist een alarm afgaat. Vaak is het handiger om de configuratie van de virusscanner aan te passen, zodat deze niet scant op de plek waar de malware staat.”

Een andere truc is het gebruik van vertrouwde communicatieprotocollen om data weg te sluizen. “Er zijn allerlei processen die vanuit beheeroogpunt onschuldig lijken. Een voorbeeld hiervan is ping, dat het ICMP-protocol gebruikt om verbindingen te testen. Het is mogelijk om een dataframe mee te sturen met zo’n ping. Het ontvangende systeem kan al die dataframes weer samenvoegen. Zo zijn er nog veel meer gewiekste methoden om data ongemerkt te exfiltreren.”
Verder benadrukt De Groot dat de cyber kill chain een iteratief

proces is dat meerdere keren wordt doorlopen. “Het komt maar zelden voor dat je via het eerste gecompromitteerde systeem direct toegang hebt tot de kroonjuwelen. Je begint meestal aan de buitenkant van het netwerk. Vanaf dat punt ga je als aanvaller weer op verkenning uit. Welke systemen zijn verbonden met het netwerk? Met welke wapens kan ik daar controle over krijgen? Zo ga je net zolang door tot je je doel hebt bereikt.”

Bijna 100 procent veilig

Als leider van het KPN REDteam is De Groot het gewend om als een aanvaller te denken. Daarnaast helpt hij organisaties om hier een solide beveiliging tegenover te stellen. Eenvoudig is dat niet. “Als aanvaller sta je altijd met 1-0 voor. Zelfs als je alles dichttimmert, zijn er mogelijkheden om binnen te komen. Een cybercrimineel kan bijvoorbeeld werknemers omkopen en zo toegang tot waardevolle data krijgen. Het doel moet zijn om bijna 100 procent secure te worden.”

Volgens De Groot is dat absoluut haalbaar. Maar hoe bepaal je welke maatregelen prioriteit hebben? “Cybersecurity begint bij weten wie je bent. Welke assets en data zijn cruciaal voor je primaire bedrijfsprocessen? Wat gebeurt er als kwaadwillenden daar toegang toe krijgen? Voor wie ben je een interessant doelwit en welke aanvalsvectoren gebruiken zij? Zorg eerst dat je een goed beeld hebt van je kroonjuwelen en risico’s. Vervolgens kun je dat vertalen naar securitymaatregelen.”

“Security moet in balans zijn met de rest van je bedrijf.”

Mark de Groot

“Security is altijd een samenspel van mensen, processen en techniek”, vervolgt De Groot. “Deze componenten moeten complementair zijn aan elkaar.” Als voorbeeld noemt hij wachtwoordhygiëne. “In je beleid leg je vast hoe een veilige omgang met wachtwoorden eruitziet. Technisch dwing je het minimum aantal karakers en de complexiteit af, evenals het aantal dagen dat een wachtwoord geldig is. En met bewustwordingscampagnes leg je uit aan de gebruiker waarom dit belangrijk is.”

“Een virusscanner op je laptop is feitelijk al een soort mini-SOC.”

Mark de Groot

Elk bedrijf kan secure worden

Dergelijke preventieve maatregelen zijn belangrijk, maar de securityexpert breekt ook een lans voor monitoring en detectie. “Als er dan toch iets tussendoor glipt, moet je het snel in de gaten hebben.” Een van de opties hiervoor is een SOC/SIEM-oplossing. “Dat is de heilige graal, maar niet ieder bedrijf heeft hier de financiële middelen voor. Gelukkig kun je ook heel laagdrempelig monitoren. Als jij een virusscanner op je laptop installeert en de meldingen opvolgt, heb je feitelijk al een soort mini-SOC.”

“Security moet in balans zijn met de rest van je bedrijf”, besluit De Groot. “Je hoeft niet altijd hypermoderne technologie in te zetten om je securityniveau te verhogen. Een middelgroot mkb-bedrijf is al veel beter beschermd met multifactorauthenticatie op alle devices en de standaard endpointbeveiliging van Office 365. En de slager op de hoek kan in ieder geval back-ups van zijn gegevens maken. Vanuit die basis leg je de lat telkens een stukje hoger.”

Mark de Groot heeft zo’n 25 jaar ervaring in de cybersecurity-industrie, onder andere als securityconsultant en als ethical hacker. Sinds april 2013 geeft hij leiding aan het KPN REDteam.

» Nog nooit was het delen van informatie over cyberaanvallen zo cruciaal. Toch zijn veel organisaties hiervoor huiverig, uit angst voor een knauw in imago en klantvertrouwen. Volgens Petra Oldengarm, directeur van Cyberveilig Nederland, is het tijd voor een kentering. “We moeten toe naar een klimaat waarin juist een gesloten houding imagoschade veroorzaakt.”

Juist een gesloten houding zou imagoschade moeten veroorzaken

Petra Oldengarm
Directeur, Cyberveilig Nederland

Een van de taken van Cyberveilig Nederland is het faciliteren van kennisdeling tussen securitybedrijven en stakeholders, zoals de overheid. De leden moeten daarbij wel over hun eigen schaduw heen stappen, want het zijn onderling ook concurrenten. Toch is het volgens Oldengarm een van de belangrijkste missies van de belangenvereniging. “De dreiging neemt toe, aanvallen zijn steeds complexer. Dat betekent ook dat we aan de verdedigende kant de handen ineen moeten slaan en nog intensiever informatie moeten uitwisselen. Informatiedeling staat dan ook in onze top-3 van prioriteiten.”

Taboe

Niet alleen door securitybedrijven, maar ook vanuit de getroffen organisaties is openheid noodzakelijk. Dat is geen gemakkelijke opgave. Volgens Oldengarm heerst er nog steeds een taboe op het delen van incidentinformatie. “We moeten die gêne wegnemen, en de bedrijven die het wel doen in een positief daglicht zetten.”

De media spelen hierin ook een belangrijk rol, merkt Oldengarm op. “Securityincidenten worden vaak breed uitgemeten met een negatieve insteek. Securityexperts mogen vanaf de zijlijn uitgebreid vertellen wat er allemaal mankeerde aan de procedures of de beveiliging. Deze manier van verslaggeving stimuleert niet bepaald een open houding. Je mag als journalist natuurlijk kritisch zijn, maar wees dan ook kritisch op de grote hoeveelheid bedrijven die incidentinformatie onder de pet houdt.”

De media zouden openheid bovendien kunnen belonen met een ander type verhaal. “Zo stond in de Tubantia vorig jaar een artikel over het cyberweerbaarheidscentrum van de maakindustrie in Oost-Nederland. Zij bieden scans die kwetsbaarheden kunnen blootleggen. Enkele tientallen bedrijven hadden die scan aangevraagd. Je zou dan een verhaal kunnen schrijven over hoe goed het is dat zoveel bedrijven dat doen. De krant koos echter voor een negatief verhaal over

het belabberde niveau van de cybersecurity in deze bedrijven. Want uit vrijwel alle scans bleken tekortkomingen, zo schreef de krant."

Afgeschermde deelomgeving

Ook de overheid kan bijdragen aan een klimaat dat openheid beloont. "Bijvoorbeeld via een campagne die de bedrijven bewust maakt van het belang ervan." Daarnaast kan de overheid volgens Oldengarm voorzien in de middelen om kennisdeling beter te faciliteren. Informatie rondom cyberincidenten is namelijk al snel gevoelig. "We hebben in Nederland geen voorzieningen om op een structurele wijze incidentinformatie veilig vast te leggen. De overheid zou hierin het voortouw moeten nemen. Bijvoorbeeld met een veilige, afgeschermde omgeving waar alleen relevante partijen toegang toe hebben."

Als voorbeeld noemt Oldengarm de vliegtuigindustrie. Daar bestaat sinds jaar en dag een database waarin alle informatie rondom vlieginciden ten nauwgezet wordt bijgehouden. Die database kun je als buitenstaander raadplegen. "Zoiets zou er ook voor cyberincidenten moeten komen. Je zou met een paar experts moeten uitzoeken welke informatie zinvol is om te bewaren, waar nodig anonimiseren en deze op een goede manier moeten structureren en openstellen. Wel is het verstandig om deze informatie in het geval van cyberincidenten niet publiek beschikbaar te stellen. Deze is namelijk voor kwaadwillenden ook interessant."

Er zijn meer onbenutte mogelijkheden. Zo zit de Autoriteit Persoonsgegevens volgens Oldengarm op een potentiële goudmijn van waardevolle informatie. "Organisaties zijn in veel gevallen verplicht een datalek te melden bij de Autoriteit Persoonsgegevens. Ik vraag me af waar die informatie blijft. De Autoriteit publiceert slechts oppervlakkige statistieken, maar geeft geen inzicht in details. Als sector hebben we regelmatig gevraagd of we deze kunnen ontvangen, zodat de sector deze kan gebruiken voor het verhogen van de cyberweerbaarheid van hun klanten. Die data krijgen we niet. De AP benadert zijn rol vanuit een silo. Ze gebruiken die data alleen voor eigen doeleinden, maar kijken niet verder dan dat. Ik vind dat dit moet veranderen."

Spanningsveld

Een deel van het probleem zit volgens Oldengarm in de privacywetgeving. Die is – logischerwijs – heel erg gericht op het beschermen van de privacy. Dat is natuurlijk een goede zaak, maar zit in sommige gevallen een effectieve kennisdeling in de weg. "Daar zit een spanningsveld. Zo ziet de AP IP-adressen ook als persoonsgegevens. Maar juist IP-adressen bevatten vaak waardevolle informatie over een aanval. Bij toekomstige wetgeving zouden we goed moeten kijken naar de balans tussen privacybescherming en effectieve kennisdeling. Er zijn volgens mij best heldere afspraken te maken om dit soort gegevens op een verantwoorde wijze te delen."

Nieuwe wetgeving biedt daarvoor kansen. Zo is er op het moment van schrijven een nieuwe wet in de maak: de Wet gegevensverwerking door samenwerkingsverbanden (Wgs). Deze wet moet informatie-uitwisseling voor een aantal samenwerkingsverbanden makkelijker maken. "Er is vanuit de AP felle kritiek op die wet. Dat die wet gevoelig ligt, is gezien de toeslagenaffaire niet zo gek. We zijn met zijn allen heel erg benauwd voor big brother-achtige toestanden. Maar we schieten daardoor in een kramp die ons niet verder helpt. Zo geven we cybercriminelen de kans om de komende jaren een forse voorsprong op te bouwen. Je moet volgens mij naar een nieuwe fase toe. Eén waarin je wel de mogelijkheid hebt om gegevens te delen, maar zonder allerlei pijnlijke gevolgen zoals we die in het verleden hebben gezien. Je moet voldoende privacywaarborgen inbouwen en met elkaar zoeken naar hoe dit wel mogelijk gemaakt kan worden, lerend van de fouten die in de toeslagenaffaire zijn gemaakt."

Open sector

Overigens merkt Oldengarm wel een flinke verbetering in de openheid en bereidheid tot samenwerking binnen de cybersecuritysector. De commotie rondom de Log4j-kwetsbaarheid van vorig jaar maakte dat goed duidelijk. "Zaterdagavond tien uur werden we gebeld door het NCSC. Ze wilden heel graag de sector spreken. Zondagochtend zaten we in een call met zo'n 70 mensen uit de sector en het NCSC bijeen. Dat laat zien dat securitybedrijven heel vlot samen kunnen optrekken en bereid zijn hun bevindingen te delen. Door die samenwerking is de impact van de Log4j-kwetsbaarheid beperkter gebleven. Daarnaast zitten securitybedrijven niet meer boven op hun dreigingsinformatie. Ze zien in dat ze bij het delen van dreigingsinformatie ook veel informatie terugkrijgen. Zeker nu we als brancheverenging flink gegroeid zijn."

Ook het groeiend onderling vertrouwen is volgens Oldengarm een opsteker. "Er is een trusted community ontstaan van securitybedrijven. Binnen Cyberveilig Nederland zien mensen elkaar regelmatig. Dat zorgt voor een betere band en informele contacten. Daarnaast hebben we nu ook meer faciliteiten. Zo hebben we een chatplatform waardoor we op strategisch en operationeel niveau snel kunnen overleggen, met onze leden en het NCSC. In bredere zin groeit het besef dat je de strijd tegen cybercriminaliteit niet alleen kunt winnen."
Toch valt er volgens Oldengarm nog genoeg te verbeteren.

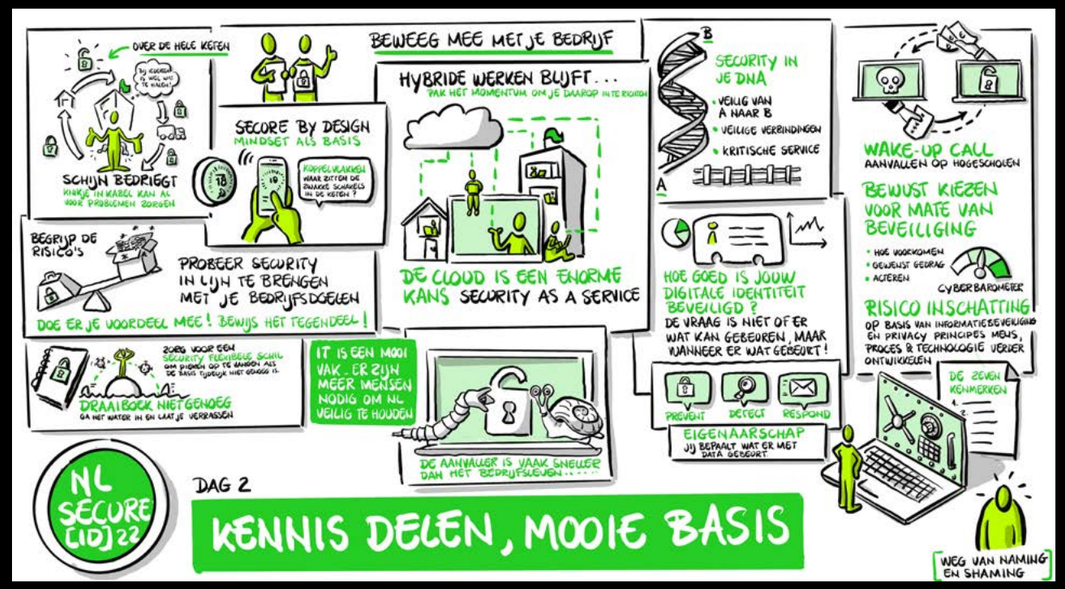
"We moeten goed kijken naar de balans tussen privacybescherming en effectieve kennisdeling."

Petra Oldengarm

"De gezamenlijke duiding van informatie kan bijvoorbeeld nog sterker. Door data samen te analysen, kun je bevindingen nog beter plaatsen. We moeten de koppen daarvoor vaker bij elkaar steken. Dat gebeurt nu nog niet op een structurele basis. Bijvoorbeeld op een onderwerp als ransomware zijn we bezig met een aantal initiatieven om hierin stappen te nemen. Er liggen nog meer dan genoeg kansen voor ons."

Petra Oldengarm is directeur van Cyberveilig Nederland. Deze brancheorganisatie zet zich in voor een optimaal ondernemingsklimaat voor cybersecuritybedrijven in Nederland. Ze heeft een achtergrond in de technische informatica en is al vele jaren actief in het cybersecuritydomein voor verschillende werkgevers, waaronder de AIVD, ECN en Hoffmann Bedrijfsrecherche. Naast haar rol als directeur bij Cyberveilig NL is ze zelfstandig strategisch adviseur cybersecurityvraagstukken en doceert ze aan de Universiteit Leiden.

NL SECURE [ID]



LET'S TALK ABOUT IT

kpn Security

» Cybercriminaliteit is een van de grote uitdagingen van deze tijd. “Elk bedrijf kan getroffen worden door een ernstig cyberincident”, zegt Mark Snel, CISO van Signify. Toch is hij optimistisch over de toekomst. “Binnen het bedrijfsleven is zoveel kennis aanwezig. Als we onze krachten bundelen, kunnen we Nederland beschermen tegen digitale verstoringen en cybercriminelen.”

De cultuur verandert pas echt door een **ernstig cyberincident**

Mark Snel
CISO, Signify

Snel begon drie jaar geleden als CISO bij Signify (voorheen Philips Lighting). Zijn grootste uitdaging is het leggen van een goede basis voor security. “Denk aan het registreren van systemen, het beheer van toegangsrechten en het maken van back-ups. Het belang hiervan wordt nog steeds onderschat. Heel veel bedrijven hebben hun assetmanagement niet op orde. Binnen Signify maak ik me voortdurend hard voor deze fundamentele zaken. Daarnaast verbeter ik continu onze detectie- en responscapaciteit. Langzaam maar zeker groeit de volwassenheid.”

Volgens de CISO komt cybersecurity binnen Signify steeds hoger op de agenda te staan. Mede door de vele incidenten zoals de grote cyberaanval op VDL Groep. “Er worden dagelijks bedrijven aangevallen, maar dit incident vond plaats in onze achtertuin in Eindhoven. Dan krijg je toch een andere dynamiek. Collega’s vroegen mij: kan dit ons ook overkomen? Ja, dat is een scenario waar we altijd rekening mee houden.”

Acceleratieplan
De aanval op VDL Groep heeft bijgedragen aan positieve veranderingen. Zo ligt er nu een acceleratieplan voor cybersecurity waar iedereen achter staat. Snel: “Elke maand zitten we met een groep executives bij elkaar om de voortgang en planning te bespreken. Zo bewaken we de voortgang van deze nieuwe roadmap.” Ook wordt elk kwartaal over security gerapporteerd aan de raad van bestuur. “Voorheen gebeurde dat slechts één keer per jaar. In algemene zin is er meer aandacht gekomen voor onze digitale weerbaarheid.”

Toch denkt Snel dat van een echte cultuurverandering binnen de sector nog geen sprake is. “Ik geloof niet dat wij als securityprofessionals de cultuur kunnen veranderen. Dat gebeurt pas als je zelf een groot incident meemaakt. Begrijp me niet verkeerd: het is heel fijn dat dit Signify nog niet overkomen is. Maar het zou wel het draagvlak voor securitymaatregelen bij iedereen vergroten. Als een bedrijf net twee weken plat heeft gelegen, is de urgentie wel duidelijk. Soms moet een kind even goed vallen voordat het inziet dat het belangrijk is om je veters te strikken.”

Convergentie van OT en IT
De CISO ziet een ernstig cyberincident als een realistisch scenario. Hij maakt zich met name zorgen over een verstoring van de productieprocessen. “OT convergeert steeds meer met IT. We knopen allerlei manufacturingprocessen aan de IT-omgeving. Onze kantooromgeving is nu in de basis goed beveiligd, maar de beveiliging van OT is een relatief nieuw vakgebied met de uitdagingen die daarbij horen.”

“We dekken de grootste IT-risico’s af met securitymaatregelen voor de endpoints, identiteiten en het netwerk. Maar op manufacturing heb ik minder grip dan ik zou willen. Vroeger kon een storing bij een productielocatie niet zomaar overslaan naar een andere locatie. Een fysieke scheiding betekent echter niet dat locaties IT-logisch van elkaar gescheiden zijn. Er loopt een kabel die de netwerken met elkaar verbindt. Als CISO probeer ik bij het manufacturing-management awareness te creëren over de risico’s. Voor hen is cyber een ver-van-mijn-bed-show.”

Door deze convergentie zijn de wijzigingen in verantwoordelijkheden ook niet altijd formeel afgebakend. “Stel dat het SOC ziet dat een infectie zich verspreidt van de ene fabriek naar de andere, dan moet iemand ingrijpen om verdere verspreiding te voorkomen. Uiteraard zullen we dit doen, maar dan heb ik wel wat uit te leggen. Als je huis in brand staat en de brandweer trapt de deur in om de vlammen te blussen, dan ben je dankbaar en koop je een nieuwe deur. Maar als wij vanuit IT iets platgooien, denk ik niet dat we in eerste instantie een bedankje hoeven te verwachten.”

“We moeten cybersecurity als een publiek belang gaan zien.”

Mark Snel

Tekort aan securityprofessionals
Volgens Snel is het voor grote bedrijven bijna onvermijdelijk dat ze op termijn worden getroffen. “En als zij hun security eenmaal goed ingericht hebben, is het midden- en kleinbedrijf aan de beurt. Helaas is er een schrijnend tekort aan securityprofessionals. Voor multinationals is het al een uitdaging om vacatures in te vullen. Zij kunnen dat oplossen door er veel geld in te steken. Maar hoe zit dat met het mkb en de burgers? Wie gaat hen beschermen?”

De CISO van Signify vindt dat we in Nederland efficiënter om moeten gaan met menselijk kapitaal. “De grote Nederlandse bedrijven investeren miljoenen in securityprofessionals. Kunnen we hen niet laten samenwerken om de hele bv Nederland veilig te houden? Nu bouwt ieder bedrijf zijn eigen securityteam op, terwijl dreigingen steeds vaker via de keten binnenkomen. Die versnippering van expertise zie je ook bij de overheid. Het Team High Tech Crime, het NCSC, het DTC, de AIVD en de MIVD hebben allemaal hun eigen taak.”

Hij trekt de vergelijking met de energietransitie. “Bij Signify zijn we heel erg bezig met duurzaamheid en het klimaat. Daarbij zoeken we de samenwerking met andere organisaties, omdat we weten dat we dit niet in ons eentje kunnen oplossen. Dat geldt ook voor de strijd tegen cybercriminaliteit. Cybersecurity moet veel meer als een publiek belang worden gezien waar iedereen een bijdrage aan levert. Alleen als we de krachten bundelen en veel meer kennis delen, liefst in Europees verband, kunnen we voor een relatief veilig internet zorgen.”

Opvoeden met security
Snel denkt niet dat we cybercriminaliteit op korte termijn overwinnen. Desondanks kijkt hij met vertrouwen naar de toekomst. “Er groeit nu een generatie van digital natives op. Als we onze kinderen de juiste basismaatregelen meegeven – zoals gebruik multifactorauthenticatie, klik niet op phishingmails, geef niet zomaar je wachtwoord of pincode af – zijn we over twee generaties security-aware. Het moet straks heel normaal zijn dat je altijd inlogt met een tweede factor zoals FaceID.”

De CISO verwacht dat security in de toekomst steeds vaker technisch gewaarborgd wordt. “Zodra een cybercrimineel een phishingmail verstuurt, zou zijn internetprovider of e-mailprovider de e-mail eigenlijk al moeten tegenhouden. Een phishingmail komt dan niet eens in de inbox van het doelwit terecht. Dit gebeurt al, maar moet overal de norm worden. Natuurlijk moeten we ook de gebruiker trainen in gevaarherkenning, maar in de praktijk blijkt dat zeer lastig. Phishingmails worden steeds overtuigender en mensen blijven uit gemak op links klikken, in plaats van zelf naar de website te navigeren.”

Mooiste vakgebied
Uitdagingen zijn er dus genoeg. Volgens Snel maakt dat het werk van een securityprofessional juist zo leuk. “Dit is gewoon het mooiste vakgebied dat er is, dat vind ik al twintig jaar. Het is zo dynamisch: geen dag is hetzelfde. We staan bovendien pas aan het begin van het digitale tijdperk. Ik kan een carrière in cybersecurity iedereen aanbevelen.” De CISO heeft ook nog een advies aan topmanagers wereldwijd. “Luister naar je securityspecialist, ook al begrijp je niet goed wat er wordt gezegd. Hij of zij probeert je bedrijf te beschermen.”

Mark Snel is als CISO & Head of Cyber Security verantwoordelijk voor de securitystrategie van Signify. Snel heeft ruim 20 jaar ervaring met informatiebeveiliging, eerst als technisch engineer en later in diverse managementfuncties.

kpn Security

» Grote cyberaanvallen halen regelmatig het nieuws. “Je kunt geen krant openslaan of je leest over de cyberdreiging”, zegt Marieke Snoep, Chief Business Market bij KPN. Volgens Snoep zijn de meeste bedrijven zich inmiddels dan ook wel bewust van die dreiging. “Maar er is nog te weinig actie. Bedrijven moeten security op de eerste plaats gaan zetten.”

Het wordt tijd dat we **securitybewustzijn vertalen naar actie**

Marieke Snoep & **Erno Doorenspleet**
Chief Business Market & Vice President Security Strategy, KPN & KPN Security

“Digitale vooruitgang brengt nieuwe risico’s met zich mee”, constateert Snoep. De transitie naar thuiswerken is daar een voorbeeld van. “Bedrijven gaan van één naar misschien wel duizend kleine kantoortjes. Het begint met de basisbeveiliging van deze werkplekken thuis die vaak niet op orde is. Daarnaast heeft de IT-afdeling lang niet altijd zicht op de tools die worden gebruikt. We hebben allemaal tientallen apps op onze telefoons staan. Shadow IT is overal. Tot slot is er het menselijke aspect. Waar werkt iemand? En welke ongeautoriseerde mensen hebben (per ongeluk) toegang tot gevoelige bedrijfsdata.”

“Het aanvalsoppervlak wordt daardoor groter”, waarschuwt Snoep. Dat komt niet alleen door het thuiswerken. “We laten leveranciers toe tot onze netwerken om de dienstverlening richting klanten te verbeteren en laten klanten toe voor selfservice. Eén zwakke plek ergens in die keten kan al funest zijn.”

Digitale vooruitgang heeft er ook voor gezorgd dat we anders zijn gaan communiceren. “We communiceren op heel veel manieren en via verschillende apps met elkaar”, zegt Erno Doorenspleet, Vice President Security Strategy bij KPN Security. “Onze communicatie is daardoor minder gestructureerd en minder gecontroleerd geworden. We kiezen voor gemak, maar laten de security daardoor wat lopen.”

Security als fundament
Tegelijkertijd neemt de dreiging toe. Cyberaanvallen worden steeds geavanceerder en gevaarlijker. “Bij digital life en digital business hoort dan ook dat je aandacht besteedt aan security. Dat is de basis voor een succesvolle bedrijfsvoering en het fundament voor digitaal zakendoen”, vindt Snoep.

“Security moet je meenemen in alles wat je doet, en bij elke transformatie die je als bedrijf doormaakt. Doe je dat niet, dan loop je meer risico dan noodzakelijk”, vult Doorenspleet aan.

“Bij alles wat je doet, moet je nadenken over security.”

“Andersom kun je met een goede security competitief voordeel behalen. Met een goede security laat je zien dat je er alles aan doet om je klant en zijn data te beschermen, en dat je een betrouwbare leverancier of partner bent.”

Managed services

De boodschap van Snoep en Doorenspleet is helder: bedrijven moeten security op de eerste plaats zetten. Security first. “Tegelijkertijd heb je te maken met een enorme war on talent”, merkt Snoep op. “Zeker mkb-bedrijven hebben vaak niet de mensen in huis om alles zelf te doen. Die bedrijven moeten goed nadenken over wat effectieve maatregelen zijn die de bedrijfsvoering en het securityniveau duurzaam verbeteren. Op welke manier kan technologie waarde toevoegen binnen onze organisatie?”

Volgens de Chief Business Market van KPN is het inkopen van managed services dan een ‘duurzame keuze’. “Nog te vaak zie ik dat bedrijven in het verleden blijven hangen en zelf hardware aanschaffen en zelfstandig netwerken opbouwen en beheren. Dat lijkt misschien goedkoper, maar als het gaat om security is goedkoop vaak duurkoop.”

“Wij geloven in een wereld waarin KPN de klant ontlast zodat die zich kan focussen op zijn business”, aldus Snoep. “Onze gehele dienstverlening is secure by design, van mobiele telefonie en internet tot networking en werken in de cloud. Je mag er altijd van uitgaan dat data bij ons veilig zijn en dat de security laagdrempelig is in gebruik. Wij zorgen ervoor dat je daar niet over na hoeft te denken.” Doorenspleet: “KPN staat voor security first. Veilige communicatie is ons bestaansrecht.”

Blijf nadenken

De gezondheidszorg is volgens Snoep een voorbeeld van een sector die is gebaat bij ‘ontzorging’. “Zorginstellingen hebben te maken met een groot tekort aan mensen, ook op IT-gebied. Dan wil je als zorgbestuurder tegen een externe partij kunnen zeggen: zorg er onder andere voor dat mijn ziekenhuis veilig blijft en dat bijvoorbeeld de machines ten behoeve van de sterilisatie van apparatuur niet worden gehackt, dat de privacy van patiënten gewaarborgd is en dat de IT beschikbaar blijft.”

Marieke Snoep is Chief Business Market en lid van de raad van bestuur van KPN, en sinds 1 februari 2019 werkzaam bij KPN. Ze heeft meer dan 25 jaar strategische en commerciële ervaring in de Nederlandse telecommunicatiemarkt. Met KPN Zakelijke Markt zorgt ze ervoor dat KPN de onestopshop is voor de grootzakelijke markt en het midden- en kleinbedrijf in Nederland op het gebied van veilige, flexibele, toekomstbestendige netwerken en any place, anytime en any device samenwerken in de cloud.

Dat wil zeker niet zeggen dat die bestuurder ook het bewustzijn over security kan uitbesteden, zo benadrukken Snoep en Doorenspleet. Snoep: “Bij security first hoort dat je altijd blijft nadenken over de risico’s die je loopt, en dat je weet wat er nodig is voor een veilige bedrijfsvoering. Waar zitten bijvoorbeeld de zwakke punten in een digitale infrastructuur? En welke personeelsleden zijn te verleiden tot ongewenste handelingen? En welke securitydiensten heb je dan nodig om die risico’s af te dekken? Dat bewustzijn kun je niet uitbesteden.”

Bij security first hoort volgens Doorenspleet ook dat bedrijven op de domeinen ‘supplychain’, ‘medewerkers’ en ‘tooling en technologie’ altijd op de hoogte zijn en blijven. “Je moet bijvoorbeeld weten waar personeel toegang toe heeft, en wat er precies zit in de securitydienstverlening die je afneemt. Ook als IT of cybersecurity niet jouw specialisme is.” Snoep: “De meeste hacks vinden via e-mail plaats. Als je dan geen e-mailsecurity afneemt, vlieg je na één klik op een kwaadaardig linkje alsnog gigantisch uit de bocht. Er is vaak nog onwetendheid over wat er precies wél en wat er níet in een dienstverlening zit.”

Geen IT-feestje

“Security first betekent ook dat je bij alles wat je doet nadenkt over de risico’s”, merkt Doorenspleet op. “Is het wel veilig om op deze link te klikken? Is het wachtwoord voor mijn wifinetwerk sterk genoeg? Kan ik deze applicatie veilig gebruiken? Deze vragen moet je continu stellen. Dat geldt voor de hele bv Nederland, tot en met de bakker op de hoek. En voor iedereen binnen een organisatie.”

“Heel veel bestuurders denken dat security een IT-feestje is, maar dat is het absoluut niet”, besluit Snoep. “Bestuurders zijn zelf ook targets.”

Erno Doorenspleet is Vice President Security Strategy en Chief Technology Officer (CTO) van KPN Security. Hij heeft meer dan 20 jaar ervaring in IT, waaronder Security & Risk Management, Governance & Operations en Outsourcing. Hij is een nationale en internationale spreker over de relatie van Cyber Security, Information Technology, Cloud computing en Internet of Things.

NL SECURE [ID]

» Cybercriminelen worden vaak neergezet als hyperintelligente superhelden met magische krachten en een ongelimiteerd budget. Donny Maasland ergert zich hieraan. Volgens de CTO van ESET Nederland ontstaat daardoor het beeld dat organisaties weerloos zijn en dat securitymaatregelen geen zin hebben. “Dat is zeer schadelijk. En het klopt ook gewoon niet.”

Cybercriminelen zijn echt niet allemaal **Einsteins**

Donny Maasland
CTO, ESET Nederland

“Urgentie creëren is goed, maar we slaan door”, zegt Maasland. “De meeste cybercriminelen zijn helemaal niet zo geavanceerd bezig. Ze zitten op underground-forums, kopen toegang tot een netwerk en voeren wat scriptjes uit. Ze hebben heus wel verstand van IT en netwerken, maar het zijn echt niet allemaal Einsteins. Het klopt ook zeker niet dat cybercriminelen alle obstakels kunnen overwinnen. Er zijn allerlei maatregelen die aanvallen detecteren en blokkeren of de verdere verspreiding over het netwerk vertragen.”

Volgens Maasland zorgt de beeldvorming voor onwetendheid en angst. “Daardoor verzinnen bedrijven oplossingen die niet bij hun situatie passen. Deze vijand is zo geavanceerd, dus we hebben ook geavanceerde oplossingen nodig. Dan wordt er een AI-tool aangeschaft, terwijl de basis niet op orde is. Bij grote ransomware-incidenten zie je bijvoorbeeld vaak dat de virusscanner wel een melding gaf, maar er niks mee is gedaan. Een nieuwe tool genereert alleen maar meer output om te negeren.”

Een hoog hek
Hoe is die beeldvorming ontstaan? “Sommige leveranciers gebruiken angst om oplossingen te verkopen. Ook verliezen securityexperts zich soms in technische details. Kijk naar multifactorauthenticatie. Onder artikelen waarin MFA wordt genoemd, roept er altijd wel iemand dat MFA omzeild kan worden. Dat klopt, maar MFA maakt het de aanvaller wel een stuk lastiger. Hij krijgt geen toegang meer door simpelweg een gelekte gebruikersnaam en wachtwoord op alle accounts te proberen. Er is een gerichte aanval nodig.”

“Zerotrust is een marketingterm voor iets dat we al jaren weigeren te doen.”

Donny Maasland

kpn Security

Zonder de hackersmentaliteit hadden we geen internet

Een kwaadaardige capuchondrager die vanaf een duistere zolderkamer bedrijven saboteert: dat is hoe veel mensen hackers zien. Nog een beeld dat Maasland graag rechtzet. Volgens hem is een hacker vergelijkbaar met een uitvinder. “Iemand met een passie voor technologie die daar nieuwe toepassingen voor zoekt. De grootste innovaties van de mensheid zijn ook gewoon hacks.”

Bij een hacker denk je misschien niet direct aan Thomas Edison en Nikola Tesla. Toch zijn deze grote uitvinders klassieke hackers, stelt Maasland. “Een van hun grootste hacks was de gloeilamp. Die bestaat uit een dun gespannen draadje tussen twee polen waar elektriciteit doorheen loopt. Precies genoeg elektriciteit om het draadje zo warm te laten worden dat het gaat gloeien, maar net koud genoeg om het niet meteen te laten smelten. Met daaromheen een glazen bol gevuld met gassen die ervoor zorgen dat het draadje niet uit elkaar valt.”

“Eigenlijk is een gloeilamp een soort kortsluiting die we onder controle houden, en die als bijproduct licht geeft”, licht Maasland toe. “Edison en Tesla experimenteerden met een combinatie van bestaande technologieën en vonden zo een nieuwe toepassing: de verlichting van huizen. Dankzij de gloeilamp was het niet meer nodig om telkens nieuwe kaarsen te kopen. Nu kunnen we ons geen wereld meer voorstellen zonder lampen. Deze hack maakte het leven voor iedereen beter. Tenzij je een lantaarnverkoper was”, grapt hij.

De CTO van ESET Nederland breekt hiermee een lans voor de hackerscommunity. “Alle technologische innovaties komen tot stand dankzij mensen die willen weten hoe iets werkt. Ze voegen componenten van technologieën samen en maken daar iets nieuws van. Dat is precies wat hackers doen, maar dan met applicaties en systemen. Zonder de hackersmentaliteit hadden we nooit mensen op de maan gezet en was er geen internet. Veel hacks maken de wereld juist veiliger. We moeten hackers en cybercriminelen niet op één hoop gooien.”

Maasland vergelijkt MFA met een hoog hek. “In mijn wijk worden nieuwe huizen gebouwd. Daar staat een groot hek omheen, omdat ze niet willen dat mensen op de bouwplaats komen. Het is mogelijk om over het hek te klimmen. Toch denkt de aannemer echt niet: we gaan geen hek neerzetten. Het hek is namelijk een effectieve maatregel om de meeste mensen buiten te houden. MFA is niet waterdicht, maar het blijft een cruciale maatregel. Het maakt je veel minder kwetsbaar voor ‘hagelschieten’.”

De CTO denkt ook dat de inhoud soms ondersneeuwt door marketingboodschappen. Als voorbeeld noemt hij zerotrust. “Dat is een marketingterm voor iets dat we al jaren weigeren te doen: het segmenteren van systemen en het goed instellen van toegangsrechten. ‘Maar dan moeten we van alles uitzoeken’, hoor je dan. Ja, dát is dus precies wat security is. Niet zomaar een lading nieuwe producten aanschaffen, maar je IT-omgeving in kaart brengen en de toegang tot systemen en data beperken. Zo maak je het een indringer moeilijk.”

Inzicht in het netwerk
Een solide IT-beveiliging begint volgens Maasland bij een fijnmazig inzicht in je netwerk. “Hoe zit mijn netwerk in elkaar? Wat zijn mijn belangrijkste assets en hoe beveilig ik deze? Uit welke bouwblokken bestaat mijn securityomgeving? En hoe zorg ik ervoor dat deze componenten goed samenwerken? In de incidentrapporten van grote cyberaanvallen lees je vaak dat dit precies de dingen zijn die misgingen. Ik vrees dat het gemiddelde Nederlandse bedrijf dit niet op orde heeft.”

“Veel bedrijven vinden het allang prima als hun netwerk in de lucht is”, vervolgt Maasland. “Alle computers zijn aangesloten op internet en alle applicaties werken. Waarom zou je dan nog extra investeren in de beveiliging? Het werkt toch, wat is het probleem?” Hij ziet verschillende oorzaken voor deze mentaliteit. “Soms is het een gebrek aan kennis. Deze bedrijven weten gewoon niet welke securityrisico’s ze creëren met bepaalde configuraties. Het kan ook een kwestie van budget zijn. Het is lastig om één generieke oorzaak aan te wijzen.”

“Een AI-tool genereert dan alleen maar meer output om te negeren.”

Donny Maasland

Belang van informatie-uitwisseling
De securityexpert heeft geen eenvoudige oplossing. Persoonlijk ziet hij weinig in strengere regelgeving. “Stel dat je een verplichte securitycertificering invoert. Dan gaan sommige bedrijven van alles verzinnen om met minimale inspanningen aan de eisen te voldoen. En andere bedrijven slaan juist door in het managen van de papieren werkelijkheid. Dat zie je ook bij de Algemene verordening gegevensbescherming, waar voor de meest futiele processen om een verwerkersovereenkomst wordt gevraagd.”

Het subsidiëren van securitymaatregelen vindt Maasland geen slecht idee. “Maar Nederland kennende zal daar ook misbruik van worden gemaakt. Ik denk dat het effectiever is om kennisdeling en informatie-uitwisseling te stimuleren. Op dat vlak zijn er positieve ontwikkelingen. Zo is het Digital Trust Center in september 2021 begonnen met het proactief informeren van individuele bedrijven over digitale dreigingen. Ook de oprichting van het Nederlands Security Meldpunt is een stap in de goede richting.”

Maasland sluit af met een advies aan alle Nederlandse organisaties. “Investeer in securitykennis, of je nu zelf mensen aanneemt of hiervoor samenwerkt met een partner. Ga niet zelf experimenteren. Misschien kun je thuis wel een paar simpele klusjes doen, maar bij een grote verbouwing schakel je een aannemer in. Zo werkt het ook bij security: je hebt vakmensen nodig.”

Donny Maasland is sinds december 2020 de CTO van ESET Nederland. Hij is verantwoordelijk voor het technisch verbeteren en doorontwikkelen van ESET’s oplossingen en diensten. Maasland werkte daarvoor onder meer als hoofd onderzoek en als pentester.

» De energiesector loopt voorop in het uitwisselen van dreigingsinformatie. Toch kunnen energiebedrijven nog beter samenwerken op het gebied van cybersecurity, vinden Justin Broeders, CISO van Eneco en Mauriche Kroos, Manager Information Security & Data Protection Team bij Enexis Groep. Zij hebben daar wel ideeën voor. “We zouden een eigen CERT moeten oprichten.”

Elke schakel moet bijdragen **aan de veiligheid**

Mauriche Kroos & **Justin Broeders**
GISO & CISO, Enexis Groep & Eneco

Eneco en Enexis vervullen een sleutelrol in de Nederlandse energievoorziening, maar doen dat elk op hun eigen manier. Eneco is een duurzame energieleverancier met zo’n zes miljoen klanten in binnen- en buitenland. Enexis Groep is een regionaal netwerkbedrijf dat de distributie van energie verzorgt. Simpel gezegd: Eneco produceert en verhandelt de energie, terwijl Enexis Groep de elektriciteitskabels en gasleidingen beheert en onderhoudt. Feitelijk zijn dit twee verschillende sectoren binnen de energiebranche.

Vitale infrastructuur

Toch hebben Eneco en Enexis Groep ook veel gemeen. Zo zetten beide bedrijven zwaar in op duurzaamheid. Daarmee zijn ze een drijvende kracht achter de energietransitie. Ook maken Eneco en Enexis Groep allebei deel uit van de vitale infrastructuur. Uitval of verstoring van de energievoorziening, bijvoorbeeld door een cyberaanval, zou tot ernstige maatschappelijke ontwrichting kunnen leiden. Hun beveiliging moet dan ook aan strenge eisen voldoen. Zo houdt Agentschap Telecom toezicht op de naleving van de zorgplicht en meldplicht uit de Wet beveiliging netwerk- en informatiesystemen (Wbni).

Dat is niet voor niks. Vitale infrastructuren, waaronder de energiesector, komen steeds meer in beeld bij cybercriminelen. “De aanvallen worden steeds complexer en professioneler”, vertelt Kroos. “De ene keer is het CEO-fraude, dan zijn het weer phishingcampagnes of zeroday-aanvallen. Elk onderdeel van Enexis Groep is een potentieel doelwit.” Broeders ziet bij Eneco dat het dreigingslandschap zeer dynamisch wordt. “Kwetsbaarheden zoals Log4Shell worden heel snel op hackerscommunity’s gedeeld en actief misbruikt. Je organisatie moet continu alert zijn.”

Security-awareness
Broeders stimuleert die waakzaamheid op verschillende manieren. “Zo organiseren we binnen Eneco periodiek security-awarenesstrainingen. Daarmee trainen we onze mensen in gevaarherkenning en maken we hen bewust van de risico’s. Maar we willen ook dat werknemers een phishingmail of andere aanvalspoging zo snel mogelijk rapporteren. Na een melding kunnen wij centraal de lijnen uitzetten om de aanval op meerdere plekken af te slaan. Dat is zó belangrijk.”

“Eneco en Enexis zijn onderdeel van hetzelfde cyberecosysteem.”

Mauriche Kroos

Ook Enexis versterkt de menselijke schakel. Kroos: “De werknemers zijn onze ogen en oren. Wij zorgen dat zij verdachte zaken laagdrempelig kunnen melden. In ons awareness-programma passen we diverse technieken toe, zoals progressieve e-learning. Daarbij komt een fout beantwoorde vraag telkens in een andere vorm terug. Daar leer je meer van dan van een traditioneel klasje. We verbeteren onze aanpak continu. Ontvangen we opeens veel telefoontjes of sms’jes van oplichters? Dan passen we de trainingen daarop aan.”

Broeders vindt het soms lastig om mensen voortdurend alert te houden. “Kijk naar Log4Shell. Als er een kwetsbaarheid bekend wordt, wil je dat alle werknemers extra goed opletten. Zo’n situatie duurt soms meerdere maanden. In het begin heb je iedereen mee, maar je kan mensen moeilijk continu in crisismodus houden. Na verloop van tijd treedt toch een soort afvlakking op, en juist op dat moment ben je kwetsbaar.” Dat herkent Kroos wel. “De boog kan niet altijd gespannen zijn.”

Cybersecurity in de keten
Een andere uitdaging voor Kroos en Broeders is het waarborgen van veiligheid in de keten. “Eneco en Enexis zijn onderdeel van hetzelfde cyberecosysteem”, zegt Kroos. “Als een van onze leveranciers of een ander energiebedrijf getroffen wordt door een ernstig incident, lopen wij eveneens risico. En op een hoger niveau is ook alles met elkaar verbonden. Een grote storing in de energiesector werkt door naar de rest van Nederland. Alle bedrijven hebben stroom en gas nodig.”

“De digitale afhankelijkheid van elkaar neemt toe”, vult Broeders aan. “Elke schakel in de keten moet een bijdrage leveren aan de veiligheid. Dat betekent dat je als ketenpartners met elkaar in gesprek moet gaan. Wat is de impact op onze keten als er bij een van de bedrijven iets misgaat? Hoe voorkomen we dit samen? En wat doen we als het toch gebeurt? Als je goed op elkaar ingespeeld bent, kun je sneller schakelen in het geval van een incident.”

Die informatie-uitwisseling vindt mede plaats via een publiek-privaat samenwerkingsverband tussen het NCSC en de energiesector, een zogenaamd Information Sharing Analysis Center (ISAC), waarvan Kroos zelf voorzitter is. “In de energie-ISAC komen verschillende partijen uit de energiesector samen om informatie over aanvallen en incidenten te delen”, licht hij toe. “Het is dus een sectoraal samenwerkingsverband en dit gebeurt op vrijwillige en vertrouwelijke basis.”

“Je mag de informatie alleen gebruiken om je eigen beveiliging te verbeteren”, vervolgt Kroos. “Hierbij wordt ook gebruik gemaakt van het zogenaamde Traffic Light Protocol (TLP) dat helpt bij de vraag in hoeverre gevoelige informatie verder kan worden gedeeld binnen en buiten de organisatie. Deze kennisdeling is van grote waarde, want vaak wordt een aanval uitgevoerd op de gehele energiesector. Samen staan we sterker.”

CERT voor de energiesector
Broeders en Kroos zijn dan ook een voorstander van gezamenlijke crisisoefeningen zoals ISIDOOR. Dit is een grootschalige oefening voor digitale weerbaarheid in de vitale infrastructuur, georganiseerd door het NCSC in samenwerking met de NCTV. “Zo’n landelijke oefening waarin een enorme keten wordt meegenomen is zeer waardevol”, vindt Broeders. “Dit zouden we ook in de energiesector veel meer moeten doen. Samen oefenen is een goede manier om de ketenweerbaarheid te verhogen.”

De twee securityexperts pleiten daarnaast voor de oprichting van een energie-CERT. “De informatie-uitwisseling hebben we prima op orde”, stelt Kroos. “Maar met een eigen CERT zou je nog een stap kunnen zetten in de onderlinge samenwerking.”

Broeders: “Vanuit een CERT zou je bijvoorbeeld gezamenlijke redteamingacties kunnen opzetten door de hele keten heen. Een CERT kan ook dreigingsinformatie snel combineren en verspreiden, of ondersteunen bij de respons. Daar profiteert iedereen van.”

Kroos zou ook graag zien dat er meer cross-sectorale kennisdeling plaatsvindt. “Dat gebeurt nu nog te weinig. Elke sector heeft zijn eigen toezichthouder, dat geldt ook voor de ISAC’s. Als energie-ISAC zien wij niet welke dreigingsinformatie binnen de ISAC’s voor de financiële sector en de chemiesector wordt gedeeld, en andersom ook niet. Er zijn wel wat overleggen tussen de sectoren, maar heel beperkt en meestal op hoofdlijnen. Daar valt zeker nog winst te behalen.”

Geen technisch feestje
Broeders en Kroos zijn beiden doorgewinterde securityprofessionals. Hebben zij nog een advies voor hun vakgenoten? “Cybersecurity wordt nog weleens als een technisch feestje gezien, maar het is een businessvraagstuk”, stelt Broeders. “Het is belangrijk dat de risicoafweging op de juiste plaats wordt genomen. Ga als securityprofessional niet continu op de stoel van een ander zitten en dingen opleggen. Je kunt beter inzichten aanreiken en met mensen meedenken, zodat zij zelf de juiste keuzes maken.”

Kroos raadt elke securityprofessional aan om risicogebaseerd te werken en deze risico’s ook goed te duiden. “Een IT-beveiligingsmaatregel is nooit 100 procent waterdicht, dus je moet prioriteiten stellen op basis van de risico’s. Vertaal de risico’s naar actiegerichte informatie en duiding. Zo zorg je ervoor dat de business een weloverwogen besluit kan nemen. En wees niet bang om informatie over incidenten te delen. Alleen ga je sneller, maar samen kom je verder.”

“Samen oefenen is een goede manier om de ketenweerbaarheid te verhogen.”

Justin Broeders

Mauriche Kroos werkt al bijna 10 jaar bij Enexis Groep. Sinds 2018 vervult hij de functie van GISO en Manager Information Security & Data Protection Team binnen de afdeling Bestuurlijke Zaken, Juridische Zaken & Digitale Veiligheid. Daarnaast is Kroos sinds 2017 de voorzitter van het sectoraal samenwerkingsverband genaamd de energie-ISAC.

Justin Broeders is sinds 2019 werkzaam als CISO van Eneco. Daarnaast staat hij aan het hoofd van het domein IT Strategic Change. Broeders werkte eerder in diverse risk- en securityleiderschapsfuncties bij bedrijven als a.s.r. en Coöperatie DELA.

NL SECURE [ID]

» AI-systemen nemen taken over van mensen, en nemen zelfstandig beslissingen. Dat biedt een enorme potentie, maar introduceert ook geheel eigen, specifieke risico's. De beveiliging van AI verdient dan ook veel meer aandacht dan het nu doorgaans krijgt, stelt Henk-Jan van der Molen. Als docent aan de Security Academy pleit hij voor een meerlaagse aanpak. "Maar uiteindelijk is de inzet van AI altijd risicovol en een menselijke afweging."

De impact van AI **is een twee-snijdend zwaard**

Henk-Jan van der Molen
Docent, Security Academy

AI is in opkomst. Chipfabrikanten gebruiken kunstmatige intelligentie bijvoorbeeld om te zoeken naar nog slimmere manieren om transistoren te plaatsen. Daarmee neemt de rekenkracht verder toe, en in het kielzog ook de kracht en de mogelijkheden van AI-systemen. Het is daarmee een zichzelf versterkende katalysator voor de wet van Moore. "Uiteindelijk gaan we naar een AI-systeem dat de Turing-test doorstaat en dus kan communiceren als een mens", voorspelt Van der Molen.

AI-systemen spelen door die toenemende rekenkracht en mogelijkheden een steeds belangrijkere rol in ons dagelijks leven. Deze systemen hebben een waardevol voordeel ten opzichte van reguliere IT: ze kunnen in nieuwe situaties autonoom beslissingen nemen, zonder dat ze expliciet daarvoor zijn geprogrammeerd. Dat is een welkome eigenschap voor tal van toepassingen. Denk aan een zelfrijdende auto die zelfstandig een route bepaalt in een drukke ochtendspits. Of denk aan een HR-systeem dat uit duizenden vacatures de tien meest geschikte kandidaten voor een nieuwe vacature destilleert.

Die autonomie maakt AI waardevol, maar ook risicovol. We moeten erop kunnen vertrouwen dat zo'n systeem integer handelt, zonder manipulatie van kwaadwillenden. Dat kan volgens Van der Molen namelijk onvoorziene, mogelijk rampzalige gevolgen hebben. "Als bij een regulier IT-systeem de data gemanipuleerd is, dan is er nog niet per se veel aan de hand. Maar stel je voor dat een zelfrijdende auto door een hack denkt dat het 100 meter achter een andere auto zit, terwijl dat in werkelijkheid 10 centimeter is. Dat kan leiden tot levensgevaarlijke situaties. Dan is het wel belangrijk dat er een bepaalde controle is die de scope van die autonomie toetst."

kpn Security

Autonomie vraagt om beveiliging
Het autonome karakter van AI-systemen vraagt dus om beveiligingsmaatregelen. Die beveiliging wijkt af van die van traditionele systemen, legt Van der Molen uit: "Bij traditionele IT draait security om het beschermen van processen tegen falen. Je kunt je afvragen of dat uitgangspunt ook opgaat bij AI-systemen. Het gaat dan niet alleen om falen, maar vooral ook om het voorkomen van ongewenst handelen."
Een belangrijke factor die dat handelen bepaalt, zijn de trainingsdata. "Bij traditionele systemen is de logica grotendeels voorgeprogrammeerd. Bij AI-systemen is dat anders. Daarbij wordt de logica grotendeels bepaald door de gegevens waarmee het algoritme getraind wordt. Bij spellen zoals schaken en Go gaat dat goed, AI-systemen zijn hierin heer en meester. Maar bij veel andere toepassingen is het verschil tussen succesvolle inzet en levensgevaarlijke situaties flinterdun. Daarom is het belangrijk dat er voldoende controle is over de authenticiteit van die trainingsdata."

Die controle is volgens Van der Molen cruciaal. "Aanvallers kunnen door het manipuleren van trainingsdata de werking van het systeem beïnvloeden. Een AI-systeem gebruikt trainingsdata om bijvoorbeeld patronen te leren herkennen, en zo te bepalen op basis van welke condities het beslissingen neemt. Veranderen die data, bijvoorbeeld doordat een hacker deze manipuleert, dan verandert uiteindelijk de werking van het systeem. Daarnaast kan een AI-systeem ook veel privacygevoelige persoonsgegevens bevatten. Deze verdienen natuurlijk sowieso bescherming tegen datalekken."

"Autonomie maakt AI waardevol, maar ook risicovol."

Henk-Jan van der Molen

Databescherming cruciaal
Het beveiligen van (trainings)data is dan ook cruciaal voor een betrouwbare werking van AI-systemen. Volgens Van der Molen bestaan daarvoor al jaren goede strategieën. "Een aantal modellen voor informatiebeveiliging is heel bruikbaar, zoals Bell-LaPadula en Biba (zie kader). Deze methoden zijn weliswaar al tientallen jaren oud, maar nog altijd heel waardevol. Deze voorkomen dat gegevens naar buiten lekken, of worden gemanipuleerd door onbevoegden."

ISO-normeringen kunnen verdere houvast bieden. "Zonder objectieve standaarden is het erg lastig om verbeterpunten in de beveiliging te identificeren. ISO-normeringen die specifiek bruikbaar zijn voor AI-beveiliging zijn nog schaars, maar volop in ontwikkeling. De gepubliceerde normen dekken nog maar een beperkt deel van het AI-vakgebied af. Wel zitten er nog 22 normen in de pijplijn, waarmee ISO uiteindelijk de hele Plan Do Check Act (PDCA)-cyclus voor AI-beveiliging wil afdekken. Voor het zover is, is het voor eigenaren van AI-systemen raadzaam regelmatig te controleren of er nieuwe normen zijn uitgevaardigd."

Situational awareness
Ondanks een zo goed mogelijke beveiliging van de data kan het alsnog in de praktijk misgaan. "De beveiliging van AI is uiterst complex. Naast de manipulatie van trainingsdata kunnen hackers ook knoeien met het algoritme, of met de data die het systeem verwerkt. Daarnaast is ook nog simpelweg een Denial of Service (DoS)-aanval mogelijk." Een van de voorwaarden voor het gebruik van AI-systemen zou volgens Van der Molen dan ook een soort 'situational awareness voor het eigen functioneren' moeten zijn. "Als een AI-systeem zijn werk niet meer betrouwbaar kan uitvoeren, dan zou het systeem zijn eigen ambities moeten beperken om erger te voorkomen."

"Neem bijvoorbeeld de zelfrijdende auto", vervolgt Van der Molen. "Die zou zichzelf tijdens een cyberaanval direct moeten parkeren langs de kant van de weg, in plaats van met 100 kilometer per uur door te rijden. Daar is een soort kunstmatig bewustzijn voor nodig dat continu checkt op verdachte of afwijkende omstandigheden. Zodat wanneer het misgaat, het zelfstandig kan ingrijpen en zichzelf desnoods kan uitschakelen."

Bell-LaPadula: bewaken van vertrouwelijkheid
Een bruikbaar model voor de beveiliging van AI-systemen is het model Bell-LaPadula. Deze methode voorkomt datalekken met het credo 'no read up, no write down'. In dit model is het voor gebruikers onmogelijk om informatie te raadplegen of te wijzigen met een hogere kwalificatie dan zijn of haar screening. Tegelijkertijd kan iemand met de juiste screening geen geheime informatie kopiëren naar lagen met een lager classificatieniveau.

Biba: bewaken van integriteit
Een ander nuttig model voor de beveiliging van AI-systemen is Biba. Dit model hanteert het credo 'no write up, no read down'. Dit model voorkomt ongewenste wijzigingen van gegevens, en daarmee datavervuiling. Iemand met toegang tot laagwaardige informatie mag deze niet kopiëren naar locaties voor hoogwaardige informatie. Tegelijkertijd mag een uitvraag van hoogwaardige informatie geen laagwaardige data bevatten.

Tweesnijdend zwaard
AI heeft een interessante eigenschap: deze technologie kan helpen bij zijn eigen verdediging. Veel fabrikanten hebben kunstmatige intelligentie op de een of andere manier verwerkt in hun securityproducten. Denk aan detectie-oplossingen die uit grote hoeveelheden dataverkeer verdachte onregelmatigheden kunnen opsporen die mogelijk wijzen op indringers. Ook is AI waardevol voor het opsporen van kwetsbaarheden. “Veelbelovend is de technologie om uit grote hoeveelheden regels code volautomatisch te speuren naar bugs. Die vormen namelijk dankbare ingangen voor cybercriminelen, die deze kunnen misbruiken voor een hack.”

AI heeft voor zijn eigen verdediging nog veel meer in zijn mars. “Mits je voldoende flexibele logica hebt, kun je bijvoorbeeld met AI een systeem ontwikkelen dat trainingsdata kan controleren op verdachte afwijkingen die mogelijk kunnen wijzen op manipulatie.”

Wel maakt Van der Molen een scherpe kanttekening: het gebruik van AI binnen de cybersecurity is helaas een tweesnijdend zwaard. “Ook aanvallers kunnen misbruik maken van kunstmatige intelligentie. Ze kunnen het inzetten als wapen. AI in 2008 ontwikkelde de Carnegie Mellon-universiteit een proof of concept systeem dat volautomatisch malware kon ontwikkelen aan de hand van een software-update.” Een recenter voorbeeld is volgens Van der Molen het algoritme Mayhem, dat in 2016 het levenslicht zag. “Tijdens een DARPA Grand Cyber Challenge wist dit algoritme volledig automatisch de meeste kwetsbaarheden te ontdekken in aangeboden software.”

Volautomatische, AI-gedreven cyberwapens zijn problematisch. “Het cyberdomein is ook zonder AI al een asymmetrisch speelveld”, benadrukt Van der Molen. “Aanvallers hoeven voor een succesvolle hack maar één kwetsbaarheid te vinden en te misbruiken. Terwijl de verdedigende partij alle mogelijke kwetsbaarheden moet dichten. AI maakt dat speelveld nog meer asymmetrisch, bijvoorbeeld omdat een AI-cyberwapen een succesvolle aanval kan uitvoeren voordat een mens kan reageren. Verdedigers die daartegen een AI-firewall inzetten die zich automatisch kan afkoppelen het internet, moeten rekening houden met de impact van valse alarmen.”

“Bij AI-systemen draait beveiliging niet langer om de vraag: hoe beschermen we processen tegen falen? Het doel moet zijn: hoe beschermen we mensen tegen het falen van AI-systemen? Door de grote risico’s van AI is een goede risicoafweging dan ook altijd noodzakelijk. Uiteindelijk kunnen en moeten alleen mensen bepalen of, waar en hoe een AI-systeem zijn werk mag doen.”

“Hoe beschermen we mensen tegen het falen van AI-systemen?”

Henk-Jan van der Molen

Henk-Jan van der Molen
is docent aan de Security Academy.

» Het tekort aan professionals hangt al jaren als een zwaard van Damocles boven de securitymarkt. “Maar we zullen nooit genoeg mensen vinden om alle securityproblemen in ons land op te lossen”, stelt Erwin van Eijk, hoofd van de divisie Digitale en Biometrische Sporen bij het NFI. “We moeten ervoor zorgen dat er minder ongelukken gebeuren, en echt werk gaan maken van security-onderwijs voor niet-securityprofessionals.”

De skill gap is een **groot probleem voor de bv Nederland**

Erwin van Eijk
Hoofd divisie Digitale en Biometrische Sporen, NFI

De divisie Digitale en Biometrische Sporen van het Nederlands Forensisch Instituut houdt zich bezig met het achterhalen en duiden van digitale sporen in strafzaken. Die sporen kunnen zich bijvoorbeeld op telefoons, laptops of virtuele servers bevinden. Maar ook op minder voor de hand liggende apparaten. “Wij onderzoeken de raarste dingen”, zegt Van Eijk.

Als voorbeeld geeft Van Eijk windmolens waar volgens hem ‘wel eens ongelukken mee gebeuren’. “Die apparaten zijn vergeven van elektronica. De vraag aan ons is dan of we op basis van data uit de windmolen kunnen achterhalen wat er is gebeurd. Stond die windmolen netjes in maintenance-stand? Is er mechanisch iets kapot gegaan? Of was er misschien sabotage in het spel?”

Bijzondere onderzoeken
“De kick voor ons is om de puzzel op te lossen, om het onmogelijke voor elkaar te krijgen”, vervolgt Van Eijk. “Hoe mooi is het als door jouw onderzoek bijvoorbeeld miljoenen aan crimineel geld in beslag worden genomen? Dat is best gaaf.”

De onderzoeken die het team van Van Eijk uitvoert, zijn bovendien altijd bijzonder. “Als wij een apparaat binnenkrijgen, dan bestaat er nog geen methode voor het verkrijgen en duiden van de data. Anders had de politie dat zelf wel gedaan.

Ons uitgangspunt is: we doen iets één keer, we doen het nog een tweede keer ter controle en de derde keer doet iemand anders het, of we hebben het geautomatiseerd.”

Automatiseren of snel overdragen is volgens Van Eijk noodzakelijk om als NFI bij te kunnen blijven. “Ons domein ontwikkelt zich enorm snel. Neem een ontwikkeling als Android Automotive. Daarmee is een auto feitelijk een telefoon geworden, maar dan met vier wielen. En uit de rotaties van die wielen kun je ook locaties herleiden, mochten gps-signalen niet beschikbaar zijn. Maar daar moeten we ons als team dan wel in kunnen verdiepen. Dat gaat niet als we steeds maar weer met dezelfde dingen bezig blijven. Dan is onze kennis over twee jaar achterhaald.”

R&D en onderwijs
Research en development is dan ook een belangrijke kerntaak van de divisie Digitale en Biometrische Sporen. Deze kerntaak is gericht op de ontwikkeling van methodes en systemen waar bijvoorbeeld de politie zelf mee aan de slag kan. Zo heeft de divisie de forensische zoekmachine Hansken ontwikkeld. Hiermee kan de politie snel en efficiënt zoeken in grote hoeveelheden in beslag genomen gegevensdragers zoals computers en mobiele telefoons.

“Maar we hebben bijvoorbeeld ook een methode ontwikkeld voor het uitlezen en interpreteren van het geheugen van een insulinepomp”, vertelt Van Eijk. “Hiermee is na een overdosis insuline te achterhalen op welke momenten insuline is toegediend en hoeveel. Als er volgens een toxicoloog nog insuline is toegediend nadat het slachtoffer in coma moet zijn geraakt, dan kan die persoon dat niet zelf hebben gedaan.”

Een andere kerntaak is het geven van onderwijs op het gebied van digitaal forensisch onderzoek aan bijvoorbeeld politie en justitie. “Maar ook aan studenten Digital Forensics”, benadrukt Van Eijk. “We laten zien wat we doen, en waarom we dat doen. Studenten interesseren voor ons werk en stage laten lopen of laten afstuderen bij het NFI zijn voor ons de eerste stappen om aan nieuwe mensen te komen.”

Schaap met zes poten
Ook het NFI merkt dat het lastig is om aan mensen met de juiste skills te komen. “We vragen ook best wel een redelijk rare skills set. We zoeken naar het schaap met misschien wel zes poten”, zegt Van Eijk. “Onze onderzoekers moeten gevoel hebben bij digitaal materiaal en weten hoe ze data uit een app halen, maar ook verstand hebben van grootschalige analytics. En tot slot dat ook nog begrijpelijk aan leken uitleggen. Wat zegt een spoor over de kans dat een activiteit heeft plaatsgevonden?”

“Een foto op mijn telefoon met als geo-tag ‘Oekraïne’ is nog niet het bewijs dat ik in Oekraïne ben geweest”, zo geeft hij als voorbeeld. “Die foto kan ook door iemand anders op mijn telefoon zijn gezet. Die foto is er, maar wat doet dat met de waarschijnlijkheid van een activiteit? Daar moet je als onderzoeker een antwoord op kunnen geven. We zijn gewend om altijd de kortste weg te nemen als we iets willen verklaren. Dat ‘mailtje van Jan’ zal wel afkomstig zijn van Jan. Meestal is dat ook zo, maar het kan ook afkomstig zijn van een oplichter.”

“Onze divisie heeft mensen nodig die out-of-the-box kunnen denken, want op de gebaande paden liggen de antwoorden meestal niet”, vervolgt Van Eijk. “Mensen die het leuk vinden om GitHub-projectjes te onderhouden. En die bij alles wat ze in handen krijgen denken: hoe krijg ik het stuk? Niet voor niets dat de koffieautomaten bij ons nooit een gangbare taal tonen. Daar is altijd mee gerommeld. Dat vindt de beheerder van de automaten niet altijd even leuk, maar het past wel helemaal bij onze organisatie.”

Skill gap
Lesgeven aan studenten is voor het NFI een manier om met toekomstige onderzoekers in contact te komen. “Maar dan nog is het voor ons een uitdaging om mensen met de juiste kennis aan te trekken en te behouden”, onderkent Van Eijk. “De skill gap is een groot probleem voor de bv Nederland.”

“Je ziet nu een generatie opgroeien die heel goed is met apps en technologie, maar geen idee heeft wat er onder water met de data gebeurt. Ze zijn digitally illiterate”, vervolgt Van Eijk. “En kijk naar een opleiding als Psychologie. Het vak statistiek is daar redelijk standaard, maar hoe je privacy en security inregelt helemaal niet. Terwijl psychologen continu met bijzondere persoonsgegevens werken. Daar moeten we als samenleving echt mee aan de bak.”

“De kick voor ons is om de puzzel op te lossen.”

Erwin van Eijk

Security in basiscurriculum
“Het wordt tijd dat we als maatschappij vorm gaan geven aan het security-onderwijs voor niet-securityprofessionals”, concludeert Van Eijk. We moeten veilig gedrag stimuleren zodat er minder ongelukken gebeuren. ‘Digitaal verkeersonderwijs’ kan daarbij helpen. “Nu leggen kinderen op hun tiende een verkeersexamen af waar ze laten zien dat ze de regels kunnen toepassen. De kennis wordt nog eens opgefrist als ze hun brommerrijbewijs en later hun autorijbewijs willen halen. Ze krijgen de stof meerdere keren toegediend, telkens op het niveau dat op dat moment passend is.”

Op eenzelfde manier moeten de onderwerpen security en privacy worden verweven in het onderwijs. “Een eerste stap is kinderen op de basisschool uitleggen hoe internetwijsheid werkt. Zo’n filter op Snapchat is misschien heel gaaf, maar wil je dat jouw gezicht bij Snapchat ligt? Middelbare scholieren die games ontwikkelen, moeten meteen ook onderwijs krijgen in hoe je dan de security aan de backend inricht. En bijvoorbeeld een opleiding Psychologie moet ook aandacht besteden aan hoe je omgaat met de privacy van cliënten.”

“De omgang met security en privacy moet deel gaan uitmaken van het basiscurriculum”, besluit Van Eijk. “We kunnen namelijk nooit voldoende securityprofessionals opleiden om iedereen te helpen. Net zoals we niet op ieder kruispunt een politieagent kunnen neerzetten die toeziet op de veiligheid.”

Erwin van Eijk werkt al bijna 25 jaar voor het Nederlands Forensisch Instituut, onder andere als Senior Forensic Scientist en Data Forensic Scientist. Sinds 2018 is hij hoofd van de divisie Digitale en Biometrische Sporen.

» Veilige digitale identiteiten zijn cruciaal voor een datagedreven bedrijfsvoering. Maar hoe kies je de juiste securitymaatregelen? “Cybercriminaliteit is een businessrisico dat je dus ook vanuit de business moet benaderen”, zegt Guus van Es, Partner Cyber Risk bij Deloitte. “Alleen dan kom je tot een geïntegreerde aanpak om de risico’s te managen.”

Digitale identiteit raakt alle aspecten van de business

Guus van Es
Partner Cyber Risk, Deloitte

Tegenwoordig kunnen we niet meer zonder onze digitale identiteit. Van de belastingaangifte tot het bestellen van producten: op internet moeten we ons continu identificeren. Bijvoorbeeld met een gebruikersnaam en wachtwoord, een code via een smartphone-app of een biometrisch kenmerk. Dankzij die digitale identiteit weten bedrijven en overheidsinstanties met wie ze te maken hebben. Vervolgens kunnen ze die persoon toegang geven tot hun dienstverlening of tot bepaalde informatie.

Volgens Van Es onderschatten veel organisaties hoe belangrijk een zorgvuldige omgang met digitale identiteiten is. “Op directieniveau krijgt dit onderwerp nog vaak onvoldoende aandacht, terwijl digitale identiteiten de verbindende factor zijn tussen de stakeholders van een organisatie en de data in haar ecosysteem. Daarmee raakt digitale identiteit alle aspecten van de business. Elke c-level manager heeft hierin een eigen belang én verantwoordelijkheid. Die belangen kunnen met elkaar botsen. En als er niet strategisch is nagedacht over digitale identiteiten, gebeurt dat vaak ook.”

Conflicterende belangen
Als voorbeeld noemt hij het spanningsveld tussen commercie en privacy. “Een goede inrichting van het proces rondom digitale identiteiten draagt bij aan een betere klantervaring. Iemand met een commerciële functie wil dat het prettig is om zaken met het bedrijf te doen. Elke interactie moet soepel en intuïtief verlopen. Veiligheid is belangrijk, maar mag niet storend zijn of te veel kosten. De marketingmanager is daarbij gebaat om zoveel mogelijk informatie te verzamelen over de klant, bijvoorbeeld voor advertentiedoeleinden.”

De privacyofficer zit heel anders in de wedstrijd. “Sommige klanten vinden het helemaal niet prettig dat je hun data verzamelt en gebruikt. Zij willen inspraak hebben in de dataverwerking, zoals dat ook is vastgelegd in de Algemene verordening gegevensbescherming. De privacyofficer ziet toe op de naleving van de regels. Welke informatie slaan we op en hoelang bewaren we die? Wie hebben toegang tot de informatie? Wat doen ze daarmee? Vanuit dit perspectief maak je andere keuzes.”

Veiligheid versus gemak
Securityprofessionals zijn vooral bezig met de risico’s rondom slecht beveiligde identiteiten en de toegekende toegangsrechten. “Stel dat het heel eenvoudig is om de inloggegevens van klanten te achterhalen. Daarmee kan een cybercrimineel bijvoorbeeld identiteitsfraude plegen. En wat als een CFO een simpel wachtwoord gebruikt voor zijn zakelijk e-mailadres? Dan is er een groot risico op CFO-fraude, waarbij een cybercrimineel bijvoorbeeld met een gehackt e-mailadres een frauduleuze betaling kan goedkeuren.”

“Voor een HR-manager is werknemerstevredenheid dan weer belangrijk. Mensen moeten makkelijk toegang hebben tot de tools die nodig zijn om hun werk te doen. Zo moet een medewerker van de helpdesk altijd in het systeem met klantgegevens kunnen. De CISO wil de toegang juist beperken en extra goed beveiligen. Dat kan tot frustraties leiden: de helpdeskmedewerker moet wéér een nieuw wachtwoord aanvragen terwijl de klant wacht.”

Geïsoleerde perspectieven
In dit specifieke geval speelt er nog iets anders. “In de meeste organisaties zijn de digitale identiteiten van collega’s en klanten van elkaar gescheiden, met een andere persoon die ervoor verantwoordelijk is”, aldus Van Es. “Maar digitale identiteiten kun je niet vanuit een isolement bekijken. Niet vanuit één functie, en ook niet vanuit alleen de techniek, processen of het beleid. Het is juist zaak om al die perspectieven samen te brengen.”

In de praktijk gebeurt dit nog niet genoeg. “Veel organisaties zijn heel snel gedigitaliseerd en hebben niet strategisch nagedacht over digitale identiteiten toen ze ermee begonnen. De digitale identiteit wordt ook vaak puur vanuit de technologie benaderd. Welke oplossing hebben we nodig om onze klanten toegang te geven tot de juiste gegevens? Maar de technologie is slechts één puzzelstukje en zou eigenlijk pas aan het einde moeten komen.”

Geïntegreerde risicoaanpak
Voor een optimale beveiliging van digitale identiteiten moeten we terug naar de basis. Van Es adviseert organisaties om eerst een aantal fundamentele vragen te beantwoorden. “Wat betekent digitalisering voor ons? Wat is de rol van data in ons businessmodel? Om welke data gaat het en wie moet daar toegang toe hebben? Welke risicoclusters horen daarbij? Pas als je een geïntegreerd beeld van de risico’s hebt, kun je prioriteiten stellen. Hoe richt ik mijn governance en processen in om de grootste risico’s te minimaliseren? En welke technologie werkt hierin ondersteunend?”

Een risicocluster is een overkoepelend risico voor de business. Dat kan bijvoorbeeld het verlies van intellectueel eigendom zijn door malafide of nalatig gedrag van werknemers. “Hieronder vallen verschillende securitycomponenten, waaronder het screenen van werknemers, data loss prevention en user behaviour analytics. Maar misschien kun je het risico ook deels beperken met interne communicatie of een verbeterde beveiliging van bepaalde ruimtes. Werken vanuit risicoclusters is een essentieel onderdeel van een geïntegreerde risico-aanpak.”
“Securityprofessionals zijn vaak gericht op het verhogen van het maturitylevel op bepaalde onderdelen”, vervolgt Van Es. “Maar als je niet de connectie maakt tussen risicocomponenten, weet je helemaal niet of je het risico echt aan het verkleinen bent en doe je onbedoeld aan symptoombestrijding.” De risicoclusters zijn ook concreter, wat helpt om de business mee te krijgen. “Met een geïntegreerde aanpak voorkom je dat een securitymaatregel niet wordt omarmd door de business.”

“In een crisissituatie heb je altijd extra capaciteit nodig.”
Guus van Es

De Partner Cyber Risk bij Deloitte benadrukt dat cybercriminaliteit een businessrisico is. “Een datagedreven bedrijfsvoering kan op lange termijn alleen succesvol zijn als je de risico’s rondom digitale identiteiten managet. Dit is een gedeelde verantwoordelijkheid van alle c-level executives en vereist dus ook een gezamenlijke strategie en consistente richting en communicatie naar de organisatie.”

Crisisoefeningen en incident-response
Van Es beseft dat veel organisaties beperkte middelen hebben voor risicomanagement en cybersecurity. “Zelfs als je verder niets doet, zorg dan in ieder geval dat je weet wie je moet bellen in het geval van een ernstig cyberincident. Een vakkundige partij waarmee je de afspraak hebt: als het misgaat, zitten zij dezelfde dag nog naast je. Hulp bij incident-response is altijd waardevol, ook als je zelf wél de benodigde securityexpertise in huis hebt. In zo’n crisissituatie heb je altijd extra capaciteit nodig.”

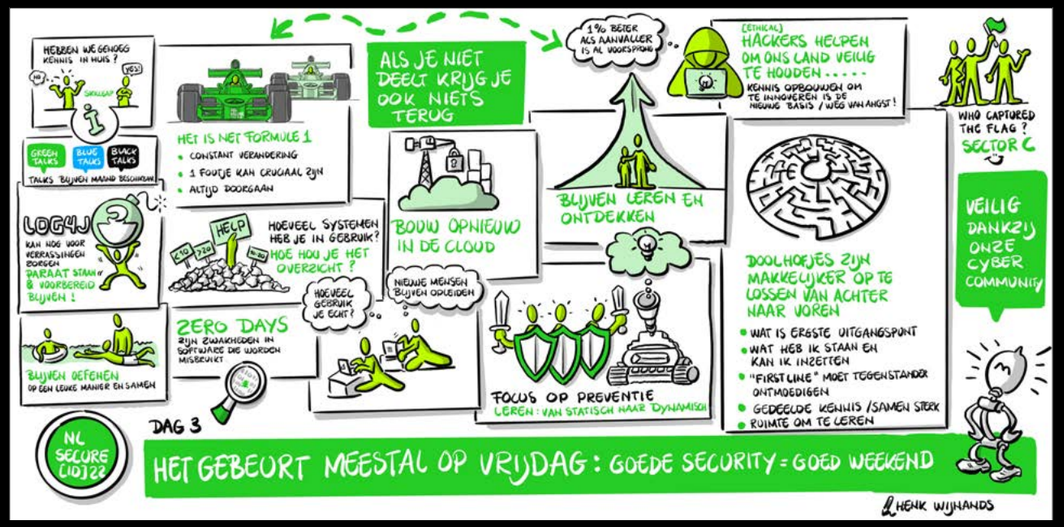
Daarnaast drukt hij iedere organisatie op het hart om worstcasescenario’s te definiëren. “Welke digitale verstoringen hebben de meeste impact op jouw organisatie? Waarvan hoop je echt dat het niet gebeurt? Denk dan juist daarover na. Oefen deze scenario’s ook periodiek met je management en vertegenwoordigers van alle afdelingen. Een soort brandoefening, maar dan voor een cyberaanval. Zo ben je voorbereid op het ergste en draag je bij aan een cultuur waarin iedereen zich medeverantwoordelijk voelt voor het beschermen van de organisatie. Je moet het dak repareren als de zon schijnt.”

Volgens Van Es is elk bedrijf immers een potentieel doelwit. “Van geld en informatie tot digitale identiteiten: bij iedere organisatie valt iets te halen. Bovendien komen gerichte aanvallen niet vaak voor. Veel vaker zijn cybercriminelen breed op zoek naar kwetsbaarheden en vindt men een manier om bij meerdere organisaties binnen te komen. Ga ervan uit dat je op een dag getroffen wordt. Daarmee creëer je ook de juiste mindset. Dat is beter dan continu beargumenteren dat het jou niet zal overkomen.”

Denk vanuit de business
Van Es heeft nog een laatste advies specifiek voor securityprofessionals. “Benader security vanuit de business. Zoek de verbinding met anderen binnen je bedrijf. Wat is de rol van digitalisering in jullie organisatie? Wat is het belang van security in het grotere geheel? Hoe zorg je dat securitymaatregelen in dienst staan van de bedrijfsdoelstellingen? Met deze denkwijze wordt je werk relevanter, effectiever én leuker.”

Guus van Es werkt sinds begin 2019 bij Deloitte als Partner binnen Risk Advisory. In deze rol helpt hij beslissers binnen de overheid en het bedrijfsleven om op een verantwoorde manier risico te nemen en te managen. Hierbij ligt zijn focus op cybersecurity en digitale identiteiten.

NL SECURE [ID]



LET'S TALK ABOUT IT

kpn Security

Colofon

Cyber Security Perspectives 2022
is een uitgave van KPN Security
Roxy Meints - Spaargaren
Babette Kersten
Susan Leliveld
Bram Reinders
Carolien Hoogerwaard
Marcel Heezen

Volume 8

Tekst
Co-Workx
KPN Security

Vormgeving
KPN Kreatie

Drukkerij
HH Global

KPN Security
Wilhelminakade 123
3072 AP Rotterdam

Twitter
www.twitter.com/kpnsecurity

LinkedIn
www.linkedin.com/showcase/kpn-corporate-market

Website
www.kpn.com/security

NLSecure[ID] page
www.kpn.com/nlsecure

kpn Security