NL SECURE [ID]

» 2023

CYBER SECURITY PERSPECTIVES

"Red teaming kan gewoon veilig"
Joost Boele Antoni van Leeuwenhoek

"Ons landschap is om je vingers bij af te likken"
Arjen Boersma ProRail

Security as a SOCIAL PURPOSE

ASML OVER DE CIRCLES OF TRUST | **RABOBANK** OVER VERTROUWEN IN IT | **NORTHWAVE & HOPPENBROUWERS** OVER DE IMPACT VAN EEN RANSOMWARE AANVAL | **TNO** OVER DE FALENDE SECURITYFILOSOFIE **DTC** OVER DE INVOERING VAN NIS2 | EN NOG VEEL MEER

Voorwoord

Cybersecurity hoort ook te gaan over mensen

Cybercriminaliteit is nog altijd de grootste bedreiging voor bedrijven. Goede IT-beveiliging is dan ook belangrijker dan ooit. Toch hoort security niet alleen om techniek, processen en procedures te draaien, maar ook om mensen. Een integrale, inclusieve aanpak. In meerdere opzichten ligt de sleutel voor een cyberveiliger Nederland bij ons allemaal. Op de eerste plaats omdat een groot deel van security-incidenten ontstaat door mensen. Zij creëren onveilige situaties volgens hoogleraar Klinische Neuropsychologie Margriet Sitskoorn als de hersenen bijvoorbeeld onder druk worden gezet. In een interview verderop in dit magazine legt Sitskoorn uit hoe slow information processing helpt fouten te voorkomen en bijdraagt aan security als een state of mind. Nog een reden waarom er meer focus moet komen op mensen: een goede security is het resultaat van een goede samenwerking tussen mensen, kwetsbaarheden zitten in de hele keten. Op de eerste plaats binnen de eigen organisatie, maar ook daar buiten. Als securityprofessional moet je niet op een eiland opereren, maar juist de verbinding zoeken met je omgeving. Of het nu gaat om het creëren van bewustwording, het trainen van cybersecure gedrag, het zoeken naar kwetsbaarheden of het creëren van draagvlak voor securitymaatregelen: cybersecurity valt en staat met team effort. Daarin heeft iedereen een rol. Samenwerken moeten we ook binnen de keten en binnen branches beter doen met elkaar. Hoe meer organisaties en mensen met elkaar samenwerken, hoe veiliger Nederland wordt. Dat kan door het delen van kennis, door het bouwen van community's, door het aan elkaar beschikbaar stellen van best practices en door te praten over dilemma's. Zoals we bijvoorbeeld via deze editie van de Cyber Security Perspectives doen. Met wie ga jij het komende jaar samen werken aan een digitaal veilig Nederland?

Lisette Oosterbroek

Executive Vice President bij KPN Security

Red teaming kan gewoon veilig

met Joost Boele
CISO bij Antoni van Leeuwenhoek

CISO Joost Boele van het Antoni van Leeuwenhoek zorgde met zijn team voor een primeur. Het AVL was de eerste Nederlandse zorginstelling die de eigen cyberweerbaarheid liet testen door een ‘red team’. Hoe kijkt Boele terug op die exercitie? “De belangrijkste conclusie was dat je red teaming gewoon veilig kunt doen, ook in een sector waar patiëntveiligheid centraal staat.”

Het Amsterdamse Antoni van Leeuwenhoek is een in kanker gespecialiseerd ziekenhuis en onderzoeksinstituut. Sinds de oprichting in 1913 combineert het AVL de zorg voor kankerpatiënten met grensverleggend onderzoek. “Het is het enige academische ziekenhuis in Nederland dat geen academisch ziekenhuis is”, zegt Boele met een lach.

Hoogtechnologische oplossingen

Voor een CISO een mooie omgeving om in te werken, vindt Boele. “Het beeld is vaak dat de zorgsector een beetje ouderwets is, alsof we nog met papieren dossiers werken, maar dat beeld klopt totaal niet meer. De uitdagingen waar we mee te maken hebben, worden met hoogtechnologische en goed doordachte oplossingen getackeld. Alles is computergebonden en computergedreven. Ik hoop dan ook dat meer IT- en securityprofessionals gaan kiezen voor een carrière in de zorgsector.”

Volgens Boele is een keuze voor een carrière in de zorg ook een keuze voor maatschappelijk relevant werk. “De zingeving is bij een instituut zoals het AVL overal om je heen. Als je hier naar binnen loopt, lopen er voor en achter je mensen hand in hand en arm in arm. Kanker heb je niet in je eentje. Die mensen hebben nooit met mij te maken, maar ik ben er wel voor ze. Ik zorg ervoor dat mijn collega’s hun werk op een veilige manier kunnen doen, zonder zich zorgen te moeten maken om zaken als cyberdreigingen. Zo kunnen zij zich richten op de zorg voor patiënten.”

Uit de krant blijven

“De uitdaging zit voor mij in het relatiemanagement”, vervolgt Boele. “Als IT’er kun je je bedenkingen hebben als heel veel computersystemen aan elkaar worden geknoopt, maar met ‘nee’ bereik je niets. Dan regelen gebruikers het zelf wel. Het is beter om samen te kijken wat de behoefte is, en wat de beste manier is om iets te bewerkstelligen. Dan duurt het misschien allemaal iets langer, en wordt het net ietsje duurder, maar wel veiliger. Ik wil als CISO niet in de weg lopen, maar ook niet met een security-incident in de krant komen.”

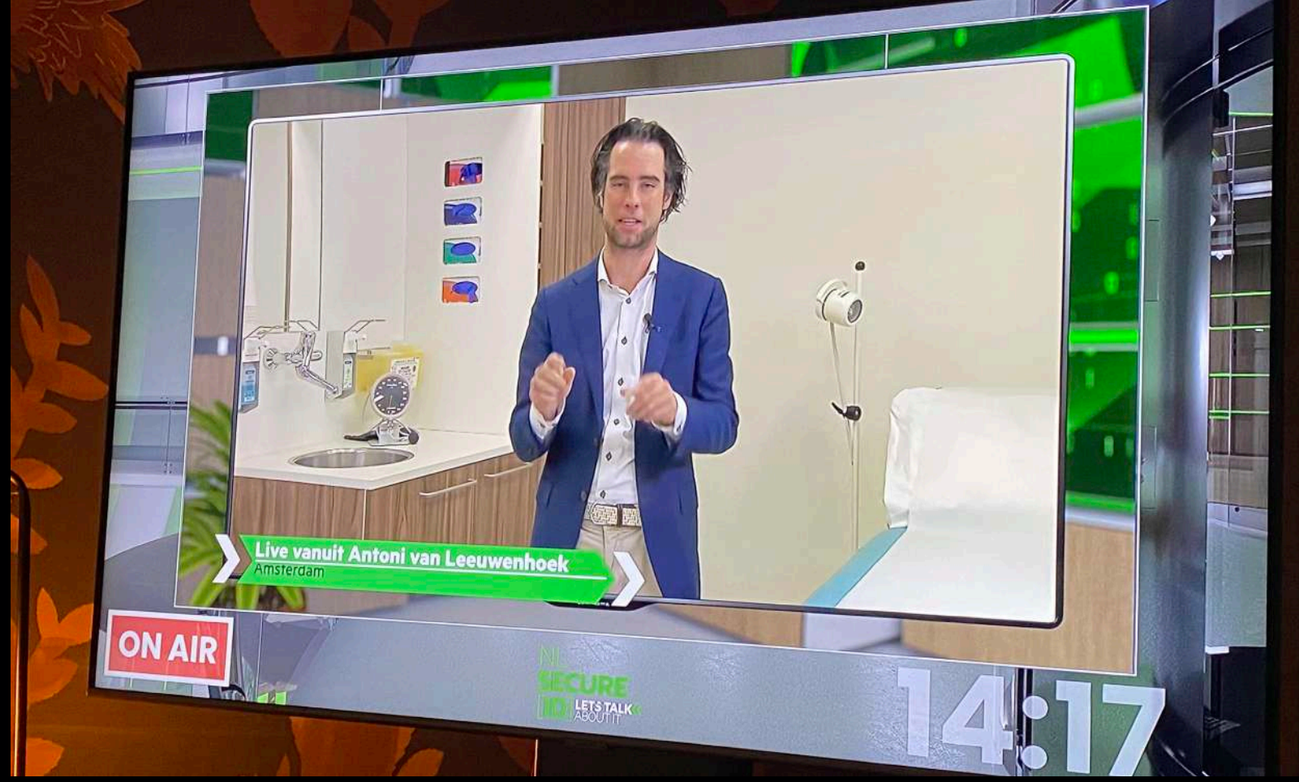
‘Met red teaming krijg je inzichten die je met losse testen nooit zou kunnen krijgen’

Dat ‘veiliger’ begint bij compliance met normen zoals de NEN 7510. “Compliance helpt bij het op orde brengen van je basisbeveiliging. Je toont hiermee aan dat je de juiste dingen op de juiste manier doet. Tegelijkertijd is het ook echt de basis. Je kunt alles doen wat in de norm staat, alle punten afvinken, en nog steeds onveilig zijn. Dan krijg je van de auditor een schouderklopje, maar ondertussen staat de tent in brand. Het gaat erom wat je nog bovenop die basis zet. Waar zet je extra stappen om de cyberdreiging voor te blijven?”

Realistische dreiging nabootsen

Red teaming is volgens de CISO van het AVL een voorbeeld van zo’n extra stap. “Er staat in de NEN 7510 dat het bij wijze van spreken ‘verstandig’ is om een ethisch hacker mee te laten kijken in je systemen, maar nergens dat red teaming verplicht is. Nergens staat dat je in een realistische setting een realistische dreiging moet nabootsen. Een red-teamingoefening laat zien welke beveiligingsmaatregelen je nog moet treffen om je tegen zo’n realistisch scenario te wapenen. Zo krijg je inzichten die je met losse testen nooit zou kunnen krijgen.”

“Als je met red teaming aan de slag gaat, moet je wel zeker weten dat je de basisbeveiliging op orde hebt. Heb je dat niet, dan weet je van tevoren al wat de uitkomst is van de oefening”, waarschuwt Boele. “Pas als je op een bepaald niveau zit, laat je door een externe partij controleren of je inderdaad goed gewapend bent tegen de dreiging die je simuleert. Voor red teaming heb je bovendien draagvlak nodig. Je moet er met elkaar vertrouwen in hebben dat je zo’n oefening kunt uitvoeren, en dat die zinvol is. Dat vertrouwen was binnen het AVL ruimschoots aanwezig.”



ZORRO-raamwerk

Het voornemen van het AVL om met red teaming aan de slag te gaan, viel samen met een pilot van Z-CERT, het Computer Emergency Response Team voor de zorg. Stichting Z-CERT ontwikkelde samen met Nederlandse zorginstellingen een raamwerk voor red teaming genaamd ZORRO (**ZO**rg **R**edteaming **R**esilience **O**efeningen). Dit raamwerk is gebaseerd op de TIBER-methode uit de financiële sector en op maat gemaakt voor de zorg. Risicobeheersing en patiëntveiligheid staan voorop. “Ik heb toen direct mijn vinger opgestoken met de vraag of wij mee konden doen aan een ZORRO-test”, vertelt Boele. “Het was voor ons een kwalitatief hoogwaardige en bovendien zeer betaalbare manier om onze cyberweerbaarheid te testen. Z-CERT had de leverancier al geselecteerd die de aanval uitvoert binnen de kaders van het ZORRO-raamwerk en het ministerie van VWS betaalde in de vorm van een subsidie een deel van de kosten.”

‘De securityawareness kreeg tijdens de oefening al een enorme boost’

AVL heeft primeur

Het AVL was zodoende in 2021 de eerste partij in Nederland die een ZORRO-test uitvoerde. Om een realistisch beeld van de detectie- en verdedigingscapaciteit te krijgen, is tijdens zo’n test alleen een klein kernteam op de hoogte van de gesimuleerde aanval. Boele: “Dat is het

white team. Daarin zaten mensen van het instituut zelf die verantwoordelijk zijn voor de risicobeheersing. Tijdens de voorbereiding bespreek je met het red team de scope van het onderzoek en hoe je storingen voorkomt. Maar als je ethisch hackers zonder verder toezicht loslaat binnen je organisatie, kunnen er dingen stuk gaan. Daarom moet je de juiste mensen stand-by hebben staan om het risico van alle voorgenomen acties in te schatten, en waar nodig bij te sturen."

'Je kunt dit veilig doen, als je maar de juiste mensen in het white team hebt zitten'

Alle andere medewerkers van het AVL - waaronder de IT'ers en security-professionals - behoorden tot het blue team en wisten van niets. "Toen de oefening voorbij was, waren sommige mensen nog bezig met het pareren van wat zij dachten dat het een aanval was. Die mensen heb ik moeten bellen met de boodschap: laat nu je toetsenbord maar los, want het is maar een oefening. Er was iemand bij die in vijf seconden tijd alle vijf de stadia van rouwverwerking doorliep, van ontkenning en boosheid tot uiteindelijk acceptatie. Om vervolgens te zeggen: Joost, dat was niet zo aardig van je, maar gaan we dit nog een keer doen?"

Veiligheid gewaarborgd

"Het gaat er uiteindelijk om wat je van zo'n oefening leert en welke maatregelen je vervolgens treft om te voorkomen dat zwakke plekken die door de ethisch hackers zijn aangetroffen worden uitgebuit door cybercriminelen", concludeert Boele. "De oefening liet ons bijvoorbeeld zien waar we de detectie van narigheid op het netwerk konden verbeteren. De securityawareness kreeg tijdens de oefening al een enorme boost, ook dat van IT'ers. Die gingen zich realiseren hoe eenvoudig het bijvoorbeeld is om iemands inlogportaal na te bouwen. Ook zagen we dat de aanval gelukkig werd opgemerkt en dat mensen elkaar waarschuwden."

"Maar de hoofdbevinding is toch wel dat red teaming gewoon kan in een sector waar een grote nadruk ligt op patiëntveiligheid", besluit Boele. "Je kunt dit veilig doen, als je maar de juiste mensen in het white team hebt zitten die tijdens de oefening de veiligheid waarborgen. Gelukkig merk ik dat de interesse voor red teaming binnen de zorgsector toeneemt." «

Security as a Social Purpose

Cybersecurity is geen baan waarin je van 9 tot 5 taken afvinkt om de eigen KPI's te halen. Nog te weinig wordt onderkend dat het werk van securityprofessionals een maatschappelijke impact heeft, en ook moet hebben. Juist daarom is het onderscheid tussen de security professionals die het benaderen als baan of zij die het zien als missie, erg zichtbaar.

Tekst: Artie Debidien

Voor weerbaarheid in de keten moet je investeren in elkaar binnen en buiten je eigen organisatie. Verbindingen aangaan met andere marktpartijen in je keten. Zelfs concurrenten binnnen je eigen sector en de non-marktpartijen oftewel publieke, controlerende en overkoepelende organisaties. Je moet iets willen doen, zonder er iets terug voor te vragen of krijgen. ESG (Environmental, Social Governance framework) is een raamwerk voor de niet-financiële sectoren die van invloed zijn op risico's, rendementen, sociale en bestuurlijke factoren. Op grond van deze factoren kunnen betere besluiten genomen worden. Bedrijven hebben een houvast nodig om duurzaamheid en impact op de maatschappij te bevorderen. Dat deze duurzaamheid en impact op de maatschappij commerciële doelen in de weg staat, is een misvatting. Bedrijven kunnen het immers financieel goed doen door goed te doen! Hoe meer je samenwerkt in belang van de maatschappij, hoe meer duurzame impact we maken. Tijd om cybersecurity in het ESG-raamwerk op te nemen onder de 'S' van Social!

Over de auteur
Artie Debidien is Chief Information Officer en Executive Vice President bij KPN.

Door het toenemende gebruik van technologie en digitale systemen in bedrijfsprocessen, zijn bedrijven steeds kwetsbaarder voor cyberdreigingen zoals hacking, datalekken en phishingaanvallen. Die trend wordt nog eens versterkt door ontwikkelingen als remote en hybride werken. Door de toenemende afhankelijkheid van IT stijgen bovendien de kosten van een datalek per geval. Uit een wereldwijd onderzoek van JP Morgan blijkt dat een datalek een bedrijf gemiddeld zo'n 4 miljoen dollar kost, de gemiddelde kosten stijgen per geval met zo'n 137 duizend dollar als gevolg van dat hybride en altijd aan werken. In onze booming digital-economy is cybersecurity geen applicatie of software industrie aangelegenheid. Het is geen IT alleen, maar integraal onderdeel bij alles wat we doen. Het is een major topic geworden voor de totale context waarin we werken en leven.

Groene status reporting kleuren geven aan dat je niet snel genoeg beweegt

Op IT-organisaties is de druk dan groot om 'het huis op orde' te hebben, onder meer van het management dat zelf weer onder druk staat van andere belanghebbenden. En terwijl bijvoorbeeld klanten, het management en aandeelhouders vragen om meer digitalisering, verwachten diezelfde stakeholders en de toezichthouder dat de informatiebeveiliging op hetzelfde niveau blijft. Dat kan bijna niet samengaan! Hoe meer je in beweging bent op het pad van reductie legacy en complexiteit in je architectuur en tegelijkertijd investereren in operationele kwaliteit en digitalisering hoe meer je continuiteit en daarmee dus ook de kwetsbaarheid beinvloed.

Organisatorische houdgreep

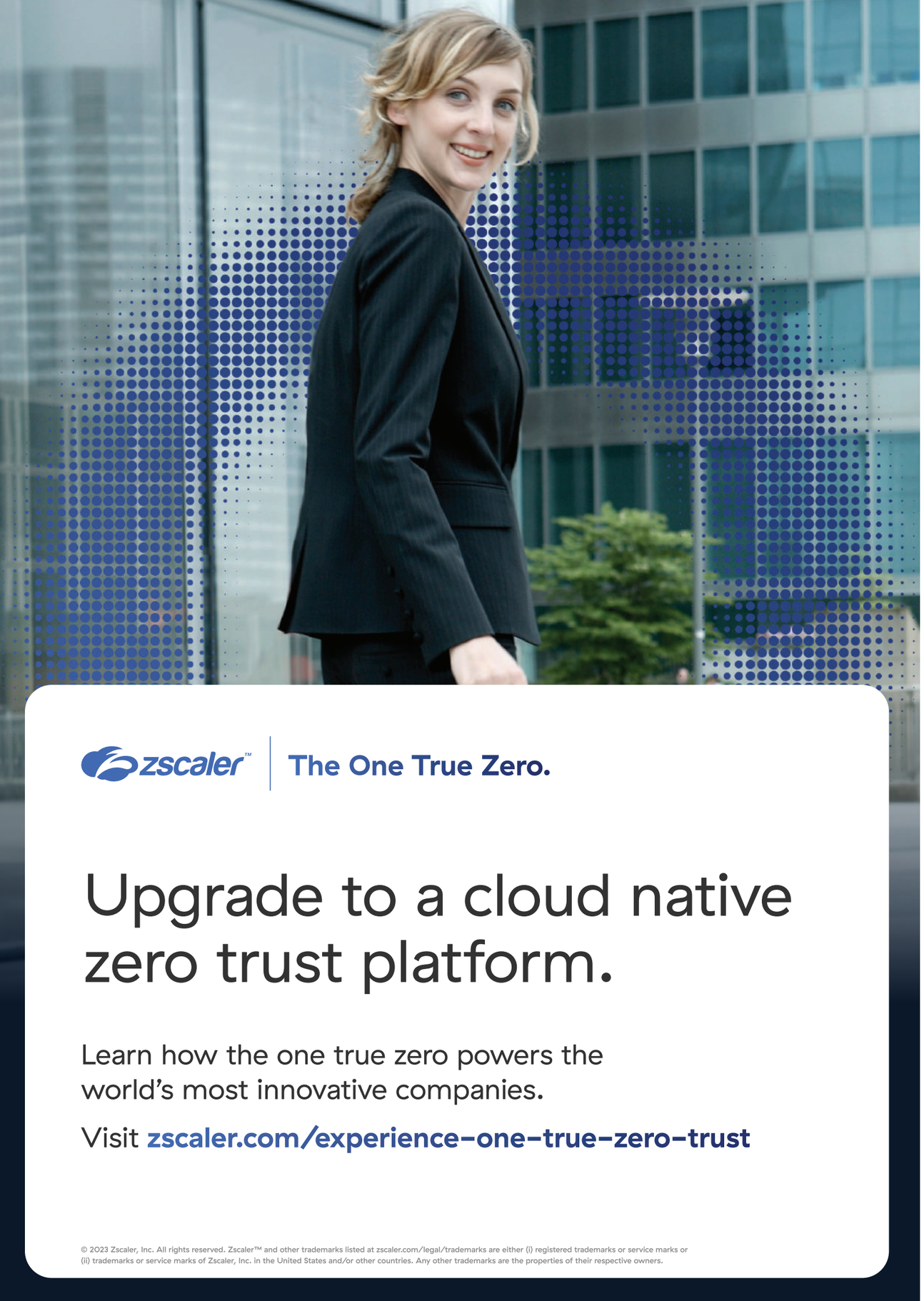
De druk die verschillende partijen op elkaar uitoefenen, houdt securityprofessionals gevangen in een organisatorische houdgreep. In die houdgreep gaat de aandacht met name uit naar compliance en het in-control-vraagstuk. Informatiebeveiliging is dan een baan die vooral intern en op functies is gericht en voor een groot deel draait om het overbrengen van in-control-statements. Maar die interne focus maakt je niet veilig. Security is zo sterk als de zwakste schakel in een keten, en die keten bevindt zich buiten de eigen organisatie. Laat ik banken als voorbeeld geven. Als je een betaling doet naar iemand die bankiert bij een andere bank heb je in de technische keten al te maken met twee verschillende organisaties. Die twee organisaties moeten voldoen aan hetzelfde niveau van informatiebeveiliging om de financiële dienstverlening voor de klant veilig te maken. Dat betekent dat de banken uit dit voorbeeld ook in elkaar moeten investeren en moeten inzien dat security een 'social purpose' heeft.

Maatschappelijke impact

De keten in zijn geheel is alleen sterker te maken door samen te werken. En door oog te hebben voor de maatschappelijke impact van het werk dat securityprofessionals doen. Dat ze door 'goed te doen' Nederland veiliger en het leven beter maken. In het geval van de banken door er in gezamenlijkheid voor te zorgen dat financiële transacties veilig zijn. Die maatschappelijke inspanningen kunnen en mogen in het belang van de eigen organisatie zijn en bijvoorbeeld financiële winst opleveren. Doing well by doing good. Maar wat is dat, 'doing good'? En hoe kunnen organisaties - zowel commercieel als niet-commercieel - daar profijt van hebben?

Doing good

'Doing good' begint bij samenwerking en het opbouwen van contacten en relaties, zoals met overheden en toezichthouders. Hoe meer organisaties en mensen met elkaar samenwerken vanuit een maatschappelijke doelstelling, hoe veiliger Nederland wordt op het gebied van cybersecurity. Iedereen heeft elkaar nodig. Transformaties mislukken bovendien als je elkaar niet meeneemt. In die samenwerking is het belangrijk om informatie, kennis en oplossingen genereus met elkaar te delen. Ben jij op de hoogte van een nieuwe cyberdreiging en weet je hoe je die dreiging kunt mitigeren? Deel die kennis dan met de maatschappij, zodat iedereen weer een stukje wijzer en de keten sterker wordt. Dit gebeurt gelukkig al. Zo schreef Hoppenbrouwers Techniek een boek over de ransomware-aanval waar het bedrijf in juli 2021 mee te maken had. Of denk aan het evenement NLSecure[ID] van KPN



Security dat is gericht op het delen van kennis binnen de securitygemeenschap zodat cybersecurityprofessionals weer een stukje beter worden. Ook de selectie van partners is een belangrijk aandachtspunt bij 'doing good'. Ga niet voor de goedkoopste partner, maar voor een partner die eveneens oog heeft voor de impact op de maatschappij. Een partner die bijvoorbeeld streeft naar klimaatneutraal opereren en 'secure by design' als uitgangspunt heeft. Dat is uiteindelijk ook in het belang van je klanten.

Doing well

Als meer mensen en organisaties werken vanuit een maatschappelijke doelstelling, wordt het leven makkelijker én veiliger. Je beschermt de keten. Daarbij hoeft investeren in 'doing good' zeker niet ten koste te gaan van de eigen inkomsten, zoals vaak wel de gedachte is. Zoals eerder al opgemerkt: aan 'doing good' kan en mag ook geld worden verdiend. Handelen vanuit een maatschappelijk belang is goed voor de eigen reputatie. Klanten kiezen sneller voor een partij die het maatschappelijk belang voorop stelt. Door security als een 'social purpose' te benaderen, wordt het ook eenvoudiger om mensen aan te trekken, te inspireren en te behouden. Mensen zijn gelukkiger als ze een bijdrage kunnen leveren aan de maatschappij, en niet alleen iets doen om geld te verdienen. Security als een 'social purpose' werkt op die manier als een magneet op nieuw talent.

ESG-framework

Hoe zetten we nu stappen richting 'security as a social purpose'? Op de eerste plaats door intern aandacht te vragen voor de maatschappelijke relevantie van cybersecurity. Securityprofessionals moeten de ruimte krijgen om hun maatschappelijk relevante taak uit te voeren. CEO's zouden zich daarbij activistischer moeten opstellen door te laten zien waar ze voor staan en voor gaan. Met alleen een focus op geld komt het niet goed. Ook de sociale KPI's zijn van belang. Maar ik wil vooral een oproep doen om cybersecurity op te nemen in het ESG-framework waarin milieu, maatschappij en goed bestuur samenkomen. Een sterk cybersecuritybeleid is namelijk niet alleen een kwestie van risicobeheer, maar ook van maatschappelijke verantwoordelijkheid en duurzaamheid. Bij goed bestuur hoort bovendien aandacht voor veiligheid en stabiliteit van bedrijven en hun stakeholders. Niet onbelangrijk nu datalekken en aanvallen een steeds groter risico vormen voor de waarde van bedrijven en uiteindelijk de stabiliteit van de samenleving. ««

ProRail is een van de grootste IT-werkgevers van Nederland. Ruim 700 IT’ers zorgen ervoor dat Nederland bereikbaar blijft. “Zonder IT rijdt er geen trein in Nederland”, zegt Arjen Boersma, CIO bij ProRail. Die afhankelijkheid van IT wordt steeds groter, en dus ook de aandacht voor cybersecurity.

‘Externe werving is echt een probleem aan het worden in Nederland’

1. Voor welke uitdaging staat ProRail op het gebied van IT en cybersecurity?

“De digitalisering in de breedte. De komende jaren moeten we een grote sprong maken in de capaciteit op het spoor en dat lukt niet door alleen maar bij te bouwen. We moeten de beschikbare capaciteit efficiënter benutten, onder andere door de inzet van IT en een herinrichting van de bedrijfsprocessen.”

“Daarnaast zien we dat de operationele technologie voor bijvoorbeeld brug-bedieningen, tunneltechnische installatie en schakelingen aan de bovenleidingen steeds meer IT wordt. En ook het European Rail Traffic Management System (ERTMS) dat het huidige treinbeveiligingssysteem gaat vervangen, is in belangrijke mate een IT-systeem.”

“Er komt dus een steeds grotere vraag op onze IT-afdeling af. We worden meer en meer een integraal IT-bedrijf, in plaats van een bedrijf met een clubje IT’ers. Dat betekent ook dat we onze securityvaardigheden verder moeten uitbreiden. Het gaat immers om de veiligheid van de treinen en de reizigers zelf. Dat zijn best forse transities waar we voor staan.”

2. Hoe bereidt ProRail zich voor op een eventuele cyberaanval?

“Dat doen we op meerdere manieren. We treffen preventieve maatregelen, monitoren de systemen en houden bij welke softwarelekken wereldwijd worden ontdekt. Daarnaast oefenen we regelmatig onze reactie op een cybercrisis, zowel zelfstandig als samen met andere partijen binnen de sector. We zijn ook een vaste deelnemer aan ISIDOOR, de grootschalige Nederlandse cybercrisisoefening”.

“Daarnaast doen we heel veel aan pentesting door ethical hackers die we binnen en buiten ons netwerk helemaal los laten gaan. En we werken continu aan de security-awareness van alle ProRail-

Werken in security bij KPN
Een greep uit de mogelijkheden

Wil je KPN, het grootste netwerk van Nederland, veilig houden en beschermen?

Wil je systemen analyseren en kwetsbaarheden identificeren?

Wil je web app, mobiele app, infra, hardware, software pentesten en redteamen?

CISO REDteam
- ✓Ethical Hackers

Wil je security diensten voor onze klanten ontwikkelen en bouwen?

KPN Security
- ✓Commercieel product manager
- ✓Dienstenmanager
- ✓DevOPS

Wil je incidenten oplossen voor klanten of pentesten?

KPN Security
- ✓Incident response (CSIRT)
- ✓Pentesters

Wil je beleidsmatig, inhoudelijk of met compliance bezig zijn in het security werkveld of rapporteren over de status van security binnen KPN?

Wil je beleid schrijven of uitdragen of linking pin zijn naar de rest van de organisatie?

CISO Office
- ✓Beleidsadviseur
- ✓Procesmanager
- ✓Senior Security Officer

Wil je werken aan compliance / rapporteren?

CISO M&R
- ✓Security Compliance Officer
- ✓Reporting Specialist
- ✓Data Engineer

Wil je bedrijven helpen hun veiligheidsvoorziening naar een hoger niveau te brengen?

Wil je de overheid helpen bij digitale authenticatie & validatie?

KPN Security
- ✓DevOPS PKI
- ✓DevOPS E-herkenning

Wil je klanten adviseren en samenwerken om hen te behoeden voor cybercrime?

KPN Security
- ✓Accountmanager
- ✓Business Consultant
- ✓Solution Consultant
- ✓Architect

Wil je operationeel bezig zijn in het security werkveld?

Wil je hackers en cyber criminelen continue een stap voorblijven?

CISO BLUEteam SOC
- ✓Monitoring & Triage Analist (TIER 1)
- ✓Senior Security Analist (TIER 2)

Wil je incidenten oplossen?

CISO BLUEteam CERT
- ✓Incident response

Wil je ontwikkelen en scripten t.a.v. security tooling?

CISO BLUEteam
- ✓Security Engineer
- ✓Developer

Interesse? Kijk voor alle vacatures op **jobs.kpn.com/security**

medewerkers. We gebruiken hiervoor diverse middelen, van phishingmails tot cybergames. Dit heeft succes; we zien dat steeds minder mensen op phishingmails klikken en dat het beveiligingsbewustzijn toeneemt."

3. Waar ben je trots op binnen ProRail? En wat kan beter?

"Als aanbieder van een essentiële dienst moet onze dienstverlening 24x7 beschikbaar zijn. Als treinen door een storing bij Amsterdam of Utrecht Centraal tien minuten niet kunnen rijden, heeft dat de hele dag impact. Dan ben ik trots als ik zie hoe snel we problemen kunnen oplossen en wat we allemaal weten te voorkomen. En dat met het enorme landschap dat wij onder onze hoede hebben. We hebben een van de grootste glasvezelnetwerken van Nederland en zijn de vierde telecomprovider van Nederland.
"We hebben een gedigitaliseerd landschap en zijn vergaand geautomatiseerd in alles wat wij doen. Een volgende stap is dat we het hele bedrijf meenemen in de digitalisering. Het gaat erom dat je digitalisering effectief inzet in je bedrijfsvoering, in je operatie en in je normale manier van werken."

4. Hoe zorg je ervoor dat je altijd over voldoende cybersecuritykennis beschikt?

"Externe werving is echt een probleem aan het worden in Nederland. We vissen met z'n allen in een kleine vijver. Dan moet je goed kijken wat je zelf nog kunt doen en welke dienstverlening je moet inkopen. Ook leiden we intern mensen op om ze verder te brengen binnen het vakgebied van cybersecurity."

'We vissen met z'n allen in een best wel kleine vijver'

"En natuurlijk blijven we buiten aan de boom schudden, om te kijken of we securityprofessionals kunnen interesseren voor een carrière bij ProRail. Helaas zijn er altijd partijen met diepere zakken."

5. Waarom moeten security-professionals kiezen voor een carrière bij ProRail?

"Nergens in Nederland krijg je zo'n scope onder je hoede, als je kijkt naar het landschap dat wij hebben staan, de diversiteit van de onderwerpen en de uitdagingen voor de komende jaren. Dat is voor elke IT'er om je vingers bij af te likken. En dan doe je ook nog eens maatschappelijk relevant werk, en draag je bij aan de meest duurzame modaliteit in Nederland." «

Een dag in het leven van

Sanne Maasakkers

Securityspecialist bij het NCSC

Ethisch hacker Sanne Maasakkers trad in januari 2022 toe tot het Nationaal Cyber Security Centrum (NCSC), onderdeel van het Ministerie van Justitie en Veiligheid. Als securityspecialist duidt ze incidenten, kwetsbaarheden en dreigingen. Niet alleen voor de doelgroep van het NCSC, maar ook voor de media en de politiek. Hoe ziet een werkdag eruit als ze een 'dienstweek' heeft?

7.45 uur: de wekker

"Ik ben geen typische hacker die het redt met drie uurtjes slaap. Ik blijf dus het liefst zo lang mogelijk liggen 's ochtends! Ik woon gelukkig dichtbij mijn werk. Binnen een kwartiertje ben ik op kantoor. Maar eerst drink ik thuis nog een dubbele espresso, want die is echt vele malen beter dan de koffie uit de automaat op kantoor."

8.30 uur: op kantoor

"Eens in de vijf á zes weken heb ik een dienstweek op kantoor. In die week ben je verantwoordelijk voor duiding in de huidige operatie. De dagen verlopen dan volgens een redelijk strak stramien, al plannen incidenten zich natuurlijk niet. In de ochtend staat er veel informatie klaar waar 'iets' mee moet gebeuren maar niet urgent genoeg was om wakker voor gebeld te hoeven worden, bijvoorbeeld van internationale samenwerkingpartners met een andere tijdzone. Ook ontvangen we per dag tientallen meldingen van securityonderzoekers. Het team waar ik in zit, het Fusion Centre, fungeert als de oren en ogen van een digitaal veilig Nederland."

"Of het een rustige of drukke dag wordt, is meestal in de ochtend al duidelijk. Geef mij maar spanning en sensatie. Dat heb ik nodig om geboeid te blijven; hoe meer chaos, hoe beter. Wat dat betreft viel ik bij het binnenkomen bij het NCSC met mijn neus in de boter met het incident log4j. Sinds die tijd zijn dat soort kwetsbaarheden met impact op vergelijkbare schaal er niet meer geweest."

'Hoe meer chaos, hoe beter'

9.30 uur: overleg

"Met een multidisciplinair team bestaande uit onder andere incident-responsespecialisten en dreigings-analisten, maar ook leden uit andere (ondersteunende) teams spreken we de dag door. Wat zijn de lopende incidenten? Met welke nieuwe dreigingen krijgt onze doelgroep mogelijk te maken? En waar moeten we verder nog rekening mee houden? Er ontstaat dan vrij snel een beeld van de dag."

"Als er sprake is van een nieuwe kwetsbaarheid in systemen die veel worden gebruikt door de rijksoverheid of de vitale infrastructuur, dan weten we dat het een hectische dag kan worden. We onderzoeken wat de kwetsbaarheid precies inhoudt, schrijven een beveiligingsadvies en als het een ernstige kwetsbaarheid betreft

brengen we het op meerdere manieren direct onder de aandacht. Een aantal keren hebben we afgelopen jaar een GitHub-pagina opgetuigd, waarbij extra informatie over getroffen systemen en preventie-, detectie- en huntingmaatregelen werden verzameld. Denk daarbij aan kwetsbaarheden zoals log4j, maar ook spring4shell en SpookySSL. Gelukkig viel het in de laatste twee gevallen mee, maar better safe than sorry."

"Het kan ook zijn dat een incident in de media groot uitgelicht wordt terwijl het helemaal niet zo spannend is. Dan is het de taak van ons team om extra duiding te geven richting onze doelgroep. Wat is daadwerkelijk de ernst, en wat raden wij aan als handelingsperspectief? Daar horen ook het input geven op politieke stukken en de media te woord staan bij."

15.30 uur: de 24/7 ploeg

"We zijn 24 uur per dag bereikbaar, en dat houdt in dat we naast een dagploeg ook nog een avondploeg en nachtbereikbaarheid hebben. De avondploeg moet natuurlijk op de hoogte zijn van de lopende incidenten, dus die worden aan het einde van de dag geïnformeerd. Zelf ben ik in mijn dienstweek ook 's nachts en in het weekend bereikbaar, gelukkig ben ik nog nooit uit mijn bed gebeld."

Na 18.00 uur: neerploffen, of...?

"Omdat een dag vol incidenten best weleens hectisch kan zijn, houd ik het 's avonds meestal rustig. Aangezien ik binnenkort een examen heb voor een training die ik heb gevolgd, ben ik daarvoor aan het studeren en malware aan het analyseren. Daarnaast doe ik presentatie- en mediagerelateerd werk, dus sluit ik wel eens aan bij een nieuws podcast van BNR na mijn dienst of bereid ik een presentatie voor."

"Ook werk ik in de avonduren aan nieuw lesmateriaal voor hackchallenges.nl, mijn platform met challenges voor kinderen in de leeftijd van ongeveer 8 tot 16 jaar om ze (ethisch) te leren hacken. Ik beantwoord dan mail van scholen die gebruik willen maken van het platform of maak een nieuwe challenge."

In de securitycommunity

"Buiten de dienstweek zien mijn werkdagen er weer heel anders uit. Dit zijn heel andere werkzaamheden dan de werkzaamheden tijdens mijn dienst. Zo ben ik coach van het Europese hackteam dat in 2022 de eerste editie van de International Cybersecurity Challenge won, maar houd ik me ook bezig binnen het malwareanalyseteam en de voorbereiding voor een grote crisisoefening."

"Ik vind het leuk om midden in de securitygemeenschap te staan en dit vanuit het NCSC op te pakken. Het is belangrijk dat we een goede relatie onderhouden met onderzoekers die kwetsbaarheden bij ons melden. De informatie die zij hebben over (mogelijke) kwetsbaarheden in overheidssystemen is voor ons ontzettend belangrijk. Als een kwetsbaarheid is opgepakt en verholpen ontvangt de melder het felbegeerde 'I hacked the Dutch government and all I got was this lousy t-shirt'-shirt', of tegenwoordig zelfs een hoodie wanneer we de melder extra willen bedanken. Dat doen we nu met een Wall of Fame; naast onderzoekers staat ook het Dutch Institute for Vulnerability Disclosure op deze Wall of Fame. Zonder de vrijwilligers van de DIVD hadden we bepaalde kwetsbaarheden misschien wel veel later gezien." «

'I hacked the Dutch government and all I got was this lousy t-shirt'

Het Digital Trust Center viert dit jaar zijn eerste lustrum. Het onderdeel van het ministerie van Economische Zaken en Klimaat zet zich al vijf jaar in voor de cyberweerbaarheid van ruim 2 miljoen Nederlandse bedrijven. “Samen moeten we de cyberweerbaarheid op een hoger niveau zien te krijgen”, zegt Michel Verhagen, manager van het DTC.

1. Wat zie je als het belangrijkste wapenfeit van het DTC?

“Onze naamsbekendheid. Uit cijfers van het CBS blijkt dat tien procent van de bedrijven met meer dan twee werknemers wel eens van ons heeft gehoord. Dat is best veel in zo’n betrekkelijk korte tijd, en zeker voor een organisatie waar je als ondernemer misschien liever niet mee te maken hebt. Daarnaast werkt het DTC samen met inmiddels meer dan vijftig samenwerkingsverbanden die ondernemers helpen met veilig digitaal ondernemen. Ook dat hebben we in vijf jaar tijd voor elkaar gekregen.”

“Gelukkig zien we een toenemende aandacht voor beveiligingsmaatregelen zoals multifactorauthenticatie, het maken van back-ups en het automatisch updaten van software. Dat zijn ook onderwerpen waar we als DTC veel aandacht aan besteden. Helaas zijn er nog altijd veel bedrijven die achterblijven, maar we zien vooruitgang. Die toenemende aandacht voor cybersecurity is natuurlijk niet alleen onze verdienste, maar bijvoorbeeld ook het gevolg van de media-aandacht voor cyberaanvallen. Ondernemers komen erachter dat cybercrime ook hen kan treffen.”

‘We zien een toenemende aandacht voor beveiligingsmaatregelen’

2. Is de invoering van NIS2 goed nieuws voor het mkb?

“Ik denk het wel. De NIS-richtlijn gaat voor meer sectoren gelden, en dan voor bedrijven vanaf 50 medewerkers. Duizenden bedrijven krijgen daardoor een zorgplicht en een meldplicht voor cyberincidenten, en worden dus gedwongen om meer aandacht te besteden aan cyberweerbaarheid.”

“Kleinere bedrijven krijgen geen meldplicht en zorgplicht door deze nieuwe richtlijn, maar zullen wel merken dat de grotere bedrijven waar ze in de keten mee samenwerken hogere securityeisen gaan stellen. En dat ze hulp krijgen bij

het verbeteren van de cybersecurity, bijvoorbeeld in de vorm van training of het samen uitvoeren van cyber-securityoefeningen. Dat 'groot helpt klein' krijgt een extra impuls door de NIS2."

3. Het DTC, NCSC en CSIRT-DSP gaan in 2026 samen in één centraal expertisecentrum en informatieknooppunt. Wat betekent dit voor de betrokken organisaties?

"Door de krachten te bundelen kunnen we onze dienstverlening uitbreiden. Het NCSC is een stuk groter dan het DTC, maar wij weten wel als geen ander hoe we het mkb moeten bereiken. We voorzien ondernemers in duidelijk taal van informatie en advies, en notificeren sinds kort ook individuele bedrijven als wij weet hebben van een concrete kwetsbaarheid. Binnen een grotere organisatie kunnen we die dienstverlening met nog meer expertise aanbieden."

4. Welke hack zal je altijd bijblijven?

"Niet een specifieke hack, maar de impact van ransomware-aanvallen zal me altijd bijblijven. Dat bedrijven niet meer bij hun data kunnen en in het ergste geval zelfs failliet gaan. Typerend voor ondernemers is dat ze niet bij de pakken neer gaan zitten maar zo snel mogelijk kijken hoe ze er weer

'Ondernemers komen erachter dat cybercrime ook hen kan treffen'

bovenop kunnen komen."

"Daarnaast hebben heel veel bedrijven last gehad van de kwetsbaarheid in Log4j. Dat merkten wij ook. Direct toen de kwetsbaarheid bekend werd, hebben we samen met het NCSC een webinar georganiseerd over de stand van zaken. Binnen één dag trokken we drieduizend kijkers en kregen we honderden vragen die we ook allemaal hebben beantwoord."

5. Wat is je belangrijkste oproep aan mkb-bedrijven?

"Investeer in cyberweerbaarheid, want dat is van deze tijd. Die investering is nú nodig. En laat je helpen door een partij die verder is in het securityproces. Ga met je IT-dienstenleverancier praten over hoe je de bescherming tegen aanvallen beter op orde krijgt. En zoek bijvoorbeeld aansluiting bij een samenwerkingsverband of brancheorganisatie. Er zijn best veel partijen die hun kennis willen delen. Vertrouw op elkaar, en op het feit dat je elkaar kunt helpen. 'Trust' zit niet voor niets in onze naam. Vertrouwen is echt enorm belangrijk." «

De lol van langzaam

met Margriet Sitskoorn

professor in de Klinische Neuropsychologie

“We zijn voorgeprogrammeerd om slachtoffer te worden van cyberhacking”, stelt Margriet Sitskoorn, neuropsycholoog en hoogleraar Klinische Neuropsychologie aan de universiteit van Tilburg. Gelukkig is die programmering ook te doorbreken. Door de hersenen te hacken.

‘Cyberschaamte’ was het cybersecurity-woord van het jaar 2022. Het woord verwijst naar de schaamte die mensen hebben als ze bijvoorbeeld op een phishinglink hebben geklikt. Maar die schaamte is volledig onterecht, vindt Sitskoorn. “Het is zo menselijk om in de valkuilen van cyberhacking te vallen. Het kan ons allemaal overkomen.” Volgens de hoogleraar heeft dat onder andere te maken met de huidige wereld waarin we leven. Die wereld wordt gekenmerkt door een complexiteit en snelheid waar we nog niet goed mee om kunnen gaan. “Veel informatie en interacties zijn digitaal, terwijl onze hersenen daar nog niet op zijn ingesteld.”

Standaard reflexen

Een van de problemen is dat onze hersenen zijn ‘voorgeprogrammeerd’ om uit een automatisme te reageren. “Zeker als we de hersenen onder druk zetten”, aldus Sitskoorn. Hoe dat werkt, toonde ze aan tijdens NLSecure[ID]. Tijdens haar presentatie liet ze de kijkers eerst enkele rekensommen oplossen, en vroeg ze vervolgens om een gereedschap te noemen. Daarna volgende een afbeelding van... een hamer. “Het automatisme om ‘hamer’ te zeggen, is zo voorspelbaar dat ik het een week geleden al kon opschrijven.”

‘Het is menselijk om in de valkuilen van cyberhacking te vallen’

Hersenen reageren niet alleen uit een automatisme, maar ook op wat ze denken te zien. “Als je iemand een lange lap tekst laat lezen, dan kost dat de hersenen veel energie. Om energie te besparen, reageert het snelle systeem in de hersenen op wat het denkt te hebben gezien. Dat kan risico’s opleveren. Je hebt dan bijvoorbeeld te snel een mailtje geopend dat van je moeder af lijkt te komen, maar dat niet is.”

Pijn en genot

Cybercriminelen doen er alles aan om dit soort standaardreflexen uit te lokken, waarschuwt Sitskoorn. Dat doen ze onder andere door het pijn- en genotsysteem te prikkelen. Ze spiegelen het slachtoffer bijvoorbeeld een nieuwe en statusverhogende baan voor (genot). “Dan kom je meteen in actie om te doen wat je denkt dat je moet doen om die hogere status te krijgen.”

“Maar het kan ook zijn dat ze dreigen je status te verlagen door naaktfoto’s van je te publiceren”, vervolgt de hoogleraar. “Dan wordt je pijnsysteem geprikkeld en ga je alles doen wat je denkt dat nodig is om statusverlies te voorkomen.”

‘Cybercriminelen doen er alles aan om standaardreflexen uit te lokken’

De prikkels van het pijn- en genotsysteem zijn niet alleen gericht op de status van het slachtoffer. Binnen het SCARF-model gaat het naast Status ook om Certainty (zekerheid), Autonomy, Relatedness (verbinding) en Fairness (rechtvaardigheid). Zo kan een cybercrimineel je laten denken dat je wel moet klikken om de zekerheid te hebben dat je morgen nog bij je geld kunt. “Eigenlijk alle cybersecurityaanvallen op personen zijn aan de hand van dit SCARF-model uit te leggen.”

HersenHack

Over hersenmechanismen en hoe daar misbruik van wordt gemaakt, schreef Sitskoorn het boek HersenHack. In die titel ligt ook de oplossing verscholen. Het woord ‘hack’ slaat namelijk niet alleen op het inbreken in computersystemen, maar betekent ook ‘verbeteren’. “Hersenen zijn neuroplastisch en in staat om te veranderen. Als je ze het juiste aanbiedt, ontstaan er nieuwe verbindingen en passen ze zich aan.”

Maar wat is dan ‘het juiste’? Volgens Sitskoorn is het op de eerste plaats belangrijk om kennis te hebben van hoe de hersenen werken. “Je kunt tegen iemand zeggen: klik niet op die link. Maar dat is lastig als een automatisme wordt uitgelokt. Cybercriminelen krijgen steeds meer kennis van het gedrag en de emoties van mensen, en spelen daarop in. Misbruik moet je een stap voor zien te blijven, onder andere door je eigen aandacht en emoties onder controle te hebben. Daarvoor moet je begrijpen hoe de ander een reactie bij je probeert uit te lokken.”

“Ook moeten we mensen aanzetten tot ‘slow information processing’, vervolgt de neuropsycholoog. “Onze hersenen zijn er al helemaal op ingesteld dat we dingen snel moeten doen, zonder daarbij op te letten of na te denken. Maar als je mensen onder druk zet, maken ze fouten die ze anders niet zouden maken. We moeten de lol weer in gaan zien van langzaam, en weer de tijd nemen om dingen uit te zoeken. Werkgevers moeten de tijd geven voor ontspanning. Als je ontspannen bent vallen meer dingen je op en trap je minder snel in de valkuilen van cybercrime.”

Gedragsverandering

Het hacken van hersenen is niet eenvoudig, weet ook Sitskoorn. “Af en toe een halve dag of een dag aandacht besteden aan securityawareness werkt niet. Er moet op de langere termijn een gedragsverandering komen. Daarvoor is tijd nodig, training en de hulp van mensen die verstand hebben van de relatie tussen hersenen en gedrag.”

“Je kunt het proces versnellen door in security-awarenessprogramma’s gebruik te maken van humor en emotie, en de deelnemers zelf laten ervaren hoe psychologische trucs werken”, besluit Sitskoorn. “Laat ze ervaren hoe eenvoudig het is om gedrag te manipuleren. Dan beklijven nieuwe informatie en nieuw gedrag beter.” «

Inge van der Beijl

Northwave

Marcel de Boer

Hoppenbrouwers

Bij een ransomware-aanval gaat het meestal over de cijfertjes. Wat is de downtime en de gemiste omzet? En hoe hoog zijn de kosten voor herstel? “Het gaat nooit over de mentale impact van een aanval”, zegt Inge van der Beijl, director Behavior & Resilience bij Northwave. “Maar die impact moeten we niet onderschatten.” Welke mentale sporen laat een ransomware-aanval na?

‘Onderzoek onder ransomwareslachtoffers laat zien dat leden van het crisisteam later ernstige klachten kunnen krijgen’

Vrijdagavond 2 juli 2021. Marcel de Boer, financieel directeur bij Hoppenbrouwers Techniek, ontvangt een alarmerend bericht van een collega. “Door een ransomwareaanval stonden alle systemen op slot. Je bedrijf is dan als het ware hersendood. Het meubilair is er nog, maar niets werkt meer. Alleen het koffiezetapparaat, en in ons geval de mail.” Van securitypartner Northwave kreeg De Boer al snel te horen dat het herstellen van alle systemen gemiddeld ruim drie weken duurt. Dat was voor Hoppenbrouwers Techniek geen optie. Maandagochtend moesten alle vestigingen weer back in business zijn. “Daarmee werd bij iedereen een zaadje geplant om er vol tegenaan te gaan. Maar we hadden geen oplossing, geen plan, we hadden niets.”

Aan de slag

Via WhatsApp-groepen wist het crisisteam voor de zaterdagochtend na de aanval tweehonderd medewerkers te mobiliseren. De Boer: “Iedereen ging gewoon aan de slag en deed wat nodig was, van herstelwerkzaamheden tot het regelen van de broodjes en het opvangen van kinderen. Die ondernemende houding zit ook wel in het DNA van ons bedrijf. We hebben veel zelfsturende teams die gewend zijn om direct in een actiestand te komen.”
Hoppenbrouwers slaagde erin om nog in het weekend de belangrijkste processen te herstellen zodat alle vestigingen maandagochtend open konden. Daarbij had het bedrijf uit het Brabantse Udenhout ook een beetje geluk. De technische dienstverlener had enkele maanden voor de aanval een nieuw en geavanceerd storagesysteem in gebruik genomen. Met behulp van snapshottechnologie bleek het mogelijk om 150 servers in enkele minuten tijd te herstellen.

Lange hersteltijd

“Maar dan ben je er nog niet”, benadrukt De Boer. “Tijdens zo’n crisis leg je heel veel noodverbanden aan. Zo hadden we alle laptops en andere endpoints afgesloten van het wifinetwerk. Endpoints die na een controle schoon bleken te zijn, kregen een groene sticker en mochten het netwerk weer op. Vervolgens heb je ook nog te maken met werkzaamheden die door de crisis zijn blijven liggen. Het heeft nog wel een week of vier tot zes geduurd voordat we echt weer volledig hersteld waren.”
“Dat is nog relatief snel”, weet Van der Beijl uit ervaring. “Het verhaal van Hoppenbrouwers is daarmee een hoopvol verhaal dat laat zien dat je door samen te werken en met een beetje geluk waanzinnig mooie stappen kunt zetten. In veel gevallen hebben bedrijven veel meer hersteltijd nodig. Het komt voor dat slachtoffers twee jaar nodig hebben voor een volledig herstel, inclusief de juridische afwikkeling.”

‘Eén op de zeven werknemers heeft na de aanval psychologische traumahulp nodig’

“Dan zie je op een gegeven moment ook het commitment verdwijnen”, vervolgt Van der Beijl. “De eerste dagen na de aanval is de motivatie eigenlijk bij alle bedrijven megahoog. Dan is er de spirit en de drang om met het herstel aan de slag te gaan en worden er bij het crisisteam fruitschalen langsgebracht. Die stemming slaat om als het herstel te lang duurt. Dan ontstaat er irritatie omdat zaken nog steeds niet werken, of wel werken, maar op een andere manier.”

Impact op betrokkenen

Vooral een lange hersteltijd heeft een mentale impact op zowel de direct als indirect betrokkenen. “Onderzoek van Northwave onder ransomware-slachtoffers laat zien dat leden van het crisisteam later ernstige klachten kunnen krijgen”, zegt Van der Beijl. Ook mensen buiten het crisisteam ondervinden de psychologische effecten. “Zij zien welke impact een aanval heeft op het bedrijf en maken zich daar zorgen over.” Volgens Van der Beijl uit stress zich bijvoorbeeld in slecht eten, ruzie thuis of een slechte nachtrust. Een enkeling gaat zelfs weer roken. “We ontdekten dat ongeveer één op de zeven werknemers na de aanval zulke ernstige symptomen heeft

‘Herstel van een ransomware-aanval is een marathon en dan houd je een sprint niet vol’

dat psychologische traumahulp nodig is. Eén op de vijf medewerkers geeft aan achteraf meer professionele hulp nodig te hebben gehad bij het verwerken van de aanval. Eén op de drie had graag meer kennis en concrete handvatten gezien om de mentale gevolgen van de aanval het hoofd te bieden.”

De ernstige symptomen kunnen onder andere leiden tot uitval of vertrek van medewerkers. Van der Beijl: “Dat brengt ook kosten met zich mee, maar die zijn veel minder zichtbaar. Voor die verborgen impact van ransomware-aanvallen zou veel meer aandacht moeten komen. Zeker ook omdat de mentale gevolgen zijn te voorkomen.”

Stel grenzen

Het advies van De Boer en Van der Beijl is duidelijk: heb in alle fases van een crisis oog voor de mens. “De eerste dagen is het eigenlijk altijd chaos en is er bij iedereen een enorme drive om aan de slag te gaan met het herstel”, schetst de directeur Behaviour & Resilience van Northwave. “Maar het herstel van een ransomware-aanval is meestal een marathon en dan houd je een sprint niet vol. Na een paar dagen moet je grenzen gaan stellen, en mensen opdragen om regelmatig te pauzeren of zelfs vrij te nemen.”

“In de middag na de aanval kregen we door dat we vrij snel konden herstellen via back-ups. Als dat niet het geval was geweest, hadden we onszelf ook andere vragen moeten stellen”, merkt De Boer op. “Wat als je na een weekend ploeteren nog niet tot een oplossing bent gekomen? Hoe ga je dan om met de mensen die hard aan het werk zijn en lange dagen maken? En wat betekent dat voor het thuisfront?”

Manage de werklast

Een ander advies is om de mensen die direct betrokken zijn bij de crisis niet zwaarder te belasten dan nodig is. Maak onderscheid tussen incidentgerelateerde werkzaamheden en reguliere taken, en probeer de reguliere werkzaamheden elders te beleggen.

“We hebben tijdens het crisisweekend aan 1600 medewerkers nieuwe wachtwoorden verstrekt. Dan weet je dat daar op maandagochtend veel telefoontjes over komen”, vertelt De Boer. “Al tijdens het weekend hebben we erover nagedacht hoe we die telefoontjes weg konden houden van het crisisteam. Gelukkig zijn we een bedrijf met veel techneuten die graag de eerstelijnsondersteuning op zich namen.”

Blijf alert

Omdat mentale problemen soms pas maanden na de aanval aan het licht komen, is het ook belangrijk om een vinger aan de pols te blijven houden. Van der Beijl: “Hier ligt een rol voor de bedrijfsleiding en beslist ook voor HRM. Plan evaluaties in en blijf in gesprek over wat er is gebeurd. En schakel indien nodig professionele hulp in, zoals van een klinisch psycholoog die bijvoorbeeld EMDR-therapie kan aanbieden.”

Als het aan Van der Beijl ligt, nemen bedrijven het ‘menselijk aspect’ zelfs op in het business-continuityplan. “Hoe ga je om met je mensen? Hoe organiseer je het als je te maken hebt met een aanval, ook vanuit menselijk perspectief? Denk na over de hulpverlening, begeleiding en coaching die je kunt bieden.”

“Maak dat plan ook niet te gedetailleerd, want tijdens een crisis lopen dingen toch altijd weer anders. En zorg ervoor dat je het ook in geprinte vorm beschikbaar hebt”, zo geeft De Boer afsluitend als advies. “Bij ons stond het alleen op de computer, en dat is niet handig als ransomware alles heeft versleuteld.” ««

Een dag in het leven van

Evelien Bras

Directeur FERM Rotterdam & The Cyber Partners

De functie van security-duizendpoot Evelien Bras laat zich niet in een paar woorden omschrijven. De grootste gemene deler van haar werkzaamheden? Met gevraagd en ongevraagd advies bedrijven digitaal veilig proberen te houden en daar praktische handelingsperspectieven voor te bieden. “Een werkweek is nooit hetzelfde, en daarom ook nooit saai.” Hoe ziet een ‘redelijk’ gemiddelde dag er voor Evelien uit?

5.00 uur: uit de veren

“Ik ben van nature een vroege vogel. Op reisdagen sta ik om 5 uur op. Andere dagen een uur later. Op een reisdag ga ik met de trein van mijn thuishaven in het oosten van het land naar Rotterdam, waar ik mensen en bedrijven spreek vanuit mijn rol als directeur van FERM Rotterdam. De stichting FERM bestaat sinds 2021 en helpt bij het verbeteren van de cyberweerbaarheid van bedrijven in de Rotterdamse haven en industrie. Ik reis de ene dag heen, blijf daar overnachten en reis de volgende dag weer terug.”

8.30 uur: op kantoor

“Voor FERM, waar ongeveer 60 procent van mijn tijd naar uitgaat, heb ik vaak afspraken op de Kop van Zuid in Rotterdam. Het is zo mooi om vanuit de trein de kalme weilanden te zien en dan bij de Erasmusbrug de metro uit te stappen. Sta je direct midden in de bedrijvig- en levendigheid. Ik kan daar elke keer echt van genieten.”

9.00 uur: interview

“Mijn eerste afspraak van de dag heb ik met een reporter van het Algemeen Dagblad, Sander van der Werff. Hij schrijft specifiek over de haven en soms is cyber een onderwerp waarvoor hij mij wil bevragen. We spreken af bij het World Port Center, vlakbij Hotel New York. Wederom een prachtige omgeving.”

10.00 uur: haventafel cyberprojecten

“Na het interview voeg ik mij bij een overleg met onze publieke partners, waaronder het Havenbedrijf en de gemeente Rotterdam. Wij houden één keer per maand een ‘haventafel cyberprojecten’. FERM is uiteraard niet de enige die iets doet met cybersecurity in het havengebied. In dit overleg schuiven alle publieke partners aan die een project of programma uitvoeren op het gebied van cyber in de haven. Dit om onderling afstemming te vinden en het voor bedrijven ook te kunnen uitleggen wie waarmee bezig is. Ook mensen vanuit de ministeries, het Digital Trust Center

en NCSC schuiven bij deze gesprekken aan." "Deze keer is incident response het onderwerp. Als er iets gebeurt, waar kunnen bedrijven uit de haven dan terecht? Zo is in het kader van het International Ship & Port Facility Security (ISPS) een meldpunt ingericht bij het havenbedrijf. En er is een meldplicht bij Autoriteit Persoonsgegevens (AP). En zo zijn er nog meer. Hiervan hebben we een meldpuntenkaart opgesteld. De stap in dit overleg is om dit overzicht te controleren. Klopt het overzicht? En bij wie meld je je eerst? Hoe zien de (communicatie) lijntjes achter de kaart eruit? Dit is belangrijk, want de veiligheidsregio heeft bijvoorbeeld een crisisteam, maar het Havenbedrijf ook. We werken toe naar een praktische aanpak, waarbij alle partijen samenwerken. We zitten bij dit overleg vaak met een tiental mensen aan tafel. Er zijn meer agendaleden, afhankelijk van het onderwerp haken de mensen aan voor wie interessant is."

12.00 uur: lunch en werkbezoek

"Tegen lunchtijd bezoek ik Bas van de Velde in de raffinaderij van Shell in Pernis, een van onze participanten. Shell heeft naast IT veel OT-technologie en wil gelukkig informatie delen over hoe ze dit veilig houden met onze andere participanten. Na de lunch krijg ik een interessante rondleiding over de plant en spreek ik met vertegenwoordigers van enkele Information Sharing and Analyzing Centra (ISAC's) waar Shell deel van uitmaakt. Hierbij komt bijvoorbeeld de stand van de wetgeving ter sprake en stellen we vragen als: waar zitten kritieke factoren in de keten? Hoe kunnen we deze definiëren en stapsgewijs aanpakken?"

"Naast participanten van FERM, spreek ik ook veel andere stakeholders. Security is een complex onderwerp die ik probeer te vertalen naar praktische stappen. Het management heeft er soms geen tijd, ruimte of expertise voor, dus blijft het liggen. Wat dat betreft heb ik toch iets van de Rotterdamse mentaliteit meegekregen. Wat gaan we nu concreet doen? Actie in de tent."

"Voor de toekomst hoop ik de uitvoer en operatie wat meer bij het team te kunnen leggen en mij meer op de bestuurlijke, strategische rollen te richten. Digitale continuïteit wordt steeds meer een prioriteit, maar we zijn er nog niet. Ik denk dat ik vooral op het gebied van corporate governance daar een mooie rol in kan vervullen."

16.00 uur: online uitzending

"Aan het einde van de middag starten we met het Port Cyber Café. Dit is een praatprogramma dat we vijf keer per jaar vanuit Main Deck maar ook online uitzenden. Hieraan nemen zo'n 90 mensen online en 30 mensen fysiek deel. Het onderwerp van vandaag is cloudsecurity. Sprekers zijn onder andere een hacker van Zolder die veel bedrijven adviseert, iemand van Microsoft als aanbieder van cloud diensten, en Godfried Boshuizen, één van onze participanten in de rol van gebruiker. Het geheel wordt gemodereerd en gehost door Chris van 't Hof, directeur van het Dutch Institute for Vulnerability Disclosure (DIVD)."

"Na afloop eten we een hapje, drinken een drankje en praten rustig nog een beetje bij met elkaar. Zo komt mijn dag in Rotterdam op een gezellige manier tot zijn einde. Morgen weer richting de thuishaven, waar ik voor The Cyber Partners mijn activiteiten oppak. Dat maakt werken in cybersecurity voor mij zo leuk en interessant. Elke week is anders."

Uitdaging houdt het interessant

"In mijn werk heb ik met complexe securityvraagstukken te maken en spreek ik heel uiteenlopende partijen die er 'iets' mee willen om zichzelf veilig te houden. Met mijn technische achtergrond kan ik meedenken over oplossingen die in de praktijk uitvoerbaar zijn. Daarnaast heeft het vak ook veel raakvlakken met innovatie, projectmanagement, subsidies ophalen en samenwerkingsverbanden smeden. Een afwisselender en uitdagender baan bestaat er wat mij betreft niet." ««

Mensen zijn niet het probleem, maar de oplossing

met Mimoent Haddouti
CISO Rabobank Groep

Hoe zorg je ervoor dat meer dan 42.000 medewerkers veilig gedrag vertonen in een organisatie die continu blootstaat aan talloze cybersecurityrisico's? Volgens Mimoent Haddouti, als CISO bij Rabobank Groep verantwoordelijk op het gebied van informatiebeveiliging, is dat een kwestie van positieve sturing en actieve community building. "Je lost niks op door mensen als probleem te classificeren."

De Rabobank Groep heeft net als iedere andere financiële instelling te maken met een groeiende cyberdreiging. Die komt volgens Mimoent bovendien uit allerlei hoeken. "Cybercriminelen zijn uit op financieel gewin. Natiestaten zijn geïnteresseerd in intellectueel eigendom, of het ontwrichten van een land. Een ander risico kan komen van binnenuit. Denk aan medewerkers die worden omgekocht of bedreigd. Dan hebben we nog te maken met de dreiging uit de politiek gemotiveerde, activistische hoek. Ten slotte heeft de Rabobank Groep, net als iedere andere organisatie, te maken met dreigingen die via de Supply Chain de organisatie bedreigen", vat Haddouti samen. Om al die dreigingen het hoofd te bieden, hanteert de Rabobank Groep een uitgekiende securitystrategie. Menselijk gedrag vervult daarin een cruciale rol. "Security begint bij onze mensen. We kunnen heel veel maatregelen bedenken en invoeren, maar uiteindelijk bepaalt het gedrag van onze medewerkers voor een belangrijk deel hoe effectief die maatregelen zijn."

Niet vanzelfsprekend

Dat veilige gedrag is niet vanzelfsprekend en vergt continue aandacht. Daarom zet Rabobank Groep uitgebreid in op security awareness campagnes. Daarin is maatwerk voor iedere medewerker logischerwijs onmogelijk, maar toch scheren ze volgens Haddouti niet iedereen over dezelfde kam. "We bekijken ieder jaar op welke groepen we ons extra moeten focussen. Dat kunnen tech-medewerkers zijn, die dicht op het betalingsverkeer zitten. Maar denk ook aan mensen in leidinggevende posities. We kijken vervolgens per groep waar die extra aandacht uit moet bestaan."

Een meet- en tevens leermoment dat voor alle medewerkers regelmatig terugkomt, is een phishing campagne. Daarbij stuurt het security awareness team van de Rabobank Groep phishing mails naar alle medewerkers, om te zien hoe zij hierop reageren. "We kiezen voor die mails steeds een thema dat op dat moment speelt. Denk aan een e-mail waarin medewerkers gevraagd wordt hun wachtwoord aan

te passen omdat anders hun account geblokkeerd wordt. Oplettende medewerkers kunnen herkennen dat die mails nep zijn. Bijvoorbeeld aan een vreemd verzendadres dat niet van onze IT-afdeling is.”

‘Fietsen leer je niet door eenmalig op het zadel te klimmen’

‘Stilstand is in dit vakgebied echt achteruitgang’

Die phishing campagnes zijn geen ‘one-offs’. “Herhaling is heel belangrijk voor een effectieve campagne. Daarom doen we deze zo’n zes tot acht keer per jaar.” Die herhaling is volgens haar een bewuste strategie. “Awareness creëren is een kwestie van vaak doen. Vergelijk het met fietsen. Dat leer je ook niet door eenmalig op het zadel te klimmen. Maar als je het veel vaker doet, ben je voor dat je het weet aan het wielrennen.”

You Are Key

De Rabobank Groep probeert haar awareness-inspanningen nooit vanuit een ivoren toren over de organisatie uit te rollen. Volgens Haddouti gaat security namelijk pas echt leven bij medewerkers als je het samen doet. Een goed voorbeeld is de website met de veelzeggende titel ‘You Are Key’. “Dit is een kennisplatform waarop we regelmatig content rondom security publiceren”, licht Haddouti toe. “Medewerkers kunnen daar allerlei zaken rondom security posten en met elkaar delen.” Via dit platform heeft de Rabobank Groep tijdens de Cyber Security Month in 2022 voor het eerst ook de Rabo Security Awards uitgereikt. “Medewerkers konden praktijkverhalen insturen over hoe zij hebben gezorgd voor het vergroten van de digitale veiligheid binnen de bank. Daaruit werden binnen vier categorieën winnaars gekozen. Op die manier inspireren we elkaar en zetten we elkaar aan tot veilig gedrag.”
Een ander voorbeeld van die gezamenlijke aanpak is purple teaming. “Onze ethical hackers doen naast red teaming oefeningen ook aan purple teaming. Waar red teaming zonder medeweten van medewerkers gebeurt, gaan we bij purple teaming juist samen aan de slag. Bijvoorbeeld door te kijken waar zwakke plekken zitten en hoe die eventueel veiliger kunnen. Zo zien medewerkers direct waar verbeteringen in hun gedrag mogelijk zijn. Sowieso delen we de resultaten van dit soort tests altijd met de hele organisatie. Dat creëert echt impact en awareness.”

Rabobank Groep zet niet alleen in op awareness en kennisdeling om veilig gedrag te stimuleren, maar probeert dit ook zo gemakkelijk mogelijk te maken. “Zo kunnen medewerkers verdachte e-mails met een druk op een knop rapporteren. Deze e-mails gaan direct naar ons securityteam voor nadere inspectie en verdwijnen uit je inbox. Vervolgens koppelen we terug of het inderdaad ging om een valse e-mail.” Wel waarschuwt Haddouti voor het bewaken van de balans hierin. “Gebruiksvriendelijkheid mag niet ten koste gaan van de veiligheid. Waar precies die balans ligt, is vooral een kwestie van de organisatie in trekken en met medewerkers in gesprek blijven.”

Positieve insteek

Alle security-inspanningen op het gebied van het creëren van bewustzijn hebben één ding gemeen: ze hebben een positieve insteek. “We belonen en stimuleren gewenst gedrag. Mensen die bijvoorbeeld een securityincident melden, krijgen direct positieve feedback. We houden hen bovendien op de hoogte wat er met de melding gedaan is. Zo betrekken we hen actief bij het hele proces.” Volgens Haddouti is dat een heel bewuste en logische strategie. “Je kunt heel veel tooling en processen hebben, maar uiteindelijk worden die door mensen uitgevoerd. Daarom moet je de samenwerking met ze opzoeken en ze niet als probleem classificeren. Daarmee los je niks op. Sterker nog, als jij op je falie krijgt nadat je een incident hebt gemeld dat je had kunnen voorkomen, dan ga jij dat een volgende keer niet meer doen.”

De Rabobank Groep houdt de vinger aan de pols als het gaat om de effecten van de awareness campagnes. “We brengen van de

verschillende doelgroepen regelmatig het securityvolwassenheidsniveau in kaart. Zo kunnen we per doelgroep bepalen wat de aandachtspunten zijn." Wel is de effectiviteit van de awareness campagnes op korte termijn wat lastig meetbaar. "De organisatie is continu in beweging. We hebben een natuurlijke in- en uitstroom van mensen. In die zin vergelijk ik ook niet het ene moment direct met het andere." Toch ziet Haddouti op de langere termijn wel degelijk positieve trends. "We krijgen steeds vaker proactief verzoeken voor awareness trainingen. Ook is de hoeveelheid activiteit en de content op You Are Key in de afgelopen jaren enorm toegenomen. Wat dat betreft merk je echt dat security de afgelopen jaren veel meer is gaan leven in de organisatie."

Onlangs ervoer Haddouti de positieve effecten van alle campagnes aan den lijve. "Ons awarenessteam stuurde in een recente campagne LinkedIn-berichten naar de Rabobank-mailbox van medewerkers. Deze berichten waren zogenaamd van mij afkomstig. Bij veel medewerkers gingen de alarmbellen af. Bijvoorbeeld omdat ze beseften dat hun zakelijke e-mailadres helemaal niet gekoppeld was met hun persoonlijke LinkedIn-account. Ik vond het toen echt mooi om te zien dat veel collega's naar me toe kwamen om te waarschuwen dat ik misschien gehackt was. Voor mij een bewijs dat we een lerende organisatie zijn. Dat is mooi, want stilstand is in dit vakgebied echt achteruitgang. Je bent nooit klaar." «

Volgens Haddouti begint een betere security awareness al bij goede educatie voor de jeugd. "Jonge mensen adopteren nieuwe technologie heel makkelijk, maar missen vaak het vermogen om risico's goed in te schatten. Het onderwijs heeft een belangrijke rol hen daarin beter te begeleiden, in samenwerking met publieke en private instellingen. Security zou de nieuwe wiskunde moeten zijn."

Een dag in het leven van

Shairesh Algoe

CISO en DIVD-bestuurslid

CISO van de fintech TM-Pro, freelance CISO bij Stichting Studielink, bestuurslid van de DIVD Instituut en Academy, bestuurslid van DIVD's CSIRT.global, gastdocent, spreker... Bij Shairesh Algoe komen al deze functies samen in één persoon. Hoe ziet een drukke dag er dan uit?

> “Het compliancestuk vind ik het minder leuke deel van mijn werk. Als je de juiste dingen doet, ben je by default compliant. Het aanleveren van het bewijs dat je voldoet en de controle door een auditor kost echter veel tijd, maar is minstens net zo belangrijk.”

6.30 uur: de wekker

“Ik begin de dag met het smeren van het brood voor onze twee kinderen en met het ontbijt. Vervolgens heb ik meestal nog wel een kwartiertje om een beetje te sporten. Gewoon even opdrukken, het lichaam warm maken voor de werkdag. Daarna douchen, tandenpoetsen en op pad.”

8.30 uur: onderweg

“In de auto luister ik naar podcasts. Het is in onze branche belangrijk om het nieuws te volgen. Niet alleen het securitynieuws, maar ook technology trends in het algemeen en de ontwikkeling van nieuwe wetgevingen. Ik houd van technologie, en denk graag na over de impact die technologie zoals quantum computing nu en in de toekomst kan hebben op de wereld.”

“Quantumtechnologie kan verdedigend worden ingezet, zoals bij quantum key distribution het geval is. Maar quantumcomputers kunnen cryptografie ook breken en zorgen voor een ‘quantum apocalypse’. Misschien is daar over vijftien jaar pas sprake van, maar daar moet je nu al in de boardroom over nadenken. Je moet nu al een strategie hebben hoe je daarmee omgaat.”

9.30 uur: op kantoor

“Bij TM-Pro begin ik de werkdag meestal met het lezen van het securitynieuws, mocht ik dit in de ochtend en onderweg te weinig gedaan hebben. En ik spreek heel veel mensen, van operations en sales tot het management en de productteams. Bij mijn andere opdrachtgever heb ik ook een check-in met het security team, om te kijken waar iedereen mee bezig is, welke hulp ze nodig hebben en waar we staan ten aanzien van de securityroadmap.”

“Security heeft meerdere facetten en wordt allang niet meer alleen door techneuten uitgevoerd. Heel veel partijen horen een rol te hebben. De CISO is vooral de stakeholdermanager die ervoor zorgt dat je de draai kunt maken van security in de kelder naar security die is ingebed in alle lagen van de organisatie en daarnaast iemand die leiding geeft aan het definiëren van de security strategie en vaak ook op het toezien of implementatie hiervan binnen de organisatie. In de ideale wereld zit security uiteindelijk zo goed in het DNA van de organisatie dat een CISO-office helemaal niet meer nodig is. Dan heb je alleen nog een kleine securityafdeling voor de echt moeilijke problemen. Maar dat is een utopie.”

“Iedereen praat over shift left security, dat je security al vanaf het begin moet opnemen in je productontwikkeling. Dat doen sommige organisaties al, maar security moet ook onderdeel zijn van je bedrijfsstructuur, je processen en de trainingen en opleidingen van het personeel. Zover zijn de meeste organisaties nog helemaal nog niet. Het is vooral nog een technisch praatje.”

10.00 uur: trainen en coachen

“Na het wegwerken van de mail houd ik me onder andere bezig met het maken van dreigingsanalyses, het bewaken van de securityroadmap en met securitytrainingen en coaching gericht op awareness en gedrag. Iedere nieuwe medewerker - ongeacht de rol die hij of zij krijgt - heeft sowieso een discussie met de ISO of CISO. Ik ben er graag altijd bij, zodat ik ook een band heb met de mensen.

16.00 uur: contacten leggen

“Mijn werkzaamheden als gastdocent probeer ik een beetje aan het einde van de dag te plannen, zodat ik daarna door kan rijden naar huis. Zo heb ik onlangs op de Hogeschool van Amsterdam lesgegeven over cybersecurity en quantum computing.”

“Ook bel ik aan het einde van de dag collega-CISO’s om te kijken wat er speelt en welke dreigingen op ons afkomen. En om te kijken of je elkaar op het gebied van security kunt helpen, want dat maakt iedereen in de keten sterker en daarnaast onderdeel van mijn “threat watching” ritueel. Je bent zo sterk als de zwakste schakel.” Daarnaast is het belangrijk om te leren van verschillende disciplines, zodat je een bredere kijk ontwikkelt om uit de tunnelvissie van security te kunnen stappen. Security zonder context bestaat niet.

“In de ideale situatie heb je een speciale eenheid paraat staan - een S.W.A.T.-team - die in geval van problemen kan uitrukken. De stichting Dutch Institute for Vulnerability Disclosure doet dat al een beetje. We scannen het internet op kwetsbaarheden, melden kwetsbaarheden bij organisaties en helpen om een kwetsbaarheid te fixen.”

18.00 uur: boulderen

“Op weg naar huis luister ik weer podcasts,

Fortinet Security Fabric

Broad

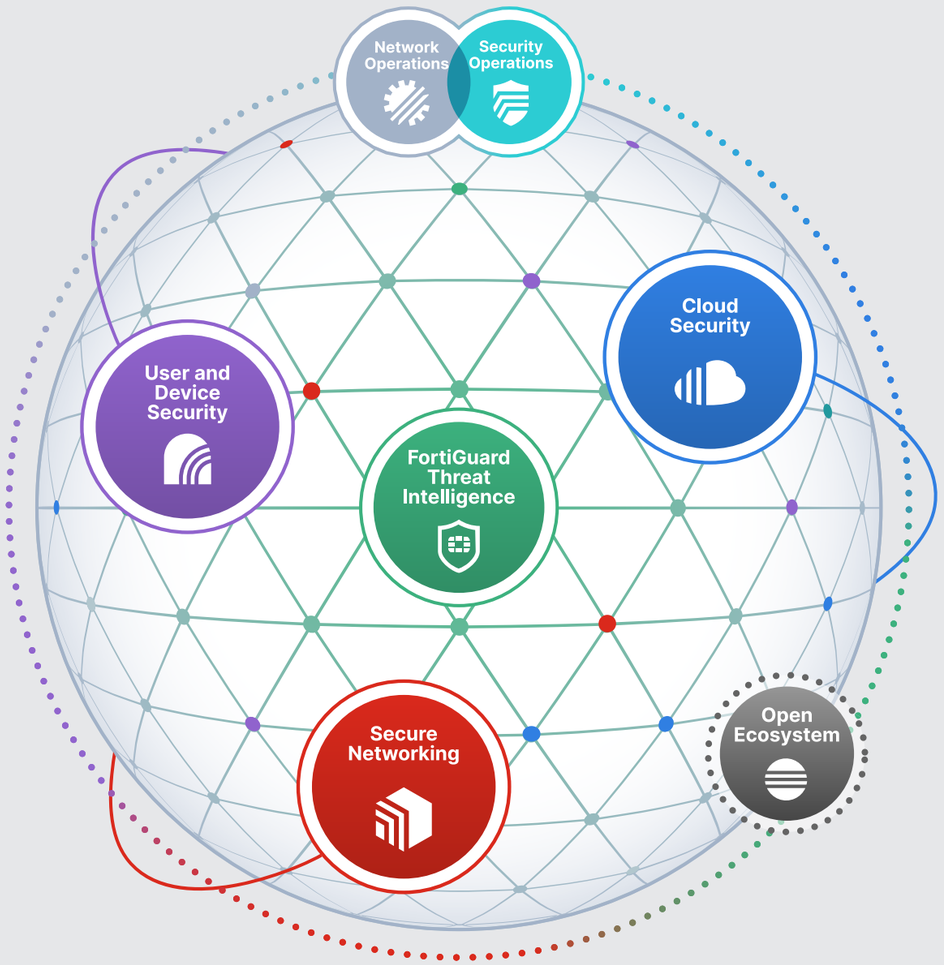
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

Automated

self-healing networks with AI-driven security for fast and efficient operations



FORTINET

www.fortinet.com

‘Je moet nu al nadenken over de quantum apocalypse’

of doe ik helemaal niets. Gewoon een beetje naar buiten kijken, staren, vervelen. Dat is goed voor je mind. Voor extra ontspanning ga ik een keer per week klimmen en een keer boulderen.”

19.00 uur - tot laat: meetings DIVD

“Op een vergaderavond beginnen we om 19.00 uur met een MT-meeting, die een keer in de maand om 20.00 uur wordt gevolgd door een algemene vergadering. Om 21.00 uur stoppen we met notuleren en starten de off the record-sessies. Dan wordt werk hobby en heb je het als hackers onder elkaar over wat je allemaal ziet. Die sessies duren meestal tot laat.”

Geen dag hetzelfde

“Gelukkig zijn niet alle dagen zo druk. Ook zien alle dagen er anders uit. Geen dag is hetzelfde. Wel zie ik het altijd als mijn uitdaging om telkens weer van andere mensen te leren, om zo je dreigingsanalyses en je verdediging beter te maken. Als we dat goed doen dan hoeft security helemaal geen kat-en-muisspel te zijn. Dan kan het een kat-en-katspel worden.” ❮❮

Vaisha Bernard

Eye Security

Zawadi Done

Hunt & Hackett

Security in-house regelen? Volgens de securityspecialisten Zawadi Done en Vaisha Bernard is dat onmogelijk. “Zelfs je IT-leverancier kan je daar eigenlijk niet meer bij helpen.”

Security is voor veel bedrijven lange tijd een blinde vlek geweest. “Voorheen waren onze klanten vooral bedrijven met heel gevoelige data, zoals advocatenkantoren. Maar nu zie je dat ook bij wijze van spreken de ijzerhandel op de hoek zich verdiept in het onderwerp”, zegt Bernard. Volgens Done heeft dat ook te maken met de toegenomen ernst van incidenten. “Met name ransomware is verantwoordelijk voor veel ellende. Ransomware heeft zoveel impact dat bedrijven noodgedwongen met security aan de slag moeten.”

Schijnveiligheid

Dat is makkelijker gezegd dan gedaan. De securitymarkt is booming, met een overweldigend aanbod aan oplossingen als gevolg. Het maken van de juiste keuzes in die zee van opties is allerminst vanzelfsprekend. Zeker omdat een deel van die oplossingen volgens Bernard simpelweg niet voldoet. “Er zijn zo ontzettend veel oplossingen op de markt die jou echt niet verder helpen. Simpelweg omdat de kwaliteit niet deugt. Of omdat ze je overladen met onbegrijpelijke alerts. Zo’n zwart kastje in je netwerk kan je het gevoel geven dat je veilig bent. Maar wie kijkt ernaar? Wie begrijpt daadwerkelijk wat die alerts inhouden en wie kan ze opvolgen? Als je vervolgens vier jaar niet wordt aangevallen, denk je vier jaar lang dat die oplossing jou goed beschermt. Pure schijnveiligheid.”

“Blind gebruik van technologie is inderdaad een groot probleem”, valt Done hem bij. “Vaak werpen dat soort oplossingen een rookgordijn op met cijfers die indruk moeten maken. Bijvoorbeeld over het aantal tegengehouden spammails of verdachte netwerkpakketjes. Dan heb je al snel het idee dat zo’n oplossing jou veilig houdt. Terwijl je in werkelijkheid maar een heel klein stukje van het aanvalsoppervlak hebt afgedicht.”

‘Preventieve maatregelen zijn niet meer genoeg’

Mensen geen excuus

En de rol van de medewerker? Volgens Done blijven mensen onverminderd belangrijk in de strijd tegen cybercriminaliteit. Toch brengt hij hierbij enige nuancering aan. “Ik vind dat organisaties soms onterecht naar mensen wijzen als excuus voor incidenten. Anno 2023 kun je niet meer aankomen met het verhaal dat een aanval is veroorzaakt door een medewerker die zijn inloggegevens heeft ingevuld op een valse webpagina. Dan had je als organisatie moeten zorgen voor tweefactorauthenticatie.”

Bernard is het daar roerend mee eens. “Natuurlijk moet je er bijvoorbeeld voor zorgen dat zo min mogelijk mensen klikken op foute links. Awarenesstrainingen zijn absoluut waardevol. Maar er zullen altijd mensen blijven trappen in dat soort trucs, hoeveel trainingen je er ook tegenaan gooit. Zeker als die trucs steeds slinkser worden. Daar moet je op zijn voorbereid.”

Voor die voorbereiding kunnen organisaties volgens Bernard niet meer terecht bij hun IT-leverancier. “Een aantal jaar geleden kon je nog verwachten dat je IT-partner de security er zelf bij deed. Ik zie in de praktijk nog wel dat IT-leveranciers het denken te kunnen. Of dat bedrijven hiervoor onterecht vertrouwen op hun IT-leverancier. Vaak blijkt de security in de praktijk dan toch niet helemaal goed ingericht. Dan vindt bijvoorbeeld een ransomware-aanval plaats, waarbij de geïnstalleerde endpointsecurity (EDR)-oplossing allerlei alerts afvuurt die vervolgens niemand opvolgt. Of niemand duidt ze, zodat je niet kunt inschatten of een dreiging nog aanwezig is.”

‘Incident response zou veel meer moeten gaan over veerkracht’

Uitbesteden

Security is volgens beiden inmiddels echt een ander specialisme dan IT. Het uitbesteden ervan aan een specialistische partij is dan ook een logische keuze. “Securitykennis is enorm schaars”, aldus Done. “Het is voor de meeste bedrijven niet te doen om eigen securityspecialisten in dienst te nemen. Niet alleen omdat er niet genoeg van zijn, maar ook omdat dat kostentechnisch niet haalbaar is. Voor het gros van de organisaties is het simpelweg niet realistisch om een eigen SOC op te zetten.”

Dat uitbesteden kan volgens Bernard het beste in de vorm van managed detection & response (MDR). Hierbij besteed je monitoring uit aan een specialistische partij die de infrastructuur 24/7 monitort en ingrijpt bij een aanval. ”MDR geeft je de meeste kans dat je een aanval tijdig opmerkt en in de kiem smoort voordat er daadwerkelijk schade ontstaat.” Volgens hem is het wel verstandig MDR te combineren met cloudmonitoring.

“Ongeveer de helft van de aanvallen die veel schade kunnen aanrichten, vindt plaats in cloudomgevingen. Omdat steeds meer mensen gebruikmaken van dergelijke cloudomgevingen zijn ze steeds vaker het doelwit. Vaak gaat het om hele simpele phishingaanvallen op bijvoorbeeld Microsoft 365-omgevingen. Goede cloudmonitoring kan dat voorkomen.”

‘Organisaties wanen zich in de cloud onterecht veilig’

Organisaties wanen zich volgens Done nog wel eens onterecht veilig in de cloud. Niet alleen vanwege de toenemende aanvalsfrequentie. “Ik zie dat organisaties vaak dezelfde fouten in de cloud maken als on-premises. Dan gaat het bijvoorbeeld om foutieve configuratie van een server of applicatie. Een foutief geconfigureerde server in de cloud is net zo kwetsbaar als wanneer die server in-house zou staan. Daarnaast vertrouwen ze nog teveel op de cloudprovider. Terwijl die niet verantwoordelijk is voor de veiligheid van de data die je als organisatie in hun cloud plaatst.”

Incident-response

Een cruciaal onderdeel van MDR is incident-response. “Organisaties hadden tot op enkele jaren geleden nog veelal het idee dat ze de wapenwedloop konden winnen”, aldus Bernard. “Als je maar genoeg dikke firewalls en andere securityoplossingen plaatst, dat je jezelf dan kon beschermen. Dat is gewoon niet meer zo. Malware blijft zich in een enorm tempo ontwikkelen. En mensen blijven op phishinglinks klikken.”

Impactreductie in de vorm van effectieve incident-response is volgens hem dan ook noodzakelijk. “Organisaties moeten zich de vraag stellen hoe ze bij een incident weer zo snel mogelijk up-and-running zijn.” Done vult hem aan: “Uiteindelijk word je een keer gehackt. Dan kun je je beter maar zo goed mogelijk voorbereiden en precies weten wat je moet doen om de impact te beperken. En natuurlijk vervolgens kijken hoe je de kans op een soortgelijke aanval in de toekomst verkleint.”

Grondigheid versus veerkracht

Toch komt die groeiende aandacht voor en belang van incident-response niet zonder merkwaardige bijverschijnselen. Bernard: “Securitybedrijven die dit specialisme hebben omarmd, verdienen er veel geld mee. Daar is niks mis mee, maar soms zijn de kosten ervan onnodig hoog. Dat komt vooral omdat ze vaak heel grondig te werk gaan.” Die grondigheid is volgens Bernard lang niet altijd terecht. “Incident-responsebedrijven halen vaak alles uit de kast om te achterhalen hoe een incident precies heeft kunnen plaatsvinden, of welke medewerker op een verkeerde link klikte. Dan worden bij zelfs de meest simpele aanval alle logs en alle apparaten handmatig nageplozen op malware of bruikbare sporen. Enerzijds omdat securityspecialisten dat vaak leuk werk vinden en vaak ook zo geleerd hebben. Maar ook omdat ze op die manier simpelweg veel geld kunnen verdienen.”

‘EDR heeft als security-voorziening de beste papieren’

Volgens Bernard zou incident-response veel meer moeten gaan over veerkracht. “Wat dat betreft geldt voor incident-response dezelfde filosofie als voor preventieve maatregelen: de 100 procent score bereik je nooit. Dat vraagt om slimme keuzes. Het is cruciaal dat je als organisatie het lek zo snel mogelijk dicht, en vervolgens de downtime zoveel mogelijk beperkt. Hoe eerder je weer volledig ‘up and running’ bent, hoe beter. Het machine voor machine helemaal opschonen en opnieuw inrichten kost veel te veel tijd. Dan kun je beter goede monitoring en response inrichten op de machines waaraan je twijfelt. Mochten er dan toch nog kwaadaardige elementen aanwezig zijn, dan pak je die een week later bij een nieuwe aanvalspoging. Onder de streep scheelt dat enorm in impact.”

Schreeuwend tekort

De hyperspecialisatie die security inmiddels is, kent wel een enorme keerzijde: een schreeuwend tekort aan securityspecialisten. Done: “Security is enorm complex. Iedere rol die je daarbinnen kunt vervullen, kost professionals makkelijk tien jaar aan studie en praktijkervaring voor ze de fijne kneepjes beheersen.”

Done geeft mensen die zich in het vakgebied willen verdiepen als tip om in eerste instantie te kiezen voor een brede ontwikkeling. “Je moet als securityspecialist overal een beetje van weten. Maar daarna moet je ook keuzes maken in de richting waarin je je ontwikkelt. Uiteindelijk leidt dat tot een kennismix die waardevol is voor jou als individuele specialist, maar ook voor de securitymarkt als geheel.” ««

Herstel de mens als sterkste schakel

Al jarenlang is het een gevleugelde uitspraak binnen het cybersecuritydomein: de mens is de zwakste schakel. Die uitspraak is niet alleen onnodig negatief, maar doet bovendien meer kwaad dan goed. En is bovendien niet waar. Omdat veel van de incidenten waarvan mensen de schuld krijgen hun oorsprong helemaal niet vinden bij de eindgebruiker, maar bij andere elementen in het securitysysteem. Het is niet de mens, maar de heersende securityfilosofie die faalt.

Tekst: Dr. Rick van der Kleij

Veel organisaties zien securityoplossingen als het belangrijkste middel om het digitale kwaad te bestrijden. Anno 2023 mogen we echter best concluderen dat die hyperfocus op technologie heeft gefaald. Goede security is niet alleen een kwestie van bits en bytes. Naast krachtige securityoplossingen zijn een degelijk securitybeleid en veilig gedrag cruciaal om de oprukkende cybercriminaliteit de kop in te drukken. Want jazeker: de meeste cyberincidenten ontstaan door menselijk handelen.

Dat het vaak misgaat op 'veilig gedrag', ligt echter niet per se aan de mens zelf. Mensen worden namelijk niet vanzelf onderdeel van dat 'socio-technische' securitysysteem. Waar het misgaat? Allereerst bij de erkenning van de rol van de mens binnen cybersecurity.

Volgens Gartner ligt de verhouding tussen investeringen in technologie, processen en de mens op respectievelijk 85, 14 en 1 procent.

Security-awarenesstrainingen

Die gigantische scheefgroei is op zichzelf al zorgwekkend. Het wordt nog problematischer als organisaties die ene procent ook nog op een ineffectieve manier inzetten. Er valt vaak veel af te dingen op de manier waarop veel organisaties hun security-awarenesstrainingen inzetten. Zo zijn ze vaak eenmalig. Ook is er nauwelijks sprake van maatwerk. Iedereen ondergaat dezelfde training. En zonder goede metingen van de effectiviteit zijn de resultaten van zo'n training een blinde vlek.

Dat is niet het enige probleem met de meeste security-awarenesstrainingen. Veelal staan de verkeerde mensen voor de groep. Deze trainingen worden namelijk doorgaans gegeven door IT'ers. Hun insteek is kennisoverdracht. Niet verwonderlijk, want die kennis is hun specialiteit. Kennis alleen is echter niet genoeg. Het is niet kennis die

Over de auteur
Dr. Rick van der Kleij is security-onderzoeker bij TNO. Vanuit die rol onderzoekt hij de menselijke factor binnen cybersecurity.

'Awarenesstrainingen worden vaak gegeven door de verkeerde mensen'

hackers buiten de deur houdt, maar veilig gedrag. IT'ers hebben niet per definitie verstand van menselijk gedrag, laat staan dat ze gedragsverandering kunnen realiseren.

Meer dan rationaliteit

Bovendien komt veilig gedrag niet alleen voort uit rationaliteit. Daar is meer voor nodig. Een veilige werksfeer bijvoorbeeld. Zo'n sfeer ontstaat niet door mensen te straffen als ze op een verkeerde link klikken. Die negatieve benadering zorgt er vooral voor dat mensen incidenten niet meer melden, met alle gevolgen van dien. In plaats daarvan zouden organisaties het melden van incidenten moeten aanmoedigen.

Daarnaast is securitybeleid vaak te ingewikkeld. Zo ingewikkeld dat mensen daarop falen wat juist zorgt voor onveiligheid. Denk aan een beleid dat om het gebruik van sterke – en dus ingewikkelde – wachtwoorden vraagt. Dat is op papier goed verdedigbaar, maar zorgt in de praktijk juist voor onveiligheid. Mensen zijn namelijk van nature slecht in het onthouden van ingewikkelde tekenreeksen. Met als gevolg dat ze wachtwoorden hergebruiken, of op post-its schrijven. In zo'n geval zorgt securitybeleid dus juist voor onveilig gedrag.

Veilig gedrag faciliteren

Technologie en beleid moeten veilig gedrag juist faciliteren, en dat zo eenvoudig mogelijk maken. Dat betekent onder andere dat deze zaken zo min mogelijk dagelijkse werkprocessen verstoren. Daarvoor zijn mogelijkheden genoeg. Zo bestaat al een tijd het idee om wachtwoorden te vervangen door een reeks zelfgekozen emoji's. Zolang de set emoji's groot genoeg is, heb je bij vier stuks al een zeer sterk 'wachtwoord'. Niet alleen kunnen wachtwoorden zo korter worden, emoji's zijn ook nog veel eenvoudiger te onthouden.

Gelukkig leeft dit besef bij een groeiende groep securityleveranciers. Er bestaan zelfs oplossingen die niet alleen de focus leggen op gebruiksvriendelijkheid, maar zelfs veilig gedrag actief stimuleren. Denk aan software die waarschuwt op het moment dat medewerkers privacygevoelige persoonsgegevens in hun e-mail verwerken. Zo'n waarschuwing maakt direct bewust en kan het aantal onbedoelde datalekken via e-mail flink verkleinen.

Organisaties zijn aan zet. Het is hun verantwoordelijkheid om de mens als sterkste schakel te herstellen. Een goede

start is te kijken hoe mensen precies hun werk uitoefenen. Met welke processen en handelingen hebben zij dagelijks te maken? En ook: welke drempels ervaren zij als het gaat om security? Worden deze issues niet bij de kern aangepakt, dan bestaat het risico dat medewerkers manieren zoeken om eromheen te werken. Die 'workarounds' brengen weer nieuwe risico's met zich mee.

Nieuwe rol

Het is tijd voor een nieuwe rol binnen cybersecurity. Een die de menselijke factor serieus meeweegt in het socio-technische securitysysteem, en die mensen begeleidt naar veiliger gedrag. Belangrijk is om die rol weg te houden bij IT'ers, want het vertrekpunt is niet technologie. In plaats daarvan ligt hier een grote kans voor psychologen en gedragsexperts. Zij zijn immers bij uitstek de personen die menselijk gedrag kunnen veranderen. Is er geen budget voor dergelijke specialisten? Dan is het goed om je als cybersecurityprofessional te verdiepen in menselijk gedrag. Want uiteindelijk hebben we niet meer security-awareness nodig, maar meer human-awareness. Alleen zo maken we van de mens de sterkste schakel. "De hier gepresenteerde inzichten zijn mede tot stand gekomen door intensieve samenwerking binnen het Partnership for Cyber Security Innovation (pcsi.nl)." ‹‹

Cybersecurity nieuwe stijl

Het sturen van menselijk gedrag gaat het beste vanuit een positieve benadering. Een waarbinnen de mens onderdeel is van een socio-technisch securitysysteem. Dat betekent dat organisaties afscheid moeten nemen van veel traditionele denkwijzen over sturing van gedrag. Onderstaande tabel maakt dat duidelijk.

Traditioneel	Nieuwe stijl
Controle op naleven regels	Mensen helpen
Straffen	Belonen
Negatieve opdracht	Positieve businesscase
Mens als losstaand element	Systeembenadering
Bewustzijn als doel	Veilig gedrag als streven
IT-insteek/achtergrond	Psychologie als basis
Losstaande acties	Continu proces
Mens als probleem	Mens als onderdeel van de oplossing

Erno Doorenspleet

KPN Security

Hans Buurman

KPN

Een veilige digitale verbondenheid tussen organisaties, apparaten en mensen is tegenwoordig missiekritisch. De stabiliteit en continuïteit van onze maatschappij is ervan afhankelijk. Daarom is het erg belangrijk dat onze digitale infrastructuur vanuit de basis veilig is, betoogt Hans Buurman, EVP Integration bij KPN: "Digitale dienstverlening zou ontworpen moeten zijn vanuit het 'security first'-principe."

Veilige digitale verbondenheid is helaas niet vanzelfsprekend. Cybercriminelen en hackers worden steeds beter en hun aanvallen zijn steeds moeilijker te stoppen. Ook nieuwe manieren van werken, zoals thuiswerken, vergroten het risico op cyberincidenten enorm. Daarnaast is het wantrouwen tussen natiestaten door geopolitieke spanningen toegenomen. "Vijf jaar geleden had niemand het over de mogelijke risico's van een app als TikTok", merkt Buurman op.

Aan de andere kant is er het sluimerende gevaar van datalekken. Buurman: "Daarbij hebben organisaties nogal eens de neiging om naar elkaar te wijzen als het gaat om de schuldvraag. Onterecht, want je blijft zelf altijd eindverantwoordelijk voor de beveiliging van de persoonsgegevens die met jou worden gedeeld. Dat betekent wel dat je naar je supplychainpartners moet kijken als het gaat om de beveiliging van die data. De security van een organisatie is in toenemende mate afhankelijk van de security van anderen."

'Security moet in het DNA van je businesspartners zitten'

Een andere oorzaak van de toegenomen cyberdreigingen is volgens Erno Doorenspleet, VP Security Strategy and Innovation, het tekort aan kennis en kunde. "Digitalisering gaat momenteel in een razend tempo. In het bedrijfsleven koppelt men allerlei systemen aan elkaar, maar hebben daarbij niet altijd oog voor de securitygevolgen. Dat komt omdat er een groot tekort is aan specialisten. Niet alleen securityspecialisten, maar ook aan IT-specialisten die het geheel goed kunnen overzien."

Zero Trust

Zero Trust is een populaire security-benadering die de toegenomen risico's het hoofd moet bieden. In die benadering is alles en iedereen in principe verdacht. Geen enkele verbinding komt tot stand totdat de betrouwbaarheid van die verbinding en de identiteit van de betrokkenen voldoende bewezen is. "De basis van dit model is dat je zeker weet dat die ander ook daadwerkelijk is die hij of zij zegt te zijn", licht Doorenspleet toe. "Bovendien wordt dat ook herhaaldelijk gecheckt. Is die identiteit met enige zekerheid vastgesteld, dan worden de minimale rechten uitgedeeld om de beoogde taak gedaan te krijgen."

Volgens Doorenspleet verschilt het uitgangspunt wezenlijk met de securitybenadering van een aantal jaar geleden, waar bijvoorbeeld VPN nog een exponent van is. "In het oude model gingen we uit van het kantoor als het streng beveiligde fort met de ophaalbrug die het van de boze buitenwereld scheidde. Eenmaal 'binnen' – of dat nou via VPN was of door je fysieke aanwezigheid op de zaak - had je alle vrijheid. Het probleem is nu dat dat kantoor niet meer de centrale plek is waar mensen hun werk doen. Je mist nu door het vele remote werken die visuele check van iemands identiteit."

'Je moet ook met Zero Trust nog steeds je dataverkeer controleren'

Het zekerstellen van iemands identiteit wil overigens niet zeggen dat vervolgens geen enkele vorm van controle meer nodig is over wat er gebeurt op het netwerk. "Je moet ook met Zero Trust nog steeds je dataverkeer controleren", merkt Doorenspleet op. "Het is namelijk maar de vraag of degene die bij de data kan, ook daadwerkelijk goede bedoelingen heeft. Er bestaat natuurlijk altijd de 'insider threat'. Medewerkers kunnen bijvoorbeeld gevoelige data mee naar buiten loodsen. Bijvoorbeeld uit wraak, of omdat diegene onder druk wordt gezet. Aanvullende controlemechanismen zijn dan ook nodig. Denk aan securitymonitoring. Welke gegevens gaan er van A naar B, wat zit er in die datapakketjes? Die check is een belangrijke voorwaarde om een gezond Zero Trust-model goed te kunnen uitvoeren."

Security first

Zero Trust mag dan het aangewezen model zijn voor het opzetten van een veilige en toekomstbestendige security-

architectuur, het komt niet zonder valkuilen. Een grote valkuil is volgens Buurman dat organisaties vergeten te zorgen voor een veilige basis. “Een complete Zero Trust-architectuur is niet van maandag op dinsdag gereed. Maar je kunt vandaag al wel beginnen met het leggen van een veilige basis. Dat begint bij het gebruik van veilige technologie. Alle diensten die je afneemt, van welke provider dan ook, moeten in de kern veilig zijn. Dat hoeft echt niet ingewikkeld te zijn. Denk aan iets als veilig internet. Zo leveren we de dienst EVI (Extra Veilig Internet) waarmee je vanuit het KPN-netwerk bent beveiligd tegen onveilige websites waarop virussen, malware en ransomware staan. Zo’n dienst kun je gewoon kant-en-klaar afnemen.” Die ‘security first’-filosofie is volgens Buurman ook een van de belangrijkste kernwaarden van KPN. “KPN heeft sinds de oprichting altijd een sterke maatschappelijke rol vervuld. We zetten in op het veilig verbinden van mensen. Onze dienstverlening is in de kern ontworpen met veiligheid als uitgangspunt. Die veilige basis is een integraal onderdeel van onze complete dienstverlening. Dankzij die veilige ‘core’ hoeven onze klanten zich over de veiligheid van bijvoorbeeld de internetverbinding of de digitale werkplek geen zorgen meer te maken. Ze kunnen ervan uitgaan dat dat gewoon goed geregeld is.”

Die veilige basis houdt volgens Buurman niet op bij de eigen voordeur. “Het is belangrijk dat je verder kijkt dan je eigen organisatie. Je bent voor je security ook afhankelijk van de veiligheid van je partners. Daarom zorgen we dat alles wat wij als KPN doen end-to-end secure is, ook binnen de keten. We borgen dat door onze security policy te delen met onze partners. Alle oplossingen, zowel onze diensten als producten, moeten voldoen aan deze basis. Daar zorgen we samen met onze partners voor.”

Maatschappelijk verantwoord ondernemen

Dat ‘security first’-principe hoeft zich niet te beperken tot IT- en technologiepartners. Buurman: “Security moet in het DNA zitten van alle partners waar je mee samenwerkt. Vanuit KPN zien we ‘security first’ dan ook als een belangrijke pilaar van maatschappelijk verantwoord ondernemen. Een die we samen met onze partners realiseren. Gelukkig zijn er met ons steeds meer bedrijven in Nederland die dit uitgangspunt hanteren.”

Volgens Buurman is het ten slotte belangrijk dat we blijven samenwerken in het securitydomein. “We moeten van de schaarse kennis optimaal gebruikmaken. Dat kan alleen als de community er voor elkaar is, als we samen bouwen aan veiligheid. Dat zit niet in het verkopen van oplossingen, maar in het delen van kennis en het samen oplossen van problemen. Dat is volgens hem niet alleen een kwestie van liefdadigheid. ”Je bent voor je security sterk afhankelijk van je keten. Als jouw partners een beetje veiliger worden doordat jij bijvoorbeeld best practices met hen deelt, dan profiteer jij daarvan mee.” «

Met navelstaren zie je niet dat er inbrekers rondlopen

met Aernout Reijmer

CISO bij ASML

Voor CISO's is het verleidelijk om alleen op het eigen 'huis' te letten. "Maar dan zie je niet dat er inbrekers in je straat rondlopen", waarschuwt Aernout Reijmer, CISO bij ASML. Hoe zorgt het hightechbedrijf met Circles of Trust voor meer veiligheid 'op straat', en daarmee voor meer veiligheid in het ecosysteem?

In de acht jaar dat Reijmer voor ASML werkt, heeft hij bij de chipmachinefabrikant uit Veldhoven veel zien veranderen. Zo nam het aantal medewerkers toe van bijna vijftienduizend in 2015 naar bijna veertigduizend in 2022. Door die groei nam de zichtbaarheid van het bedrijf enorm toe. "Maar door het succes van een technologie als extreem ultraviolet (EUV) is ook onze positie in de markt veranderd."

"We zijn voor ransomware-criminelen, nation states en terroristen meer in beeld gekomen", concludeert Reijmer. "En daarmee zijn voor ons ook de risico's op bijvoorbeeld diefstal van intellectueel eigendom of verstoring van de bedrijfscontinuïteit toegenomen."

Aangezien ASML samenwerkt met heel veel toeleveranciers in binnen en buitenland (het ecosysteem), is ASML zich zeer bewust van de risicos die voortkomen uit dit ecosysteem. Om deze risico's te verkleinen en de toeleveranciers te helpen met het verhogen van hun weerbaarheid tegen cyber risico's is ASML Security Circles of Trust opgezet. Veelal zijn deze toeleveranciers zeer gespecialiseerde high tech MKB bedrijven, die relatief weinig eigen security experts hebben en hulp nodig hebben om hun weerbaarheid te verhogen.

Afhankelijkheid supplychain

"Binnen de grenzen van ons bedrijf doen we er alles aan om die risico's te beperken", vervolgt de CISO van ASML. Sinds 2015 is het securitydomein van ASML dan ook gegroeid van 7 naar 330 fte. Als systeemintegrator zijn we voor onze security ook afhankelijk van onze supplychain." Dat bleek bijvoorbeeld in 2021. Een cyberaanval op VDL maakte duidelijk dat cybersecurity niet ophoudt bij de eigen voordeur.

Een EUV-machine van ASML bestaat uit meer dan driehonderdduizend elementen.

Voor de productie en ontwikkeling is ASML afhankelijk van zo'n vijfduizend leveranciers. Deze leveranciers maken naast fysieke componenten ook software en samen met Universiteiten ontwikkelen we kennis van toekomstige machines. "Meer dan tachtig procent van het ASML-eindproduct wordt ontwikkeld en geproduceerd door onze toeleveranciers", aldus Reijmer. "Dan ben je er niet door alleen de beveiliging van je eigen huis op orde te brengen. Als het op straat onveilig is, loop je nog steeds een onaanvaardbaar risico."

'Meer dan tachtig procent van het ASML-eindproduct wordt ontwikkeld en geproduceerd door onze toeleveranciers'

Context beter managen

Nog te vaak ziet Reijmer dat CISO's zich schuldig maken aan 'navelstaren', door alleen te kijken naar de eigen processen, de eigen sensoren en de eigen IT-infrastructuur. "Maar dan negeer je het feit dat er op straat inbrekers rondlopen en dat de toegangswegen onveilig zijn. Je moet je heel goed bewust zijn van de context waarin je opereert en van je afhankelijkheid van andere bedrijven. Die hele context moet je goed managen."

Dat 'managen van de context' doet ASML op meerdere manieren. "Op de eerste plaats door ervoor te zorgen dat de securityclausules zijn bijgewerkt en dat leverende partijen weten aan welke security-eisen ze moeten voldoen. Dat is de commerciële kant. Maar er is ook een zachte kant. Bij je toeleveranciers heb je te maken met peers, met collega-securityprofessionals. Die moet je helpen om de security op orde te krijgen."

Circles of Trust

ASML heeft daarvoor verschillende Circles of Trust in het leven geroepen, bijvoorbeeld met de belangrijkste toeleveranciers. De chipmachinefabrikant helpt de deelnemers om de security op orde te krijgen - onder andere door kennis, informatie en best practices te delen - en gaat bij een aanval naast ze zitten. "Als belangrijke klant kunnen we securityprofessionals met onze 'voice of the customer' bovendien helpen om aansluiting te vinden bij de boardroom. We helpen onze partners complexe security vraagstukken bespreekbaar te maken met hun directie en vertalen deze security vraagstukken in termen van bedrijfsrisicos en hoe deze risico's gemitigeerd moeten worden. Onze directie nodigt regelmatig de directieleden van andere high tech maakbedrijven uit de Brainport regio uit voor events waar nadrukkelijk over cybersecurity gesproken wordt."

Die aansluiting is volgens Reijmer erg belangrijk. "Security heeft de afgelopen twee decennia de ontwikkeling doorgemaakt van een functie in de kelder naar een gespreksonderwerp aan de directietafel. Daardoor is ook de rol van de CISO veranderd. Als Chief Information Security Officer moet je de 'securitytaal' spreken, maar ook weten welke aspecten belangrijk zijn voor je bedrijf. Je moet weten aan welke knoppen je moet draaien om een businesscase te laten slagen. Dan helpt het als je kunt terugvallen op peers. Wat je in de boardroom zegt snijdt meer hout als je je kunt beroepen op wat andere, peers, bedrijven doen." Onze directieleden benadrukken in gesprekken met hun peers in de Brainport Regio het belang van het hebben van goede security. Want een probleem bij een van de bedrijven in de keten, heeft een enorm effect op de ketenpartners."

Multinationals werken samen

"We moeten met elkaar samenwerken en van elkaar leren", benadrukt Reijmer. En als het aan ASML ligt niet alleen binnen de eigen supplychains. Zo is Reijmer een van de aanjagers van de Stichting NL CISO Circle of Trust, een samenwerkingsverband van de tien grootste Nederlandse multinationals. Dat zijn naast ASML onder andere Shell, NS, Philips, ABN AMRO en KPN.

'Dan ben je er niet door alleen de beveiliging van je eigen huis op orde te brengen'

De CISO's van deze bedrijven komen een keer per kwartaal bij elkaar om de lopende projecten te bespreken. Die projecten staan onder leiding van een projectmanager. Ook is er een belangrijke rol weggelegd voor subject matter experts. "Deze experts praten met elkaar en komen met concrete voorstellen waar wij als CISO's alleen maar een 'go' op hoeven te geven. Zo voorkomen we vertragingen in de ontwikkelprocessen en doen dubbel werk, we kunnen van elkaar leren ipv het wiel steeds opnieuw uit te vinden."

"Ook leveren we gezamenlijk een constructieve bijdrage aan diverse maatchappelijke security gerelateerde vraagstukken middels een goede dialoog met diverse overheidsinstanties zoals het DTC en NCSC."

Alarmsystemen gekoppeld

Een belangrijk project van deze NL CISO Circle of Trust is de ontwikkeling van een gezamenlijk cyber threat intelligence (CTI)sharing -platform. Via dit platform delen de deelnemende bedrijven dreigingsinformatie met elkaar, zonder dat de herkomst van de data is te herleiden. De radarsystemen van de tien bedrijven worden hier als het ware aan elkaar gekoppeld.

En doordat de NL CISO Circle of Trust een samenwerkingsverband is, kan ook het NCSC via de stichting dreigingsinformatie delen met de deelnemende bedrijven.

“Het platform staat nu, en na een pilot zullen we het initiatief verder uit gaan rollen”, licht Reijmer toe. “De echte waarde blijkt pas als we inzichten met elkaar kunnen delen, bijvoorbeeld over kwetsbaarheden en nieuwe aanvalspaden die naar voren komen.”

Netwerk van netwerken

“Uiteindelijk willen we een netwerk van netwerken hebben”, besluit Reijmer. De NL CISO Circle of Trust vormt daarbinnen het ‘kernnetwerk’. “De deelnemers aan deze Circle of Trust hebben zelf ook allemaal netwerken waarbinnen informatie wordt gedeeld, zoals wij dat doen binnen Brainport Eindhoven.”

‘Je moet je peers helpen om de security op orde te krijgen’

“Het netwerk van netwerken zorgt ervoor dat dreigingsinformatie en expertise snel op de juiste plaats terechtkomen, zodat de straat waarin je huis staat beter beveiligd wordt. Daar hebben we allemaal profijt van. De grootste uitdaging is vervolgens het gestructureerd delen van kennis.”

“Langzamerhand zien we, mede door de aankondiging van NIS2 wetgeving, dat ook andere grote bedrijven een soortgelijke strategie ontwikkelen waarbij niet alleen gekeken wordt naar de veiligheid van het eigen bedrijf, maar ook de weerbaarheid van het ecosysteem.” <<

NL CISO Circle of Trust

De stichting NL CISO Circle of Trust is opgericht door ASML en ABN AMRO, in nauwe samenwerking met het NCSC. In het samenwerkingsverband zitten de tien grootste multinationals van Nederland. Dat zijn naast de oprichters Ahold Delhaize, Akzo, ING, KPN, NS, Philips, Rabobank en Shell. De oprichting werd in oktober 2022 bekendgemaakt tijdens de ONE Conference in Den Haag.

Het is voor veel ethical hackers nog altijd een geliefd instrumentarium: de pentest. “Maar voor een reëel zicht op de staat van je cybersecurity is zo’n test niet meer afdoende”, zegt Sjoerd Peerlkamp, Director Industrial Market Group (IT/OT Security) bij Secura.

1. Op welke manier is de securitywereld veranderd ten opzichte van het begin van je carrière?

“De belangrijkste verandering is dat we tegenwoordig altijd online zijn. Dat geldt niet alleen voor mensen en bijvoorbeeld laptops en smartphones, maar ook voor bijna elk apparaat en ook operationele technologie (OT). IT en OT raken steeds meer met elkaar verbonden. Vrijwel ieder bedrijf is tegenwoordig afhankelijk van connected apparatuur.”

“De operationele risico’s zijn voor vrijwel iedere organisatie enorm toegenomen. Security is daardoor steeds meer een synoniem geworden van risico-management en continuïteitsbeheersing. Een toenemend aantal organisaties beseft dat cyberincidenten een risico vormen voor hun primaire bedrijfsprocessen. Zij moeten zich dan steeds afvragen welke risico’s zij bereid zijn te nemen, en welke zaken zorgen voor onacceptabele stilstand en gevolgschade. Digitalisering biedt enorme kansen, mits je de bijbehorende risico’s goed weet te beheersen.”

2. Je stelt dat de klassieke pentest dood is. Wat bedoel je daar precies mee?

“Een klassieke pentest heeft verschillende nadelen. Zo is het altijd een moment-opname. Doe je de pentest vlak voordat een voor jou cruciale kwetsbaarheid wordt ontdekt, dan mis je die en waan je je onterecht veilig. En met een beetje pech doe je de volgende test nadat de kwetsbaarheid verholpen is, maar waarbij een hacker in de tussenliggende periode al toegang heeft verkregen. Je toont dan twee keer aan dat het op dat moment veilig was, maar tussendoor heeft de hack al plaatsgevonden.”

‘Een pentest is altijd een momentopname’

“Daarnaast biedt een klassieke pentest geen zicht op de volledige aanvalsvector. Er is buiten de eigen muren van de organisatie een levendige handel in buitgemaakte inloggegevens en netwerk-informatie. Cybercriminelen bieden deze te koop aan op het darkweb, of de buit belandt

‘Security is een zaak van risicomanagement’

in openbare databases. Daarnaast zien we ook regelmatig dat toegangssleutels onbewust belanden op openbare plekken zoals software repositories (b.v. GitHub). Dan kun je wel je eigen sloten testen, maar als de sleutel gewoon op straat ligt ben je alsnog kwetsbaar.”

“Dat wil niet zeggen dat pentests waardeloos zijn. In specifieke gevallen hebben ze zeker nog waarde. Zo kun je met een pentest bijvoorbeeld heel grondig de kwetsbaarheden van een nieuwe onlinedienst opsporen voordat deze live gaat.”

3. Het darkweb is voor veel organisaties een plek waar ze totaal geen zicht op hebben. Hoe zou men dat moeten veranderen?

“Het is volstrekt logisch dat het darkweb veelal onbekend terrein is. Deze uithoek van het internet is in principe niet zonder speciale tools toegankelijk. Bovendien moet je voor toegang tot de content van bepaalde fora binnen het darkweb ook zelf iets aan te bieden hebben. Wie alleen maar komt kijken valt doorgaans snel door de mand, met als gevolg dat je als onderzoeker niet aan de juiste informatie komt.”

“Toch bevat het darkweb belangrijke informatie over je aanvalsoppervlak. Zo kunnen hier belangrijke gegevens over je netwerk te koop zijn aangeboden. De enige manier om toch zicht te houden hierop is door deze expertise uit te besteden aan specialisten. Deze analisten zijn ‘undercover’ aanwezig op het darkweb en werken continue aan een goede informatiepositie. Ook security bedrijven zoals Secura maken gebruik van deze gespecialiseerde bedrijven om de juiste informatie over het aanvalsoppervlak op het darkweb te vinden.”

4. Wat is volgens jou een goed alternatief voor pentesting?

“In plaats van periodieke testen van je eigen IT-infrastructuur is een continue ‘attack surface monitoring‘ cruciaal. Alleen zo kun je kwetsbaarheden tijdig ontdekken voordat hackers er misbruik van maken. Bij die monitoring zijn vier aandachtspunten belangrijk: asset discovery, credentials, vulnerabilities en exposures.”

“Asset discovery is onmisbaar. Wie niet weet uit welke devices en diensten het aanvalsoppervlak bestaat, kan deze ook niet goed beschermen. Ook is het belangrijk dat je weet welke credentials op straat liggen. Daarvoor kun je gebruikmaken van openbare ‘dumps’ of diensten van derden.”

“Daarnaast is een goed zicht op exposures cruciaal. Denk aan een sleutel die nog openbaar staat in je code op Github, of een configuratiefout in een cloudopslagdienst of database waardoor deze toegankelijk is voor derden. Ten slotte is het opsporen van technische kwetsbaarheden nog steeds belangrijk. Daarvoor zijn pentests zoals gezegd nog altijd een geschikt middel. Maar de pentest alleen is zeker niet meer afdoende.”

5. Wat is je belangrijkste advies voor collega-securityprofessionals?

“Doe een goede risico-inventarisatie. Je moet je heel goed afvragen welke risico’s acceptabel zijn, en welke scenario’s echt leiden tot grote schade. Vervolgens is het belangrijk om met die risico’s in het achterhoofd aan de slag te gaan met alle vier de pijlers die ik noemde. Alleen zo krijg én behoud je een reëel zicht op dreigingen en risico’s voor jouw organisatie.” «

‘Attack surface monitoring is cruciaal voor een reëel zicht op dreigingen’

COLOFON

Cyber Security Perspectives
is een uitgave van KPN Security
Volume 9, 2023

Redactie: Lucinda Sterk, Susan Leliveld, Babette Kersten, Carolien Hoogerwaard, Bram Reinders, Marcel Heezen
Tekst: Co-Workx, KPN Security
Vormgeving: Susan Leliveld
Drukkerij: HH Global

KPN Security
Wilhelminakade 123
3072 AP Rotterdam
kpnsecurity@kpn.com
Twitter
LinkedIn
kpn.com/security
kpn.com/NLSecure

Met dank aan:
Antoni van Leeuwenhoek, ASML, DIVD, DTC, Eye Security, FERM Rotterdam, Hoppenbrouwers, Hunt & Hackett, KPN, NCSC, Northwave, ProRail, Rabobank Groep, Secura, TNO
Fotografie: Sjors Massar (P31)
Op de cover: Artie Debidien (KPN)

kpn Security

Cyberaanval?

Bel 0888-HACKED

Ontdek meer op
kpn.com/incident-response

Samen maken we Nederland veiliger