Er moet een betere coördinatie komen op cybersecurity
Hans de Vries, NCSC

Informatie-beveiliging draait om het managen van onzekerheden
Martijn Dekker, ABN AMRO

Meten van Phishing-scenario's versterkt security awareness
Sanne Maasakkers, Fox-IT

NL SECURE [ID]

Cyber Security Perspectives



















Samen maken we Nederland veiliger

LETS TALK ABOUT IT

kpn Security

NL SECURE [ID]

Voorwoord

kpn Security

» Het gaat niet goed met cybersecurity in Nederland. Ondanks alle inspanningen van de overheid en het bedrijfsleven is de dreiging van cybercriminaliteit groter dan ooit. Het aantal cybercrimezaken is volgens het Openbaar Ministerie in 2020 meer dan verdubbeld. Ook voor 2021 zijn de verwachtingen niet rooskleurig. Er moet iets veranderen, maar wat?

Samen optrekken om **cyber-crime het hoofd te bieden**

De opkomst van cybercrime blijkt ook uit andere cijfers. Zo meldt de Autoriteit Persoonsgegevens een explosieve toename van het aantal hacks gericht op het stelen van persoonsgegevens. Wie denkt dat het allemaal wel meevalt, hoeft alleen maar het nieuws te volgen. Van een ransomwarebesmetting bij de HvA en de UvA tot een groot datalek bij Ticketcounter: vrijwel dagelijks gaat het mis.

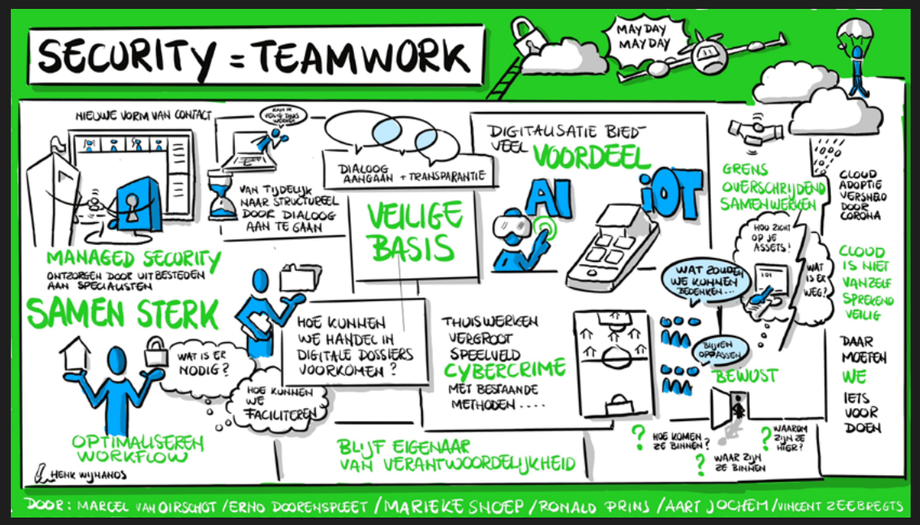
Als u dit leest, is het volgende grote cyberincident waarschijnlijk al een feit. Het lukt ons vooralsnog niet om cybercriminaliteit terug te dringen. Dat is geen schande. Cybercriminelen staan per definitie met 1-0 voor. Waar wij alle gaten moeten dichten, hebben zij er maar één nodig voor een succesvolle aanval. Daarnaast zijn ze goed georganiseerd en beschikken ze over onbeperkte middelen en mogelijkheden.

De overheid en het bedrijfsleven zijn een soort snoepwinkel voor cybercriminelen. Soms proberen zij geld los te peuteren, soms gaan ze op zoek naar interessante informatie, technologie of persoonsgegevens. Bij elke organisatie valt wel iets te halen. Veel van hen zijn een makkelijke prooi, bijvoorbeeld doordat hun basisbeveiliging niet op orde is. Dit is echt een van de grote uitdagingen van deze tijd.

In dit magazine komen verschillende toonaangevende securityexperts aan het woord. Zij leggen niet alleen de vinger op de zere plek, maar presenteren ook plannen voor structurele verbetering. Uiteraard bekijkt iedereen deze problematiek vanuit zijn eigen perspectief. Maar uiteindelijk hebben we als Nederlandse securitycommunity hetzelfde doel: de digitale weerbaarheid van Nederland vergroten. En dat kan geen enkele partij in zijn eentje.

Ook in coronatijd moeten we dus vooral samen blijven bouwen aan een veiliger Nederland. Kennisdeling is juist nu cruciaal. Dit magazine is dan ook geen verzameling commerciële boodschappen, maar een oprechte poging om te informeren en inspireren. We hopen dat u tijdens het lezen nieuwe inzichten opdoet die u kunt toepassen binnen uw eigen organisatie.

Marcel van Oirschot
Executive Vice President, KPN Security



LET'S TALK ABOUT IT

Inhoud

» PAGINA 3
Voorwoord
Marcel van Oirschot, KPN Security

» PAGINA 6 T/M 8
CoronaMelder is de meest privacyvriendelijke app van Europa
Brenno de Winter, Ministerie van VWS

» PAGINA 9 T/M 11
Er moet een betere coördinatie komen op cybersecurity
Hans de Vries, NCSC

» PAGINA 12 T/M 14
Psychologen zijn hard nodig in de securitywereld
Inge Wetzer, Secura

» PAGINA 15 T/M 17
We kloppen ons vaak ten onrechte op de borst
Ronald Prins, Hunt & Hackett

» PAGINA 18 T/M 20
Omarm de cloud, maar onderschat de securityrisico's niet
Erno Doorenspleet, KPN Security

» PAGINA 21 T/M 23
Een jonge cybercrimineel kan ook een IT-talent zijn
Floor Jansen, Nederlandse politie

» PAGINA 24 T/M 26
Er is steeds meer wat we niet weten
Marcel van Oirschot, KPN Security
Paul Slootmaker, KPN CISO

» PAGINA 27 T/M 29
Cybercriminelen ontdekken de zorg
Wim Hafkamp en Jonathan Bouman, Z-CERT

» PAGINA 31 T/M 33
Wie heeft in de cloud nog een helicopterview?
Peter Sandkuijl, Check Point

» PAGINA 34 T/M 35
Chaos is de grootste vijand van security
Vincent Zeebregts, Fortinet

» PAGINA 36 T/M 38
Kwantumtechnologie komt als service beschikbaar
Victoria Lipinska, KPN CISO

» PAGINA 39 T/M 41
Informatiebeveiliging draait om het managen van onzekerheden
Martijn Dekker, ABN AMRO

» PAGINA 42 T/M 44
Delen van kennis kan en moet beter
Petra Oldengarm, Cyberveilig Nederland

» PAGINA 45 T/M 47
Er is in de cloud heel veel te verdedigen
Wesley Neelen en Rik van Duijn, Zolder

» PAGINA 48 T/M 50
Meten van phishingscenario's versterkt security-awareness
Sanne Maasakkers, Fox-IT

» PAGINA 51 T/M 53
Het draait om het stellen van de juiste vragen
Oscar Koeroo, KPN CISO

» PAGINA 55
Colofon

» De CoronaMelder-app is een belangrijke aanvulling op het bron- en contact-onderzoek van de GGD. Privacy- en securityexpert Brenno de Winter adviseerde het Ministerie van VWS bij de ontwikkeling van deze notificatie-app. “Het draait allemaal om het wekken van vertrouwen”, zegt De Winter. “Zonder vertrouwen gaan mensen de app niet op grote schaal gebruiken. Daarom staat privacy op één en security daar net achter.”

CoronaMelder is de meest privacyvriendelijke app van Europa

Brenno de Winter
Chief Security and Privacy Operations, Ministerie van VWS

De Winter was bijna vanaf het begin betrokken bij de totstandkoming van de CoronaMelder-app. In april van 2020 vroeg het ministerie hem en acht andere IT-specialisten om voorstellen voor de corona-apps te beoordelen. Deze experts uitten forse kritiek op de procedure en oordeelden dat het ministerie chaotisch en haastig te werk ging. Hun advies: ga terug naar de tekentafel. “Tussen alle oplossingen die er werden geboden en die in sommige landen ook al in de markt waren, zat er geen eentje die voldeed”, blikt De Winter terug.

In mei werd De Winter als Chief Security and Privacy Operations toegevoegd aan het 50 man sterke team van Ministerie van VWS dat de app ontwikkelt. Daarmee was een felle criticus opeens hét gezicht van de CoronaMelder-app. Deze app waarschuwt mensen als ze in contact zijn geweest met iemand die besmet is met corona. “Minister De Jonge wilde absoluut niet dat er met de privacy werd geknoeid”, zegt De Winter. “Maar hoe regel je dat dan in de praktijk? Dat was mijn voornaamste opdracht.”

Privacy gaat boven alles

Er waren twee centrale uitgangspunten bij de ontwikkeling van de CoronaMelder-app. “Enerzijds het privacyrecht – het voldoen aan de Algemene verordening gegevensbescherming (AVG) – en anderzijds het technisch bewerkstelligen van een zo privacyvriendelijk mogelijke app. Aanvullend werden er enkele onderzoeken uitgevoerd, bijvoorbeeld naar de ethische kaders. Al snel kwam het idee om een tool te ontwikkelen op basis van het decentrale DP-3T-protocol. Met het oog op de privacy besloten we alle extra functionaliteit eruit te slopen.”

Deze sterke focus op privacy bracht restricties met zich mee. “De app mag geen mensen volgen. We konden dus ook geen statistieken gebruiken, want dan krijg je een app die continu gegevens verzendt. Dit betekent dus dat als iemand ziek wordt, je in het reguliere bron- en contactonderzoek moet gaan kijken naar de effectiviteit van de app.”

Volgens De Winter was de privacy van de gebruikers leidend bij alle gemaakte keuzes. Hij somt nog meer voorbeelden op: “We vragen niets aan gebruikers, omdat het telefoonnummer dan identificeerbaar zou zijn. In Duitsland versturen ze soms sms’jes, maar wij doen dat bewust niet. We gebruiken ook alleen de data die we nodig hebben. Bovendien gooien we deze gegevens na 14 dagen weg, want dan kan iemand niet meer besmettelijk zijn. En we voorkomen uiteraard dat data te herleiden zijn tot een persoon.”

Identiteit is niet te achterhalen

“Kijk bijvoorbeeld naar de contactmomenten met andere smartphones”, vervolgt De Winter. “Deze sleutels worden naar Ministerie van VWS geüpload, maar niet naar de gemeentelijke GGD’en. Zij kunnen dus niet zien welke sleutels worden geüpload.

En omdat wij niet zien wie ze vrijgeven, weten wij ook niet bij wie de sleutels horen. Alle IP-adressen worden bij binnenkomst meteen gescheiden van de data. Met verwerker KPN is ook geregeld dat wij daar geen toegang tot hebben. Daarnaast voegen we dummyverkeer toe, zodat verkeersanalyses niet mogelijk zijn."

"We hebben langs meerdere lijnen – technisch maar ook procedureel – geborgd dat wij dit niet kunnen achterhalen. Zelfs als we dat zouden willen, dan zit er nog een laag van Apple en Google onder die ons weghoudt bij de verzamelde sleutels. Die laag zorgt er ook voor dat er geen back-up gemaakt wordt. Dus als je van telefoon wisselt, ben je ook je historie van de laatste 14 dagen kwijt. Verder worden de sleutels bij het vrijgeven gesorteerd op alfabet. Door al deze maatregelen is het bijzonder lastig om iets te achterhalen over een gebruiker."

Eerste app met eigen wetgeving

Het privacyrecht speelde eveneens een cruciale rol. "We hebben een zeer uitgebreide data protection impact assessment (DPIA) uitgevoerd. De minister had beloofd dat hierover advies zou worden gevraagd aan de Autoriteit Persoonsgegevens. Maar dat kunnen zij niet geven tenzij er een hoog risico is. Wij kwamen in onze risico-inschatting echter niet uit op een hoog risico. De AP kon dit advies dus niet geven, tenzij er een voorafgaande raadpleging werd uitgevoerd. Uiteindelijk hebben we daarin een soort tussenvorm in gevonden en een advies gekregen."

Een van de adviezen was dat er met spoed een aparte wet moest komen voor de CoronaMelder-app. "Binnen een week tijd lag de wet bij de Tweede Kamer. Meteen daarop kregen we meer dan 300 Kamervragen die we in 48 uur kloppend en naar waarheid moesten beantwoorden. Het resultaat was de eerste Nederlandse app met eigen wetgeving. In de wet staat bijvoorbeeld dat de Tweede Kamer het gebruik van de app moet verlengen. Gebeurt dat niet, dan stopt de app. Ook is het verboden om mensen onder druk te zetten de app te gebruiken."

Los van de wet is er natuurlijk de reguliere beveiliging van de app. "We hebben een risico- en dreigingsanalyse opgesteld in samenwerking met overheidsinstanties zoals de NCSC, de NCTV en de AIVD. Wat kan er misgaan? Daarnaast lieten we een hele reeks phishingtesten en codereviews uitvoeren, door allerlei verschillende partijen. De resultaten daarvan zijn openbaar. Verder hebben we heel zwaar gestuurd op functiescheiding. Zo wordt de cryptografie door iemand anders beheerd dan bijvoorbeeld de back-end en de applicatie."

Media volgen CoronaMelder kritisch

Ondanks alle maatregelen kwam de CoronaMelder-app eind september 2020 negatief in het nieuws vanwege een 'privacyprobleem'. Zorgmedewerkers konden volgens een artikel van de Volkskrant zien of besmette personen in de app hadden gemeld dat ze besmet waren, en ze eventueel onder druk zetten om de app te gebruiken. De fout werd ontdekt door non-profitconsultant Radically Open Security.

De Winter nuanceert de berichtgeving. "Het ging hier om een tijdelijke functie voor de testfase van de app."

"We hebben op een gegeven moment in de testfase een vinkje mogelijk gemaakt waarmee de bron- en contactonderzoeker kon zien dat er sleutels geüpload waren: het proces werkt dus. Voor een testfase is dat helemaal prima, als de functionaliteit maar niet permanent is. Ondertussen werd er broncodeonderzoek gedaan door Radically Open Security. Die hebben we op pad gestuurd zonder ze beperkingen op te leggen, omdat we zo transparant mogelijk willen zijn. Het is goed dat zij dit ontdekt hebben, dat is ook hun werk, maar in de berichtgeving ontbrak de context volledig."

De Winter benadrukt dat er wel degelijk dingen mis zijn gegaan bij de totstandkoming van de CoronaMelder-app. "Een teamlid stuurde in haar enthousiasme een bericht naar een brancheorganisatie van maaltijdbezorgers. Of zij ervoor konden zorgen dat bezorgers de CoronaMelder gingen installeren. Dat deugt niet en wilden we juist voorkomen met de wet. Sindsdien kijken we vanuit de privacy nu ook wat strakker mee naar de uitingen van werknemers. Klopt dit wel met onze eigen spelregels voor privacy?"

"CoronaMelder was de eerste Nederlandse app met eigen wetgeving."

Zo snel mogelijk uit de pandemie

De CoronaMelder-app is inmiddels ruim 4,3 miljoen keer gedownload. Volgens deskundigen is de app effectief als zo'n 10 tot 15 procent van de bevolking deze gebruikt. Dat percentage is dus al ruimschoots behaald. "Het is mooi, maar eigenlijk ben ik daar nauwelijks mee bezig. We willen er met zijn allen gewoon voor zorgen dat we zo snel mogelijk uit deze pandemie komen. Ik hoop dat de app hier een bijdrage aan levert."

Zijn er dan echt geen elementen die hij achteraf graag anders had gezien? "Nee", zegt hij stellig. "We hebben alle noodzakelijke privacy- en securitymaatregelen getroffen, ook als dat ten koste ging van de functionaliteit. Daardoor is dit de meest privacyvriendelijke app van Europa geworden."

Brenno de Winter stelde als onderzoeksjournalist misstanden op het gebied van privacy en security aan de kaak. Zo kraakte hij de ov-chipkaart om aan te tonen dat de beveiliging van het reisbewijs niet deugde. Sinds 2016 is hij geen journalist meer, maar een veelzijdig privacy- en beveiligingsexpert. De Winter schrijft boeken, geeft lezingen, verzorgt trainingen en verricht onderzoek. Ook adviseert hij organisaties over privacy en beveiliging.

kpn Security

» Het op orde brengen van de basisbeveiliging blijft voor bedrijven een hele opgave. "De basisbeginselen van cybersecurity worden lang niet altijd uitgevoerd", zo merkt ook NCSC-directeur Hans de Vries op. Als het aan hem ligt, wordt cybersecurity 'chefsache'.

Er moet een betere coördinatie komen **op cybersecurity**

Hans de Vries
Directeur, Nationaal Cyber Security Centrum (NCSC)

Het aanvalsoppervlak voor cybercriminelen groeit hard, onder andere door de toename van het aantal thuiswerkers. "Veel organisaties hebben echter nog lang niet alle securitymaatregelen getroffen die je zou mogen verwachten", constateert De Vries. "Er zijn positieve uitzonderingen, maar in veel gevallen ontbreekt bijvoorbeeld de compartimentering, vindt er geen multifactorauthenticatie plaats en zijn data na een ransomwareaanval niet terug te halen van een back-up."

Het is een geluid dat al jaren doorklinkt in het Cybersecuritybeeld Nederland dat de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) jaarlijks vaststelt. In de 2013-editie stond al dat 'een brede groep organisaties belangrijke (technische) basismaatregelen, zoals het patchen en updaten van systemen of het wachtwoordbeleid, niet op orde heeft'.

Als het aan de directeur van het NCSC ligt, komt daar echter snel verandering in. En die verandering begint in de bestuurskamer. "Cybersecurity moet chefsache worden, en niet een noodzakelijk dingetje waar je een IT-manager voor aanstelt en klaar. Nee, de inrichting van je cybersecurity bepaalt of je als organisatie kunt blijven overleven. Als je dit niet goed regelt, kan bijvoorbeeld een ransomwareaanval het einde van je bedrijf betekenen."

Cybersecurity raakt iedereen
Die ‘chef’ moet er in de visie van De Vries voor zorgen dat cybersecurityspecialisten de tijd en de financiële mogelijkheden krijgen om de informatiebeveiliging goed te regelen. En openstaan voor samenwerking. “Kijk wat je kunt leren van collega’s in de sector. Realiseer je dat je kunt leren van andermans fouten”, zo drukt hij bestuurders op het hart. “En dat die collega’s ook kunnen leren van jouw fouten. Een security-incident kan een klein drama zijn, maar is als je laat zien hoe je daarop hebt gereageerd ook een succesverhaal over incident-response op zichzelf.”

In die ‘cybersecuritysamenwerking’ is volgens De Vries geen plaats voor concurrentie. In dat opzicht zouden veel sectoren een voorbeeld kunnen nemen aan hoe bijvoorbeeld sommige banken elkaar helpen binnen één gezamenlijk Security Operations Center.

“Die banken zijn grote concurrenten van elkaar, maar werken op het gebied van cybersecurity samen en delen dreigingsinformatie met elkaar. Cybersecurity raakt dan ook iedereen.”

Spaken in het wiel
De ambitie van het NCSC is om te zorgen dat informatie op de juiste plaatsen terechtkomt en vraagstukken te delen. “Wij hebben een operationeel coördinerende rol in een landelijk dekkend stelsel. Politie doet bijvoorbeeld forensisch onderzoek en de inlichtingendiensten onderzoeken statelijke actoren, waarbij wij ervoor zorgen dat de informatie bij elkaar komt. Wij proberen de verschillende cirkels met elkaar te verbinden.”

De Vries benadrukt dat het NCSC als ‘coördinator’ niet alleen overheidsdiensten en de vitale infrastructuur bedient, maar ook de partners in de cybersecuritygemeenschap en het bredere publiek. Zo deelt het NCSC informatie met Cyberveilig Nederland, de belangenvereniging van de cybersecuritysector. En via Information Sharing and Analysis Centres (ISAC’s) deelt het NCSC informatie met vertegenwoordigers uit verschillende sectoren.

“Maar het is ook belangrijk dat bedrijven informatie over incidenten met ons delen”, benadrukt De Vries. “Generieke constateringen van wat er aan de hand is, kunnen we dan weer doorspelen naar andere sectoren. Het delen van informatie

Hans de Vries is sinds 1 november 2014 hoofd van het Nationaal Cyber Security Centrum (NCSC). Daarvoor was hij als afdelingshoofd Klant & Ontwikkeling werkzaam bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De Vries heeft rechten gestudeerd aan de Universiteit Leiden.

met het NCSC gaat volledig vertrouwelijk. Wij hebben een uitzondering op de Wet openbaarheid van bestuur. Wij hoeven details over incidenten niet te delen, niet met journalisten, en ook niet met de Tweede Kamer. Als we dat wel zouden doen, gaat het hele stelsel van samenwerking plat.”

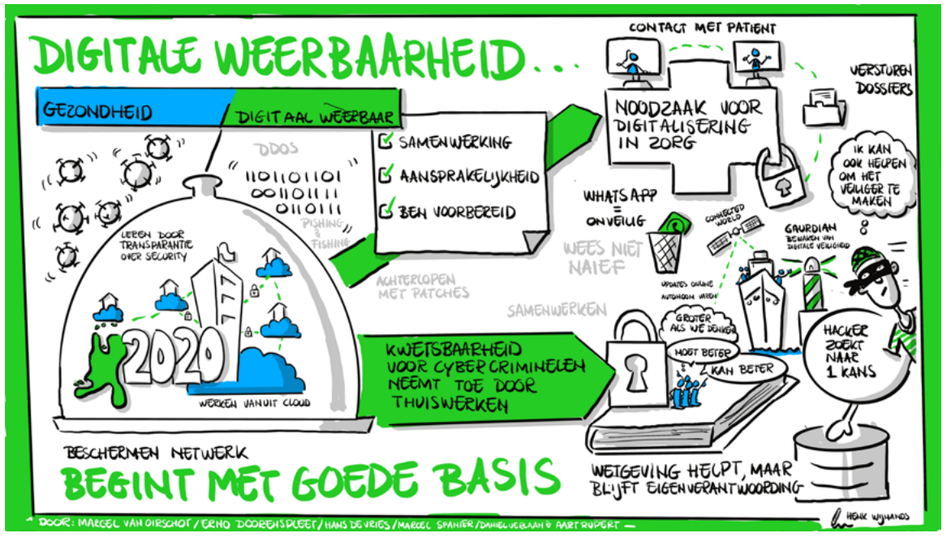
“Ik geloof niet in één grote organisatie die even de BV Nederland gaat beschermen.”

Federatief model
“Alles om Nederland veiliger te maken”, benadrukt De Vries. Het geschetste ‘landelijk dekkend stelsel’ stuit echter ook regelmatig op kritiek. Het zou met een veelheid aan ‘clubjes’ te versnipperd zijn, waardoor informatie verloren gaat. “Maar hoe we het hebben opgezet, past wel bij ons poldermodel. We zijn groot geworden door te polderen. Een te grote bemoeienis van bijvoorbeeld het NCSC wordt niet geaccepteerd. De reactie is dan al snel: ‘maar jij kent mijn sector niet.’ Ik geloof dan ook niet in één grote cyberorganisatie zoals in Engeland die even de BV Nederland gaat beschermen.”

Toch is De Vries het ook niet oneens met de kritiek. Integendeel. “Ik ben voorstander van het federatieve model, maar nu is alles zo verknipt dat mijn bereik minder effectief is dan het zou kunnen zijn. Er moet een betere coördinatie komen, een meer gecentraliseerde blik op cybersecurity. Er zijn nu teveel partijen die allemaal een stukje doen en niemand die de hele keten overziet.”

Versterkte samenwerking
De directeur pleit daarom voor wat hij noemt een ‘versterkte samenwerking’, onder andere met marktpartijen zoals KPN Security die een grote stempel drukken op de beveiliging van BV Nederland. “Bijvoorbeeld door in hetzelfde gebouw te gaan zitten”, licht De Vries toe. “Alleen al het feit dat er in het pand van het NCSC ruimtes zijn ingericht voor bijvoorbeeld de AIVD en de MIVD, maakt dat we sneller en effectiever kunnen praten over de incidenten die voorbij komen.”

“Maar naast een ‘publieke kamer’ zou er ook een ‘privaat stukje’ moeten komen waar dus iemand van bijvoorbeeld KPN Security zou kunnen zitten. Als er dan iets aan de hand is, kunnen we direct schakelen. In de versterkte samenwerking moeten de publieke en private lijnen veel dichter bij elkaar komen te liggen. Dat hopen we ook in te brengen in de nieuwe kabinetsplannen.” Volgens De Vries is niets onmogelijk. “Zo spannend is het allemaal niet. Samenwerken is gewoon doen.”



» Cyberincidenten ontstaan vaak door onveilig gedrag. Het middel om dat gedrag te verbeteren is vaak hetzelfde: vergroten van kennis en bewustzijn. Toch is dat volgens gedragswetenschapper Wetzer lang niet voldoende, of soms zelfs simpelweg een foute aanpak. Volgens Wetzer, bij securitybedrijf Secura actief als sociaal psycholoog cybersecurity & compliance, is er nog veel te winnen op dit gebied. “Ik voel me soms een roepende in de woestijn.”

Psychologen zijn hard nodig in de securitywereld

Inge Wetzer
Sociaal psycholoog cybersecurity & compliance, Secura

Het is al heel wat jaren een mantra in de securitywereld: de mens is de zwakste schakel. Veilig gedrag speelt een cruciale rol in het voorkomen van cyberincidenten. Trainingen voor het verbeteren van security awareness zijn dan ook inmiddels een vaste waarde in het portfolio van veel IT-bedrijven. Het doel van die trainingen is doorgaans het verbeteren van kennis en bewustzijn rondom cybergevaren. Dat uitgangspunt lijkt logisch: wie zijn vijand niet kent, of zelfs niet van zijn bestaan op de hoogte is, kan zich lastig verdedigen.

Bredere benadering

Toch is die benadering veel te smal, betoogt Wetzer. Kennis is weliswaar belangrijk, maar kennis van de regels leidt niet automatisch tot het juiste gedrag. Dat is voor cybersecurity niet anders dan in het verkeer of bijvoorbeeld de coronamaatregelen. Vanuit haar achtergrond als psycholoog pleit ze dus voor een aanpak die zich richt op veilig gedrag als einddoel, en gaat daarmee verder dan awareness. Ze doet onderzoek naar onveilig gedrag binnen organisaties en ontwikkelt interventies om dat gedrag te veranderen. Ze pleit voor een grotere rol van gedragswetenschappers in de securitywereld. Want wie daadwerkelijk menselijk gedrag wil veranderen, moet breder kijken dan het kennisniveau van de medewerkers. “Kennis en bewustzijn is natuurlijk een belangrijke basis. Het is belangrijk dat medewerkers goed op de hoogte zijn van alle gevaren. Maar dat is niet genoeg. Je wilt dat ze veilig gedrag vertonen in omgang met informatie en systemen. Dan ontkom je niet aan de psychologie, de wetenschap die dat menselijk gedrag bestudeert en beïnvloedt.”

Hoe stuur je dat menselijk gedrag dan precies? Volgens Wetzer begint dat bij de ‘waarom’-vraag. Waarom vertonen mensen nu nog niet het veilige gedrag? Het antwoord op die vraag ligt volgens haar besloten in drie dimensies. Als iemand zich niet veilig gedraagt ontbreekt het aan één van deze drie:

1. Capaciteit

Dit is de laag die in de securitywereld de meeste aandacht krijgt. Zonder kennis geen veilig gedrag. Het gaat hierbij niet alleen om kennis over de gevaren, maar ook hoe je die risico’s met veilig gedrag kunt minimaliseren. “Weten mensen wat er van ze verwacht wordt?”

2. Motivatie

Het is essentieel dat mensen weten hoe ze door veilig gedrag cyberrisico’s kunnen minimaliseren. Toch is dat niet genoeg. Het zegt namelijk niks of mensen ook daadwerkelijk daartoe bereid zijn. “In een wereld waarin mensen perfect rationele wezens zijn, volstaat het zenden van kennis. Maar in die wereld leven we niet. Kijk maar naar de coronacrisis! Mensen weten best wat de regels zijn, maar dat wil niet zeggen dat iedereen zich daar altijd aan houdt. Een deel van de bevolking vindt het simpelweg belachelijk, een ander deel is het misschien niet eens met het beleid.” Voor security geldt dat net zo. “Zien ze het nut ervan in? Willen ze moeite ervoor doen? Als mensen niet willen, zullen ze het niet doen. Ze moeten er de noodzaak van inzien en eventueel bereid zijn extra moeite te doen.”

3. Gelegenheid

Ook gelegenheid is een belangrijke factor. Wetzer bedoelt hiermee dat je mensen wel de mogelijkheid moet geven om met veilig gedrag risico’s te verkleinen. Dat is deels afhankelijk van de context, en deels van de cultuur van de organisatie. “Met context bedoel ik de voorzieningen die getroffen zijn om veilig gedrag mogelijk te maken”, zegt Wetzer.

“Denk aan de beschikking over een account met de juiste rechten, zodat je niet van het account van je collega gebruik hoeft te maken om een bepaalde taak gedaan te krijgen. Of denk aan het beschikbaar stellen van een wachtwoordmanager, zodat mensen niet in de verleiding komen overal hetzelfde wachtwoord te gebruiken.”
Overigens staan deze drie aspecten niet helemaal los van elkaar. Ze overlappen elkaar. “Stel, de afspraak is dat je papier met persoonsgegevens weggooit in een afgesloten blauwe bak. Maar die bak staat drie verdiepingen hoger. Dan is dat zowel gelegenheid als motivatie. Er is immers geen gelegenheid om papier op je eigen verdieping weg te gooien. Bovendien kan de motivatie ontbreken om steeds drie trappen op te lopen enkel en alleen om papier weg te gooien.”

Gesprekken

Deze drie componenten vormen voor Wetzer de basis van de trajecten die ze met bedrijven en overheden doorloopt. Een belangrijk onderdeel van zo’n traject is de onderzoeksfase. Daarin verkent ze binnen organisaties op basis van steekproeven welke van deze drie componenten voor het gewenste gedrag ontbreekt. Vaak met verrassende resultaten. “Mensen gaan snel op de stoel van een psycholoog zitten en nemen aan waarom anderen dingen niet doen. Maar ga je vervolgens met mensen praten, dan blijken er vaak heel andere redenen te zijn. Redenen die je bovendien niet kunt weten als je er niet naar vraagt. Bijvoorbeeld dat ze een voorbeeld nemen aan een manager die ook bepaalde dingen niet doet. Of dat ze in het verleden een nare ervaring hebben gehad met het melden van een incident.”

Uit dat onderzoek komen specifieke verbeterpunten naar voren. Met behulp van interventies neemt ze deze vervolgens beet. Iedere situatie vraagt weer om andere oplossingen. “Soms is het eenvoudig. Dan luidt bijvoorbeeld het advies: zet meer blauwe afvalbakken voor gevoelige papieren documenten

neer.” In andere situaties is het veel complexer. Bijvoorbeeld wanneer psychologische drempels het draagvlak voor bepaalde securityvoorzieningen ondermijnen. “Medewerkers kunnen huiverig zijn voor bijvoorbeeld een wachtwoordmanager, omdat ze denken dat het te ingewikkeld voor ze is. Dat is een motivationele reden”, schetst Wetzer. “We organiseren dan een demo waarin we laten zien hoe makkelijk het is. Dat ze binnen een half uur een wachtwoord-manager met al hun wachtwoorden up-and-running kunnen hebben.”

Patronen

Geen twee mensen zijn gelijk, laat staan twee organisaties vol medewerkers. Toch herkent Wetzer bepaalde zaken die vaker misgaan. ”Bijvoorbeeld als het gaat om kennis rondom veilige wachtwoorden. Veel mensen gaan daarbij uit van verouderde principes. Ze denken dan dat wachtwoorden met daarin bestaande woorden veilig zijn, zolang ze maar wat cijfers en leestekens toevoegen. Dat was misschien enkele jaren geleden zo, maar inmiddels niet meer.” Haar achtergrond als psycholoog komt bij zo’n interventie goed van pas. “Ik leg niet alleen uit hoe hackers te werk gaan bij het kraken van wachtwoorden.

Ik kan het ook in begrijpelijke taal uitleggen en aansturen op daadwerkelijke gedragsverandering. Bijvoorbeeld door het geven van bruikbare tips, zoals het nemen van een wachtwoord dat bestaat uit de eerste letters van ieder woord uit een zin. Zo verveel je ze niet met materie die ofwel te lastig, ofwel al bekend is.”

Ook komt ze veel gelegenheidszaken tegen. Dingen die eenvoudig zijn op te lossen, maar waar de organisatie zelf een blinde vlek voor gecreëerd heeft. “Denk aan de regel om zichtbaar een personeelspas te dragen. Soms zijn de badgehouders van zo’n slechte kwaliteit dat die pas er steeds uitvalt. Dat kan een reden zijn om ze thuis te laten. Met als gevolg dat hackers of de Alberto Stegemans van deze wereld makkelijker fysiek kunnen binnendringen. In zo’n geval is de oplossing simpel: koop fatsoenlijke badgehouders.”

“Mensen gaan snel op de stoel van een psycho-loog zitten.”

Maatwerk

Alle genoemde voorbeelden hebben een gemene deler. De verbeterpunten zijn niet het gevolg van een laag bewustzijn of een gebrekkige kennis rondom security. Een reguliere bewustwordingstraining had deze problemen niet opgelost. Sterker nog, het inzetten van dit soort algemene kennistrainingen werkt volgens Wetzer vaak contraproductief. “Voor een deel van de medewerkers bevat zo’n training niets nieuws. Zij vervelen zich flink. Voor anderen is het wellicht te ingewikkeld. Daardoor nemen ze net zo goed geen nieuwe kennis op. Pas na grondig onderzoek van de daadwerkelijke barrières (capaciteit, motivatie of gelegenheid) kun je zinvolle interventies doen. Maatwerk is echt belangrijk, omdat je dan weet waar je mensen echt mee helpt.”

De boodschap van Wetzer is beslist nog geen gemeengoed. “Organisaties begrijpen op zich steeds beter de rol van gedrag. Helaas denken ze daarbij wel dat ze zelf dat gedrag met bijvoorbeeld zelfontwikkelde trainingen kunnen veranderen. Met het risico op gefröbel. Toch heeft ze goede hoop. “In een discipline als gedragseconomie weten we de rol van psychologen op waarde te schatten. Het is tijd dat we dat ook voor security gaan doen. In gesprekken met organisaties merk ik wel dat ze mijn boodschap begrijpen. Het verhaal begint tractie te krijgen. Maar voorlopig ligt er nog genoeg werk.”

Inge Wetzer is gepromoveerd in de sociale psychologie. Na tien jaar onderzoek naar gedragsbeïnvloeding bij TNO is zij sinds 2015 gespecial-iseerd in cybersecurity. Ze werkt bij Secura als sociaal psycholoog cybersecurity & compliance in het team dat zich richt op de ‘menskant’ van informatiebeveiliging. Hun opdracht is om hun kennis en ervaring op het gebied van menselijk gedrag te koppelen aan de domeinen compliance & cybersecurity om zo medewerkers van organisaties weerbaarder te maken.

» Nederland ligt digitaal zwaar onder vuur. Statelijke actoren hacken onze bedrijven voor spionagedoeleinden en ransomware veroorzaakt elk jaar miljoenen euro’s aan schade. Ronald Prins maakt zich zorgen. “De overheid faalt in het bestrijden van cybercriminaliteit. De regie ontbreekt volledig en onze economische belangen worden niet bewaakt.” Hij pleit daarom voor een Deltaplan Cybersecurity én een agressieve aanpak van ransomwarebendes.

Ronald Prins is vooral bekend als medeoprichter van Fox-IT. Na zijn vertrek in 2018 was hij betrokken bij de Toetsingscommissie van de AIVD en MIVD. In oktober 2020 richtte Prins zijn nieuwe bedrijf Hunt & Hackett op. Hunt & Hackett maakt organisaties weerbaarder tegen digitale spionage en cybercriminaliteit. Het bedrijf onderscheidt zich via een datagedreven aanpak. Daarin herkennen datascientists nieuwe typen cyberaanvallen met behulp van kunstmatige intelligentie en machine learning.

We kloppen ons vaak ten onrechte op de borst

Ronald Prins
Medeoprichter, Hunt & Hackett

Prins richtte in oktober van 2020 zijn nieuwe securitybedrijf Hunt & Hackett op. Inmiddels loopt het storm. “Ik had niet gedacht dat we nu al vol zouden zitten met klanten die niet alleen bang zijn voor cyberaanvallen, maar bij wie ook daadwerkelijk van alles aan de hand is”, vertelt hij. “Sommige bedrijven zijn vooral bezorgd over spionage door buitenlandse mogendheden, terwijl andere zich met name druk maken over ransomware en continuïteit. Dit zijn allebei grote problemen waar Nederland momenteel geen oplossing voor heeft.”

Volgens Prins is de dreiging van statelijke actoren nu groter dan ooit. Hij benadrukt dat het stelen van informatie en intellectueel eigendom niet altijd het primaire doel is. “Er worden ook allerlei partijen gehackt waarbij niet direct duidelijk is wat er te halen valt. Maar als ze platliggen, heeft dat een grote impact op de vitale infrastructuur. Voor landen als Noord-Korea is dit een manier om relevant te blijven op het wereldtoneel. En als ze dan met een land in conflict komen, weet hun cyberleger precies waar en hoe ze schade aan kunnen richten. Dat is goedkoop en zeer effectief.”

‘We zijn aan het polderen’
Prins is uiterst kritisch op het Nederlandse securitybeleid. “Ik denk dat we ons vaak ten onrechte op de borst kloppen. We zijn erg vocaal over hoe goed we het als land doen, maar de landen om ons heen gaan echt veel daadkrachtiger te werk. Wij zijn aan het polderen, met veel te veel clubjes die zich ertegenaan bemoeien. We hebben het NCSC, de NCTV, de MIVD en AIVD, de Cyber Security Raad, het Team High Tech Crime, het Defensie Cyber Commando en dan zijn er nog allerlei private partijen. Maar er zit geen regie op, er is geen overkoepelende visie.”

De securityexpert vindt vooral dat er vanuit de overheid te weinig aandacht is voor de economische belangen. “Al die clubjes worstelen met de vraag of zij deze belangen ook moeten bewaken. In het Verenigd Koninkrijk is dit een belangrijk onderdeel van de nationale cybersecuritystrategie. En dan zijn wij nog aan het uitvogelen hoe nationale veiligheid en economische veiligheid in elkaar passen. Bovendien kun je niet verwachten dat kleine, kennisintensieve partijen de Chinezen buiten de deur houden. Dat moet in een groter geheel gebeuren.”

Het regeringsbeleid van de afgelopen jaren op dit vlak noemt Prins ‘afwezig’. “Het totale budget voor cybersecurity is dan wel opgevoerd naar 95 miljoen euro per jaar, maar dat blijft veel te weinig. Bovendien wordt die taart dan weer verdeeld over alle clubjes die daarmee zelf wat extra mensen aannemen. Het geld wordt niet effectief ingezet. En bij het volgende grote incident komen er weer wat kritische Kamervragen van politici die niet genoeg kennis van de materie hebben. Zo schieten we niks op.”

Geen overkoepelende strategie
“De fundamentele vragen worden niet beantwoord”, stelt Prins. “Welke kant gaan we op? In hoeverre vinden we dat de inlichtingendiensten onze economische belangen moeten beschermen? Hoe werken we als overheid samen met private partijen? Durven we het ook aan om de vitale infrastructuur bepaalde securitymaatregelen op te leggen? In het Verenigd Koninkrijk moet de ‘critical infrastructure zich laten testen en monitoren door een gecertificeerde partij. Nu wordt dat in Nederland gewoon vrijgelaten. Bij een waterleidingsbedrijf zijn er wel allerlei eisen over bijvoorbeeld het chloorgehalte, maar de digitale huishouding krijgt nauwelijks aandacht.”

Ook de informatievoorziening richting het bedrijfsleven hebben de Britten beter voor elkaar, aldus Prins. “Bij mijn vorige bedrijf Fox-IT kregen klanten met een vestiging in het Verenigd Koninkrijk een belletje van de inlichtingendienst als er ingebroken was op systemen. Dan gingen we op onderzoek uit en konden we het inderdaad vinden. Dat heb ik in Nederland echt zelden meegemaakt, alleen in uitzonderlijke gevallen. Het is geen onwil van de AIVD. Als er echt iets aan de hand is, komen ze heus wel in actie. Maar het is allemaal niet structureel geregeld.”

Prins vindt dat de overheid het roer om moet gooien. “We moeten het internet zien als een publieke ruimte. De politie surveilleert op straat en komt in actie bij verdachte zaken. Als ik zie dat er bij de buurman wordt ingebroken, kan ik de politie bellen. Agenten dragen vuurwapens om de orde te handhaven. Incident-response is netjes geregeld. In cyberspace is er nog te weinig actieve bemoeienis van de overheid. Maar het bedrijfsleven heeft zelf niet de bevoegdheid om een antwoord te geven op al die dreigingen die op ons afkomen.”

Politie is onzichtbaar
Over de rol van de politie is hij overigens ook niet te spreken. “Ze komen drie keer per jaar met een persbericht dat er een darkweb is opgerold. Verder vind ik de politie onzichtbaar in de strijd tegen cybercriminaliteit. In het afgelopen jaar zijn er tientallen grote ransomwarezaken geweest in Nederland, maar je leest nooit dat er daders worden aangehouden. Het is niet zo dat er bij de politie geen slimme mensen zitten. De vraag is alleen of zij de juiste toolkit hebben om deze grensoverschrijdende problematiek op te lossen.”

Volgens Prins is de wet Computercriminaliteit III (de ‘hackwet’) in de praktijk niet goed toepasbaar. “De politie mag niet hacken in het buitenland en er zijn allerlei idiote waarborgen ingebouwd. Zo moeten alle hackwerkzaamheden gefilmd worden, mogen alleen gecertificeerde mensen hacken en is hacken alleen toegestaan voor delicten waar minimaal 8 jaar celstraf op staat. Ook is het gebruik van zerodays niet toegestaan en mag de politie geen tooling kopen van partners die niet door de AIVD gescreend kunnen worden. Zo is het digitale pistool van de politie feitelijk een klappertjespistool.”

“Het digitale pistool van de politie is feitelijk een klappertjes-pistool.”

Deltaplan Cybersecurity
Wie kritisch is, moet natuurlijk ook oplossingen aandragen. Dat doet Prins dan ook graag. “Er is meer geld nodig, maar ook een doordacht plan. En we moeten zeker geen nieuwe clubjes oprichten, maar de huidige clubjes meer centraliseren. Een model met een regeringscommissaris zou kunnen werken. Vanaf 2010 kreeg deltacommissaris Wim Kuijken een miljard per jaar om te voorkomen dat Nederland onder water zou komen te staan. Deze aanpak liep dwars door alle ministeries heen. Zoiets hebben we ook nodig om cybercriminaliteit terug te dringen.”
Maar hoe voorkomen we dan dat buitenlandse hackers nu ‘onze’ kennis stelen? Wordt het niet tijd om terug te slaan? “Nee, dat werkt alleen maar escalerend. De focus moet liggen op monitoring, detectie en diplomatieke maatregelen. Ik ben ook wel gecharmeerd van forward defense. Wordt er gespioneerd in bijvoorbeeld de maritieme of agrarische sector? Wat is de vijand aan het uitspoken en kan ik een aanval verwachten? Wat mij betreft neemt de AIVD hierin het voortouw.”

Prins heeft ook een suggestie om de informatievoorziening richting het bedrijfsleven te verbeteren. “De inlichtingen-diensten zijn vaak huiverig om informatie te delen. Stel dat je een trucje hebt om een bepaalde Chinese hackersgroep te ontdekken, dan wil je niet dat die groep erachter komt, omdat ze dan hun werkwijze aanpassen. Ik snap ook wel dat de AIVD niet zijn eigen mensen kan inzetten om bij die bedrijven rond te lopen. Maar laat die bedrijven dan zelf een securitypartij inhuren waar tien mensen werken die gescreend zijn door de AIVD. Met hen kan de gevoelige informatie dan wel gedeeld worden. Zo belandt de informatie niet ongebruikt in een la.”

Oorlog verklaren aan ransomware
Voor de strijd tegen ransomware ziet Prins een agressieve aanpak wél zitten. “Ransomwarebendes worden vaak beschermd door het land van waaruit ze opereren, en gebruiken doorgaans computers in een ander land. De diplomatieke weg is dan lang en vol juridische obstakels. Meestal leidt zo’n traject nergens toe. Maar als cybercriminelen zoveel schade aanrichten in Nederland, is het toch geoorloofd om dat een halt toe te roepen? Dan moeten we deze groepen misschien maar actief durven te hacken en hun apparatuur slopen.”
“Deze bendes kunnen kiezen op welk land ze hun pijlen richten”, vervolgt hij. “Als hun spullen telkens kapot gaan als ze Nederland aanvallen, kiezen ze misschien de volgende keer voor Italië. Uiteindelijk maken cybercriminelen ook een risicoafweging. Dat risico is nu nihil. De pakkans is klein, mede omdat de geldstromen niet te volgen zijn. Keihard terugslaan is uiteraard een laatste redmiddel. We moeten zoveel mogelijk de officiële routes bewandelen. Maar als dat allemaal niet werkt, moet je die criminelen ergens pijn gaan doen. En dat kan door in te grijpen op hun infrastructuur.”

‘Security alleen is niet genoeg’
Prins benadrukt het belang van een goede basishygiëne en een solide beveiliging tegen ransomware. Volgens hem is echter meer mogelijk nodig dan dat. “Natuurlijk moeten we het cybercriminelen zo moeilijk mogelijk maken. Maar er worden ook bedrijven slachtoffer die hun security prima op orde hebben. Als we verder niks doen, wordt dit probleem alleen maar groter. We proberen al twintig jaar om hackers buiten de deur te houden en we maken wel degelijk vorderingen. Alleen die hackers worden ook steeds beter, en dat gaat in veel grotere stappen.”

De securityexpert begrijpt dat er haken en ogen zitten aan deze agressieve aanpak. “Als wij de oorlog verklaren aan cybercriminelen en over de landsgrenzen gaan hacken, legitimeert dat wellicht andere landen om dat ook bij ons te doen. Misschien gaat Erdogan dan wel servers uit de lucht halen als er in Nederland negatief over hem geschreven wordt. Er zitten wel dilemma’s aan vast, maar we moeten een signaal afgeven. Anders verandert er nooit iets.”

» Een overstap naar de cloud kan vanuit securityoogpunt verstandig zijn. Zo hebben de grote cloudproviders hun basishygiëne prima op orde. “De cloud ontzorgt op het gebied van security, maar het is zeker niet zo dat de cloud per definitie veilig is”, zegt Erno Doorenspleet, CTO van KPN Security. Toch is hij een groot voorstander van ‘cloud-first’. “Als u de cloud niet omarmt, doet uw personeel dat wel.”

Omarm de cloud, maar onderschat de securityrisico’s niet

Erno Doorenspleet
CTO, KPN Security

Zowel zakelijk als privé zijn clouddiensten niet meer weg te denken uit ons leven. “De nieuwe generatie beseft niet eens dat Netflix, WhatsApp en Steam gebruikmaken van de cloud”, aldus Doorenspleet. “Ze vinden het ook helemaal niet relevant: het werkt toch? Het contrast met het bedrijfsleven is groot. De cloud betekent een andere manier van werken dan bedrijven gewend zijn. Zeker organisaties met veel legacysystemen staan soms huiverig tegenover de cloud.”

De CTO van KPN Security ziet gelukkig dat er een kentering gaande is. “Steeds meer bedrijven kiezen voor cloud-first. Dat heeft wel even geduurd. Cloudcomputing werd rond het jaar 2000 al gebruikt, maar het concept van flexibele IT stamt al uit de jaren 60. Toen was het heel gewoon om mainframecapaciteit te huren voor complexe berekeningen. Dit was veel goedkoper en makkelijker dan het kopen van een eigen mainframe.”

Basisbeveiliging in de cloud
Volgens Doorenspleet hangt de groeiende populariteit van cloud niet alleen samen met de operationele voordelen, zoals schaalbaarheid en flexibiliteit. “Ook qua security zijn cloud-providers echt volwassen geworden. Enkele jaren geleden werd de beveiliging nog als obstakel gezien om workloads naar de cloud te verplaatsen. Dat beeld is toch wel gekanteld. Tegenwoordig is security juist een argument om wél naar de cloud te gaan.”

Steeds meer IT-professionals beschouwen de cloud als zeer veilig. “Tot op zekere hoogte klopt dat ook. U hoeft zelf geen servers te patchen, en cloudproviders zoals AWS en Microsoft kunnen het zich niet permitteren om patches uit te stellen. Het is in hun belang dat de clouddienst zo veilig mogelijk is. Als u uw data bij zo’n partij in de cloud heeft staan, hoeft u zich ook geen zorgen te maken over een lek zoals Heartbleed. Zo ontzorgt de cloud bedrijven in hun basisbeveiliging.”

Transparantie ontbreekt
Toch is dat niet het hele verhaal. “Ik vind dat cloudproviders wel transparanter moeten worden. Allereerst is de configuratie van clouddiensten vaak erg complex. Zonder specialistische kennis is onduidelijk welke instellingen veilig zijn. Als ik bijvoorbeeld in de cloud een microservice wil bouwen, moet ik allerlei keuzes maken. Vaak staat er meer open dan dicht. Het lijkt simpel aanvinken, maar je moet bijna een cursus volgen om het te begrijpen.”

Ook de locatie van de data is een heikel punt. “Vanuit wet- en regelgeving zoals de AVG moeten bedrijven altijd exact weten waar persoonsgegevens staan”, licht Doorenspleet toe. “En in sommige landen mogen gegevens niet de grens over. Positief is dat steeds meer cloudproviders vermelden waar de servers staan. Maar wie heeft toegang tot de data? Kan de helpdesk uit India of de Verenigde Staten er ook bij? Dat blijft vaak in het midden.”

Eigen verantwoordelijkheid
Bovendien moet het bedrijf zelf ook securitymaatregelen treffen. “Als ik een workload naar de cloud breng, is het nog steeds aan mij om ervoor te zorgen dat de applicatielaag goed beveiligd is. Ook het Identity & Access Management, de toegang tot data dus, moet ik zelf op de juiste manier inrichten. De cloudprovider houdt zich daar niet mee bezig. Die weet ook niet welke gevoelige data ik in de cloud plaats en of deze mogelijk interessant zijn voor kwaadwillenden.”

De CTO noemt enkele voorbeelden uit de praktijk. “Netflix draait op AWS. Maar AWS zorgt er niet voor dat gebruikers veilig kunnen inloggen en dat hun creditcard-gegevens op de juiste manier worden opgeslagen. Dat doet Netflix zelf. En banken zijn er zelf verantwoordelijk voor dat internetbankieren goed beveiligd is en dat hun klanten alleen toegang krijgen tot hun eigen rekening. Een bedrijf wordt echt niet volledig ontzorgd, terwijl het soms wel zo overkomt.” “Als u dit niet op orde heeft, kunnen uw data zomaar in verkeerde handen komen, met verstrekkende consequenties”, waarschuwt Doorenspleet. “Bij een lokale server is een klein foutje nog geen ramp. Een goede firewall en monitoring helpen dan voorkomen dat data worden ontsloten naar de buiten-wereld. Proactieve monitoring is ook in de cloud cruciaal. Eén verkeerd vinkje en de data zijn voor de hele wereld toegankelijk.”

Cloudmigratie kan riskant zijn
De migratie naar de cloud kan eveneens risico’s met zich meebrengen. “Dat geldt met name voor bedrijven die al langer bestaan. Een start-up zal niet gauw kiezen voor een eigen datacenter. De cloud is dan de logische keuze. Maar oudere bedrijven hebben waarschijnlijk een behoorlijke lokale infra-structuur neergezet waar de meeste diensten op draaien. Dan vraagt de move naar de cloud veel aandacht en een secure uitvoering.”

“Bij zo’n migratie bestaat het risico dat er meer mensen bij de data kunnen dan noodzakelijk is”, legt hij uit. “We kunnen heel slecht inschatten hoe die data zich gedragen. In veel gevallen is het simpelweg niet verantwoord om oude diensten te kopiëren naar de cloud. Dan is het beter om opnieuw te beginnen met een nieuw design. Dit is vanuit securityperspectief minder riskant en kost waarschijnlijk nog minder tijd ook.”

Ondanks de risico’s is Doorenspleet ervan overtuigd dat cloud-first de weg voorwaarts is. “Als u de cloud niet omarmt, doet uw personeel dat wel. Veel bedrijven die weg willen blijven van de cloud, zitten er waarschijnlijk onbewust al in. Natuurlijk kunnen er zwaarwegende argumenten zijn om alles lokaal te doen. Wellicht zijn uw data dermate gevoelig dat u absoluut ‘in control’ wilt blijven. Maar zorg er in ieder geval voor dat u vanuit een strategie werkt en communiceer deze ook naar de medewerkers.”

Voer een risicoanalyse uit
De CTO heeft nog een belangrijk advies voor organisaties die een gang naar de cloud overwegen of daar juist middenin zitten. “Laat een goede risicoanalyse uitvoeren.

“De cloud is geen must, maar het kan ons leven wel veel makkelijker maken.”

Erno Doorenspleet is sinds februari 2020 werkzaam als Vice President Security Strategy en CTO van KPN Security. Hij overziet de onderzoeksactiviteiten van KPN Security en het KPN Security Lab. Doorenspleet heeft meer dan 20 jaar ervaring in de IT-industrie en is gespecialiseerd in thema’s als security- en risicomanagement, governance, cloudcomputing en het Internet of Things.

Welke data wilt u naar de cloud brengen en waarom? Welke risico’s levert dit op? Misschien komt u er dan achter dat het helemaal niet zo erg is. Of u concludeert juist dat de cloud vanwege wet- en regelgeving geen optie is. Betrek ook de data privacy officer in deze afweging.”

Doorenspleet raadt IT-professionals verder aan om geen concessies te doen bij de selectie van een cloudprovider. “Waar wil ik dat de provider mijn data opslaat en wie mag er onderhoud plegen op die omgeving? Als uw data binnen de Europese Unie moeten blijven, dan is dat het belangrijkste criterium. Want als u simpelweg voor de goedkoopste aanbieder gaat, staan de data straks alsnog in de Verenigde Staten of Canada.”

“De cloud is geen must, maar het kan ons leven wel veel makkelijker maken”, besluit Doorenspleet. “De wereld om ons heen is al cloud-first en dit wordt ook de norm in het bedrijfsleven. Daar ben ik blij mee: de cloud verbetert bedrijfsprocessen en versnelt innovatie. Tegelijkertijd mogen we niet blind zijn voor de securityrisico’s, want die zijn er wel degelijk.”

» Het opsporen van cybercriminelen kost de politie veel capaciteit. Bovendien leidt het lang niet altijd tot een veroordeling. Daarnaast komen personen vaak pas in beeld als ze al zijn afgegleden naar zware vormen van cybercrime. Daarom zet de politie steeds meer in op daderpreventie. De Cyber Offender Prevention Squad (COPS) ontwikkelt interventies die jongeren weerhouden van het starten of doorontwikkelen van een cybercriminele carrière. “Zo voorkomen we schade én helpen we jongeren om hun talent te benutten”, zegt COPS-teamleider Floor Jansen.

Floor Jansen werkt al ruim 12 jaar in diverse functies bij de politie, vanuit haar achtergrond als criminoloog, sociaal wetenschapper en cybersecurityspecialist. Ze hield zich onder meer bezig met de aanpak van mensenhandel, georganiseerde hennepteelt en synthetische drugs. Acht jaar geleden stapte ze over naar het Team High Tech Crime dat zich richt op de bestrijding van cybercriminaliteit.

Een jonge cyber-crimineel kan ook **een IT-talent zijn**

Floor Jansen
Teamleider COPS, Nederlandse politie

COPS is een gespecialiseerde politie-eenheid die in de zomer van 2020 werd opgericht. Naast initiatiefnemer en teamleider Jansen bestaat COPS uit een gedragswetenschapper, digitaal specialist, interventiespecialist, projectsecretaris en de Britse daderpreventie-expert Greg Francis. “Hij heeft het cybercrimepreventieteam van de Britse politie opgezet. Vanwege de verschillen tussen de rechtssystemen is zijn aanpak niet een-op-een te kopiëren, maar we beginnen zeker niet op nul.”

COPS bouwt voort op eerdere preventieprojecten van de politie, zoals Hack_Right. Hack_Right werd zo’n drie jaar geleden opgezet door Jansen en een collega van het OM. Dit is een alternatieve straf voor jonge cybercriminelen waarbij de politie samenwerkt met het Openbaar Ministerie, de Raad voor de Kinderbescherming, Reclassering Nederland, Halt en het bedrijfsleven. Hack_Right is gericht op jongeren tussen de 12 en 23 jaar (in uitzonderingsgevallen tot 30 jaar) die voor het eerst vervolgd worden voor een cyberdelict. In dit traject krijgen zij informatie aangereikt over de impact van hun delict en moeten ze opdrachten uitvoeren in het kader van hun straf, deels ook bij een deelnemend bedrijf.

Het belang van preventie
Jansen ziet daderpreventie als een cruciaal wapen in de strijd tegen cybercriminaliteit. “Preventie voorkomt schade en ontlast de rechtsketen. Als de politie een server vindt met 2000 accounts van mensen die een DDoS-aanval hebben gekocht, kunnen we er daarvan ongeveer tien vervolgen. Gemiddeld wordt de helft van de zaken geseponeerd. Dan kom je uiteindelijk tot een paar veroordelingen. Door het toevoegen van interventies gericht op preventie, zoals stopgesprekken, bereiken we een veel groter aantal daders.

Hierdoor maken we de bestrijding van cybercrime efficiënter.” “Met preventie willen we vooral het laaghangende fruit afvangen, en voorkomen dat jongeren het verkeerde pad op gaan”, vervolgt Jansen. “Zo kan de recherche zich bezighouden met de echt grote boeven.” Overigens vindt zij dat er sowieso meer capaciteit moet komen voor de bestrijding van cybercriminaliteit. “Binnen de politie ligt de focus nog vooral op ‘traditionele’ criminaliteit, terwijl deze al jaren afneemt. Cybercrime zit juist in de lift en zou prioriteit nummer één moeten zijn.”

Volgens Jansen is preventie ook belangrijk om een gelijk speelveld te creëren. “Er zijn al veel manieren om jongeren te weerhouden van offline criminaliteit”, legt ze uit. “Je ouders zeggen dat je geen snoep mag stelen, er hangen beveiligingscamera’s in de winkel en als de winkelier je betrapt, kom je misschien weg met een waarschuwing. Deze bijsturingsmomenten zijn er niet voor cybercriminelen. Ouders, docenten en de politie hebben er geen zicht op. En als iemand dan de eerste keer met de politie in aanraking komt, is het meteen voor een groot vergrijp.”

Hack_Right: niet voor iedereen

Niet alle cyberdaders komen in aanmerking voor Hack_Right. “We kijken onder andere naar hun affiniteit met ICT. Wat drijft iemand om een delict te plegen? Een jongere die al vanaf zijn elfde aan het programmeren of hacken is en daar steeds beter in wordt, kan vanuit de interesse in IT afdalen naar illegale handelingen. Maar er zijn ook mensen die het duidelijk voor het geld doen. Zij hebben niet noodzakelijk IT-skills, maar willen gewoon snel geld verdienen.”

Volgens Jansen is het type delict niet bepalend. “Als jij je eigen botnet helemaal bij elkaar hackt en daarmee een DDoS-aanval pleegt, is de impact van het delict vergelijkbaar met iemand die een DDoS-aanval inkoopt bij een booter. Qua technisch niveau is dat echter totaal onvergelijkbaar. Maar als iemand een DDoS-aanval inkoopt en precies weet op welk onderdeel van het netwerk de aanval gericht moet zijn, dan is dat technisch ook vrij complex. We bepalen dus per geval of Hack_Right aansluit bij het profiel van de dader.”

Leren staat centraal

Sinds de start van de pilot startten 25 jongeren met Hack_Right. “Je kunt dit vergelijken met een taakstraf, maar dan met leren als uitgangspunt. Een first offender krijgt al behoorlijk veel voor zijn kiezen. Denk hierbij aan de aanhouding en inval in huis, de inbeslagname van computers en gegevensdragers, de gesprekken bij de reclassering... Dat is al zwaar. Het doel van Hack_Right is om te zorgen dat jongeren niet opnieuw de fout ingaan en dat ze hun digitaal talent op een goede manier leren inzetten. Voor sommigen horen daar ook andere basisvaardigheden bij, bijvoorbeeld dat ze op tijd moeten komen op hun werk en mensen netjes moeten aanspreken. Maar we helpen de jongeren vooral om te reflecteren op hun delict.”

Jansen noemt een aantal voorbeelden uit de praktijk. “Iemand moest een richtlijn voor responsible disclosure herschrijven, zodat deze ook voor jongeren begrijpelijk is.

Een andere jongere lieten we een werknemer van de afdeling netwerkbeveiliging interviewen. Wat zijn de gevolgen van een DDoS-aanval? Daar hebben ze vaak geen idee van. Weer een ander kreeg de opdracht om een plan te bedenken voor de beveiliging van IoT-apparaten voor consumenten. Het is mooi om te zien wat dit met de jongeren doet. Sommigen hebben echt een draai gemaakt.”

Interventies voor risicojongeren

Hack_Right zet zich in voor recidivepreventie, maar feitelijk is de politie er dan al te laat bij. Het delict heeft immers al plaatsgevonden. Jansen en haar team willen voorkomen dat risicojongeren überhaupt met de politie in aanraking komen. “We zijn nu bezig met een pilot voor een kortere interventie genaamd Hack_Light. Deze is bedoeld voor jongeren die erg bezig zijn met techniek, maar de ethische en juridische grenzen niet kennen. Zij zijn lekker aan het experimenteren. Dat is een accident waiting to happen.”

Deelname aan Hack_Light is vrijwillig. “We moeten de jongeren dus iets te bieden hebben. We informeren ze bijvoorbeeld over de kansen die er liggen als ze zich wél aan de regels houden. Hoe werkt een responsible disclosure? Welke bug-bountyprogramma’s zijn er? En welke opleidingen bereiden je voor op een carrière in cybersecurity? Ook hier zoeken we de samenwerking met het bedrijfsleven. Wij vertellen wat de regels zijn en de bedrijven kunnen de jongeren motiveren. Die combinatie is effectief. Het heeft geen zin om alleen met het vingertje te wijzen.”

Een ander voorbeeld van een preventieve interventie is het platform Gamechangers. “Jongeren van 15 zijn echt niet alleen maar bezig met carrièreplanning. Zij willen ook gewoon wat te doen hebben, zeker in coronatijd. Op Gamechangers staan games en opdrachten waarmee jongeren hun digitale skills kunnen verbeteren zonder de wet te overtreden. Veel bedrijven hebben hiervoor content aangeleverd, zoals cybersecurity-challenges. Zo brengen we positieve alternatieven voor illegaal hacken onder de aandacht.”

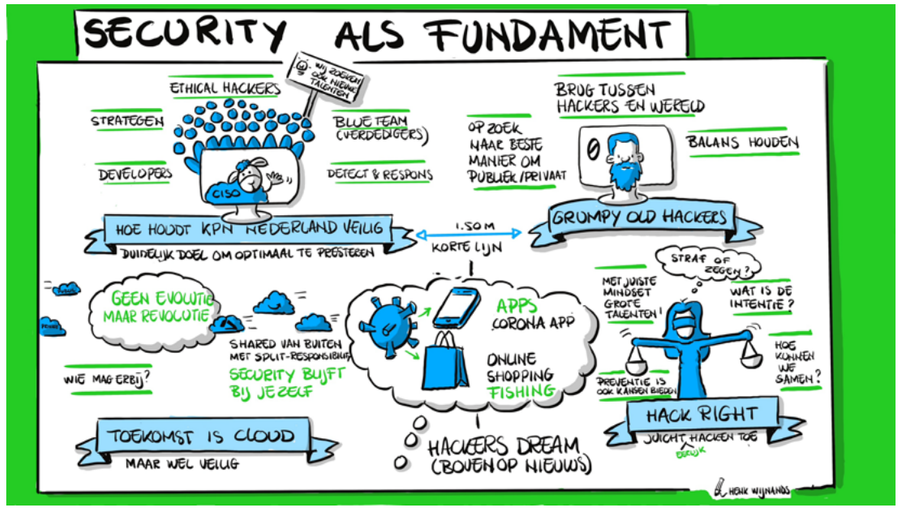
Werving van securitytalent

Voor de bedrijven zelf is het ook interessant om deel te nemen aan Hack_Right, Hack_Light en andere interventies. “Allereerst past dit goed binnen een strategie voor maatschappelijk verantwoord ondernemen. Ook verhogen bedrijven hiermee de algemene cybersecurity door daderschap te voorkomen. Daarnaast kunnen bedrijven via dit soort samenwerkingen in contact komen met IT-talenten. Er is in Nederland een schrijnend tekort aan securityprofessionals. Het is zonde als we deze groep niet benutten.”

De teamleider van COPS kan zich voorstellen dat bedrijven er huiverig voor zijn om een veroordeelde cybercrimineel in dienst te nemen. “Als jij voor een grote klant de digitale beveiliging verzorgt en die klant wil alleen mensen met een Verklaring Omtrent het Gedrag (VOG), dan wordt het een lastige discussie. Maar de mensen die het betreft zijn nog jong en de meeste jongeren kunnen na een aantal jaren weer starten met een clean slate.”

Jansen benadrukt dat elk bedrijf zijn steentje bij kan dragen. “Ik hoop dat bedrijven hierover gaan nadenken. Wat is onze verantwoordelijkheid? Stopt dat bij het ontwikkelen van de techniek of willen we méér doen? Juist op het gebied van daderpreventie kan het bedrijfsleven een belangrijke rol spelen. Zo zoeken we nu naar een partij die jongeren wil informeren over IT-opleidingen. De overheid kan deze complexe problematiek niet alleen oplossen. Alle hulp vanuit het bedrijfsleven is welkom.”

Heeft u interesse in een samenwerking met COPS? Via **daderpreventie@politie.nl** kunt u in contact komen met het team van Jansen.



» Het is een boodschap die in deze Cyber Security Persepectives vaker doorklinkt: voor securityprofessionals neemt de onzekerheid toe. “Er is steeds meer wat we niet weten”, stelt Marcel van Oirschot, Executive Vice President KPN Security. Volgens KPN’s Chief Information Security Officer Paul Slootmaker doen bedrijven er goed aan om die onzekerheid te accepteren. “En bereid je erop voor dat het misgaat.”

Er is steeds meer wat we niet weten

Marcel van Oirschot en Paul Slootmaker
EVP, KPN Security en CISO, KPN

We spreken Van Oirschot en Slootmaker via Teams. Het is tekenend voor het coronatijdperk waarin evenementen zoals NLSecure[ID] volledig online plaatsvinden. We videobellen met familie en collega’s en vanuit het thuiskantoor doen we ons werk. Volgens Slootmaker is deze manier van werken en leven gedeeltelijk here to stay. “Ook al gaan we terug naar een vorm die lijkt op die we voor corona hadden, bijvoorbeeld thuiswerken blijft.”

Van Oirschot sluit zich daarbij aan. “Er zullen na corona maar weinig mensen zijn die vijf dagen per week naar kantoor gaan. Misschien één of twee dagen voor de sociale contacten en voor creatieve processen. Maar de dagen dat medewerkers thuiswerken, moeten ze bijvoorbeeld wel de beschikking hebben over de juiste applicaties, kunnen printen en grote bestanden kunnen versturen. Daar moeten werkgevers in investeren, anders gaan werknemers op zoek naar U-bochten.”

Minder zicht
Die U-bochten zijn in de cloud zo gevonden, waarschuwt Van Oirschot. “Als de thuiswerkplek niet wordt gemonitord, kan ik als thuiswerker clouddiensten inkopen zonder dat de CISO daar überhaupt weet van heeft. Met een creditcard is alles te regelen. Weet je dan als werkgever of securityprofessional nog wel wat je digitaal allemaal hebt?”

Die onzekerheid wordt volgens hem versterkt door het feit dat er door thuiswerken minder zicht is op medewerkers. “Als je bijvoorbeeld callcentermedewerkers op een afdeling hebt zitten, dan is er nog enige sociale controle en zichtbaarheid. Maar nu zitten er mensen thuis die eigenlijk te veel functionaliteit onder de knoppen hebben. Ik denk dan ook dat we meer lekken gaan zien zoals bij de GGD.” Dit lek werd groot nieuws toen bleek dat medewerkers data uit de twee belangrijkste coronasystemen van de GGD hadden verhandeld.

Slootmaker ziet ook in de SolarWinds-hack een aanwijzing dat de onzekerheid voor securityprofessionals toeneemt, in dit geval door onzekerheden binnen de supplychain. Via een achterdeurtje slaagden aanvallers erin om gebruikers van SolarWinds’ Orion-software te bespioneren. “Zo’n backdoor in software zit er soms al een jaar in, maar in veel gevallen gaat de logging niet zover terug. Dan heb je als aanvaller tijd en gelegenheid om een aanval uit te voeren. Het is slechts een kwestie van tijd voordat er een nieuwe SolarWinds is.”

Onzekerheid accepteren
Voor bedrijven valt het echter niet mee om alle assets te inventariseren, inclusief de kwetsbaarheden van die assets. “Er is binnen een grotere organisatie nooit één persoon die alles weet te staan”, zegt Van Oirschot stellig. “En ik betwijfel of er tooling bestaat die je op je infrastructuur plaatst, inschakelt en die dan een lijst genereert met echt alles wat er te vinden is. Geen enkele tooling is feilloos, en zelfs als je een nauwkeurigheid van 99 procent haalt, is dat niet goed genoeg.” Net die ene ongepatchte server of die ene onbeheerde laptop kan voor problemen zorgen. “Dat is dan die laptop waarvan iedereen zegt ‘oh, die!’ als de data al op straat liggen.”

“Je kunt risico-analyses doen, maar uiteindelijk word je in verlegenheid gebracht door wat je niet weet”, vervolgt Slootmaker. “Dan is het beter om die onzekerheid te accepteren. Ga er maar vanuit dat het een keer misgaat, en bereid je daar goed op voor.”

Gedegen voorbereiding
Maar hoe kan een bedrijf zich voorbereiden als de toekomst onzeker is? Slootmaker en Van Oirschot halen een aantal stappen aan die tijdens de voorbereiding in ieder geval aan bod moeten komen:

1. Zorg voor een goede basishygiëne
“Het is misschien geen sexy onderwerp”, geeft Slootmaker toe, “maar het gaat toch eerst en vooral om de interne hygiëne. De kleine dingen die je moet doen aan het begin van de dag. Breng allereerst je assetmanagement op orde, hoe lastig dat ook is. Zorg er vervolgens voor dat je de aanwezige software structureel en zo snel mogelijk patcht, en dat je die patches zo mogelijk ook controleert op bijvoorbeeld backdoors.”

Bij die basishygiëne hoort ook aandacht voor Identity & Access Management. Van Oirschot: “Het beschermen van de digitale identiteit is door het GGD-lek uitermate hip geworden, maar daardoor is het nog niet eenvoudig. Wij hebben er heel veel voor moeten inrichten om iets vergelijkbaars niet bij KPN te laten gebeuren.”

2. Richt een goed crisisteam in
Volgens Van Oirschot zijn crisisteams vaak getraind in het reageren op ‘traditionele crisissen’, bijvoorbeeld na een brand of ontploffing. “Maar ook ‘cyber’ moet de aandacht hebben van een regulier crisisteam. Oefeningen moeten niet alleen zijn gericht op continuïteit, maar ook op cybersecurityscenario’s. Wat doe je als je met ransomware te maken hebt?”

“En zorg ervoor dat het crisisteam breed gedragen is”, vervolgt Van Oirschot. “Bijvoorbeeld legal en de raad van bestuur moeten een rol hebben binnen het crisisteam, maar denk zeker ook aan communicatie. Vragen van klanten die zich zorgen maken, moeten worden beantwoord.

3. Werk samen
“Het leger waar we tegen vechten is veel groter”, stelt Van Oirschot. Om enige kans te maken, moet de verdediging beter samenwerken. Bijvoorbeeld door dreigingsinformatie en best practices actiever met elkaar te delen. “Die samenwerking is nu nog wel wat versnipperd”, merkt Slootmaker op. Van Oirschot: “De overheid zou daar meer de regiefunctie moeten pakken.”

Vaart maken
Van Oirschot en Slootmaker roepen bedrijven op om vaart te maken met de geschetste voorbereiding, want in alle onzekerheid is er helaas ook een zekerheid. “Het aantal aanvallen zal blijven toenemen, mede door het aanvalsoppervlak dat door onder andere thuiswerken groter wordt”, aldus Van Oirschot.

Kijkend naar de eigen organisatie ziet Slootmaker de toekomst met vertrouwen tegemoet. “We beschikken bijvoorbeeld over goed beveiligde werkplekken, een gelaagd defensiemodel en detectie- en responstooling waarmee we veel op tijd zien. Maar als ik dan kijk naar ransomwareaanvallen zoals bij de Universiteit Maastricht en Hof van Twente, dan krijg ik toch wel een zware steen op mijn maag. Bij dergelijke aanvallen ben je afgesloten van je bestanden en beland je direct in een ongekende crisissituatie.”

Paul Slootmaker heeft in zijn professionele loopbaan meerdere leidinggevende functies gehad op het gebied van cyberbeveiliging en informatierisicomanagement. Sinds 2019 is hij als CISO verantwoordelijk voor de security binnen KPN.

Marcel van Oirschot is een echte securityexpert. Zijn kennis van de securitymarkt heeft hij onder andere opgebouwd bij Fox-IT en bij IBM, waar hij verantwoordelijk was voor het securityportfolio in de Benelux. Sinds 2019 geeft hij als Executive Vice President leiding aan KPN Security.

kpn Security

» De zorg is voor hackers een nog relatief onontgonnen terrein. “Maar daar zien we snel verandering in komen”, waarschuwt Wim Hafkamp, directeur van Z-CERT, het computer emergency response team voor de zorgsector. Hoe voorkomen we dat cybercriminelen mensenlevens op het spel zetten? We vroegen het aan Hafkamp en de ‘hackende huisarts’ Jonathan Bouman.

Cybercriminelen ontdekken de zorg

Wim Hafkamp & **Jonathan Bouman**
Directeur, Z-CERT en Huisarts & ethisch hacker

Security-incidenten in de zorg, van grootschalige datadiefstallen tot ongeoorloofde inzage in dossiers, halen regelmatig het nieuws. Toch is Hafkamp van mening dat vergeleken met andere sectoren het aantal ‘serieus geslaagde incidenten in de zorg’ nog meevalt. “Maar ik heb wel de indruk dat cybercriminelen de zorg aan het ontdekken zijn. We zien binnen de zorgsector een flinke toename in het aantal phishing- en malware-incidenten.”

Gerichte aanvallen
Als voorbeeld geeft de directeur de gijzelsoftware Ryuk die de zorgsector in de Verenigde Staten eind 2020 hard trof. “We zagen toen gerichte aanvallen op ziekenhuizen. Ook zien we dat succesvolle malware uit het verleden opnieuw wordt ingezet, maar dan gericht op de zorg. Een voorbeeld daarvan is de opleving van Emotet in 2020.” Deze van oorsprong ‘banking trojan’ werd toen ook waargenomen door Nederlandse ziekenhuizen.

Het is volgens Hafkamp niet met zekerheid te zeggen waarom hackers het in toenemende mate op zorg hebben gemunt. “Dat zou je eigenlijk die hackers moeten vragen”, aldus de directeur. “Maar ik denk dat digitalisering zeker een rol speelt. Met name aan de cure-kant wordt de afhankelijkheid van ICT steeds groter, en de digitale ketens tussen instanties worden steeds belangrijker. Data springen van hub naar hub. Dat hebben cybercriminelen ook in de gaten. Zij weten: daar valt iets te halen, en daar kunnen we geld mee verdienen.”

Zorg is fragiel

Jonathan Bouman, parttime huisarts en als ‘healing hacker’ verbonden aan het Z-CERT, ziet de toenemende belangstelling van cybercriminelen voor de zorg als een bedreiging voor zijn relatie met de patiënt. “Vertrouwen is in mijn vak de basis. Je komt naar me toe, vertelt me van alles, en ik zet het in die computer. Maar wat vertel je nog als je het gevoel hebt dat informatie vervolgens op straat belandt? Als het vertrouwen verdwijnt, wordt mijn werk bijzonder complex. De zorg is in dat opzicht heel fragiel.”

“En vergeet niet dat bij een verstoring van digitale processen in bijvoorbeeld een ziekenhuis mensenlevens op het spel kunnen staan”, vervolgt Hafkamp. Zo werd het Universitair Medisch Centrum in het Duitse Düsseldorf september vorig jaar geraakt door wat de boeken in ging als ‘de eerste ransomwareaanval met dodelijke afloop’. “Die claim kunnen wij niet hardmaken, maar het is wel duidelijk dat het ziekenhuis hard werd geraakt. Het zijn signalen dat we alert moeten zijn.”

Grote samenhorigheid

Volgens Hafkamp timmert de zorg al hard aan de weg als het gaat om digitale beveiliging. “Ik ben blij verrast door de samenhorigheid in de sector. Het aantal deelnemers aan Z-CERT groeit snel en er is een grote bereidheid om best practices, kennis en ervaringen met elkaar te delen. Het ZorgDetectieNetwerk – voor het delen van informatie over malware, phishing en cyberspionage – is een goed voorbeeld van hoe snel dingen kunnen gaan. In drie maanden tijd sloten zich vijftig ziekenhuizen aan bij dit nieuwe netwerk.”

“Het delen van informatie kan in het begin heel erg eng zijn”, weet Bouman. “Ga ik echt vertellen wat er bij mijn organisatie verkeerd is gegaan? En hoe ga ik dat doen? Maar kennis delen is echt ontzettend belangrijk. Daarin schuilt veel kracht. Het draagt bij aan een betere beveiliging.”

Basishygiëne

Er is echter ook nog genoeg ‘werk aan de winkel’. Hafkamp: “Cybersecurity is een onderwerp dat in de zorg op de bestuurstafel moet komen te liggen. Bestuurders moeten in control zijn over het gehele informatiebeveiligingsvraagstuk. Dat besef is er nog niet overal. Een doorvertaling naar meer budget en meer mensen komt vaak pas na een incident. Omdat het om mensenlevens gaat, is het beter om incidenten voor te zijn.”

Volgens de directeur is het op orde brengen van de ‘basisbeveiliging’ een goed begin. “Met een basishygiëne voorkom je misschien geen geavanceerde aanvallen, maar wel heel veel andere ellende. Het mooie is dat de zorg met de NEN 7510 een specifieke norm heeft voor informatiebeveiliging Daar staan zeer praktische zaken in, zoals de inrichting van multifactorauthenticatie. Als je die opvolgt, heb je al heel veel gewonnen.”

Threat modelling

Als het aan Bouman ligt, komt er ook meer aandacht voor threat modelling. Zorgprofessionals moeten beter in staat zijn om dreigingen zoals het ontbreken van een passende beveiliging te identificeren. “Ik verwacht niet dat zorgprofessionals security-audits kunnen uitvoeren, maar ze moeten wel een globaal beeld hebben van hoe een hacker denkt en wat er nodig is om bijvoorbeeld een applicatie veilig te gebruiken. Mijn hoop is dat threat modelling uiteindelijk wordt toegepast op alle zorgprocessen waarin automatisering een rol speelt.”

“En blijf systemen en programmatuur testen. Er zullen altijd bugs zijn. Daar moet je continu alert op blijven”, vervolgt Bouman. Ook hecht het computer emergency response team voor de zorg veel waarde aan red teaming. Hafkamp: “Je kunt beter worden aangevallen door een red team, dan dat je slachtoffer wordt van een echte hack. En door een realistische aanval te simuleren, open je ook weer ogen.”

Coordinated Vulnerability Disclosure

Soms ontdekken ethical hackers ‘ongevraagd’ kwetsbaarheden in websites, apparatuur of programmatuur van de deelnemers aan Z-CERT. Daar kunnen ze een Coordinated Vulnerability Disclosure (CVD)-melding van doen. Z-CERT neemt deze meldingen over van haar deelnemers en regelt de communicatie met de hackers. In 2020 ging het in totaal om 75 meldingen van ontdekte kwetsbaarheden bij zorginstellingen.
Als het aan Hafkamp ligt, wordt dat aantal in 2021 overtroffen. Een melding betekent dat er beschermende maatregelen kunnen worden getroffen. “Het kunnen er nooit genoeg zijn, dus kom maar op. Ik denk dat de 75 meldingen in 2020 ook nog maar het topje van de ijsberg vormden. Als er gericht wordt gezocht, wordt er ook meer gevonden.”

Wim Hafkamp is op 1 april 2020 gestart als directeur van Stichting Z-CERT. Daarvoor was hij als plaatsvervangend directeur werkzaam bij het Nationaal Cyber Security Centrum. Bij de Rabobank bekleedde hij gedurende ruim twintig jaar verschillende securityfuncties, waaronder die van CISO.

Jonathan Bouman is naast huisarts ook beveiligingsonderzoeker en mede-oprichter van het CMIO Netwerk Eerste Lijn. Als ‘healing hacker’ treedt hij op als ambassadeur van Z-CERT.

kpn Security

» COVID-19 – en de oproep om thuis te werken – heeft de cloudadoptie in een stroomversnelling gebracht. Peter Sandkuijl, VP Engineering EMEA, Check Point bij Check Point Software Technologies, ziet zelfs een ‘hockeystickcurve’ waardoor ook het aantal bedrijven dat ‘alles in de cloud doet’ snel toeneemt. “Voor die bedrijven draait het niet meer om het netwerk, maar om de applicaties. Dat betekent ook dat je anders na moet gaan denken over security.”

Wie heeft in de cloud **nog een helicopterview?**

Peter Sandkuijl
VP Engineering EMEA, Check Point

Sandkuijl onderscheidt drie fases in de adoptie van de cloud. In de eerste fase is er vooral sprake van ‘lift and shift’. Applicaties worden opgepakt en verplaatst naar de cloud. “In een volgende fase omarmen bedrijven de waarde van de cloud, en automatiseren ze processen door met API’s koppelingen te maken.” Het overgrote deel van de bedrijven bevindt zich nu nog in deze eerste twee fases. Het aantal bedrijven in de derde fase neemt volgens de SE Director van Check Point echter snel toe.

“In die derde fase gebruiken bedrijven simpelweg alle cloud-services die beschikbaar zijn, van verschillende cloudproviders. Ze hebben zelf geen applicaties meer, maar code en die draaien ze op een functie die je serverless noemt”, legt Sandkuijl uit. “Waar ze voorheen bijvoorbeeld een eigen DNS-server draaiden, roepen ze nu via een API een dienst als Route 53 van Amazon Web Services aan. Want waarom zou je een DNS-omgeving nog zelf bouwen en beheren? Makes sense.

Aandachtsgebieden
“Het zijn van die vraagstukken waar bedrijven eerder nooit bij stil hebben gestaan, maar waar ze wel iets mee moeten”, concludeert Sandkuijl. De SE Director EMEA adviseert bedrijven om onder andere stil te staan bij deze vier aandachtsgebieden:

1. Interne securitypolicy’s
“Stel, je hebt eerder bepaald dat een database niet met het internet mag communiceren en dat data geëncrypteerd moeten zijn? Hoe weet je zeker dat nog steeds aan die policy’s wordt voldaan als er geen sprake meer is van een gateway in een eigen datacenter?”

Die vragen zijn bijvoorbeeld te beantwoorden met behulp van Cloud Security Posture Management. Een dergelijke oplossing waarschuwt organisaties over risicovolle configuratiefouten en kwetsbaarheden in cloudinfrastructuren. “Dan kijk je via de metadata van de cloud naar de status van de systemen die daarin staan, en kun je onder andere achterhalen of er daadwerkelijk encryptie wordt toegepast. Het is een 24/7 monitoring op je nieuwe bedrijfsomgeving om de dreigingen te ondervangen waar je voorheen nog niet mee te maken had.”

2. Identity and Access Management
Volgens Sandkuijl wint Identity and Access Management (IAM) door de cloud aan belang. “Op een kantoor waren de toegangsrechten meestal wel geregeld. De context waarbinnen een gebruiker toegang nodig had, was meestal wel duidelijk. Binnen de muren van het pand waren applicaties – die vaak niet communiceerden met het internet – bovendien beter af te schermen.”

“In de cloud is alles gebaseerd op identiteiten”, zegt Sandkuijl stellig. “Op basis van wie je bent, wie je op dít moment bent en je context wordt bepaald of je toegang hebt tot data of applicaties. Dat Identity and Access Management wordt nog te vaak los ingeregeld. Door code te scannen kun je erachter komen welke permissies welke functies hebben en waarom.”

3. Endpointsecurity
“Naast toegangscontrole wordt ook de status van het device waarmee je connectie maakt steeds belangrijker”, vervolgt Sandkuijl. “Zo zou je kunnen inrichten dat een gebruiker met een goed beveiligde laptop meer toegangsrechten krijgt dan een gebruiker met een privésmartphone.”

Volgens Sandkuijl neemt de vraag naar endpointsecurity en veilige remote access dan ook snel toe. “En dat omvat meer dan alleen het installeren van een antivirusclientje.” Check Point kan de devices van Azure-gebruikers bijvoorbeeld aan een ‘compliancecheck’ onderwerpen. Via Microsoft Intune, een clouddienst voor Mobile Device Management en Mobile Application Management, wordt dan gecontroleerd of het device op het juiste beveiligingsniveau is. “Als dat het geval is, geven we een VPN-verbinding vrij.”

4. Inzicht en intelligence
Bij de meeste bedrijven zal sprake zijn van een multicloud, waarin clouddiensten van verschillende providers met elkaar worden gecombineerd. “Dan moet je niet alleen een beeld hebben van bijvoorbeeld de status van je systemen en de kwaliteit van je code in die verschillende clouds, maar ook een beeld hebben van hoe aanvallen per cloudplatform verlopen. Het gaat wederom om die helicopterview. Die moet je hebben over je gehele landschap.”

“Met een ‘Cloud Checkup’ kunnen we bijvoorbeeld precies laten zien wat er in zo’n multicloudomgeving gebeurt”, besluit Sandkuijl. “Er moet één beeld zijn, met één uniform securitybeleid. Vervolgens kunnen we kijken wat ervoor nodig is om op een veilige manier in de cloud te opereren. Hoe zorgen we ervoor dat developers veilig nieuwe applicaties kunnen uitrollen, en de bedrijfscontinuïteit gewaarborgd blijft? Dat gesprek aangaan, is erg belangrijk. Als security moeten we niet de afdeling van ‘no’ worden.”

“In de cloud is alles gebaseerd op identiteiten.”

Netwerksegmentatie in de cloud?
Toch moet Sandkuijl daar wel een kanttekening bij plaatsen: die derde fase brengt ook nieuwe uitdagingen op het gebied van beveiliging met zich mee. Op de eerste plaats verandert het standaard netwerkmodel drastisch. “Er is nog wel een netwerk, maar dat beheer je niet meer zelf. En daardoor is er geen ‘visuele mapping’ meer die helpt om te begrijpen waar welke pakketjes naartoe gaan, en wat die pakketjes op een bepaald punt in het netwerk mogen. Dat inzicht is nog wel nodig voor security.”

“In de oude situatie werd een applicatie in een datacenter in een demilitarized zone geplaatst, en kwamen de data voor inspectie uit bij een firewall”, vervolgt Sandkuijl. “Er was sprake van een segmentatie tussen database en applicatieserver. De noodzaak voor segmentatie is er nog steeds, maar weet je zeker dat daar nog steeds sprake van is nu het netwerk is opgeheven? In de cloud drukt de developer op een knopje waarna een nieuwe machine live is, zonder dat er sprake is van changemanagement.”

Is de code wel veilig?
Een andere uitdaging schuilt in de veiligheid van code. “Applicaties worden niet meer monolitisch opgebouwd en pas opgeleverd als er een 1.0-versie is. Ontwikkelaars linken naar soms wel tientallen projecten op Github om zo een eigen applicatie op te bouwen. Op die manier kunnen ze een applicatie sneller en goedkoper op de markt brengen.”

In deze werkwijze schuilt echter ook een gevaar. “Als applicatiebouwer heb je zelf niet de controle over de projecten die je opneemt. Het kan zelfs zo zijn dat een project eigendom is van een hacker die er een backdoor in heeft verstopt. Wie heeft dan nog een helicopterview? Wie kan dan nog zeggen dat een applicatie goed en veilig is ontwikkeld en geen backdoor bevat?”

Peter Sandkuijl is al ruim 25 jaar actief in de securitymarkt, en is sinds 2000 werkzaam voor Check Point. Als SE Director EMEA geeft hij bij Check Point leiding aan een team van 300 system engineers en heeft hij een actieve rol bij het delen van informatie.

» Security is door allerlei maatschappelijke en technologische ontwikkelingen uitgegroeid tot een ingewikkelde, meerlaagse discipline. Met de hulp van AI, automation, een goede integratie en de juiste mindset kunnen organisaties veel winnen, betoogt Vincent Zeebregts, Country Manager Netherlands bij Fortinet. “Security-by-design is cruciaal geworden.”

Chaos is de grootste **vijand van security**

Vincent Zeebregts
Country Manager Netherlands, Fortinet

De wereld is de afgelopen tijd enorm veranderd. De grenzen van het traditionele bedrijfsnetwerk zijn vervaagd. Werken doen we niet enkel en alleen meer achter de centrale firewall. De term BYOD doet geen wenkbrauwen meer fronsen, en steeds meer mensen laten de cloudwatervrees achter zich. Afgelopen jaar heeft de coronacrisis die veranderingen in een stroomversnelling gebracht. Thuiswerken is onderdeel van het ‘nieuwe normaal’ geworden.

Het resultaat? We werken steeds vaker waar we willen, hoe we willen, met het apparaat naar keuze. Dat is vanuit functioneel oogpunt fantastisch. Maar vanuit IT-securityoogpunt zorgen al die lagen, systemen, locaties, providers en een keur aan al dan niet mobiele apparaten voor een grote chaos. Een chaos die volgens Zeebregts zonder speciale hulpmiddelen nauwelijks nog te overzien is.

Lappendeken
“Veel organisaties hebben in de loop der jaren allerlei securityvoorzieningen verzameld. Een firewall, e-mailsecurity, misschien een oplossing voor endpointsecurity. Bij veel organisaties zijn dat bovendien puntoplossingen waarbij integratie ontbreekt.” Die lappendeken van securityvoorzieningen geeft in het beste geval overbodige overlap, maar zorgt minstens zo vaak voor gevaarlijke gaten.

“Al die oplossingen genereren enorme hoeveelheden logs, over een in toenemende mate complexe IT-omgeving. Als IT- of securityofficer moet je daaruit zinnige conclusies gaan trekken. Dat is niet te doen. Securityofficers dreigen daarmee het overzicht te verliezen. Met alle mogelijke gevolgen van dien.”

Intelligentie en automatisering
Zeebregts pleit dan ook voor het toevoegen van intelligentie in de securitystack, bijvoorbeeld via AI en machine learning. Daarmee kunnen securityvoorzieningen bijvoorbeeld verbanden leggen tussen gebeurtenissen die op zichzelf onschuldig lijken. De verschillende onderdelen moeten daarbij wel met elkaar kunnen communiceren. “Denk aan een situatie waarin een endpointsecurityoplossing op een smartphone een besmetting detecteert. Dan wil je eigenlijk dat die endpointoplossing die bevinding automatisch communiceert met de firewall, zodat het toestel op het netwerk geen verdere schade kan aanrichten. Dat is met een best-of-breedstrategie van puntoplossingen lang niet altijd mogelijk.”

Ook automation is tegenwoordig haast een noodzaak geworden. “Securitykennis is enorm schaars. Je moet beschikbare menselijke resources zo efficiënt mogelijk benutten. Gelukkig kun je met automation heel veel taken wegnemen.” Securityvoorzieningen moeten volgens hem bijvoorbeeld zelfstandig en proactief mogelijke gevaren kunnen detecteren, nader onderzoeken en prioriteren. “Denk bijvoorbeeld aan het automatisch plaatsen van een binnenkomende verdachte e-mail in een sandboxomgeving”, licht Zeebregts toe.

Mindset
Security is niet alleen een zaak van planning en techniek. Het belang moet ook daadwerkelijk ‘top of mind’ zijn. Toch is die noodzaak voor security nog lang niet bij iedereen doorgedrongen. “De datacenter- en IT-manager beseffen de noodzaak van security nog wel. Zij beschouwen het steeds vaker als een integraal onderdeel van IT, en hun werkzaamheden. Maar dankzij met name de cloud is er een hele nieuwe groep gebruikers ontstaan, die in de eerste plaats naar de functionaliteit kijkt. Bijvoorbeeld devops-teams. Voor hen moet het vooral gewoon werken.”

Volgens Zeebregts moet je juist die mensen bewust maken van security. “Sommigen verwachten dat security een zaak is van de cloudprovider. ‘Die zal het wel regelen’, is de gedachtegang.” In de praktijk is dat slechts deels waar, waarschuwt hij. “Cloudproviders hebben inderdaad vaak allerlei veiligheids-voorzieningen genomen. Maar alles wat je bovenop die cloud zet, en hoe je vervolgens die cloud gebruikt, daar ben je als organisatie zelf verantwoordelijk voor. Steeds meer providers bieden kant-en-klare oplossingen waarin security is geïntegreerd, zoals Secure SD-WAN. Maar die lijn van security-integratie moet je wel doortrekken in je eigen processen. Security-by-design is cruciaal geworden en wint alleen maar aan belang.”

Bovendien zorgt het gebruik van de cloud nog voor een andere dimensie. Vaak blijft het niet bij een cloudomgeving of een cloudprovider. De multicloud heeft volgens Zeebregts steeds meer organisaties bereikt. “Je krijgt daarmee te maken met een wirwar van verschillende beveiligingsmiddelen die deze cloudproviders hebben ingezet. Je zult dat wel op de een of andere manier moeten orkestreren. Ook dat is je eigen verantwoordelijkheid.”

Stip op de horizon
Die harmonisering van de securitystack en het inherent veilig maken van processen is geen vrijdagmiddagklus. Organisaties beginnen bovendien zelden helemaal op nul. Ze hebben in de loop der jaren geïnvesteerd in allerlei oplossingen. “Ik begrijp dat organisaties niet al hun eerdere investeringen teniet willen doen”, merkt Zeebregts op. “In de praktijk is dat vaak ook niet nodig. Mijn advies is: maak een nulmeting. Zet vervolgens een stip op de horizon. Waar wil ik heen? Werk vervolgens geleidelijk toe naar dat doel met een uitgedacht securityontwerp, maar zorg dat de securitystack een geconsolideerd geheel blijft.”

Uniformiteit is belangrijk voor het bestrijden van chaos. “Een klant van ons werkt met grotendeels zelfstandig opererende vestigingen. Voor de security maken zij een uitzondering, en met goede reden. Die consolidatieslag betekent overigens niet dat alle securityoplossingen per se uit één stal moeten komen. “Een vendor lock-in is niet wenselijk, en technisch gezien ook lang niet altijd een noodzaak. Zolang je maar oplossingen kiest die met elkaar kunnen communiceren. Het moet vooral een geheel blijven. Chaos is de grootste vijand van security.”

Vincent Zeebregts is Country Manager voor Nederland bij Fortinet en heeft meer dan 20 jaar aan channel-, marketing- en managementervaring in netwerken, cloud en endpointsecurity. De kennis die Vincent heeft vergaard in de afgelopen jaren bij bedrijven zoals Imtech ICT en McAfee, maken hem een expert op het vlak van cybercrime en securitytrends. Vincent ervaart iedere dag wat er gebeurt op de securitymarkt en met welke belangrijke problemen klanten worstelen.

» Het duurt nog wel even voordat we met een kwantumcomputer op zak lopen. Toch zijn er al hier en daar veelbelovende initiatieven. Zo ontwikkelt KPN momenteel samen met andere partijen een kwantumnetwerk. “Binnen enkele jaren kunnen organisaties quantum networking en quantum computing als service afnemen”, voorspelt Victoria Lipinska, Quantum Advisor bij KPN. Dat is goed nieuws, want kwantumcommunicatie is niet te kraken.

Kwantum-technologie **komt als service beschikbaar**

Victoria Lipinska
Quantum Advisor, KPN CISO

De meeste verbindingen op het reguliere internet zijn beveiligd met een zogeheten ‘asymmetrische versleuteling’. Iedere buitenstaander kan in theorie de verbinding met de juiste sleutel weer leesbaar maken en zo de communicatie onderscheppen. De veiligheid van zo’n verbinding is echter gebaseerd op een wankel uitgangspunt: het idee dat het kraken van die sleutel enorm lastig is. Met genoeg tijd en/of rekenkracht is het echter wel degelijk mogelijk.

Qubits
Kwantumcommunicatie kent die beperking niet. Dat komt vanwege enkele bijzondere eigenschappen van kwantumprocessoren. Die werken net even anders dan ‘normale’ binaire computers, legt Lipinska uit. “Traditionele processoren zijn gebaseerd op bits. Die zijn altijd of 0, of 1. Iets is waar, of niet. In een kwantumprocessor ligt dat anders. De werking van deze processor berust op een beschrijving van de staat van kwantumdeeltjes, een van de kleinste deeltjes van ons universum. We noemen die beschrijving ‘qubits’. Deze qubits kunnen naast 0 of 1 ook beide tegelijk zijn. Althans, zo lang we ze niet waarnemen. Bij een waarneming verandert de staat direct naar 0 of 1.”

Met die qubits is nog wat bijzonders aan de hand. “Een kwantumdeeltje kan verstrengeld zijn met een ander quantum-deeltje, ook als ze fysiek van elkaar verwijderd zijn. In de praktijk betekent die verstrengeling dat ze elkaar spiegelen. Is de een 0 of juist 1, dan moet de ander dat ook zijn.”

Precies die eigenschap is enorm waardevol voor een veilige communicatie. “Stel dat op het netwerk twee individuen met elkaar communiceren: Alice en Bob. Beiden hebben een qubit die met de ander verstrengeld is. Stel dat je beide qubits naar hun status zou vragen. Ben je een 1 of ben je een 0? Het antwoord moet voor beide qubits altijd op ieder moment exact gelijk zijn, vanwege die verstrengeling.”

Onvoorspelbaar
Dat antwoord is bovendien niet van tevoren te voorspellen. “Stel je die vraag een aantal keer achter elkaar op willekeurige momenten, dan krijg je een willekeurige reeks van enen en nullen. Alice en Bob zouden een test kunnen doen om te zien of die reeks met elkaar matcht. Is dat niet het geval, dan weet je dat een derde partij meeluistert.”

Die verstrengeling van qubits is bovendien de basis voor geavanceerde protocollen. Bijvoorbeeld voor het volstrekt anoniem versturen van berichten. Ook maakt die eigenschap bijvoorbeeld het zeer nauwkeurig synchroniseren van klokken of het samenvoegen van telescopen mogelijk.

Snelle berekeningen
Kwantumnetwerken zijn niet het enige dat in het vat zit. Naarmate kwantumtechnologie zich verder ontwikkelt, groeit ook het aantal toepassingen. Qubit-chips hebben namelijk nog een voordeel: je kunt er enorm snelle berekeningen mee uitvoeren. “Dat geldt overigens niet voor alle type berekeningen”, nuanceert Lipinska. “Kwantumcomputers zijn bijzonder goed in factorisatie. Dat is de ontleding van een samengesteld getal in een product van kleinere gehele getallen. Zo is het nummer 15 te verdelen in de factoren 3 en 5, want 3 keer 5 is 15.”

De praktische toepassingen daarvan zijn enorm waardevol. “Denk aan het simuleren van de effecten van medicijnen op moleculair niveau. Het ontleden van getallen in factoren is echter ook de basis voor het versleutelen, en ontsleutelen van gegevens. Daarmee is een kwantumcomputer in theorie

een zeer gevaarlijk wapen in handen van cybercriminelen. Dat is een extra argument voor een kwantumnetwerk, want dat is niet gevoelig voor een aanval van een kwantumcomputer."

In ontwikkeling
Dat een kwantumnetwerk er komt, is zo goed als zeker. Er zijn wereldwijd diverse initiatieven waarin een dergelijk netwerk in de steigers staat. Ook in Nederland. KPN, QuTech (een samenwerking tussen TU Delft en TNO), SURF en OPNT zijn in 2019 een samenwerking hiervoor gestart. Het consortium bouwt momenteel een kwantumnetwerk waarbij meerdere kwantumprocessoren op diverse plekken in de Randstad via glasvezel aan elkaar zijn gekoppeld.

Zo'n inherent veilig netwerk is enorm welkom. Veel sectoren hebben baat bij honderd procent gegarandeerd veilige verbindingen. Denk aan de financiële sector, maar ook aan overheden en defensie. Bovendien zitten ook andere landen niet stil. China is volgens Lipinska het verst met deze technologie. "Zij gebruiken naast glasvezel ook satellieten voor de communicatie tussen kwantumprocessoren. Daarmee kunnen ze een grotere afstand overbruggen." In Europa worden inmiddels de eerste proeven met satellieten voorbereid.

Europese samenwerking
De diverse wereldwijde initiatieven delen op sommige fronten kennis uit, maar van een gemeenschappelijk, wereldwijd omspannend netwerk is nog geen sprake. "We zijn momenteel echt nog in de onderzoek- en testfase. Bovendien opereren de verschillende initiatieven momenteel nog min of meer zelfstandig, al zie je hier en daar wel samenwerkingen ontstaan voor het uitwisselen van kennis. Zo werken wij samen met diverse andere initiatieven in Europa in de EuroQCI. We werken gezamenlijk toe naar een Europees netwerk en wisselen kennis uit. Zo'n Europees netwerk moet de komende tien jaar vorm krijgen. Maar voor een wereldwijd kwantumnetwerk is meer nodig, zoals gemeenschappelijk aanvaarde protocollen. Zover is het allemaal nog niet." Een brede adoptie zal dan ook nog even op zich laten wachten. "Ik verwacht dat kwantumcommunicatie in eerste instantie als extra laag op het reguliere internet beschikbaar komt. Als eerste zullen ze waarschijnlijk gebruikt worden voor veilige communicatie tussen bijvoorbeeld landen, of voor defensiedoeleinden."

Twee verdiepingen
Op dit moment zijn ook kwantumcomputers nog geen gemeengoed. Ze zijn simpelweg te groot en te kostbaar voor brede adoptie. "De processor zelf is enkele vierkante centimeters groot, maar door de enorme koeling zijn sommige kwantumcomputers nu nog twee verdiepingen hoog. Het duurt dan ook nog wel even voordat organisaties zelf een kwantumcomputer kunnen aanschaffen. Maar de gigantische rekenkracht van zo'n systeem zou al veel eerder via de cloud breed beschikbaar kunnen komen."

Hoewel de brede beschikbaarheid van kwantumtechnologie nog even op zich laat wachten, kan het volgens Lipinska absoluut geen kwaad om nu al voorbereidingen te treffen. Vooral door het opdoen van kennis. "Verdiep je goed in de technologie, en vooral in de mogelijkheden ervan. Bedenk hoe veilige communicatie of enorme rekenkracht in je voordeel kan werken. Dan heb je straks een voorsprong."

Victoria Lipinska promoveerde in QuTech aan de TU Delft in de groep van Stephanie Wehner, gespecialiseerd in toepassingen voor vroege kwantumnetwerken. Daarvoor werkte ze op het gebied van kwantuminformatie in verschillende wetenschappelijke instituten in Europa, o.a. in Barcelona en Stockholm. Haar doel is om praktische en toegankelijke kwantumcommunicatie en een kwantuminternet werkelijkheid te laten worden.

kpn Security

» Securityprofessionals baseren hun besluitvorming vooral op risicoanalyses. Maar volgens dr. Martijn Dekker, CISO bij ABN AMRO, is deze werkwijze ingehaald door de realiteit. "De toekomst is fundamenteel onvoorspelbaar. Je kunt geen kansberekening loslaten op cyberincidenten. Daarvoor zijn de systemen die we proberen te beveiligen veel te complex geworden." Dekker pleit dan ook voor een nieuw model waarin onzekerheid centraal staat.

Informatie-beveiliging draait om het managen van onzekerheden

Dr. Martijn Dekker
CISO, ABN AMRO & Visiting Professor, UVA

"Het leven zit vol onzekerheden", zegt Dekker. "De coronacrisis heeft wel aangetoond dat de wereld om ons heen maar tot op zekere hoogte voorspelbaar is. Maatregelen worden ingevoerd en een week later al weer aangepast of ingetrokken. Dat is niet fout of stom, het is gewoon ontzettend moeilijk om beslissingen te nemen als er zoveel onzekere factoren zijn. Je weet niet hoe groot de kans is dat iets gebeurt of wat de impact daarvan is, laat staan hoe effectief een maatregel zal zijn."

De CISO ziet een parallel met zijn vakgebied informatiebeveiliging. "Cybersecurity draait in 2021 om besluitvorming in onzekere omstandigheden. Cyberincidenten zijn geen vaststaande gebeurtenissen die we kunnen voorkomen, en zelfs geen waarschijnlijke gebeurtenissen die we als risico's kunnen managen. Het is simpelweg onmogelijk om de kans op en de impact van een specifiek incident te berekenen. Wel kunnen we als CISO de onzekere factoren managen."

Van a priori naar a posteriori
Dekker beseft evenwel dat veel CISO's zich wel degelijk focussen op risicomanagement. "Dat is niet altijd zo geweest. Oorspronkelijk gingen securityprofessionals ervan uit dat alle mogelijke incidenten voorspeld konden worden, evenals de gevolgen voor het systeem dat ze probeerden te beveiligen. Op basis daarvan bouwden ze tegenmaatregelen in om deze incidenten te voorkomen. Feitelijk wilden we alle securitybeslissingen vooraf maken, zodat het systeem compleet veilig zou zijn." Soms werden systemen natuurlijk wel gehackt of bleken ze niet goed beveiligd. "Maar dat was dan meestal te herleiden naar een menselijke fout, zoals een programmeerfout. Via pentests en codecontroles hielden we de beveiliging op een acceptabel niveau. Deze strategie werd vanaf 2007 minder levensvatbaar. Steeds vaker zagen we gerichte aanvallen op specifieke systemen. Bovendien werden de systemen complexer en met elkaar

verweven, vooral vanwege de opkomst van internet."
Als gevolg hiervan was een 'a priori'-besluitvorming voor informatiebeveiliging niet meer realistisch of haalbaar. "Securityprofessionals moesten accepteren dat hacks en cyberincidenten niet altijd te voorkomen zijn, en overstappen op een strategie voor 'a posteriori'-besluitvorming", legt Dekker uit. "Dit resulteerde in een focus op detectie en respons, en de vorming van nieuwe securityteams. Voor deze strategie waren investeringen nodig en dus ook een businesscase."

Wat is de rol van de CISO?
Risicomanagement voorzag in deze behoefte. "Wellicht konden we berekenen hoe waarschijnlijk een bepaalde gebeurtenis was, en hoeveel operationele schade deze teweeg zou brengen. Zo werd het mogelijk om de kosten van security te rechtvaardigen. Inmiddels is risicomanagement een zeer breed gebruikte besluitvormingsmethode. We kunnen de toekomst niet voorspellen, maar we weten in ieder geval wel hoe waarschijnlijk alle verschillende toekomstscenario's zijn, toch?"

Dekker heeft hier zijn bedenkingen bij. "Veel organisaties hanteren het 3 lines of defence-model voor risicomanagement. Maar is de CISO dan primair verantwoordelijk voor de interne risicobeheersing (de eerste lijn) of meer ondersteunend en verantwoordelijk voor de structuur, kwaliteit en inrichting van het risicomanagement (de tweede lijn)? In mijn ervaring verschilt dit per organisatie. Soms valt de CISO in de eerste lijn, soms in de tweede en soms heeft het bedrijf twee CISO's: één in elke lijn."

"Waarom kunnen CISO's zich niet positioneren in dit model?", vraagt Dekker zich af. "Begrijpen we het model niet, of risicomanagement zelf? En hoe zit het met de risicobereidheid, ook wel risk appetite genoemd? Waarom vinden CISO's, inclusief mezelf, het zo lastig om een risicobereidheidsverklaring te formuleren?" Hij geeft een verklaring. "Ik denk dat informatiebeveiliging in de kern helemaal niet over risicomanagement gaat. Of in ieder geval zou de primaire aandacht elders moeten liggen."

"Het leven zit vol onzekerheden", zegt Dekker. "De coronacrisis heeft wel aangetoond dat de wereld om ons heen maar tot op zekere hoogte voorspelbaar is. Maatregelen worden ingevoerd en een week later al weer aangepast of ingetrokken. Dat is niet fout of stom, het is gewoon ontzettend moeilijk om beslissingen te nemen als er zoveel onzekere factoren zijn. Je weet niet hoe groot de kans is dat iets gebeurt of wat de impact daarvan is, laat staan hoe effectief een maatregel zal zijn."

De CISO ziet een parallel met zijn vakgebied informatiebeveiliging. "Cybersecurity draait in 2021 om besluitvorming in onzekere omstandigheden. Cyberincidenten zijn geen vaststaande gebeurtenissen die we kunnen voorkomen, en zelfs geen waarschijnlijke gebeurtenissen die we als risico's kunnen managen. Het is simpelweg onmogelijk om de kans op en de impact van een specifiek incident te berekenen. Wel kunnen we als CISO de onzekere factoren managen."

Van a priori naar a posteriori
Dekker beseft evenwel dat veel CISO's zich wel degelijk focussen op risicomanagement. "Dat is niet altijd zo geweest. Oorspronkelijk gingen securityprofessionals ervan uit dat alle mogelijke incidenten voorspeld konden worden, evenals de gevolgen voor het systeem dat ze probeerden te beveiligen. Op basis daarvan bouwden ze tegenmaatregelen in om deze incidenten te voorkomen. Feitelijk wilden we alle securitybeslissingen vooraf maken, zodat het systeem compleet veilig zou zijn." Soms werden systemen natuurlijk wel gehackt of bleken ze niet goed beveiligd. "Maar dat was dan meestal te herleiden naar een menselijke fout, zoals een programmeerfout. Via pentests en codecontroles hielden we de beveiliging op een acceptabel niveau. Deze strategie werd vanaf 2007 minder levensvatbaar. Steeds vaker zagen we gerichte aanvallen op specifieke systemen. Bovendien werden de systemen complexer en met elkaar

Beperkingen van risicomanagement
"Informatiebeveiliging in 2021 draait niet om het managen van risico's, maar van onzekerheden", stelt de CISO van ABN AMRO. "We moeten accepteren dat de toekomst onvoorspelbaar is, en niet eens probabilistisch. We weten niet hoe groot de kans op een specifiek incident is, of wat de impact daarvan zal zijn. Het is ook niet zo dat we het wél zouden kunnen weten als we het beter meten. Nee, de gebeurtenissen waar wij ons als CISO zorgen over maken, hébben geen kansverdeling."

Wat is dan precies het verschil tussen risico's en onzekerheden? Dekker licht de definities toe: "Elk risico is een onzekerheid, maar niet alle onzekerheden zijn een risico. We mogen onzekerheid ook niet verwarren met staartrisico of 'tail risk'. Risicomanagers hebben deze term geïntroduceerd voor de statistisch zeer kleine kans op extreme gebeurtenissen met een enorme impact. Denk hierbij aan een natuurramp of een pandemie zoals de coronacrisis. Maar een staartrisico is nog steeds een risico."

Volgens Dekker geeft risicomanagement ons een gevoel van controle. "Dat vinden we fijn. Je zou kunnen zeggen dat risicomanagement een goede benadering van onzekerheidsmanagement is, maar dat klopt niet. CISO's hebben niet de luxe om zich te beperken tot risico's. Want dan focussen we ons alleen op wat we weten uit het verleden. Maar soms is een getroffen systeem te complex om de volledige impact te overzien. Of de kans dat iets gebeurt is nul, tot een vijand een nieuwe aanval bedenkt."

Model met causale verbanden
Het managen van onzekerheden is nog moeilijker dan risicomanagement. "Een CISO heeft hiervoor een model van de wereld nodig dat de verschillende actoren en hun drijfveren in kaart brengt, evenals de causale verbanden. Incidenten vinden niet alleen willekeurig plaats; er zijn ook zeer gemotiveerde aanvallers met een specifiek doel of doelwit. De wereld draait dus niet om correlaties tussen willekeurige variabelen, maar om diepgaande causale relaties. Om oorzaak en gevolg."
Wat betekent dit concreet voor de securitystrategie? Volgens Dekker verandert de manier waarop de CISO omgaat met data. "Vanuit securitymonitoring verzamelen we enorm veel data, om vervolgens gebeurtenissen met elkaar te correleren. De hoeveelheid data zien we als een indicator van vooruitgang. Maar zo werkt het managen van onzekerheden niet. Dataverzameling leidt altijd tot 'observer bias'. Gebeurtenissen die eenvoudig waarneembaar zijn, krijgen prioriteit boven gebeurtenissen die moeilijker te zien zijn."

"CISO's moeten zich bewust zijn van deze bias en een sensor- en samplingstrategie definiëren die gebaseerd is op het eerder genoemde model van de wereld", vervolgt hij. "Op deze manier kunnen zij de juiste data verzamelen met de juiste samplingrate, om zo bias in de datasets te voorkomen. Dit zijn complexe begrippen die wellicht nieuw zijn voor securityprofessionals. Maar een moderne CISO moet ze echt toepassen, in combinatie met een constante focus op het onbekende."

Tijd voor de CISO Universalis
Dekker benadrukt dat de rol van de CISO over de jaren al veel is veranderd. "Vroeger was de CISO een technologieleider, nu zijn we businessleiders. Dat vroeg om nieuwe vaardigheden, zoals het vermogen om te communiceren met niet-professionals en het onderbouwen van investeringen richting het hoger management. En nu moeten we ons ook elementen meester maken uit andere disciplines zoals besluitvorming, psychologie, speltheorie en de levenswetenschappen."

Hij noemt deze nieuwe rol de 'CISO Universalis'. "Als een ware duizendpoot moeten we een diepgaande kennis hebben van allerlei onderwerpen, en deze inzichten integreren in onze strategieën. Dat is niet altijd makkelijk. Toch moeten we de complexiteit en het onbekende juist omarmen. Onze tegenstanders doen dat immers ook."

"Cybersecurity draait in 2021 om besluitvorming in onzekere omstandigheden."

Dr. Martijn Dekker werd in 2014 benoemd tot CISO bij ABN AMRO. Hij is verantwoordelijk voor het definiëren, implementeren en bewaken van de informatiebeveiligingsstrategie van de bank. Naast zijn rol bij ABN AMRO is Dekker lid van de raad van commissarissen van Stater N.V. Ook is hij lid van de adviesraad van het NCSC en van de ICT-adviesraad van het CBS. Sinds begin 2010 is Dekker deeltijds visiting professor information security aan de Universiteit van Amsterdam.

» Kennis is een machtig wapen in de strijd tegen cyberincidenten. Organisaties zouden daarbij volgens Petra Oldengarm niet zelf continu het wiel hoeven uitvinden. Als directeur van Cyberveilig Nederland maakt ze zich hard voor een open klimaat en meer samenwerking op dit gebied. “Als je weet wat je buurman is overkomen, kan je zelf gerichtere maatregelen nemen.”

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

Delen van kennis kan en moet beter

Petra Oldengarm
Directeur Cyberveilig Nederland

Security is volgens Oldengarm een technisch complex werkveld, met geavanceerde technieken en strategieën in zowel de aanval als de verdediging. Kennis heeft daardoor een grote intrinsieke waarde. Het is bovendien een werkveld waar je van elkaars incidenten en vergaarde informatie kunt gebruikmaken. Oldengarm maakt de vergelijking met de fysieke beveiligingswereld. “Wanneer je tijdens een inbraakgolf een camera op je voortuin hebt gericht, dan kan daar informatie uitkomen die ook voor buurtbewoners waardevol is. Wanneer er bij jou ingebroken wordt en je deelt die informatie niet, dan is de kans veel groter dat de volgende dag je buurman hetzelfde overkomt. Zo werkt het voor cybersecurity ook.”

Detectie en respons
Dat delen van informatie gebeurt helaas nog veel te weinig, constateert Oldengarm. Dat heeft gevolgen voor de staat van cybersecurity binnen Nederland. “Er gaat nog veel te weinig aandacht uit naar detectie en respons. De aandacht gaat vooral uit naar het voorkomen van incidenten. Dat is echt niet meer genoeg. Het is niet de vraag of, maar wanneer je als organisatie slachtoffer wordt. Detectie en respons is daarom net zo onmisbaar als preventie.” Dat inzicht wil volgens haar maar moeilijk landen. “Dat heeft ook te maken met die beperkte kennisdeling, organisaties houden vaak de afhandeling en nasleep van een incident binnen de eigen muren.”
Die gesloten, naar binnen gekeerde houding blijft niet zonder gevolgen. Zo was een phishingmail gericht aan de Universiteit Maastricht de aanzet voor een ernstige ransomwarebesmetting. De aanval dwong een groot aantal systemen op de knieën, waardoor onderzoek en onderwijs enige tijd stilvielen. De universiteit moest kiezen tussen twee kwaden: of het betalen van 197.000 euro, of een maand de poorten sluiten.

Na enige tijd verscheen een onderzoekrapport van het incident. Daaruit kwam een aantal opvallende zaken naar voren. Zo waren er onvoldoende preventieve maatregelen genomen. Twee maanden eerder was de Universiteit Leuven echter al slachtoffer van een soortgelijke aanval. “Was die kennis gedeeld, dan was het incident wellicht voorkomen of had misschien minder ernstige consequenties gehad.

Transparantie
Overigens is Oldengarm wel te spreken over de openheid die de Universiteit Maastricht toonde tijdens de nasleep van de besmetting. “Zowel in de media als op de eigen website verschenen regelmatig updates over de afhandeling van het incident. Ik hoop dat dat voorbeeld veel vaker wordt opgevolgd.

Organisaties zijn lang niet altijd even transparant over hun incidenten. Ze voeren de onderzoeken vaak achter gesloten deuren uit en houden de gevolgen zoveel mogelijk stil.
Security is volgens Oldengarm een technisch complex werkveld, met geavanceerde technieken en strategieën in zowel de aanval als de verdediging. Kennis heeft daardoor een grote intrinsieke waarde. Het is bovendien een werkveld waar je van elkaars incidenten en vergaarde informatie kunt gebruikmaken. Oldengarm maakt de vergelijking met de fysieke beveiligingswereld. “Wanneer je tijdens een inbraakgolf een camera op je voortuin hebt gericht, dan kan daar informatie uitkomen die ook voor buurtbewoners waardevol is. Wanneer er bij jou ingebroken wordt en je deelt die informatie niet, dan is de kans veel groter dat de volgende dag je buurman hetzelfde overkomt. Zo werkt het voor cybersecurity ook.”

Detectie en respons
Dat delen van informatie gebeurt helaas nog veel te weinig, constateert Oldengarm. Dat heeft gevolgen voor de staat van cybersecurity binnen Nederland. “Er gaat nog veel te weinig aandacht uit naar detectie en respons. De aandacht gaat vooral uit naar het voorkomen van incidenten. Dat is echt niet meer genoeg. Het is niet de vraag of, maar wanneer je als organisatie slachtoffer wordt. Detectie en respons is daarom net zo onmisbaar als preventie.” Dat inzicht wil volgens haar maar moeilijk landen. “Dat heeft ook te maken met die beperkte kennisdeling, organisaties houden vaak de afhandeling en nasleep van een incident binnen de eigen muren.”

Vaak is dat uit angst voor gezichtsverlies. Ik denk dat juist een transparante, open houding bijdraagt aan meer vertrouwen van het publiek. Juist als het is misgegaan.” Onderzoek bevestigt die stelling. “Uit een Amerikaans onderzoek blijkt dat de marktwaarde van een organisatie maar 1 of 2 procent daalt na de bekendmaking van een datalek.”

Balans
Cyberveilig Nederland, de Nederlandse brancheverenigingen van securitybedrijven, werkt actief aan het stimuleren van kennisdeling tussen securitybedrijven onderling en tussen securitybedrijven en ander organisaties, zoals de overheid en CERT’s. Die kennisuitwisseling is heel waardevol, want securitybedrijven zitten bovenop de materie. De sector voert vrijwel dagelijks securityonderzoeken uit, zoals pentesting en audits. Die data zijn waardevol voor de klanten van de securitybedrijven, maar ook voor de Nederlandse samenleving als geheel.

Toch is die kennisdeling binnen de securitysector niet vanzelfsprekend. “Ik merk dat veel securitybedrijven in eerste instantie wat terughoudend zijn, alle goede bedoelingen ten spijt. Dat is begrijpelijk, security is hun verdienmodel en klanten willen vaak dat hun identiteit beschermd blijft. Het delen van kennis en inzichten met concurrenten ligt dan vanuit businessperspectief niet voor de hand. Het dan ook veel interessanter om te kijken wat er wel kan.”

Volgens Oldengarm is het daarbij heel belangrijk om organisaties ervan te overtuigen waarom ze hun kennis en inzichten zouden moeten delen. “Organisaties moeten beseffen dat ze niet alleen hun eigen kennis delen, maar daar ook enorm veel voor terugkrijgen. Daarvoor zullen ze wel eerst zelf moeten investeren. Bedrijven willen wellicht eerst iets krijgen, voordat ze wat geven. Maar ik denk dat kennisdeling een kwestie is van eerst tien keer iets geven voordat je wat terugkrijgt. Dat vraagt om een enigszins altruïstische houding, maar ook het besef dat al die investeringen uiteindelijk gaan renderen.”

Flink investeren
Dat inzicht is volgens haar gelukkig niet helemaal afwezig. “Twee jaar geleden hebben we Cyberveilig Nederland met acht partijen opgericht. We hadden toen dezelfde discussie: gaan we dit nu doen of niet? Uiteindelijk waren alle acht eerst bereid tijd en geld te investeren in het samenwerkingsverband. Investeringen die zich uiteindelijk pas op de lange termijn terugbetalen. Inmiddels zijn we ruim 60 leden groot en hebben diverse mooie resultaten behaald, dus die eerste investering heeft positief uitgepakt. Met het delen van informatie is dat net zo. Je moet bereid zijn eerst flink te investeren, en niet direct wat terug te verwachten. Toch is het zaak dan in dat stadium niet af te haken. Die wederdienst komt echt wel.”

In eerste instantie is het een mooi streven om kennisdeling binnen branches te stimuleren. Cyberveilig Nederland heeft hier binnen de securitybranche het initiatief genomen. Toch hoeft het daar volgens Oldengarm niet bij te blijven. Uiteindelijk wil de Nederlandse overheid komen tot een soort kennisnetwerk, onder de noemer 'Landelijk Dekkend Stelsel' (LDS).
"Wij hebben daarvoor als Cyberveilig Nederland de OKTT-status gekregen van de overheid. Dat betekent dat we 'objectief kenbaar tot taak' hebben andere organisaties of het publiek te informeren. We hebben daarvoor contact met het Nationaal Cyber Security Centrum (NCSC), met wie wij onze bevindingen over en weer delen. Maar daarnaast onderzoeken we ook de mogelijkheden om met andere OKTT-organisaties die kennisdeling op te zetten. Dat is om allerlei redenen een lastig proces, maar het vordert gestaag."

Open klimaat
Actieve kennisdeling rondom cybersecurity vraagt ook om een open klimaat waarin organisaties vrijelijk hun datalekken en andere cyberincidenten willen communiceren. Een waarbij ze niet enkel en alleen hoeven te rekenen op mogelijke represailles als negatieve bijvangst. Op dat punt valt er volgens Oldengarm nog wel wat te verbeteren. "Neem bijvoorbeeld het beleid van de Autoriteit Persoonsgegevens. Die vervullen nu vooral een repressieve rol: bij incidenten loop je risico op een boete. Dat stimuleert natuurlijk geen open houding, integendeel. De balans tussen gebruik van de stok en de wortel is in mijn ogen zoek. Verder zou je kunnen denken aan het toekennen van een bepaalde volwassenheidsstatus aan organisaties als het gaat om cybersecurity. Met een dergelijke status zou je dan bevindingen rechtstreeks met het NCSC moeten kunnen delen."

Het 'kennisnetwerk' is voorlopig nog niet klaar. Er valt volgens Oldengarm sowieso nog veel te verbeteren als het gaat om de kennisinfrastructuur in Nederland rondom cybersecurity. "Het OKTT-instrument is een stap in de goede richting. Dat wil niet zeggen dat hier en daar geen herontwerp nodig is voor het optimaal faciliteren van kennisdeling. Er zijn op dit moment bijvoorbeeld best veel actoren die niet allemaal even zichtbaar zijn, en bovendien deels overlappende rollen hebben."
Die overlap kan volgens haar voor verwarring zorgen.
"Het DTC zou zich nog explicieter kunnen richten op organisaties met een lage volwassenheidsstatus rondom cybersecurity. Die zou het DTC kunnen bedienen met basiskennis en advies. Het NCSC kan zich dan puur richten op volwassen organisaties. Met scherpomlijnde taakstellingen voorkom je bovendien discussies of bepaalde vraagstukken wel binnen het takenpakket van dat specifieke orgaan behoren."

Internationaal
Kennisdeling houdt volgens haar niet op bij de grens. Toch is het nu zaak eerst binnen Nederland de zaken op orde te krijgen. "Uiteindelijk kun je toe naar een situatie waarin internationale kennisdeling structureel is gefaciliteerd. Voor nu hoop ik dat we in ieder geval binnen Nederland blijven werken aan structurele verbeteringen, en een klimaat creëren waarin communicatie rondom cyberincidenten minder schade doet dan het stilhouden daarvan."

"De balans tussen de stok en de wortel is zoek."

» De cloud onveilig? Niet volgens Wesley Neelen en Rik van Duijn, ethisch hackers en medeoprichters van securityresearchbedrijf Zolder. "Een cloudomgeving kun je vaak voor minder geld beter beveiligen dan een zelf gehoste omgeving." Ze plaatsen daar wel een belangrijke kanttekening bij: "Je moet dan wel goed gebruikmaken van de beveiligingsmogelijkheden die bijvoorbeeld Microsoft 365 standaard biedt." Wat zijn die mogelijkheden?

Er is in de cloud heel veel te verdedigen

Wesley Neelen & **Rik van Duijn**
Hackers en medeoprichters, Zolder

Microsoft 365 is veel meer dan alleen e-mail. "Het biedt Teams voor videovergaderingen, SharePoint, OneDrive voor het opslaan van documenten, en als je heel modern bezig bent met Azure AD ook mogelijkheden voor het beheer van gebruikers, wachtwoorden en policy's in de cloud", vertelt Neelen. Van Duijn: "Voordat je het weet, zit je halve bedrijf in zo'n cloudomgeving. Alle data, alle e-mail, alle gebruikers en alle wachtwoorden staan daar. Daardoor is er in die cloud ook heel veel aan te vallen, en heel veel te verdedigen."

Standaard beveiligingsopties
"Microsoft biedt standaard heel veel opties voor het beveiligen van een online 365-tenant", vervolgt Neelen. Die opties bieden bescherming tegen veelvoorkomende dreigingen. De ethisch hackers geven enkele voorbeelden van die dreigingen:

1. Phishing
"In de cloud hangt bijna alles aan je account, dus aan je gebruikersnaam en wachtwoord. Voor cybercriminelen is phishing naar die inloggegevens dan ook de eenvoudigste manier om toegang te krijgen tot je cloudomgeving", waarschuwt Neelen. "Maak daarom gebruik van de phishingdetectie die Microsoft bij iedere Microsoft 365-licentie standaard biedt. En kijk regelmatig in het securitydashboard of er phishingaanvallen zijn gedetecteerd."

Collega Van Duijn waarschuwt daarnaast voor een ander type phishing dat momenteel sterk in opkomst is: 'consentphishing'. Hierbij wordt misbruik gemaakt van het mechanisme dat apps gebruikers om rechten vragen. "Daar kun je als aanvaller heel veel mee. De vraag 'mag ik je e-mail lezen?' lijkt dan van

Microsoft te komen, maar komt in werkelijkheid van een kwaadaardige app van een cybercrimineel." Dit type aanval is volgens Van Duijn succesvol omdat gebruikers er nog niet bekend mee zijn. "Die hebben geleerd om gebruikersnaam en wachtwoord te beschermen. Een vraag om rechten is nieuw."

Microsoft 365 biedt echter al wel bescherming tegen deze nieuwe vorm van phishing. Van Duijn: "Met 'app consent policies' kun je bepalen welke eigenschappen een app die de gebruiker mag goedkeuren moet hebben. Vraagt een app om teveel rechten, dan wordt het proces afgekapt. Dat is een standaard onderdeel van Azure AD. Zorg er daarnaast voor dat de auditlogging is ingeschakeld. Dan kun je achterhalen wie wanneer welke rechten heeft weggegeven. Via de SIEM-oplossing Sentinel kun je de logging ook queryen. 'Geef mij alle consent-to-application-logregels.' En met een premium-licentie kun je via Sentinel ook achterhalen of er sprake is van misbruik. Zonder een premium-licentie zijn de signin-logs handmatig te bekijken."

2. Diefstal wachtwoorden

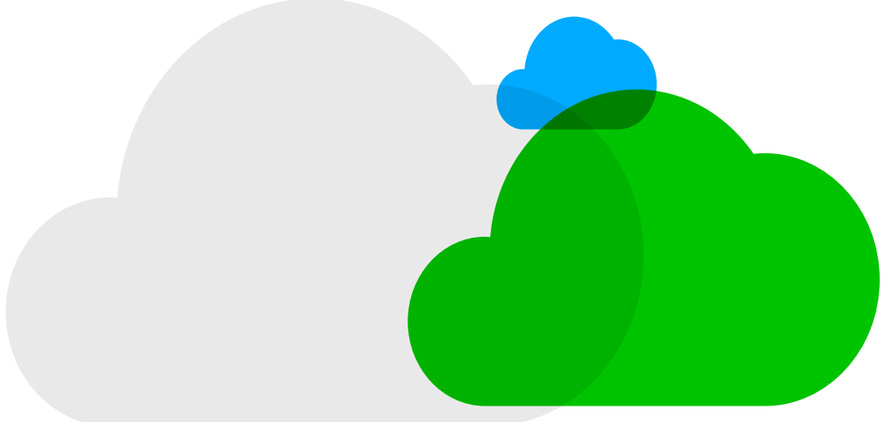
Neelen en Van Duijn haalden het eerder al aan: wachtwoorden vormen de toegang tot de cloudomgeving van de gebruiker. Neelen: "Hergebruik van wachtwoorden is echter een steeds groter probleem. Cybercriminelen kijken of eerder gelekte gebruikersnamen en wachtwoorden ook toegang bieden tot de cloudomgeving van het slachtoffer."

"Multifactorauthenticatie is daarom eigenlijk een must-have die door Microsoft 365 standaard wordt geboden", vervolgt Neelen. "Dan kun je bijvoorbeeld een sms-code, push-notificatie of zelfs een fysieke sleutel gebruiken als tweede factor. Zorg er dan wel voor dat de 'legacy authentication' is uitgeschakeld. Anders kun je als aanvaller alsnog inloggen zonder MFA, via de ouderwetse protocollen."

Volgens Neelen zijn er ook 'mooie combinaties' te maken met diensten als Have I Been Pwned. Hier kan een gebruiker controleren of zijn e-mailadres voorkomt in een database met bekende hacks. "Wij hebben een PowerShell-code gemaakt die je kunt plakken in een PowerShell-prompt (zie hieronder). Die code haalt alle gebruikers die in een tenant zitten uit Azure AD en controleert ze tegen Have I Been Pwned. Op het moment dat een account voorkomt in een datalek, krijg je daar melding van en kun je bijvoorbeeld het wachtwoord resetten."

[PowerShell-code]
ForEach ($user in Get-MSOLUser) { if ($user.UserType -eq "Member") { Write-Host $user.UserPrincipalName; Get-Pwned-Account -EmailAddress $user.UserPrincipalName -apiKey <KEY> }; Start-Sleep -m 1500 }

Commando voor het installeren van Have I Been Pwned-module:
Install-Module -Name HaveIBeen-Pwned
[/PowerShell-code]



Rik van Duijn heeft een jarenlange ervaring als pentester en beveiligingsonderzoeker, onder andere bij KPN Security. Ooit begonnen als pentester onderzoekt Rik tegenwoordig de defensieve kant. Van tactieken die criminelen toepassen tot het maken van detectieve en preventieve maatregelen.

Wesley Neelen heeft vanuit diverse functies als pentester meer dan zeven jaar ervaring in het werkveld van offensive security. Daarnaast onderzoekt hij trends binnen IT-beveiliging en ontwikkelt hij defensieve maatregelen. Zijn interesses liggen onder andere op het gebied van domotica, Internet of Things en 'smart' innovaties.

3. Business Email Compromise

Business Email Compromise (BEC) is een geavanceerde vorm van phishing waarbij het e-mailverkeer wordt gemanipuleerd. Op het moment van fraude heeft de crimineel vaak al geruime tijd toegang tot een e-mailaccount en kan zich voordoen als een leidinggevende of de toegang misbruiken om e-mailregels aan te maken. "Als er een e-mail binnenkomt met het woord 'factuur', kunnen ze dat bericht bijvoorbeeld verplaatsen naar een map die je nooit gebruikt, markeren als gelezen en later het rekeningnummer voor betaling van de factuur aanpassen", legt Van Duijn uit.

"Dat soort gedrag kun je ook detecteren en er slimme regels op toepassen, zodat je bijvoorbeeld een seintje krijgt als er sprake is van een automatische forward. Daar hebben wij ook detectieregels voor gepubliceerd op GitHub", vervolgt Van Duijn. Voorwaarde is wel dat auditlogging en de SIEM-tool Sentinel zijn ingeschakeld.

Security van enterpriseniveau

"De belangrijkste tip is toch eigenlijk wel: maak gebruik van de logging en van Sentinel dat voor specifieke datasources gratis is te gebruiken. Al kijk je verder nooit naar de logging", concludeert Neelen. "Maar als er iets misgaat, dan kun je in veel gevallen tot 90 dagen terugkijken en achterhalen wat er is gebeurd. Dat is enorm belangrijk voor de incident-response. En als je bij de Autoriteit Persoonsgegevens melding moet maken van een datalek, beschik je over de informatie die je nodig hebt voor een goed onderzoek."

"Maak kortom gebruik van de mogelijkheden die Microsoft standaard biedt", besluit Van Duijn. Met Azure AD Security Defaults is MFA met een vinkje in te schakelen, en legacy authentication uit te schakelen, zo tipt de ethisch hacker van Zolder. Microsoft Secure Score laat zien waar nog verdere verbeteringen mogelijk zijn. "Als je er tijd en moeite in steekt, kun je van een Microsoft 365-tenant een heel mooie omgeving maken. Security van enterpriseniveau is dan ook beschikbaar voor een mkb-bedrijf."

» Periodieke phishingsimulaties zijn een beproefd instrument om het security-bewustzijn rondom phishing te meten. “Maar organisaties hebben niet altijd inzicht in de complexiteit van het phishingscenario”, zegt Sanne Maasakkers, ethical hacker bij Fox-IT. “Dan weet je dus ook niet wát je precies meet.” Maasakkers heeft nu zelf een methode ontwikkeld om te beoordelen hoe overtuigend een phishingmail is.

Meten van phishing-scenario’s **versterkt security-awareness**

Sanne Maasakkers
Ethical hacker, Fox-IT

Maasakkers is onderdeel van de red team-afdeling van Fox-IT. Samen met haar collega’s kruipt ze in de huid van cybercriminelen en voert ze onder meer pentests en phishingsimulaties uit, op zoek naar zwakke plekken in de IT-beveiliging van een organisatie. Vervolgens adviseert ze over maatregelen om de digitale weerbaarheid te verhogen. “Dat kan het implementeren van een technische oplossing zijn, maar ook een organisatorische maatregel zoals het aanbieden van securitytrainingen.”

Appels met peren vergelijken

Een awarenessprogramma begint doorgaans met een nulmeting van het securitybewustzijn. Hoeveel werknemers trappen in de phishingmail? Maasakkers: “Vervolgens organiseren we een interventie, bijvoorbeeld een training. Dan volgt later nog een phishingtest. Deze uitslag vergelijken we met de nulmeting, zodat we het effect van de interventie kunnen meten. Een belangrijke voorwaarde is dat de phishingmails op beide meetmomenten even geavanceerd zijn. Anders geven de resultaten een vertekend beeld.”

In de praktijk gaat dit niet altijd goed. “Soms spelen individuele belangen een rol”, legt Maasakkers uit. “Het is weleens voorgekomen dat de CISO de cijfers zoveel mogelijk naar beneden wilde krijgen ten opzichte van de nulmeting. De eerste phishingmail was heel overtuigend, zonder taalfouten, mooi opgemaakt in de huisstijl en de afzender leek op een intern e-mailadres. En bij de tweede e-mail stuurde de CISO erop aan dat er onder andere tikfouten in de mail kwamen. Met zo’n groot verschil in complexiteit is de meting niks waard.”

Inspelen op emotie

Tot voor kort was er echter geen methode om te meten hoe geavanceerd een phishingmail is. “Als begeleider tijdens een afstudeeronderzoek van een stagiaire liep ik hier ook al tegenaan. Dit onderzoek richtte zich op de emoties waarop een phishingmail inspeelt. Wat werkt het beste om mensen te overtuigen? Is dat bijvoorbeeld angst (er is een verdachte inlogpoging gedetecteerd op je account), hebberigheid (je bent geselecteerd voor een pilot met de iPhone 11) of autoriteit (een directielid wil een-op-een met je sparren)?”

“Bij het testen van emoties moet de rest qua complexiteit gelijk zijn, anders spelen er meerdere factoren mee”, legt Maasakkers uit. “Als je bij angst een phishingmail gebruikt met een hogere moeilijkheidsgraad dan bij hebberigheid, kun je de emoties al niet meer vergelijken. Maar hoe meet je dat? Er zijn wel modellen om de technische werkwijze van aanvallers te classificeren, zoals het MITRE ATT&CK Framework. Ik kon echter geen model vinden voor de complexiteit van de e-mail.”

Het model van Maasakkers

De ethical hacker besloot daarom zelf een model te ontwikkelen. “Er was al onderzoek verricht naar het classificeren van malafide websites. Dat model heb ik uitgebreid zodat het op phishingmails van toepassing is. Daarnaast analyseerde ik eerdere phishingacties om te kijken welke elementen de overtuigingskracht van een phishingmail vergroten. Verder heb ik bestaande phishingmails uit openbare bronnen ontleed en diverse awarenesscampagnes vanuit de overheid bestudeerd.” Na het samenvoegen van al deze bronnen kwam Maasakkers tot een nieuw framework. Binnen dit model worden phishingmails beoordeeld aan de hand van vijf categorieën: de context van de e-mail, de inhoud, de domeinnaam, de bijlage, downloadlink of loginlink en de veiligheid en vertrouwelijkheid (https en signing). “Elke categorie omvat een aantal elementen die de verschillende aspecten meetbaar maken. Wanneer we nu een phishingmail op al die elementen scoren, krijgen we een goed totaalbeeld van de kwaliteit ervan.”

Phishingmail wordt meetbaar

Bij de context draait het onder meer om de aanleiding. Dat kan bijvoorbeeld een recente gebeurtenis, een actueel thema zoals het coronavirus of een onbetaalde factuur zijn. “Of de e-mail haakt in op een persoonlijke interesse, zoals een hobby. De afzender maakt ook deel uit van de context: zo is een e-mail van een collega geloofwaardiger dan een e-mail van een onbekende partij. En welk doel heeft de e-mail? Wordt er bijvoorbeeld gehengeld naar inloggegevens of geld? En hoe wordt de ontvanger overtuigd?”

De inhoud omvat de taal en tekst, het design en de persoonlijke informatie. “Is een e-mail foutloos qua taalgebruik, opgemaakt in de huisstijl, in lijn met het jargon en verrijkt met informatie die via social media is verzameld? Of niets van dit alles?” Ook bij de domeinnaam van de afzender en de URL naar de phishingsite zijn er verschillende gradaties. “Zo is een legitiem e-mailadres van de eigen organisatie, verkregen via phishing, het meest overtuigend. Een willekeurig, irrelevant e-mailadres werkt minder goed.”

Toepassingen in de praktijk
Dit is slechts een greep uit de elementen die worden meegewogen. Het model van Maasakkers maakt dus haarfijn inzichtelijk hoe complex een phishingmail is. Maar hoe past ze dit in de praktijk toe? “Allereerst waarborgen we hiermee dat resultaten van phishingtests goed met elkaar te vergelijken zijn, ook als de verstuurde e-mails een totaal andere insteek hebben. Daarnaast biedt de meetbaarheid kansen om het niveau van security-awareness op een gestructureerde wijze te verhogen.” “Het is bijvoorbeeld mogelijk om te experimenteren met verschillende niveaus van complexiteit”, vervolgt Maasakkers. “Dan blijkt wellicht dat het personeel niet in eenvoudige phishingmails trapt, maar juist wel vatbaar is voor iets geavanceerdere e-mails. Of dat de werknemers bovengemiddeld kwetsbaar zijn voor gespoofte e-mailadressen. Vervolgens kun je trainingen geven die hierop aansluiten, en zo stapje voor stapje verbeteringen realiseren. Of andersom: je gaat heel specifiek testen op het niveau van eerdere interventies om de effectiviteit daarvan te meten.”

Enthousiaste reacties
Maasakkers benadrukt dat de meetbaarheid van phishingscenario’s vooral interessant is voor partijen met een hoog securityvolwassenheidsniveau. “Deze organisaties nemen cybersecurity echt serieus en hanteren hiervoor een langetermijnstrategie. Zij organiseren meerdere phishingacties per jaar en vinden het belangrijk dat de meetwaarden betrouwbaar zijn, omdat ze hun beleid daarop baseren. Ik heb het model inmiddels bij een aantal van dit soort partijen geïntroduceerd. Zij reageren stuk voor stuk enthousiast.”

Veel organisaties zijn nog niet zover, beseft de ethical hacker. “Sommige bedrijven laten een phishingsimulatie vooral uitvoeren omdat dit vanuit wet- en regelgeving verplicht is. Zodra het vinkje binnen is, vinden zij het wel best. Het rapport met aanbevelingen belandt dan ergens onderin een la. Dat is natuurlijk zonde. Een phishingtest heeft pas zin als je er ook echt wat mee doet.”

Sanne Maasakkers hield zich al op jonge leeftijd bezig met de beveiliging van haar eigen websites. Deze passie voor cybersecurity resulteerde uiteindelijk in een baan als ethical hacker bij Fox-IT, waar ze inmiddels ruim vier jaar de security van bedrijfsnetwerken en -websites test. Naast dit werk draagt Maasakkers bij aan een veiligere samenleving via awarenesstrainingen, gastcolleges, hackdemonstraties en mediaoptredens.

» Securitytechnologie maakte de afgelopen jaren enorme sprongen. Toch zijn securityincidenten nog altijd schering en inslag. Cyberaanvallen zijn vaak helemaal niet zo geavanceerd, maar hebben wel rampzalige gevolgen. Volgens Oscar Koeroo, manager CISO-relations bij KPN CISO Office, is er bij veel van die incidenten een opvallende gemene deler. “Organisaties hebben zich dikwijls niet de juiste vragen gesteld.”

Het draait om het stellen van de juiste vragen

Oscar Koeroo
Manager CISO-relations, KPN CISO

Een goede security begint bij een goed beeld van de aanwezige IT in de bedrijfsprocessen van een organisatie. Dat beeld ontbreekt volgens Koeroo vaak. “Als IT-manager moet je je afvragen waar je precies verantwoordelijk voor bent. Hoe ziet mijn organisatie eruit? Welke systemen zijn in gebruik en hoe zijn die opgebouwd? En vooral: welke risico’s gaan ermee gepaard, en welke middelen en maatregelen zijn nodig om die risico’s te beheersen? Die vragen zijn cruciaal, maar worden veel te weinig gesteld. Vervolgens moet je de middelen en maatregelen ook nog daadwerkelijk implementeren. Ook dat wordt nogal eens vergeten.”

Nog te vaak gaat het mis. Koeroo noemt als voorbeeld de golf aan ransomware-incidenten, waarbij een deel zelfs de media haalt. “Een krachtig middel om een ransomware-aanval ongedaan te maken, is het terugzetten van een goede, onaangetaste back-up. Maar dan moet die wel voorhanden zijn. Vaak is er wel een back-up, maar is er onvoldoende nagedacht over hoe kwetsbaar die precies is bij een dergelijk incident. Dan is dat securitymiddel dus onvoldoende bevraagd. Terwijl je met goede segmentering en het plaatsen van de back-up buiten het IT-ecosysteem waarschijnlijk veel ellende had kunnen voorkomen.”

Met een goed beeld op de risico's ben je er nog niet. "Natuurlijk kun je proberen om alles waterdicht te beveiligen. De beste manier is dan gewoon alle stekkers eruit trekken. Maar dan houd je een onwerkbare situatie over. Dan krijg je een situatie als in de bekende foto van een dichte slagboom in de sneeuw, waarbij de bandensporen om de slagboom heen lopen. Het gaat om het vinden van een goede balans."

Democratisering
Die balans ontstaat niet vanzelf. Daar heb je volgens Koeroo alle lagen van de organisatie bij nodig. "We zijn geneigd de verantwoordelijkheid voor security bij de IT-manager of de security officer neer te leggen. Organisaties zien IT nog te vaak als 'nerd only'. Dat is het natuurlijk niet, iedereen in een organisatie werkt er mee en is ervan afhankelijk." Daar moet je volgens hem als securityverantwoordelijke wat mee. "Als je als CISO in een ivoren toren zit, zet je jezelf buitenspel. Je moet de organisatie in en bondjes vormen. Luister naar medewerkers. Breng in kaart welke behoefte zij hebben, wat IT voor hen moet doen en hoeveel drempels zij bereid zijn te nemen in hun dagelijkse processen. Dan kun je beter bepalen in hoeverre je iets kunt dichttimmeren."

Herhaling
Een goede methode voor een breed draagvlak is het zoveel mogelijk hergebruiken van bestaande securityprocedures. "Neem identiteitsbeheer. Niets is zo vervelend als steeds een andere gebruikersnaam en wachtwoord te moeten invoeren. Een centraal IAM (Identity & Access Management) -platform kan dat voorkomen. Zorg er vervolgens voor dat bestaande en nieuwe assets daarmee overweg kunnen. Dan hoeven medewerkers maar één keer in te loggen, en eventueel maar één keer een MFA-procedure te doorlopen. Dat vergroot het draagvlak en verkleint de kans op onveilige omwegen."
De risico's van een niet-democratisch securitybeleid zijn groot. Het is volgens Koeroo de ideale voedingsbodem voor bijvoorbeeld shadow-IT en overhaaste aankopen. Zeker nu SaaS flink is ingeburgerd. "Met enkele muisklikken neem je een tool uit de cloud in gebruik. Handig natuurlijk, maar dan is het helemaal verleidelijk voorbij te gaan aan de vraag wat je eigenlijk in huis hebt gehaald. Waar staat die tool ergens? Hoe is de beveiliging geregeld? Als je die vragen niet stelt, dan kom je ook niet achter de cruciale securitykeuzes."

Oscar Koeroo
Fotograaf: Dennis van Zuijlekom

Oscar Koeroo werkt bij KPN in het Chief Information Security Office (CISO). Zijn eigen expertises zijn identity management, toegepaste cryptografie, systeembeveiliging en netwerkbeveiliging. Hij adviseert de business op zowel operationeel als strategisch niveau. Oscar behandelt het thema overheids- en externe relaties namens de KPN CISO op het gebied van security en continuïteit. Hij doet dat vanuit het perspectief van een vitaal bedrijf dat zichzelf, haar klanten en de maatschappij veilig houdt.

Follow the money
Een goede manier om die ongecontroleerde inkoop tegen te gaan, is wat Koeroo noemt een 'follow the money-strategie'. "Je moet uitzoeken wie doorgaans de inkoop van dergelijke IT precies doet. Die 'champion' moet je erbij betrekken. Geef zo iemand bijvoorbeeld een checklist van eisen waaraan voldaan moet zijn voor überhaupt budget beschikbaar komt. Dat verplicht iemand te kijken naar securityaspecten van technologie en voorkomt wildgroei."

Een van de methoden die Koeroo vaak adviseert om risico's te inventariseren is threat modelling. Hierbij ga je na welke effecten een incident teweegbrengt. "Dat doe je door het opstellen van what-if-scenario's in een soort gedachtespel, waarbij je alle cascade-effecten van een maatregel uitdenkt." Volgens hem moeten organisaties daar niet te licht over denken. "Ieder doosje, ieder middel en iedere setup heeft een andere set beveiligingseisen. IT-ecosystemen zijn continu in beweging. Bij iedere wijziging moet je dan ook eigenlijk via threat modelling de securityaspecten doorlichten."

Simulaties
Overigens is enkel threat modelling niet voldoende. Ook simulaties zijn cruciaal. "Er zitten zoveel kleine details in het mitigeren van een aanval. Daarom is het regelmatig doen van simulaties zo belangrijk. Alleen dan kom je erachter of de security controls die je tijdens threat modelling hebt bedacht ook daadwerkelijk werken en je niks over het hoofd hebt gezien."

Toch is de ene simulatie de andere niet. "Je kunt een simulatie heel technisch insteken, met een Red Team, Blue Team of zelfs Purple Team. Of juist niet, en de simulatie heel erg praktisch houden. Doe het liefst beide. Pak het hoe dan ook niet te lichtzinnig aan. Je mag het best leuk maken, maak er desnoods een feestje van. Maar het zweet moet bij wijze van spreken wel op je voorhoofd staan. Monitor goed wat er gebeurt, en bedenk bij ieder ongewenst gevolg hoe dat voorkomen had kunnen worden."

Not invented here
Ondanks alle maatregelen zijn incidenten nooit uit te sluiten. Vroeg of laat krijgt iedere organisatie te maken met een securityincident. Dat hoeft volgens Koeroo niet alleen maar rampspoed te betekenen. Het is volgens hem ook een kans om te leren. "Ook hier gaat het weer om het stellen van de juiste vragen. Wat hebben we van een incident geleerd? Wat moeten we precies veranderen om de kans op herhaling te verkleinen?"

De blik hoeft overigens niet altijd naar binnen gericht te zijn. "Je kunt zoveel leren van incidenten die bijna dagelijks in het nieuws verschijnen. Overal om ons heen gaat het mis. Heel vaak ligt de aandacht dan vooral bij de hack zelf. Veel interessanter is welke processen, of het gebrek daaraan, die hack mogelijk heeft gemaakt. Daar wordt nog veel te weinig mee gedaan." Volgens Koeroo zijn ook incidenten bij andere organisaties daarvoor waardevol. "Zelfs wanneer een organisatie ogenschijnlijk niet op die van jou lijkt. Vaak zijn processen en de manier waarop die al dan niet zijn beveiligd goed vergelijkbaar. Veel bedrijven hebben last van het 'not invented here'-syndroom. Dat is echt een gemiste kans."

Toverdoosjes
Organisaties hoeven volgens hem niet iedere keer zelf het wiel uit te vinden. Ook een externe partij kan een belangrijke rol spelen. "Een MSSP kan helpen met het stellen van de juiste vragen, en blauwdrukken bieden voor een veilige manier van werken. De tijd van dozen schuiven is echt voorbij. Je mag van een IT-partner verwachten dat ze je helpen met een optimale inzet van de gekochte securitymiddelen. Maar bedenk altijd: securityoplossingen moeten ook passen in het ecosysteem, en matchen met de dagelijkse processen. Toverdoosjes bestaan niet."

"Incidenten bieden de kans om herhaling te voorkomen."

Colofon

Cyber Security Perspectives 2021
is een uitgave van KPN Security
Roxy Spaargaren
Babette Kersten
Bram Reinders
Carolien Hoogerwaard
Marcel Heezen

Volume 8

Tekst
Co-Workx
KPN Security

Vormgeving
KPN Kreatie

Drukkerij
HH Global

KPN Security
Wilhelminakade 123
3072 AP Rotterdam

Twitter
https://twitter.com/kpnsecurity

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

Website
https://www.kpn.com/zakelijk/
security.htm

NLSecure[ID] page
https://www.kpn.com/zakelijk/
security/bedankt_voor_uw_bezoek_
aan_nlsecureid2021.htm

LET'S TALK
ABOUT IT

kpn Security