INFORMATIEBEVEILIGING
MAGAZINE

THEMA: Thuiswerken

- Interview Dré Lemeir: ‘Business as usual, anders klopt er iets niet’
- Thuiswerken tijdens (post)corona
- De voordelen van crowdsourced security

JAARGANG 21 - 2021 - EDITIE 1

Huis-tuin-en-keukenwerken

Nicole van Deursen

De uitdrukking 'huis-tuin-en-keukending' betekent: niets bijzonders, maar juist heel gewoon en alledaags. In de loop van 2020 is thuiswerken voor velen iets alledaags geworden, maar heel gewoon is het voor de meesten nog steeds niet. In de lente vond ik het heerlijk om de dagelijkse kantoortuin te vervangen voor mijn eigen tuin, maar langdurig of structureel op afstand werken vraagt om aanpassing van zowel de werkgever als de werknemer. Omdat op dit moment het einde van het thuiswerkbeleid nog niet in zicht is, besteden we in het eerste iB-magazine van 2021 extra veel aandacht aan thuiswerken. We krijgen een exclusief kijkje in de keuken van een aantal organisaties die vertellen hoe zij deze situatie hebben ingericht.

Naast het thuiswerkthema zijn er ook nog artikelen over andere onderwerpen zoals incident response en herstelvermogen, en natuurlijk de vaste columns. Verder hebben we traditiegetrouw een overzicht geplaatst van alle artikelen die in 2020 zijn gepubliceerd zodat het opzoeken van artikelen over bepaalde onderwerpen makkelijker is. We wensen iedereen veel leesplezier.

Nicole

IN DIT NUMMER

Rectificatie

In het artikel 'VNG: overheidsbrede 'cyberoefening' in iB6 2020 is een foutje geslopen. In het artikel staat dat de cyberoefening door de VNG is georganiseerd. Zij hebben wel meegeholpen met de logistieke organisatie, maar de oefening is georganiseerd door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Auteur: Sandra Kagie is freelance tekstschrijver (Sanscript Tekstproductie).
Sandra is bereikbaar via info@sanscriptproducties.nl.

INTERVIEW

Iedereen werkt thuis, wat betekent dit voor een CISO?

‘Business as usual, anders klopt er iets niet’

“Als je als CISO binnen een thuiswerkende organisatie de afgelopen maanden hebt geconcludeerd ‘nu is ineens alles anders’ dan klopt er iets niet. Want het zou business as usual moeten zijn.” Het is de stellige overtuiging van Dré Lameir, CTO/CISO van de Enovation Group. Dit na bijna een jaar ervaring met een compleet thuiswerkende organisatie.

"We kunnen niet bij de file server, dus dan mail ik je wel even die dossiers'. "Stel dat dat nu wordt gezegd in een organisatie. Dan had je eigenlijk je toegang tot je fileserver al remote moeten regelen", geeft Lameir een voorbeeld. "Kom je dat soort red flags nu ineens heel vaak tegen dan was het dus al niet goed. Misschien moet je dan als CISO eens aan de slag met een jaarplan."
Lameir realiseert zich dat hij belerend klinkt. "Maar", zegt hij om aan te geven waarom hij dit doet, "ons beleid was al dat iedereen zijn werk van willekeurig welke plek zou moeten kunnen doen. We hebben aan onze tooling dan ook niks hoeven veranderen op het moment dat we thuis gingen werken."
"Desktops waren vrijwel allemaal al vervangen door laptops, onze telefooncentrale hadden we al in de cloud, die was al VoIP, Office 365 hadden we al uitgerold, onze file server was al benaderbaar via VPN, ons Corporate Quality Management Systeem (CQMS) draaide al op Confluence en JIRA in de cloud en dossiers op een veilige manier delen, ook met klanten, konden we al", somt hij op.

Business continuity test liep even anders

"En toen wilden we in maart eigenlijk een heel grote business continuity test doen. Met als script 'laten we nou eens allemaal twee dagen thuis gaan werken'. Precies op dat moment kwam de lockdown. Supergrappig", herinnert hij zich. "Binnen twee dagen zaten we allemaal thuis. Er waren vier mensen die we thuis een andere machine moesten geven. De rest kon gelijk aan de slag."
Het verantwoordelijkheidsgevoel van iedereen binnen de organisatie heeft in deze snelle adoptie van het thuiswerken volgens Lameir zeker een rol gespeeld. "We hebben binnen Enovation heel erg de filosofie 'informatiebeveiliging daar zijn we samen verantwoordelijk voor'. Je kan dus niet zeggen 'informatiebeveiliging dat doen Bianca (red. Brooijmans), als DPO, en ik'. Wij zijn aanjagers en we schrijven mét anderen het beleid, maar dat betekent niet dat je dingen op ons kunt afschuiven."

Opnieuw actuele risico's

Wat Lameir in maart wel merkte was dat de snelle omschakeling ervoor zorgde dat bepaalde risico's die je op kantoor al had ingeperkt, thuis weer heel actueel werden. "Op kantoor moet iedereen in principe zijn laptop aan de ketting leggen", geeft hij een voorbeeld. "Nu zie ik mensen soms op één dag vier keer op een andere plek achter de camera zitten. Ik weet zeker dat mensen dat 'aan de ketting' nu niet kunnen volhouden. En zo zijn er wel meer regeltjes te noemen."
Als het gaat over de basis, het gebruik van een VPN-verbinding en netwerkbeveiliging, is hij echter helder: "Het is bij ons sowieso niet mogelijk om zónder VPN bij kantoor- of klantspullen te komen. Daarnaast zit er op die VPN en op de inlog van applicaties nog two-factor-authentication."
In zijn algemeenheid kun je volgens Lameir zeggen dat het toezicht houden in de huidige situatie lastiger is. "Omdat mensen niet meer op een controleerbare plek bij elkaar zitten. Mensen direct aanspreken, wat je normaal bijvoorbeeld doet wanneer je even een rondje maakt, is hierdoor

moeilijker. Je weet niet hoe iemand er thuis bij zit. Je mist wat dat betreft die toevallige ontmoetingen. Je thermometer in de organisatie."

'Versnelde acceptatie'

Voor Enovation, dat zorgorganisaties ondersteunt bij informatie-uitwisseling en connected-care, betekende de lockdown in maart dat alle 250 werknemers thuis gingen werken. En dat is sindsdien zo gebleven. De keren dat Lameir bijvoorbeeld in de afgelopen maanden op het hoofdkantoor in Capelle aan den IJssel was, zijn op de vingers van twee handen te tellen.

Een situatie die in zijn ogen deels zal blijven bestaan, ook ná corona. "Ik zie een mix voor ogen. En dat geldt voor de meerderheid van de mensen binnen onze organisatie, zo bleek uit een enquête die we hebben gehouden. Wat dat betreft zorgt deze situatie voor een versnelde acceptatie van thuiswerken." Om in de toekomst tot een goede mix te komen, is het volgens hem noodzakelijk dat mensen bereid zijn hun eigen werkplek op kantoor op te geven. En ook dat vindt een meerderheid van zijn collega's, zo bleek uit de enquête, geen probleem.

"Je moet als organisatie vervolgens zorgen voor de juiste tooling zodat teams, in de toekomst, bijvoorbeeld samen een aantal bureaus bij elkaar kunnen reserveren. Kan dit niet dan kun je immers net zo goed thuis blijven werken. De toegevoegde waarde van werken op kantoor is immers het bouwen aan de sociale cohesie in een team. Het elkaar weer in één ruimte kunnen zien. Dat zijn we nu dus aan het regelen."

De basis

Ondanks dat er tot aan de lockdown in maart binnen Enovation nog niet structureel werd thuisgewerkt, was iedereen binnen het bedrijf volgens Lameir wel op de hoogte van de basisregels. "Dat het bijvoorbeeld niet de bedoeling is dat je werkgerelateerde zaken overal (in huis) laat slingeren of dat je kinderen Minecraft op je werklaptop installeren. Zo'n checklist hadden we al. En die hebben we nu herhaald."

"Dat geldt bijvoorbeeld ook voor regels wat betreft je wachtwoordkluis, of de regel dat je laptop niet openstaat wanneer er iemand over de vloer is. De clean desk policy geldt wat ons betreft thuis ook." Je thuis is nu kantoor en in principe doe je daar niet anders dan op kantoor, beaamt hij. "Waarbij we als Security Office uitzonderingen níet toestaan", benadrukt hij. "Iedereen heeft een volgens de voorschriften van kantoor geprepareerde laptop. Wanneer het verzoek komt een andere laptop in het netwerk te hangen dan is het antwoord `nee'."

Alles goed voor elkaar of...?

De vlekkeloze overgang naar het thuiswerken heeft Lameir de afgelopen tijd tot een belangrijke vraag gebracht: heb ik hier te maken met een schijnveiligheid en is er eigenlijk van alles aan de hand of hebben we als Enovation inderdaad alles goed voor elkaar? Een antwoord op die vraag heeft hij nog niet. "De tijd zal het leren", zegt hij. "Op het moment van het eerste security incident dat is te linken aan de huidige situatie gaan de alarmbellen af."

Wat Lameir ook denkt, is dat het antwoord op de genoemde vraag heel erg afhangt van het soort organisatie waarin je als CISO werkt. "Wij verkopen veilig online berichtenverkeer of datastructuren. Dat is ons werk. Ons leven speelde zich al online af. Ik kan me voorstellen dat je in een heel andere omgeving nu ineens wel te maken hebt met bepaalde documenten die normaal alleen in een vertrouwelijke ruimte werden behandeld."

"Stukken van een klant mee in een mapje. Dingen thuis ook uitprinten. Daar hebben wij niet mee te maken. De medische gegevens van onze klanten bijvoorbeeld raken onze mensen nooit aan. Dat loopt allemaal via onze centrale infrastructuur. De locatie van werken is voor ons veranderd, maar als je kijkt hoe wij op kantoor werkten dan hadden we net zo goed remote kunnen werken."

Tips tot slot

Voor collega-CISO's heeft Lameir nog een paar tips. Zo benadrukt hij hoe belangrijk het is om juist nu de achtergebleven werkplekken, het kantoor dus, niet te vergeten als het gaat om security. "Daar is in veel gevallen bijna niemand meer", legt hij uit. "Kwaadwillenden lopen er dus letterlijk gemakkelijker naar binnen."

"Geef iedereen de verantwoordelijkheid over zijn eigen thuiswerkplek", adviseert hij ook. "Benadruk dat ze daar, juist nu, alert op moeten zijn. Maar geef ze hiervoor ook de middelen. Zeg dus niet `let op security, maar werk op je eigen thuisdesktop of -laptop'."

"En ook al heeft iedereen nu veel aan zijn hoofd met de lockdown en thuiswerken, vaak in combinatie met kinderen thuis, blijf aandacht vragen voor awareness", benadrukt hij tot slot. "Een scherper passwordbeleid of een phishingactie. Sommige bedrijven stellen zaken als deze even uit. Omdat mensen al voldoende druk ervaren. Bij Enovation staan we hier anders in. We laten awareness niet verslappen. Nu niet en nooit niet."

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Safe seks

Seks en privacy zijn intrinsiek verbonden aan elkaar. Voor de swingende sekser die graag incognito naar de parenclub gaat, de exhibitionist die het graag in het openbaar doet en de ongelukkige wipper die een SOA-kit opstuurt aan een anonieme testservice.

Ook in coronatijd blijft seks een onverminderd populair onderwerp van gesprek. Was het niet onze overheid die tijdens de eerste golf de vrijgezellen zei dat ze maar even niet meer van de vleselijke geneugten moesten proeven, dan was het wel het Australische Centre for Disease Control die de Glory Hole heilig verklaarde voor coronaproof seks. Bij die laatste nog eens het bijkomend voordeel dat je daarbij niet eens meer weet met wie je het doet; anoniemer wordt het bijkans niet.

De verkoop van seksspeeltjes steeg in het eerste coronajaar explosief. In het thuiskantoor werd massaal gespeeld en geëxperimenteerd. Vaak ook met speelgoed dat verbonden kan worden met het internet. Dat is natuurlijk een prachtig target voor hackers. In oktober 2020 werden dan ook voor het eerst piemels gegijzeld. Wat? Piemels gegijzeld, je las het goed. Een hightech kuisheidsgordel voor mannen werd gehackt en bleek op afstand gesloten te kunnen worden. Het lek werd gepatcht, maar zoals bekend is niet iedereen altijd even snel met het updaten van de software en dus bracht de fabrikant ook een 'doe het zelf'-video uit waarin je met wat handigheid en een schroevendraaier het zaakje weer kon ontsluiten. Overigens voorspellen experts dat er in 2021 zeer waarschijnlijk nog veel meer hacks en kwetsbaarheden zullen volgen in de smart speelgoedlade.

Online seksualiteit brengt al tijden allerhande extra risico's met zich mee. Van wraakporno tot de gemakkelijke verspreiding van strafbare seksuele zaken en afpersing door dreiging met het openbaar maken van digitaal beeldmateriaal. Seks heeft in dat opzicht ook te maken met autonomie en vrijheid en met de beperking daarvan. Daar waar de seksuele creativiteit op meer online manieren gestalte moet worden gegeven in tijden van social distancing, zie je ook op bepaalde vlakken online verpreutsing die meer rigoureus seks en seksualiteit probeert in te dammen, vaak gericht op en tegen vrouwen.

Instagram gaat sinds kort de oorlog aan met elk vleugje seksualiteit, en laat daarin helaas ook zien dat je seks niet te veel moet reguleren omdat je dan zeer onsmakelijke ongelijkheden en ongenuanceerdheden creëert. Zo mogen mannen hun blote tepels laten zien, maar worden foto's van naakte vrouwentepels rücksichtslos gewist. Prachtige slanke vrouwen in wulpse poses blijven voor eenieder zichtbaar, maar als een vrouw met een groter en dikker lichaam in exact dezelfde wulpse pose op de foto staat, wordt dat als onzedelijk aangemerkt en verwijderd. Ook sekswerkers en kunstenaars ondervinden veel hinder doordat hun accounts worden geblokkeerd – beide door corona gedwongen de onlinewereld op te zoeken om hun waren aan te prijzen. Toppunt van betuttelende zedenhypocrisie vond ik overigens de Belgische Psychologencommissie. Kaat Bollen, psycholoog en seksuoloog verloor in januari 2021 haar titel als psychologe omdat ze sexy foto's op haar privé instagramaccount had gezet en een vrouwvriendelijke pornofilm (porna) had geregisseerd.

Doe mij dan toch maar snel die vaccinaties tegen corona. Kunnen we tenminste weer allemaal lekker offline seks hebben. Wel zo veilig.

Rachel

Auteur: Laurence Pitt is security lead bij Juniper Networks. Met meer dan twintig jaar ervaring op het gebied van cybersecurity legt Laurence in zijn rol bij Juniper duidelijk de nadruk op veiligheid in het bedrijfsleven, waar hij mensen beweegt zorgvuldig na te denken over security op het gebied van processen, beleid en oplossingen. Laurence is te bereiken via lpitt@juniper.net.

Een (thuis)werkbare oplossing

Eerder dit jaar namen duizend IT-besluitvormers in negen landen deel aan een enquête over netwerken en cybersecurity die in opdracht van Juniper Networks door Na Vanson Bourne (1) werd uitgevoerd. De vragen werden voorgelegd aan besluitvormers bij bedrijven met duizend of meer medewerkers, waaronder verschillende Nederlandse ondernemingen. Uit de enquêteresultaten blijkt dat de focus van Nederlandse IT-afdelingen hoofdzakelijk ligt op het verbeteren van de efficiëntie en het herstellen van de coronacrisis.

De enquêteresultaten schetsen een duidelijk beeld van de problemen waarmee bedrijven worden geconfronteerd. 70% van de Nederlandse respondenten is van mening dat hun bedrijfsnetwerk en -infrastructuur te gefragmenteerd zijn om effectief te kunnen worden beschermd. Evenzoveel mensen is het eens met de stelling dat het lastig is voor hun organisatie om voor een 24/7 beschikbaar en veilig netwerk te zorgen. Het blijkt dat Nederlandse IT-afdelingen nog altijd de helft van hun tijd kwijt zijn aan het draaiende houden van de infrastructuur. De IT-beveiliging wordt vaak gezien als een zware last.

Nederlandse ondernemingen geven gemiddeld € 1.136.286 uit aan cybersecurity. Dit ligt volgens de enquêteresultaten iets onder het wereldwijde gemiddelde. 97% van de respondenten zag zich de afgelopen twaalf maanden echter gedwongen om meer geld uit te trekken voor het verhelpen van beveiligingsincidenten en kwetsbaarheden. Daarmee komt het gemiddelde bedrag per bedrijf uit op ruim €245.000. Een ander, wellicht minder gebruikelijk probleem dat in de meeste landen speelt is de plotselinge massale uittocht van kantoorpersoneel naar eettafels, logeerkamers en studeerkamers. Door de lockdown moesten wereldwijd miljoenen mensen op stel en sprong hun laptop en flatscreen naar huis verkassen. Sinds de uitbraak van het coronavirus is thuiswerken voor hen uitgegroeid tot de norm. Volgens prognoses van Eurofound (2020) (2) werkt bijna 40% van alle werknemers in de EU vanwege de pandemie fulltime thuis. En volgens een grove schatting van een recent onderzoeksrapport van JRC (3) is 25% van alle werkgelegenheid in de regio afkomstig van sectoren die de mogelijkheid van thuiswerken bieden. Volgens hetzelfde onderzoek had slechts 15% van alle werknemers in de EU ooit thuisgewerkt voordat de coronacrisis zich aandiende. De kans is dan ook groot dat veel werknemers en werkgevers met problemen worden geconfronteerd als gevolg van de plotselinge overstap naar thuiswerken. De omvang van deze problemen zal per bedrijf sterk variëren, afhankelijk van factoren zoals ervaring met telewerken.

Overzicht

Alle bedrijven worden met één vraag geconfronteerd, en dat is hoe hun IT-afdeling grip kan houden op de thuiswerkomgevingen. De enquête door Vanson Bourne geeft namelijk ook aan dat het op peil houden van de netwerkprestaties en beveiliging al voor de pandemie een bijzonder tijdrovende bezigheid was. Volgens Vanson Bourne werkt 55% van alle werknemers van de ondervraagde ondernemingen thuis. Dit trekt een enorme wissel op hun bedrijfsnetwerk en kan ten koste gaan van de netwerkstabiliteit. Zo kunnen er pieken in de netwerkbelasting optreden wanneer iedereen zich om negen uur 's ochtends aanmeldt. Omdat veel werknemers dat laatste via een draadloos thuisnetwerk doen, is het niet verstandig om conference calls aan het begin van de dag te plannen.

Een probleem met een nog grotere impact is het beperkte overzicht dat de IT-afdeling heeft op alle thuisnetwerken en de apparaten die daarmee zijn verbonden. Het beveiligingsteam heeft inzicht in het bedrijfsnetwerk en toegang tot contextuele informatie waarmee het kan bepalen of er sprake is van een netwerkprobleem of beveiligingsincident. Deze context ontbreekt grotendeels wanneer er zich problemen buiten het bedrijfsnetwerk voordoen. Welke andere apparaten zijn met het lokale draadloze netwerk verbonden? Welke activiteiten voeren de gezinsleden van de thuiswerker uit? Is zoonlief weer eens films aan het downloaden? Waar is de smart home-assistent mee bezig? Dit zijn vragen waar bedrijven geen antwoorden op hoefden te vinden toen werknemers nog achter hun bureau op kantoor zaten. Maar nu moet er met al deze aspecten rekening worden gehouden om een stabiele, veilige en toekomstbestendige netwerkomgeving te waarborgen.

En het is natuurlijk heel goed mogelijk dat thuiswerkers een beroep doen op diensten en platforms die niet door de werkgever goedgekeurd zijn. Die kunnen bijdragen aan beveiligingsincidenten binnen het bedrijfsnetwerk. Het kan hierbij gaan om zakelijke platforms en diensten die onder de noemer `schaduw-IT' vallen, van de aanschaf van relatiegeschenken via webwinkels tot het downloaden van tools voor het verbeteren van de prestaties van het draadloze thuisnetwerk. De afgelopen maanden is sprake geweest van een enorme opleving in het aantal malafide websites dat speciaal door cybercriminelen werd ontwikkeld om mensen te lokken en informatie bij hen los te peuteren om toegang tot hun thuisnetwerk te krijgen.

Je kunt met recht stellen dat bedrijven weinig keuze hadden. Ze waren gedwongen om hun werknemers de mogelijkheid te bieden om vanuit huis te werken en hen te faciliteren met basisvoorzieningen, zoals een VPN-verbinding of een draadloos Virtual LAN voor multi-factorauthenticatie. De meeste bedrijven deden dit op basis van een niet-schaalbare, universele aanpak. De 'nieuw-normale' maatregelen zijn van een heel andere orde. Er is een structureel nieuwe aanpak van digitale thuiswerkomgevingen nodig, omdat veel werknemers aangeven dat ze na het verlichten of opheffen van de huidige beperkingen graag een of meer dagen per week willen thuiswerken. Volgens het onderzoek van Vanson Bourne geldt dat voor bijna 40 % van alle Nederlandse werknemers. Dat is een fundamentele verschuiving.

De kracht van drie

De vraag is nu hoe bedrijven hier vanuit het oogpunt van netwerkbeveiliging mee om moeten gaan. Veel bedrijven hebben tijdens de WFH-periode (Working From Home) voor alle gebruikers dezelfde beveiligingsmaatregelen toegepast, maar het beheer daarvan op een dergelijk grote schaal is geen sinecure. Zeker omdat het beveiligingsteam zelf grotendeels vanuit huis werkt. Een oplossing is om thuiswerkers onder te verdelen in groepen waarvoor verschillende beveiligingsniveaus gelden. Het uitgangspunt daarbij

De mogelijkheid van thuiswerken is voor veel kenniswerkers niet langer een privilege, maar een absolute noodzaak

is de mate van toegang die ze tot data en applicaties binnen het bedrijfsnetwerk nodig hebben. Op die manier kunnen eindgebruikers effectief hun werk blijven doen, terwijl het beveiligingsteam beschikt over het overzicht dat nodig is om het netwerk en de bedrijfsgegevens te beschermen. Voor de meeste organisaties zouden drie beveiligingsniveaus moeten volstaan. Hieronder leggen we uit hoe dat er in de praktijk uit kan zien.

Je kunt met recht stellen dat toegang via een VPN toereikend is voor 75 % van alle thuiswerkers die gebruikmaken van Office 365 en af en toe een paar intranetten bezoeken en een virtuele machine gebruiken. Daarmee kun je voorzien in hun basisbehoefte om productief en veilig te blijven werken. Het beheer van de VPN op hun laptop zou de IT-afdeling niet bijster veel extra werk moeten opleveren.

15% van alle thuiswerkers zijn kenniswerkers die onderzoek moeten doen, documenten moeten downloaden en toegang nodig hebben tot gevoelige informatie. Zij hebben daarom een krachtiger beveiliging nodig. Het apparaat dat ze voor hun werk gebruiken mag dan misschien veilig zijn, maar we hebben genoeg voorbeelden gezien van cybercriminelen die in thuisnetwerken infiltreren op basis van wat je als 'normaal gebruik van het netwerk' zou kunnen omschrijven. En dan zijn er nog websites met malware en gerichte phishingmails die binnen de bedrijfsomgeving geen probleem zouden opleveren, maar in thuiswerkomgevingen onzichtbaar blijven voor het beveiligingsteam.

De overige 10% van de thuiswerkers omvat professionals zoals programmeurs die met intellectueel eigendom werken, senior managers en directieleden. Het is zaak om hen thuis net zo te behandelen als op kantoor. Beveiligingsteams moeten precies weten wat er binnen hun netwerk gebeurt, omdat aanvallen op dit niveau de organisatie ingrijpende schade kunnen toebrengen.

Nu we de drie werknemersprofielen in kaart hebben gebracht, is het tijd om in te gaan op de benodigde technische maatregelen. Veel thuisnetwerken zijn ingericht op gebruiksgemak. Ze maken gebruik van de beveiligingsstandaard WPA2 in plaats van WPA3. Dit is ontoereikend voor zakelijke doeleinden. Er is dus krachtiger bescherming nodig.

Voor veel gebruikers (de eerder genoemde 75%) is de oplossing om hen te voorzien van een VPN dat hen alle toegang biedt de ze nodig hebben om hun werk te doen. Maar hoe zit het nu precies met de andere groepen?

Voor de kenniswerkers is de beste oplossing om het netwerkverkeer en het privéverkeer van elkaar te scheiden. Dit is mogelijk door hen te voorzien van een beheerd draadloos access point van de zaak. Omdat het bedrijfsnetwerk certificaten gebruikt voor authenticatiedoeleinden, kunnen consumentenapparaten binnen het thuisnetwerk geen toegang krijgen tot bedrijfssystemen. Zo blijft het netwerkverkeer veilig en behoudt het beveiligingsteam volledig overzicht op het netwerkverkeer en de gebruikspatronen. Het team kan zo bovendien beschikken over alle informatie die nodig is voor het identificeren en verhelpen van potentiële problemen en bedreigingen.

Voor de overige 10% (de programmeurs en VIP's) zou deze netwerksegmentatie een solide basis moeten vormen voor veilig thuiswerken. Maar de gevoeligheid van de informatie waarmee zij omgaan vraagt om een extra beveiligingsniveau, namelijk de combinatie van een next generation firewall met geavanceerde beveiligingsdiensten die het zakelijke verkeer veilig houden en het zakelijke en privéverkeer gescheiden houden met het oog op de privacy. In sommige gevallen kan het nodig zijn om gebruik te maken van voorgeprogrammeerde hardware of in eigen beheer ontwikkelde protocollen, zodat werknemers veilige tunnelverbindingen met bedrijfssystemen kunnen maken. Dit alles kan worden gerealiseerd met behulp van een robuust routeringsplatform.

Conclusie

De mogelijkheid van thuiswerken is voor veel kenniswerkers niet langer een privilege, maar een absolute noodzaak. Bedrijven moeten daarom een oplossing implementeren die een einde maakt aan de beveiligingsproblemen die thuiswerken met zich meebrengt. Het in kaart brengen van de verschillende risiconiveaus van groepen werknemers en het toepassen van passende maatregelen binnen hun thuisnetwerk is een must. Dit is nodig om meer grip te krijgen op de digitale werkomgevingen van thuiswerkers en bedrijfsbrede beveiliging en compliance te waarborgen.

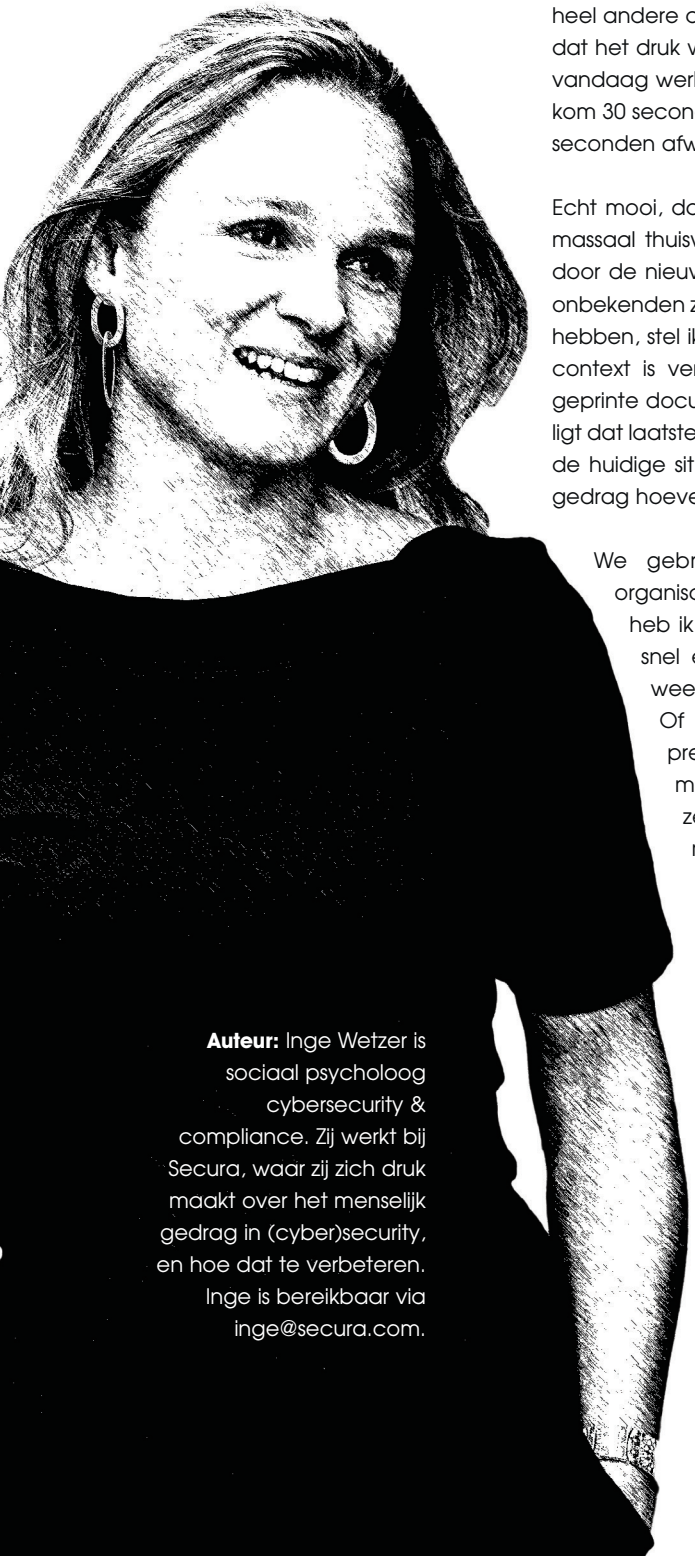
Referenties

(1) https://www.juniper.net/nl/nl/

(2)https://www.eurofound.europa.eu/publications/blog/europes-quiet-revolution-is-under-way

(3) https://ec.europa.eu/jrc/sites/jrcsh/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf

Thuiswerken



Sinds maart 2020 ziet de wereld er anders uit. We werken veelal thuis en dat geeft een heel andere dynamiek. Vandaag kwam een collega iets te laat een call in en grapte dat het druk was bij het koffieapparaat, omdat zijn vrouw voor hem was. Nee dan ik, vandaag werk ik alleen thuis. Net sta ik op om in de keuken een glas water te halen, kom 30 seconden later terug en zie dat ik mijn computer gelockt heb. Thuis ja. Voor 30 seconden afwezigheid.

Echt mooi, dat geautomatiseerde veilige gedrag. Maar is dat nog wel nodig nu we massaal thuiswerken? Jazeker! Informatieveiligheid blijft een aandachtspunt. Alleen, door de nieuwe situatie zou de focus moeten liggen op ander gedrag. Tenzij jij thuis onbekenden zonder bezoekerspas wilt aanspreken natuurlijk. Maar om meer impact te hebben, stel ik voor om vanuit de nieuwe risico's te redeneren. Simpelweg omdat de context is veranderd. Het gaat nu dus minder om het onmiddellijk ophalen van geprinte documenten, het dragen van je pas en het hebben van een clean desk, al ligt dat laatste overigens een beetje aan je relatie(status). Dat betekent echter niet dat de huidige situatie geen risico's met zich meebrengt en we dus niet meer over ons gedrag hoeven na te denken.

We gebruiken nu bijvoorbeeld massaal videoconferencing. De meeste organisaties schrijven voor welke tool daarvoor gebruikt dient te worden. Toch heb ik al menigmaal met klanten gesproken die vroegen "of we anders niet snel even via Whatsapp-bellen konden afstemmen". Dat scheelt namelijk weer het aanmaken van een afspraak…

Of het delen van je scherm tijdens videocalls. In plaats van alleen de presentatie, kreeg ik meerdere malen eerst iemands Outlook inbox te zien, met daarin mails die niet voor mijn ogen bestemd waren. Wat ik maar wil zeggen: ook in deze nieuwe situatie is er aandacht nodig voor de medewerkers in informatiebeveiliging. Alleen is de invulling daarvan nu wat anders.

Aan de slag dus, met het inventariseren van de risico's en welk gedrag we in deze situatie van de mensen willen zien! Om vervolgens op afstand mensen aan te sporen het goede gedrag te vertonen. Helaas krijgen we regelmatig in een persconferentie te zien hoe ingewikkeld die taak is. Eigenlijk voelen wij die struggle van Rutte in het klein: we kunnen de regels wel maken, maar het succes hangt af van het gedrag van de mensen. Wat niet betekent dat we niet succesvol kunnen zijn! Zo lang we ons maar realiseren dat we er niet zijn met het communiceren van de regels. Kijk verder dan de regels, denk na over wat de mensen nu tegenhoudt, inventariseer de behoeften die er leven in deze nieuwe situatie en hoe je de mensen het beste bereikt. En dus welk gedrag in deze thuiswerksituatie het belangrijkste is. Schreef zij net voor ze haar computer lockte toen ze wegliep.

Inge

Auteur: Inge Wetzer is sociaal psycholoog cybersecurity & compliance. Zij werkt bij Secura, waar zij zich druk maakt over het menselijk gedrag in (cyber)security, en hoe dat te verbeteren. Inge is bereikbaar via inge@secura.com.

Auteur: Jan Wessels is adviseur Risk & Compliance bij de Rabobank.
Jan is bereikbaar via Jan.wessels@rabobank.com.

Werken voor een financiële instelling vanuit huis

Eind 2019 leerde de wereld van het bestaan van het coronavirus. Rond de opkomst van dat virus waren we in Nederland druk met Citrixgate. De Universiteit van Maastricht was gehackt en als de wiedeweerga moesten in heel Nederland Citrixservers worden bijgewerkt. Thuiswerken was er voor ambtenaren niet meer bij en dat leidde op 20 januari 2020 tot 'Citrixfiles' (1). Het Nationaal Cyber Security Center kwam regelmatig met nieuws en updates over hoe we hiermee moesten omgaan (2, 3).

Ondertussen kwamen in januari bij de security community van de Rabobank al de eerste vragen vanuit Shanghai of het mogelijk was om vanuit huis te gaan werken. Immers, het vasteland van China zat al in een lockdown. Aan dat verzoek konden we vaak niet voldoen, omdat veel van de gebruikte systemen niet extern bereikbaar waren. Bovendien zijn veel toezichthouders in Azië tegen toegang tot systemen van buiten kantoor. Op dat moment viel het ook nog te overwegen om de werkzaamheden over te nemen op een andere locatie, zoals Hong Kong of Singapore.

Hierna ging het redelijk snel. De wereld raakte bekend met begrippen als 'lockdown' en 'thuiswerken'. In Nederland werken de meeste Rabobankmedewerkers sinds de oproep van het kabinet op zondag 16 maart 2020 thuis. Dat is inclusief de dienstverlening aan klanten. Net als bij ING en ABN AMRO zijn er een groot aantal lokale kantoren gesloten en op de kantoren die nog wel open zijn, zijn maar weinig mensen aanwezig. Bij het bestuurscentrum van de Rabobank in Utrecht werken normaal gesproken tussen zes- en achtduizend mensen per dag. Sinds de lockdown zijn dat er maximaal vierhonderd.

Het Nieuwe Werken

In veel gevallen was het al wel mogelijk dat medewerkers incidenteel thuiswerkten. De Rabobank is in Nederland zo'n tien jaar geleden al begonnen met Het Nieuwe Werken. Hierbij staat het tijd en plaats onafhankelijk werken centraal. Om thuis te kunnen werken is een laptop met VPN-software of toegang tot Citrix nodig. In beide gevallen is er sterke authenticatie vereist op basis van een token. Daarnaast zijn veel systemen die gevoelige informatie verwerken niet beschikbaar voor werken van buiten kantoor. Zoals toegang tot de kernsystemen, waarmee geld kan worden overgeboekt. De reden hiervoor is dan dat er rekening moet worden gehouden met beveiligings- en compliancevoorschriften.
Er zijn een aantal overwegingen om bepaalde zaken alleen binnen de muren van de bank plaats te laten vinden:

- Omgang met (zeer) gevoelige informatie over bedrijven en financiële markten. Dit is een zorg die ook wordt gesignaleerd door Financial Conduct Authority (4) en DNB (5);
- Bij het werken op kantoor is er ook sociale controle: collega's houden in de gaten wat er gebeurt;
- Veiligheid van de medewerkers. Bij de bankkantoren is beveiliging aanwezig en zijn er aanvullende maatregelen genomen om te voorkomen dat iedereen zo maar doorloopt. KPMG heeft een uitgebreide analyse gemaakt waarin deze punten worden behandeld (7).

Omschakelen naar thuiswerken

Vanuit toezichthouders worden er strenge eisen gesteld aan financiële instellingen. Vanuit de optiek van BCM (Business Continuity Management) moet gekeken worden hoe bedrijfsprocessen in verschillende scenario's door kunnen blijven werken. Tevens zijn er eisen vanuit informatiebeveiliging aan de integriteit en vertrouwelijkheid van informatie in de door IT-systemen ondersteunde bedrijfsprocessen.
Bij de BCM-scenario's hoort ook het 'pandemie'-scenario. In de BCM-organisatie is in zo'n soort geval een centrale rol weggelegd voor het Damage Assessment Team (oftewel DAT). Dit team coördineert de impact van de coronacrisis voor de interne organisatie en bereidt de nodige besluiten voor, in afstemming met autoriteiten en de geldende voorschriften.

De impact van de coronacrisis, en dan met name de maatregel om thuis te werken, is behoorlijk. Veel bancaire werkzaamheden werden vooral op kantoor uitgevoerd en sommige werkzaamheden mogen uitsluitend vanuit kantoor worden gedaan. De Rabobank is overgegaan op thuiswerken tenzij, waarbij de veiligheid van de IT-systemen, klanten en medewerkers voorop staat. Tevens moet het mogelijk zijn om de dienstverlening zo ongestoord mogelijk te laten verlopen.

In de eerste fase is gekeken onder welke voorwaarden medewerkers op grote schaal konden thuiswerken en of de risico's die dat opleverden, acceptabel waren. Een 'papieren exercitie' waarin we voordelen en nadelen proberen in te schatten. Het DAT-team heeft dit gecoördineerd en de besluiten voorgelegd aan de Groepsdirectie (formele risicoacceptatie). Dit in lijn met de interne risicomanagementprocessen van de Rabobank.
Aansluitend is er een uitgebreide risicoanalyse uitgevoerd, met ook voorstellen voor aanvullende maatregelen. Tevens is het zaak gebleken om het thuiswerken te monitoren op veiligheidsrisico's. Dat wordt continue in de gaten gehouden.

De rol van medewerkers en managers wordt belangrijker: er ligt een grotere verantwoordelijkheid bij hen om zich aan de maatregelen te houden.
In de praktische zin moest er ook het nodige gebeuren. Niet

iedereen (zeker in het buitenland) had al een laptop met token. Hoe kom je dan snel aan laptops en tokens, als de rest van de maatschappij daar ook mee bezig is?
De VPN voorziening moest ook heel snel worden opgeschaald. Dat was een actie die al wel voorzien was, maar nu binnen twee weken moest worden doorgevoerd. Normaal gesproken neemt de hele procedure 9 maanden in beslag. Denk ook aan het opstellen van richtlijnen voor het thuiswerken, met oog voor de menselijke factor. Hoe voorkom je te lang doorwerken, afleiding, meekijken of meeluisteren. En ook: gaat het nog goed met iedereen? Heeft iedereen een goede werkplek? Red je het wel?
Rabobank was al overgegaan op Office 365 met daarbij ook Teams. Gedeeltelijk was de organisatie al wel gewend om met Teams te werken en vergaderen. Voor veel anderen was het wel een steile leercurve in vaardigheden en `etiquette'-regels.
In de loop van de tijd zijn er min of meer spontaan activiteiten opgekomen om de informele ontmoetingen te vervangen en te zorgen voor collegiaal contact. Denk aan virtuele koffiemomenten (en borrels).

Medewerker als sterkste schakel

Het werken op kantoor heeft voordelen voor cyberveiligheid. Je kunt collega's direct spreken en als er iets gebeurt merk je dat. Als een systeem uitvalt, merkt iedereen dat direct. Ook bij vreemde telefoontjes of mails kun je dit direct delen.
Er zijn ook praktische fysieke maatregelen getroffen: het is niet goed mogelijk om buitenaf mee te kijken en je werkt vanuit compliance voorschriften in een afgesloten afdeling. Bij werken op afstand moet je daarover nadenken. De opkomst van Whatsappfraude (8) laat zien dat het vrij eenvoudig is om je als iemand anders voor te doen. Ook medewerkers kunnen op deze manier voor de gek gehouden worden door iemand die zich als een collega voordoet.

Een andere factor bij thuiswerken zijn huisgenoten en passanten: zij mogen niet zien wat je aan het doen bent en tot welke gegevens van klanten je toegang hebt. Dat is ook heel praktisch: wie kan er meekijken op jouw scherm of meeluisteren met jouw gesprekken. Dat zouden zo maar de buren kunnen zijn als het raam openstaat.
In algemene zin besteden we meer aandacht aan security awareness van de medewerkers. Het Cyber Security Beeld Nederland (3) laat zien dat er veel aanvallen zijn gericht op bedrijven en ook financiële instellingen, waarbij ook gebruik wordt gemaakt van phishing. Tijdens de coronacrisis is het aantal aanvallen toegenomen. Dit betekent dat medewerkers meer dan op kantoor zelf de afweging moeten maken welke mail of welk bericht wel betrouwbaar is en wat phishing is.
Door het Rabobank Security Awareness team is hier steeds aandacht aan besteed, met ook handige hand-outs.

In het kader van de Cyber Security Awareness maand (Alert Online) is er een onderzoek gepubliceerd naar kennis bij medewerkers (09). Medewerkers schatten over het algemeen hun kennisniveau als goed in, met de hoogste score bij bedrijven als Rabobank die onderdeel uitmaken van de vitale infrastructuur. Deze medewerkers maken zich wel weer meer zorgen over een cyberaanval.

Conclusie

Rabobank kon redelijk snel omschakelen doordat jaren geleden de ontwikkeling met Het Nieuwe Werken was ingezet. Veel medewerkers hadden al de beschikking over een laptop en een token. Er was al nagedacht over welke activiteiten wel of niet buiten kantoor mochten worden uitgevoerd vanuit risicoperspectief.
Vanuit beveiligingsoptiek komt er nu wel meer verantwoordelijkheid te liggen bij de medewerkers.

Referenties

(1) https://www.ad.nl/amsterdam/softwarecrisis-leidt-tot-citrixfiles-richting-den-haag~a662c2ec/
(2) Nationaal Cyber Security Centrum. Aanvallers zoeken actief naar kwetsbare Citrix-servers, https://www.ncsc.nl/actueel/nieuws/2020/januari/9/aanvallers-zoeken-actief-naar-kwetsbare-citrix-servers
(3) Nationaal Cyber Security Centrum. Cybersecuritybeeld Nederland (CSBN) 2020, https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020
(4) Hogget, J. (2020, 12 October). Market abuse in a time of coronavirus. Financial Conduct Authority, https://www.fca.org.uk/news/speeches/market-abuse-coronavirus
(5) https://fd.nl/beurs/1360481/toenemende-zorgen-over-thuiswerkende-bankmedewerkers
(6) https://nl.wikipedia.org/wiki/Tigerkidnapping
(7) https://home.kpmg/xx/en/home/insights/2020/05/key-cyber-risks-for-banks-during-covid-19.html
(8) https://www.ad.nl/tech/misbruik-geraffineerd-fraude-met-whatsapp-bijna-vervierVoudigd~af5f2d95/
(9) Alert Online. Medewerker onderschat digitale dreiging. https://www.alertonline.nl/nieuws/2020/medewerker-onderschat-digitale-dreiging

‘WIJ DOEN UT SOAMEN’

Terwijl buiten winterstorm Bella raast en de natuur zich van zijn ruige kant laat zien, een vrachtauto tussen Winschoten en Groningen zijn lading bieten verliest die nu over kilometers verspreid liggen, neem ik plaats achter mijn bureau om mijn bijdrage aan de eerste iB-copy van 2021 te leveren.

We sluiten over enkele dagen het boek van het jaar 2020.

Het jaar dat:
Het kabinet met ingrijpende maatregelen komt;
Rutte oproept: “We hebben iedereen nodig, 17 miljoen mensen”;
We massaal toiletpapier hamsteren;
De quarantainekilo ‘s of ook wel lockdownkilo’s zich aandienen;
Nederland op SLOT gaat;
Naar schatting 1200 festivals gecanceld worden;
We zoomen, teamsen, webexen, skypen en hangouten;
Horeca, contactberoepen en zzp’ers de hardste klappen krijgen.

En we kregen er een lexicon bij. Wat dacht u van:

> **appathon** (de, -s) bijeenkomst van deskundigen op het gebied van programmering, dataverzameling en cybersecurity om apps (bv. traceerapps t.b.v. de strijd tegen een corona-epidemie) grondig te testen en voor eventuele tekortkomingen gezamenlijk naar (technologische) oplossingen te zoeken.

Ik heb in het afgelopen jaar meer dan 2000 uur doorgebracht aan dit bureau. Dit was een zwaar en zeer bewogen jaar. Ik heb aan dit bureau extreem veel vergaderd, besluiten genomen, gerouwd, gelachen en was regelmatig diep geraakt door het leed dat velen van ons hebben geleden. Ik ben hoopvol als ik zie hoeveel solidariteit en veerkracht er is in onze samenleving. Ik denk regelmatig aan hoe het straks zal zijn, als we de pandemie onder controle hebben. Wordt het binnen onze vereniging weer zoals voorheen? Wat er ook gebeurt, hoe snel of langzaam het ook zal gaan, een ding is zeker: deze pandemie heeft ons heel duidelijk heeft gemaakt hoe kwetsbaar we zijn, hoe afhankelijk we zijn en hoe moeilijk het is om draagvlak te krijgen in een gemeenschap bij het streven naar een gemeenschappelijk doel.

Ik zie er naar uit om elkaar in 2021 weer te treffen. Dat we na een zware dag op het werk afreizen naar Utrecht om bij het Van der Valkhotel gezamenlijk – zij aan zij – te genieten van een lezing. Dat we weer onder het genot van een broodje en een drankje ideeën en ervaringen uitwisselen. Dat we als young professional een kijkje kunnen nemen in de ‘beveiligingskeuken’ van een PvIB-lid.

Ik kijk er ook naar uit te weten welke nieuwe inzichten deze pandemie met zich heeft meegebracht. Bijvoorbeeld veranderingen in het dreigingslandschap, de impact op security bij het werken op afstand, effectief deelnemen aan discussies via beeldbellen. En wellicht leiden deze nieuwe inzichten ook tot nieuwe activiteiten met onze leden. Ik ben er klaar voor. U ook?

Schroom niet om ideeën met mij en mijn collega-bestuursleden te delen. We gaan voor het nieuwe normaal verrijkt met zoveel mogelijk nieuwe inzichten.

Ik zeg 2021: “Wij doen ut soamen”

Jessica Conquet
Uw voorzitter

Auteurs: Maurice Derogee is werkzaam als Information Security Officer bij servicepunt71.
Maurice is bereikbaar via m.derogee@servicepunt71.nl

Thuiswerken in (post)coronatijd

We zijn alweer een nieuw jaar gestart en nog volop bezig met dat waarmee wij het afgelopen jaar afsloten: het coronavirus. Terugkijkend op (voor mij) thuiswerken sinds 12 maart 2020 als informatiebeveiliger, voelt het toch wel als een tropenjaar met vele gezichten en gemengde gevoelens. De titel van dit artikel waarin (post)corona staat vermeld, schrijf ik in december 2020 waarbij ik vurig hoop op het weg kunnen halen van deze haakjes maar, eigenlijk weet ik wel beter.

Wat is mij nou eigenlijk opgevallen aan het thuiswerken in het afgelopen jaar? Nu ik mij dat zo afvraag, gaan de raderen draaien en constateer ik (vanuit mijn werkveld) dat op het gebied van incidenten en datalekken het relatief stil is gebleven. En de cijfers liegen er toch weer niet om, die de AP publiceert omtrent datalekken. Achterdochtig denk ik dan: 'zouden de mensen dat dan wel netjes hebben gemeld als deze gebeurtenissen hen overkomen waren', immers thuis werk je op jouw eigen manier en tijdstippen; is er geen groep collega's die met jou de ruimte delen en zijdelings meekrijgen wat je uitvoert, lees: de sociale controle. Al zit je enkel in je overhemd met daaronder de boxershort in een video meeting, niemand zal het weten. En als beveiliger is het 'niet weten' iets waar je van wakker kan liggen en dan doel ik niet op de (in)correcte kleding van de collega's in de meeting, maar natuurlijk wat deze zo allemaal uitvoeren en of dit dan binnen onze kaders regeltjes en beleid past.

Zou ik het weten als dit niet zo was? "Een goede vraag, niet!" Gelukkig kan ik voor mijn werkveld zeggen dat ik binnen de organisatie in ieder geval een basis heb van werkplekken die hetzelfde zijn ingericht en beveiligd alsook nog centraal kunnen worden beheerd via een Mobile Device Management oplossing. Kunnen schrijf ik bewust want daarop lopen we nog achter. De e-mails worden automatisch gescand op phishing, malware, virussen, spam en de geldende e-mailstandaards (vanuit het forum standaardisatie). Voor het versturen van gevoelige zaken hebben we een voor ons goed werkend systeem ingericht met - in onze e-mail client - een plug-in die ook meeleest en jou wijst op gevoelige inhoud of de onbekende geadresseerde waarheen je deze gegevens wilt gaan sturen.
De systemen zelf zijn voorzien van goed werkende lokale beveiliging welke vanuit de cloudomgeving worden beheerd. Dat geeft wel rust en zeker met een SOC-service die goed op de hoogte is van onze omgeving, de crown jewels en dit voor ons 7x24x365 dagen bewaakt. Hieraan een escalatiematrix voor de handelingen die zij mogen verrichten in overleg met onze externe partners (want we hebben een outsourcing achter de rug dus nu meer dan drie externe partijen die alles doen).
Achterover leunen dus, zou je zo denken, helaas zo werkt het niet. De security patches vliegen om de oren en de phishingmails worden niet allemaal tegengehouden. Hier en daar wat miscommunicatie met de beheerorganisatie, waardoor belangrijke zaken (te) lang bleven liggen. Ook kom je tot de conclusie dat de werkplekken toch best veel vrijheden bieden en dus mensen allerhande apps proberen te installeren zoals Zoom, Jitsi, Google Hangouts en wat nog meer; dus beleid aanpassen, een standpunt innemen en tegelijk de antivirus applicatie aanpassen want wij willen enkel Teams als standaard. Inderdaad MS Teams, maar we zitten nu eenmaal in de 365 cloud en hebben hier kennis van en ondersteuning voor, en niet de mogelijkheid allerlei alternatieven te onderzoeken (op afstand).

Nu werken onze werkplekken buiten het kantoor ook nog via een VPN om binnen bij de bedrijfsomgeving te komen en gebruiken we de Office365 omgeving van Microsoft met als extra MFA. Wacht even? MFA?, dan moeten we een app installeren op de zakelijke smartphone maar die worden (nog) niet beheerd. Dan zenden we wel een handleiding naar onze medewerkers en dan komt alles goed?!
Ik besef echter dat met de praktische oplossing die zakelijke telefoon dus ook de Achilleshiel vormt van onze werkplekbeveiliging. Aan de telefoon zit geen beleid gekoppeld, geen specifieke beveiliging en de medewerkers zelf doen er werkelijk alles mee. En terwijl ik dit schrijf komt er een melding via e-mail van een mogelijk incident op een zakelijke telefoon binnen.

Ondanks de 5 graden buiten heb ik het warm gekregen, begint mijn onderzoek en gelukkig blijkt al snel dat het loos alarm is, want de vreemde codes en gekke nummers - waar deze vandaan gekomen zijn - betroffen de MFA-codes per SMS. Dan nog maar even een uitleg het intranet opsturen. Weer een nieuw bericht; dit keer van de IBD over gevallen van WhatsAppfraude waarbij criminelen met de 6-cijferige code - bedoeld voor overzetten van jouw account naar een nieuwe telefoon - het account kunnen overnemen. Dus weer een nieuw intranetbericht, nu om mensen te waarschuwen, te instrueren hoe te handelen en ook indien het al is misgegaan. Gelukkig geen meldingen (althans voor zover ik weet).

Ondertussen nog een Coordinated Vulnerability Disclosure (Responsible Disclosure) melding van een oplettende burger dat er een FTP-server kwetsbaar is op het SMB-protocol dus meteen hem bedanken en dat ook weer intern doorzetten zodat het verholpen kan worden. Eigenlijk business as usual, valt mij zo op, maar dan alleen vanuit huis met regelmatig de behoefte zaken direct met betrokkenen te bespreken zonder naar een scherm te praten. Want je merkt toch wel dat dit vaak een beter effect heeft en het

doel eerder wordt bereikt dan via videobellen.
Al met al toch weer dezelfde conclusies als ook in de diverse oefeningen vanuit het Rijk in oktober 2020 tijdens de Overheidsbrede Cyberoefening. Weet wat je hebt, wat hiervan extra belangrijk is en zorg dat dit up-to-date blijft. Niet meer te patchen, maak dan werk van het vervangen of uitfaseren. Kan dat echt niet, probeer dit dan te isoleren van de rest van de systemen (segmentatie). Monitoring en logging zijn van groot belang alsook wie er (waarvoor) verantwoordelijk is binnen de organisatie en hoe er ook op afstand een team kan worden samengesteld (CSIRT) bij een incident of calamiteit.

Een SOC service is van grote toegevoegde waarde, helemaal als zij de firewalls beheren en kwetsbaarheden in kaart brengen. Naast de juiste personen intern natuurlijk ook extern - als er geoutsourced is met de juiste bevoegdheden - want je wilt spijkers met koppen slaan als het nodig is.
En als laatste punt maar feitelijk als belangrijkste eerste punt het bewustzijn van de medewerkers. Naast oefenen, oefenen, is ook trainen noodzakelijk. Gooi die PowerPoint nu eens weg en zoek naar een oplossing waar je kunt bijhouden hoe de adoptie is van de uitgestuurde trainingen en ook de diversiteit aan onderwerpen. Hou het vooral leuk en afwisselend. Maar vergis je niet, want zo een awareness tool - zou je er al eentje mogen aanschaffen of al hebben - is een hele klus. Net zoals beleid moet het aansluiten bij de organisatie, de werkzaamheden per afdeling, de missie, visie en strategie van de organisatie. Last but not least, moet het ook nog eens te begrijpen zijn. Maar naast dit alles, nog een niet onbelangrijk aspect: de werkplekken én daar versta ik dan ook de telefoon onder. Deze moeten echt wel beheerd zijn, want denk maar aan een gebouw of 40 met (voor mij) 2.500 onbeheerde deuren naar binnen en nog eens 2.500 onbekende locaties erbij als je het thuiswerken meeneemt. Kan dit ook met BYOD ofwel iedereen gebruikt eigen apparatuur, al dan niet via een budget vanuit de werkgever?

Ja, dat kan zeker wel, maar ook hier zul je dan als werkgever een beleid voor moeten opstellen met behulp van de beveiligingsorganisatie. De medewerker daarbij volledig vrijlaten met betrekking tot de wijze waarop verbinding wordt gemaakt met welk apparaat van zijn keuze dan ook. Daarbij stelt de verbindingsprogrammatuur zelf de eisen waaraan het apparaat dient te voldoen om verbinding te mogen maken (verbindingsregels: profiling). Dat, alhoewel ik hier zelf geen voorstander van ben (denk aan een realisatie binnen de traditionele Citrix-omgevingen).

Ik ben wellicht wat traditioneel, maar mijns inziens moet een zakelijke omgeving met beheerde apparatuur worden benaderd en dat zeer zeker bij een organisatie die tot de overheid behoort of gevoelige gegevens van cliënten beheert. Dat kan op diverse manieren en er is altijd wel een passende oplossing denkbaar waarbij ook de medewerker tevreden kan zijn met de door de werkgever verstrekte middelen of keuzes.

Het CYOD oftewel Choose Your Own Device biedt mogelijkheden van keuzevrijheid onder voorwaarde van beheerde en beheersbare werkplekken. Ik zie al jaren discussies over de diverse scenario's en allemaal bezitten ze zowel voor- als nadelen. Het hangt vooral van het soort organisatie af. Echter, zoals zo vaak geroepen wordt en wat ik als een waarheid beschouw, dichtspijkeren is niet de weg.
Zakelijke apparatuur, zoals de smartphone, kan worden voorzien van een gewenst privé profiel; zodat je ook een eigen omgeving kunt realiseren met de foto van het gezin op de achtergrond. Als beheerder geef je dan precies aan wat er wel en niet tussen de profielen mag worden uitgewisseld. En voor de werkplek is het een vraag of die persoonlijke achtergrond echt wel zo erg is, want je kunt ook afspreken dat bij gesprekken met klanten - via bijvoorbeeld Teams - een zakelijke achtergrond wordt gebruikt met de bedrijfshuisstijl.

En verbied je de installatie van applicaties uit de Microsoft Appstore of Google Play, zorg er dan wel voor dat alle tools en applicaties die nodig zijn er al op staan of heel snel kunnen worden beoordeeld en geleverd op afstand! Langskomen op de zaak voor zoiets, is inmiddels toch zó 2019. En denk ook na over randapparatuur die thuis kunnen worden gekoppeld - zoals privéprinters en externe harddisks of ander soortige opslagmedia - want daar word je zeker mee geconfronteerd als je een werkplek beheert en uitgeeft. Laat vooral een diverse groep collega's in een pilot het werkplek-concept goed testen, zorg ervoor dat er een goed programma is opgezet voor de adoptie van het concept alsook alle tools en applicaties die er worden meegeleverd.

Wat mij in de coronacrisis vooral is opgevallen is dat mensen door alle maatregelen zich bewuster zijn geworden van de diverse risico's en dat er voor ons als beveiligers toch een soort van rode loper is uitgerold, omdat veel van ons werk hier direct naartoe te vertalen is. Mensen begrijpen de door ons geschetste risico's nu beter dan voorheen. Laten wij beveiligers die kans grijpen!

Auteurs: Tom Bakker is redactielid van iB-Magazine. Tom is bereikbaar via tombakker@pvib.nl Sandra Kagie is freelance tekstschrijver (Sanscript Tekstproducties). Sandra is bereikbaar via info@transcriptproducties.nl

INTERVIEW

PCI compliance daalt opnieuw

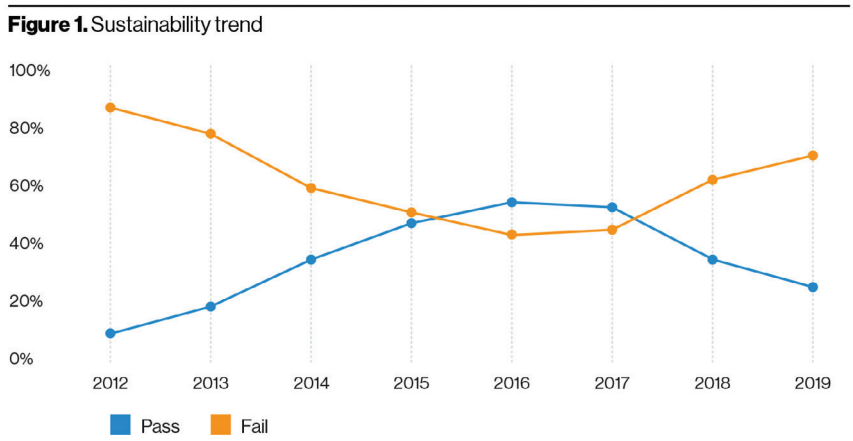
‘Verontrustend’, zeker in coronatijd

Het 2020 Payment Security Report van Verizon laat voor het derde jaar op rij een daling zien in de naleving van de Payment Card Industry Data Security Standard (PCI DSS). “Dit betekent dat organisaties wereldwijd creditcardgegevens van hun klanten in gevaar blijven brengen. Terwijl deze gegevens voor cybercriminelen juist een van de meest lucratieve en daarmee gewilde doelwitten blijven”, waarschuwt Gabriel Leperlier, senior manager security consulting EMEA van Verizon.

Phishing is niet alleen schadelijk voor particulieren, maar ook voor de bedrijven wiens handelsnaam wordt misbruikt in de phishingberichten. Het doet uw reputatie geen goed als klanten uit uw naam worden misleid. Aan beide zijden kan veel leed voorkomen Uit het jongste Payment Security Report (PSR), dat in november 2020 werd gepresenteerd, blijkt dat het percentage bedrijven dat volledig PCI DSS-compliant is, wereldwijd is gedaald van 36,7 procent in 2018 tot 27,9 procent in 2019. Terwijl in 2016 en 2017 wereldwijd nog 55,4 respectievelijk 52,5 procent van de bedrijven voldeed aan de internationale beveiligingsstandaard die is ontwikkeld om organisaties te helpen hun betaalsystemen te beschermen tegen inbreuken en diefstal van gegevens van kaarthouders.

‘Verontrustende trend’

“Verontrustend”, noemt Leperlier de nieuwe daling. Dit zeker in het licht van de coronapandemie die eraan bijdraagt dat consumenten overal ter wereld steeds meer overgaan tot contactloos betalen met bijvoorbeeld creditcards. De veiligheid van betalingen moet wat hem betreft dan ook meer dan ooit worden gezien als een `doorlopende bedrijfsprioriteit’. “En juist die duurzame aandacht voor security vormt voor veel bedrijven een probleem”, stelt hij. Dat steeds meer bedrijven niet voldoen aan de PCI-



Figuur 1 - State of compliance: Eight-year trend.

standaard is volgens Leperlier, samengevat, te wijten aan een gebrekkige security-strategie en uitvoering hiervan op de lange termijn. Dat veel bedrijven moeite hebben om gekwalificeerde CISO's of security-managers voor langere tijd aan zich te binden, speelt hierin volgens hem zonder meer een belangrijke rol. Ook ziet hij in de praktijk dat het hogere management binnen veel bedrijven initiatieven op het gebied van gegevensbeveiliging en compliance op de lange termijn onvoldoende ondersteunt.

Zeven valkuilen

In het rapport onderscheiden de opstellers daarom zeven valkuilen die het hogere management binnen veel bedrijven ervan weerhouden een gedegen langetermijn security-strategie op te stellen en uit te voeren:

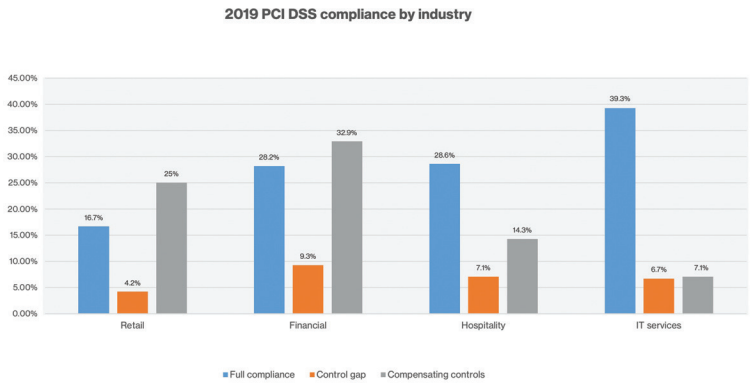
1. Inadequate leadership
2. Failing to secure strategic support
3. Lack of resourcing capabilities
4. Falling short on sound strategic design
5. Deficient strategy execution
6. Low capability and process maturity with lack of continuous improvement
7. Communication and cultural constraints

"In veel bedrijven zien we dat de betrokkenheid van de leiding wat security betreft beperkt blijft tot de benoeming van een CISO of DPO om hem vervolgens verantwoordelijk te maken voor alles", gaat Leperlier in op met name de eerste valkuil. "Dat kun je met de beste wil van de wereld geen strategie noemen."

Wat je volgens hem vervolgens ziet, is dat een CISO of DPO geen enkele steun vanuit het management ervaart waardoor geen structurele vooruitgang kan worden geboekt als het gaat om een volwassen securitybeleid. Ook is in zijn ogen de CISO vaak niet ideaal gepositioneerd. Zo rapporteren veel CISO's aan de CIO waarbij in zijn woorden `conflicts of interest' kunnen ontstaan. "Beter is rapporteren aan de CFO of nog liever aan de CEO", stelt Leperlier. Dat laatste is wat hem betreft de situatie `in de ideale wereld'.

Alles bij elkaar genomen zie je binnen veel organisaties volgens hem dat een CISO na twee of drie jaar alweer vertrekt. Soms gedwongen na ontslag dat bijvoorbeeld volgt op een serieus incident, maar vaak ook vrijwillig omdat goede CISO's nu eenmaal populair zijn bij headhunters. Maar wat de reden voor het vertrek ook is, elke twee of drie jaar een nieuwe CISO is in de woorden van Leperlier funest voor continuïteit in securitybeleid.

De Payment Card Industry Data Security Standard (PCI DSS) is de internationale beveiligingsstandaard die is opgesteld door een samenwerkingsverband van creditcardmaatschappijen. PCI DSS helpt bedrijven die betalingen met creditcards accepteren hun betaalsystemen te beschermen tegen datalekken en diefstal van gegevens van kaarthouders. Elk bedrijf dat creditcardbetalingen accepteert dient jaarlijks PCI DSS-compliance aan te tonen. Ondernemingen met meer dan zes miljoen kaarttransacties per jaar moeten elk jaar een audit op locatie laten uitvoeren door een QSA, Qualified Security Assessor. Dit geldt ook voor bedrijven die door een creditcardmaatschappij zijn aangemerkt als `Level 1 merchant'. Voor andere bedrijven geldt dat zij een online vragenlijst (self assessment) in moeten vullen in combinatie met netwerkscans om zo aan te tonen dat ze compliant zijn. (1)



Figuur 2 - 2019 PCI DSS compliance by industry.

Extra uitdaging in coronatijd

Net als in eerdere interviews die we met hem hadden, benadrukt Leperlier ook dit keer dat de meeste bedrijven die bij een tussentijds assessment niet-compliant blijken te zijn, dit bij de jaarlijkse 'final compliance validation' wel zijn. Hij noemt een percentage van zeker negentig, misschien wel 95 procent. "Punt is echter dat je als bedrijf in de tussentijd risico hebt gelopen. En je klanten dus ook. Het gaat er met andere woorden niet om dat je bij de final validation compliant bent. Het gaat erom dat je continu compliant bent", stelt hij.

Een uitdaging, in deze tijd van corona, beaamt hij meteen. "Heel veel mensen werken immers vanuit huis. En dat betekent dat bedrijven, zeker in het begin van de corona-crisis, systemen wat meer open hebben gezet. Dit om het medewerkers überhaupt mogelijk te maken van huis uit te werken. Security was hieraan op sommige momenten even ondergeschikt."

Een risico dat in zijn ogen nog altijd bestaat. Omdat we nog steeds veel vanuit huis, op bijvoorbeeld eigen computers en laptops werken. Via deze apparaten kunnen criminelen volgens hem zomaar toegang krijgen tot belangrijke documenten of zelfs het bedrijfsnetwerk. "Ook wanneer je gebruikmaakt van een VPN-verbinding, zo is het afgelopen jaar al vaker gebleken", waarschuwt hij.

Wat corona daarom vooral betekent voor bedrijven als het gaat om security en daarbinnen het voldoen aan de PCI-standaard, is dat de scope van zo'n compliance-traject veel breder is geworden. "Systemen die creditcardgegevens bevatten en alles en iedereen die hier direct mee communiceert, zijn hierdoor lastiger te scheiden van systemen waarvoor dit niet geldt", verduidelijkt hij.

Top en flop door de jaren heen

Het 2020 PSR laat duidelijk zien dat er bepaalde requirements zijn binnen de PCI-standaard waar bedrijven de afgelopen vijf jaar consequent slecht op scoren. Dit zijn achtereenvolgens:

- Requirement 11: test security systems and processes
- Requirement 12: securitymanagement
- Requirement 6: develop and maintain secure systems

Terwijl bedrijven het wat betreft deze requirements binnen de PCI-standaard de afgelopen vijf jaar juist behoorlijk goed doen:

- Requirement 7: restrict access
- Requirement 5: protect against malicious software
- Requirement 4: protect data in transit

Werk aan de winkel

Requirement 11 omvat het gebruik van vulnerability scanning, penetration testing, file intergity monitoring and intrusion detection. Dit om er zeker van te zijn dat zwakheden worden geïdentificeerd en opgelost.

Al sinds het eerste report in 2010 blijkt dit de requirement te zijn waarop organisaties het slechtst scoren. "Scores worden zelfs slechter", geeft Leperlier aan. "Vooral als het gaat om het doen van vulnerability scans en het implementeren van penetration testing."

De antwoorden op de vragen 'Do you have a vulnerability management process?' en 'Is there a penetration testing program in place' zijn wat dat betreft veelzeggend. Op beide vragen antwoordt namelijk 51% van de ondervraagden in een onderzoek door Orange Defense waar in het 2020PSR naar wordt verwezen met 'Absent'. Werk aan de winkel dus voor heel veel organisaties wanneer je het Leperlier vraagt. (2)

Of hij verwacht dat de dalende trend, wat betreft het volledig PCI DSS-compliant zijn, volgend jaar zal worden omgebogen, vindt Leperlier lastig te zeggen. "Ik heb geen glazen bol, maar we hopen het natuurlijk wel", zegt hij voorzichtig. "Wanneer het hogere management zich bewust is van de zeven genoemde valkuilen, zijn organisaties in elk geval goed op weg", besluit hij positief.

Referenties

(1) www.pcisecuritystandards.org

(2) Het complete 2020 Payment Security Report is te vinden op de website van Verizon: https://www.verizon.com/business/resources/reports/payment-security-report/

Auteur: Rob van Os is Senior Adviseur Informatiebeveiliging bij CZ.
Rob is bereikbaar via rob.van.os@cz.nl

OODA-looping your security incident response

Cyber security has a history of taking concepts from the military domain and applying them to the cyber domain. But not every military concept can be successfully transferred to the cyber domain. In this article, the application of John Boyd's OODA loop to security incident response is examined.

John Boyd was an air-force pilot and military strategist. He developed ideas around military combat based on his own experiences and by combining military strategy with scientific ideas. Boyd coined the OODA loop in a set of 5 slides called 'The Essence of Winning & Losing' (1). His visual representation describes the four phases in the OODA loop: observe (gather information), orient (information analysis and synthesis of hypotheses), decide (choose a hypothesis), act (test the hypothesis). It also outlines the feedback mechanism. The foundation of the OODA loop lies in years of earlier research. Boyd did not publish his explanation of the OODA loop but shared most of his thoughts in briefings. This leaves room for (mis)interpretation of his ideas. For example; a simplified version of the OODA loop is often used, that lacks the depth and sophisticated reasoning behind Boyd's ideas. For an in-depth analysis, the work by Osinga on Boyd (2) provides an excellent starting point. The OODA loop (figure 1).

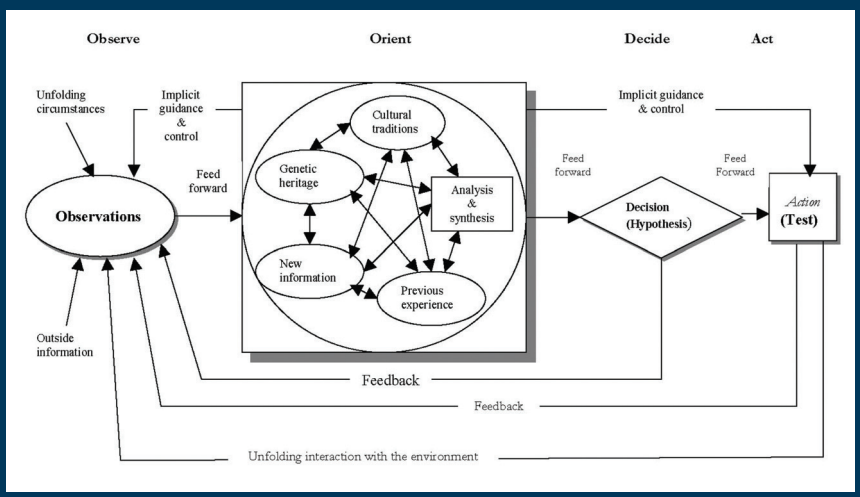


Figure 1 - OODA loop (Osinga, p.270).

Applications of the OODA loop: From a high-level perspective, the OODA loop describes the dynamic between two parties in a conflict. From a cyber security point of view, this can be translated to cyberattacks and cyber war.

Agility / adaptability: The essence of the OODA loop is the ability to adapt to unfolding circumstances and trying to prevent the other party from doing the same. Adaptability can be specific (cyberattacks) or generic (whole organizations). Thus, the OODA loop can act on the strategic, operational and tactical level, in that particular order (3). Strategy deals with goals and objectives (why and with what), operations deal with campaigns and operations (what/where), and tactics deal with de details of the actual engagement (how).

Strategic application: Applying the OODA loop at the strategic level means adapting the approach to dealing with attackers. This could be changing the allocation of means required to deal with adversaries. A strategic decision can be to implement a security operations center.

Operational application: Applying the OODA loop at the operational level means adapting operations or campaigns. In case of cyber security, this means changing security operations to deal with the attack. Or, in case of the attacker, adapting the way of working. In both cases, adapting operations means changes in procedures and processes. For cyber security, threat intelligence plays an important role to make

informed decisions on adapting operations to the new or changing threats.

Tactical application: Applying the OODA loop at the tactical level means responding to adversary actions at the lowest level of decision making. The aim of the OODA loop for the defender is to eliminate the attacker from the infrastructure, while the aim of the OODA loop for the attacker is to evade defences and achieve their goals. Adaption at the tactical level means applying changes in technology and toolsets.

Each layer will have a different processing speed: changes to the tactical level can be applied rapidly, while changes to strategy cost a significant amount of time. Additionally, changes to the strategical layer will slowly propagate to lower layers.

Rapid OODA looping: A common phrase in OODA loops is winning by `getting inside the opponents OODA loop'. Boyd puts it like this: "Get inside adversary observation-orientation-decision-action loops (at all levels) by being more subtle, more indistinct, more irregular, and quicker – yet appear to be otherwise" (Osinga, p.229). Indeed, speed is important, especially at the tactical level. But subtlety, indistinction and irregularity are also mentioned, stressing the importance of avoiding patterns and predictability.

The OODA loop in cyber attacks: In this section, the phases of the OODA loop in the context of cyber security incidents, specifically the viewpoint of the defender, is examined.

Observing cyber attacks: The core element of observing cyber attackers is based in the detection capabilities of the organization. This capability depends on visibility: availability of information required for detection and technology: tooling required for processing such information for detection purposes. The visibility triad (4) is a helpful high-level concept. Determining low-level visibility (of attack techniques) is also possible using tools like DeTT&CT (5).

The detection capability receives several inputs:

- Unfolding circumstances. The circumstances of the security incident taking place. As multiple iterations of the OODA loop are conducted, the circumstances change and the accumulated information from several observe phases will create a more complete picture of the attack as it unfolds.
- Outside information. Threat intelligence about the attacker, based on the observed techniques, tactics, malware, exploits, infrastructure, etc. Such intelligence can come from public sources (Open Source Intelligence, OSINT), intelligence partners or closed communities.
- Unfolding interaction with the environment. Part of the double-loop feedback system (6) within the OODA loop. The interaction is a result from previous actions. From the defender's point of view, this involves the changes that occur to the environment and the adversary's OODA loop when defensive actions (such as blacklisting IP addresses) are performed.
- The feedback input is also part of the observe phase. This feedback results from the decide and act phases and alter the mental model of the defender.

Situational awareness: One of the desired outcomes of the OODA loop and especially the observe phase is situational awareness: being aware of both your own environment and capabilities, and the opponent's environment (and capabilities) and adapting to those. To support achieving situational awareness, it is possible to use the diamond model for intrusion analysis (7).

Orientation in cyber attacks: Orientation is the most important activity in the OODA loop. This is where analysis & synthesis takes place, that uses the information that was observed to ultimately create hypotheses on how to proceed. The orient phase heavily depends on the mental model (8) of the security analyst. It is important to realise that analysis & synthesis is unique to each analyst, even when dealing with the same information (observations). This is due to the differences in the elements shaping analysis & synthesis, including genetic heritage and previous experience. To partly overcome these differences, the analyst's (or analyst team) mental model should be shaped through training & exercise (providing implicit guidance and control). Note that it says 'partly', as differences cannot be completely overcome. The remaining differences can be used as a strength rather than a weakness, as it allows for different solutions / hypotheses. Cognitive bias (9) and analyst fatigue (10) are also important factors to deal with in orientation.

Decisions in cyber attacks: In the decide phase, the hypothesis is chosen that is tested in the action phase. The actions that are defined in the decision phase should be:

- Efficient. Actions should be efficient, supporting the idea of rapid OODA looping;
- Effective. Actions should effectively set attackers back in their attack efforts;
- Disruptive. Actions should seek to disrupt the attacker's OODA loop.

The Pyramid of Pain and a Course of Action matrix can be used to support these goals.

Pyramid of pain

The Pyramid of pain (11) is a concept that explains how hard it is for attackers to change aspects of their attack. The pyramid is shown in figure 2.

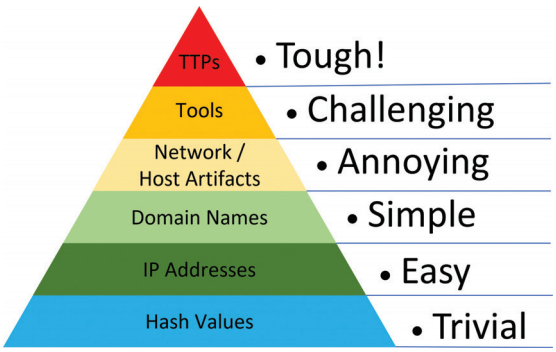


Figure 2 - Pyramid of Pain. (Detect-respond.blogspot.com)

The lower levels of the pyramid can be changed with little effort (possibly automatically) by the attacker, the higher levels represent challenging adaptations. The top level represents the modus operandi of the attacker. If the defender can take actions at this level, attackers will have to change their entire way of working. Actions higher in the pyramid of pain are more effective in disrupting the attacker's OODA loop and stopping the attack. However, the pyramid of pain also represents the difficulty of defenders to detect and act against attackers. Detection at the lower levels is a simple task that can be easily automated. The top levels require insight into the adversary's operation and way of working and are more difficult to execute. The organisation should decide whether to take immediate action in the lower levels of the pyramid, or to wait and perform additional analysis and synthesis before acting.

Course of Action matrix: To support and speed up decision making, Courses of Action (CoA) can be standardized. The correct CoA is dependent on the attack stage, the amount of information known about the attacker and the intrusion, and defensive capabilities of the organization. In the Cyber Kill Chain whitepaper (12), a course of action matrix was introduced. Military Information Operations (IO) doctrine differentiates between defensive and offensive IO (13), and mentions the following effects:

- Offensive IO: destroy (damage a system), disrupt (interrupt information flow between command & control (C&C) nodes), degrade (reduce effectiveness), deny (withhold information about the target), deceive (provide false information), exploit (gain access to attacker C&C infrastructure), influence (influence attacker behaviour).
- Defensive IO: protection (prevent attacks), detection (discover attacks), restoration (bring systems back to their original state), response (react quickly to attacks).

Some of these effects are within the technical and legal capabilities of the defending party, while some are not. A more nuanced view on offensive IO can be found in a study on active defense (14), that defines a grey area between truly offensive actions (destroy, exploit, and partly disrupt) and defensive actions (as defined in defensive IO). Figure 3 represents active defense.

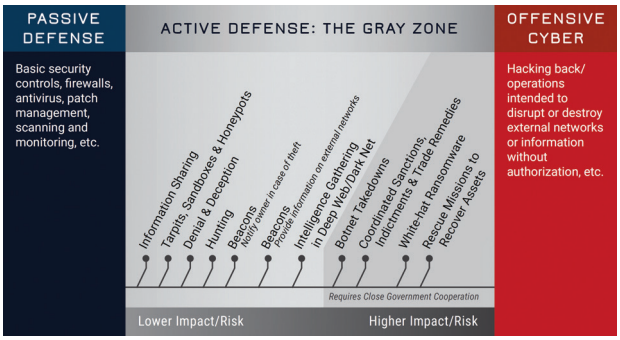


Figure 3 - Active Defense. ('Into the gray zone').

Each of the offensive IO effects impacts the attacker's OODA loop in a different way. Destroy, Exploit, Disrupt and Degrade mostly affect the attackers 'act' phase, as they are less able to perform their offensive actions. Deny and Deceive mostly affects the attacker's observe phase, as they have less information to go on. Influence mostly affects the attacker's orientation phase, as influence seeks to modify the mental model of the attacker through perception management. Using this information, a high-level CoA matrix can be created. The matrix does not include specific actions to take, but instead outlines where actions can be taken. The MITRE ATT&CK tactics (15) are used to indicate the attack stage. Figure 4 shows the CoA matrix.

The colors used in the 'IO effects' represent passive actions (green), offensive actions (red) and active defense (orange). Offensive IO is not filled in, as it is beyond the capabilities and legal possibilities of most organizations. To create a detailed CoA matrix, the techniques underlying the tactics are examined. For example, if the organisation wants to disrupt command & control, there are 16 applicable techniques. An appropriate action needs to be determined for each technique. The 'mitigations' suggested in the MITRE ATT&CK framework can serve as a basis. The table below provides an abbreviated example:

The creation of a detailed matrix can be time consuming. However, it will provide a detailed defensive capability matrix for the organization, which is very valuable in incident response efforts. To save time, the organization can take a risk-based approach on which tactics and techniques to

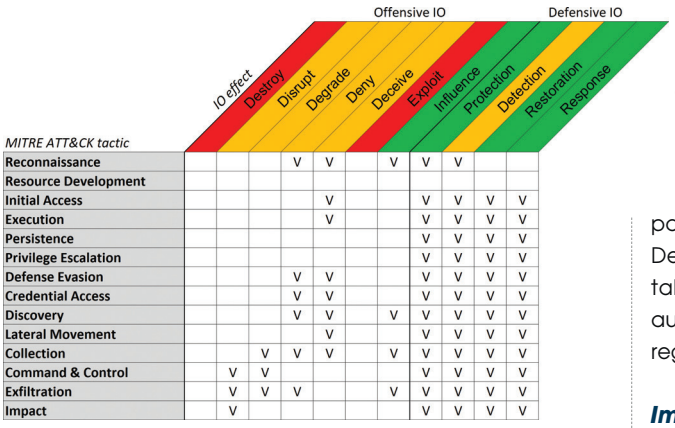


Figure 4 - High-level CoA Matrix.

MITRE ATT&CK Technique	ID	Effect	Action
Application protocol	T1071	Disrupt	Block at application layer firewall Block at gateway
Communication Through Removable Media	T1092	Disrupt	Disallow or restrict removable media
Proxy	T1090	Disrupt	Blacklist domain
Non-standard pot	T1571	Disrupt	Blacklist non-standard ports

focus on. Additionally, the organization should re-use mitigative actions, to allow for consolidation of incident handling procedures.

Actions on cyber attacks: In the Act phase, the CoA is executed, ending the OODA loop iteration, and starting a new one. Standardisation can be applied to this phase by using standard operating procedures (SOPs), that define how these actions should be carried out.

Automation: To further enhance and speed up the action phase, SOPs can be automated, possibly using Security Orchestration and Automated Response (SOAR) solutions. This may give the impression that the entire OODA loop can be automated: automation detection, automated decision on the CoA and automated execution of the CoA. This, however, is a wrong assumption, because it leaves out the most important phase of the OODA loop: orientation. Thus, automation supports rapid OODA looping, but the analyst always plays a central role in determining the correct course of action.

Patterns and predictability: A downside to standardization and automation is that it creates a predictable pattern. Any predictability can be abused by attackers. Defenders may also have difficulty adapting when having to take actions that have not been standardized and automated if they are not used to such situations. Thus, regular training and exercises is vital.

Implicit guidance and control: In the OODA loop means autonomous and consistent decision making. This requires training and exercise. Red team exercises, where simulation of attackers takes place, is especially important. In these exercises, attackers should adopt an OODA approach to their campaign. This allows for a perspective on how the defender's and attacker's OODA loops affect each other and what actions were effective to disrupt the opponent's loop. Through repeated exercises and a well-defined process, implicit guidance and control can be achieved so that individuals within the teams, and teams within the organization may observe, orient, decide and act in a similar fashion.

Summary and Conclusion: The OODA loop teaches us that security incidents should not be viewed as a chain of separate events that require follow-up, but rather as a series of adversary actions that are acted on, knowing the attacker will react too. OODA is a mindset, that can be applied to a process. By applying the OODA mindset to incident response alongside other concepts in cyber defense, organizations can deal with cyberattacks in a way that is efficient, effective and disruptive to the attacker's efforts.

References

(1) https://danford.net/boyd/essence.htm
(2) http://www.projectwhitehorse.com/pdfs/ScienceStrategyWar_Osinga.pdf
(3) https://www.doctrine.af.mil/Portals/61/documents/Volume_1/V1-D34-Levels-of-War.pdf
(4) https://medium.com/anton-on-security/back-in-2015-while-working-on-a-gartner-soc-paper-i-coined-the-concept-of-soc-nuclear-triad-8961004c734
(5) https://github.com/rabobank-cdc/DeTTECT
(6) https://en.wikipedia.org/wiki/Double-loop_learning
(7) https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf
(8) https://monoskop.org/images/d/dc/Forrester_Jay_W_World_Dynamics_2nd_ed_1973.pdf
(9) https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf
(10) https://www.securityacademy.be/soc-analyst-burnout-the-problem-and-the-solutions/
(11) http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
(12) https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf
(13) https://fas.org/irp/doddir/army/fm3-13-2003.pdf
(14) http://cchs.auburn.edu/_files/into-the-gray-zone.pdf
(15) https://attack.mitre.org/tactics/enterprise/

Auteurs: Bart Gijsen, Sterre den Breeijen, Robert Seepers, Ruggero Montalto, en Bram Poppink zijn allen werkzaam bij de unit ICT van TNO. Jeroen van der Ham is werkzaam bij het NCSC en de Design & Analysis of Communication Systems (DACS) groep van de universiteit Twente. Samen werkten ze in 2020 aan een verkennend onderzoek naar de status van herstelvermogen bij Nederlandse organisaties. Voor vragen en opmerkingen, mail naar bram.poppink@tno.nl.

ICT herstelvermogen: de stand van zaken

Herstelvermogen is het vermogen van een organisatie om haar bedrijfsvoering snel en goed weer op te pakken na een cyberaanval of niet-intentioneel ICT-incident. Uit inventarisatie onder Nederlandse organisaties blijkt dat herstelvermogen een bekend en ingebed concept is. Er blijkt ook ruimte voor verbetering van herstelvermogen te zijn, vooral ten aanzien van het periodiek bijstellen van incidentscenario's, oefenen van risicovollere scenario's en het inrichten van collectief herstelvermogen.

ICT-voorzieningen worden gebruikt om de uitvoering van bedrijfsprocessen mogelijk te maken. De toename van het gebruik van IT in de afgelopen decennia heeft ertoe geleid dat zeer veel organisaties afhankelijk zijn geworden van correct functionerende ICT. Zonder correct functionerende ICT kunnen bepaalde bedrijfsprocessen, of zelfs gehele organisatieketens, verstoord raken. Het voorkomen van verstoringen – doelbewust als gevolg van een cyberaanval of incidenteel – met betrekking tot de beschikbaarheid, vertrouwelijkheid en integriteit van ICT is daarom belangrijk. In het verleden is veel aandacht besteed aan het voorkomen van dergelijke verstoringen door het treffen van preventieve maatregelen. Dit levert echter nooit een garantie op correct functionerende ICT aangezien preventieve maatregelen nooit volledig dekkend zijn. In het geval van een verstoring zal de ICT goed hersteld moeten worden. Dit vermogen om ICT te herstellen is, in vergelijking met preventieve of responsieve maatregelen, onderbelicht.

In dit kader heeft TNO, in samenwerking met het NCSC, verkennend onderzoek gedaan naar de huidige stand van zaken op het gebied van herstelvermogen. Het doel van dit onderzoek is om zicht te krijgen op de huidige stand-van-zaken op het gebied van herstelvermogen binnen Nederlandse organisaties en mogelijke aanknopingspunten voor verbetering te identificeren. Als onderdeel van dit onderzoek is er eerst bepaald wat er precies bedoeld wordt met herstelvermogen (in vergelijking met o.a. cyberweerbaarheid) en wat typerend zou zijn aan adequaat ingericht herstelvermogen. Deze beelden zijn vervolgens getoetst aan de huidige herstelinrichting van een negental organisaties door middel van kwalitatief onderzoek (op basis van interviews). In de volgende paragraaf gaan we eerst in op de definitie van herstelvermogen. Vervolgens bespreken we wat er van belang is voor een adequate inrichting van herstelvermogen. In de daaropvolgende paragraaf lichten we toe welk type organisaties zijn geïnterviewd, waarna we de bevindingen op basis van deze interviews bespreken. Aansluitend gaan we wat dieper in op de aanknopingspunten voor verbetering, naar aanleiding van deze bevindingen. We sluiten af met een conclusie en een vooruitblik op mogelijk vervolgonderzoek.

Wat is herstelvermogen?

Het herstellen van verstoorde ICT is een concept dat terug te vinden is in onder andere cyberweerbaarheid en business continuity management. Laatstgenoemde onderwerpen zijn echter een stuk breder dan het herstellen van ICT en omvatten typisch ook het opstellen van preventieve en repressieve maatregelen. Aangezien het primaire doel van dit onderzoek zich beperkt tot het herstellen van verstoorde ICT wordt de scope van herstelvermogen een stuk enger gedefinieerd. Specifiek wordt binnen dit onderzoek de volgende definitie gehanteerd:

Herstelvermogen, is de mate waarin een organisatie efficiënt en effectief in staat is om functionaliteit, die voorzien wordt door ICT, weer beschikbaar te maken.

Deze definitie verdient enige onderbouwing. Om te beginnen met *functionaliteit, die voorzien wordt door ICT:* met herstel wordt uiteindelijk beoogd om bepaalde functionaliteiten te herstellen. We beperken ons, in het kader van dit onderzoek, daarbij tot dergelijke functionaliteiten die geleverd worden door ICT. Denk hierbij aan diensten die een organisatie kan leveren waarbij er een directe relatie is tussen ICT en dienst (e.g. het leveren van software diensten), maar ook aan bedrijfsprocessen die gebruik maken van informatiesystemen (e.g. administratie).

Figuur 1: Fases van herstelvermogen.

Het herstellen van ICT functionaliteit dient *efficiënt en effectief* te gebeuren. De middelen die ingezet worden voor herstel dienen op te wegen tegen de negatieve impact van een incident. Herstel dient doeltreffend en binnen passende tijd te worden uitgevoerd. Zoals later in dit artikel wordt toegelicht is een onderdeel hiervan de mate waarin een organisatie baat heeft bij 'acuut herstel' of 'duurzaam herstel'.

Een *organisatie* is afhankelijk van bovenstaande functionaliteiten (voorzien door ICT) om diensten te kunnen leveren. Elke organisatie is eindverantwoordelijk voor de door haar geleverde diensten en de daarvoor gebruikte functionaliteit en daarbij het herstel van deze functionaliteit. Hiervoor is in de definitie expliciet de term 'organisatie' opgenomen, refererend aan de organisatie die de diensten levert.

Wat is van belang voor het adequaat inrichten van herstelvermogen?

Goed herstelvermogen kenmerkt zich door een set activiteiten die voor, tijdens en na een incident uitgevoerd moeten worden. Er worden hierbij typisch drie fases onderscheiden zoals ook weergegeven in figuur 1.

In al deze fases vindt er een samenspel plaats tussen techniek,

processen en mensen. In de techniek zijn oplossingen te vinden om ICT-functionaliteit te herstellen, bijvoorbeeld door het aanbrengen van redundantie. Het daadwerkelijke herstel (e.g. het uitvoeren van technische maatregelen) moet worden uitgevoerd volgens bepaalde processen en procedures. Een van deze processen is hierbij het besluiten welke functionaliteit er wanneer en hoe hersteld moet worden, veelal belegd bij een crisisteam binnen een organisatie. Deze processen worden uiteindelijk uitgevoerd door mensen. Neem bijvoorbeeld het herstellen van gecompromitteerde data, die veroorzaakt zou kunnen zijn door een ransomware aanval. Om deze data op een effectieve en efficiënte manier te kunnen herstellen moet er o.a.:

- *Voorafgaand* aan een dergelijk incident, een data back-up infrastructuur worden ingericht die het mogelijk maakt om data op een later tijdsstip te herstellen. Als onderdeel van deze voorbereiding moeten er ook processen en procedures worden opgesteld om dit herstel uit te kunnen voeren;
- *Tijdens* een incident zal er een inventarisatie gemaakt moeten worden van de data die getroffen is door de aanval. Op basis van de impact die de aanval heeft op de organisatie zal er een besluit moeten worden genomen (in teamverband) over hoe de getroffen functionaliteit en data het beste hersteld kan worden. Hierbij worden de juiste processen en procedures bepaald en gevolgd (bijv. een draaiboek dat beschrijft hoe de data uit technisch perspectief moet worden hersteld). Vaak is de uitvoer van het herstel een iteratief proces;
- *Na* het herstel moet de organisatie van de gelegenheid gebruikmaken om te evalueren hoe het herstel is verlopen. Deze evaluatie wordt vervolgens gebruikt om de getroffen maatregelen en gevolgde herstelprocessen, waar mogelijk, aan te scherpen.

In deze fases – voorbereiding, uitvoering en leren van uitvoering – zijn een aantal specifieke activiteiten te benoemen die uitgevoerd kunnen worden om een verbeterd herstelvermogen te bereiken. In de komende paragrafen worden deze activiteiten per fase kort toegelicht. Vervolgens worden er nog een aantal aspecten benoemd die belangrijk zijn voor herstelvermogen, maar van toepassing zijn op al deze fases.

Voorbereiden op herstel

Het voorbereiden op herstel is cruciaal voor efficiënt en effectief herstel ten tijde van een incident. Door zoveel mogelijk herstelmaatregelen in de techniek en processen kan er ten tijde van een incident snel geschakeld worden. In de voorbereidende stap kan bijvoorbeeld een inventarisatie gemaakt worden van mogelijke incidenten, kan techniek worden ingericht die bij het herstel gebruikt kunnen worden (e.g. back-ups, monitoring system, etc.) en kan een herstelplan geschreven worden om uit te voeren ten tijde van een specifiek incident. Ook is het mogelijk om samenwerking op te zetten met ketenpartners en eventuele gezamenlijke beschermingstechnieken voor het tijdelijk uitwijken van ICT-functionaliteit.

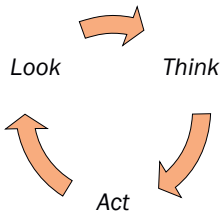
Herstel-in-uitvoering

De herstel-in-uitvoering fase begint zodra er vastgesteld wordt dat er een incident gaande is. Bijvoorbeeld wanneer een monitoringsysteem een afwijking detecteert, of een klant meldt dat een online service niet langer beschikbaar is. Afhankelijk van het type incident en de impact op de bedrijfsvoering zullen bepaalde keuzes gemaakt moeten worden. Kan dit zelf opgelost worden, of is een leverancier verantwoordelijk? Kan de 'pre-disruption state' snel hersteld worden, of is het zinvoller om eerst alternatieve functionaliteit in te zetten in plaats van de verstoorde functionaliteit? Deze keuzen tijdens uitvoering van herstel hangen sterk af van de organisatorische drijfveren, het type functionaliteit die verstoord is, en welke oorzaak hieraan ten grondslag ligt.

De fase 'herstel-in-uitvoering' vormt hiermee de kern van het herstelvermogen. Het herstel-in-uitvoering is daarbij een iteratief proces waarbij er stapsgewijs wordt toegewerkt naar een oplossing. Een representatie van dit proces is geïllustreerd in figuur 2:

- **Look:** Observeer en onderzoek wat er aan de hand is. Onder deze deelfase vallen onder andere het (steeds beter) zicht krijgen op het incident en de impact die dit heeft op de organisatie;
- **Think:** Bepaal mogelijke acties om het herstel uit te voeren. Er zal hierbij gezocht moeten worden naar de balans tussen de snelheid en duurzaamheid van herstel. Dat wil zeggen, snelle oplossingen zijn er typisch op gericht om de functionaliteit zo snel mogelijk weer aan te bieden, maar zullen zich slechts in beperkte mate richten op het voorkomen van vervolgincidenten. Langzamere (maar duurzamere) oplossingen richten zich erop om de functionaliteit in het vervolg ook beter te kunnen garanderen, maar vereisen doorgaans enige tijd om geïmplementeerd te worden. Naast het bepalen van specifieke herstelacties wordt er binnen deze fase ook gecontroleerd of het

incident nog voldoende onder controle is, of dat er moet worden geëscaleerd.
- **Act:** Voer de herstelacties uit. Indien de functionaliteit hersteld is, zal er hierbij voor enige tijd een 'verhoogde dijkbewaking' plaatsvinden om zeker te zijn dat het herstel goed is uitgevoerd.



Figuur 2 - Fases tijdens de uitvoer van herstel, een iteratief proces.

Leren van uitvoering

Als een incident is verholpen en de functionaliteit is hersteld volgt een evaluatie om verbeteringen te identificeren en waar nodig te implementeren. Belangrijk voor deze evaluatie is dat alle voorgaande processtappen goed zijn gedocumenteerd en vastgelegd. Zowel de aanleiding naar het incident, het incident zelf als de uitvoering van herstel dienen geëvalueerd te worden. Eventuele tekortkomingen die het incident teweeg hebben gebracht, of het herstel hebben belemmerd, dienen aangescherpt te worden, mits de kosten op wegen tegen de baten. Bijvoorbeeld een aanpassing in de herstelprocessen of getroffen technische maatregelen.

Overige belangrijke aspecten

Er zijn een aantal aspecten belangrijk voor de inrichting van herstelvermogen welke van toepassing zijn op het algemeen herstelvermogen. Dit zijn Training en oefening, het afstemmen met ketenpartners en collectief herstelvermogen.

Zoals eerder beschreven is herstelvermogen een samenspel tussen techniek, processen en mensen. Training is een middel dat gebruikt kan worden om ervoor te zorgen dat de medewerkers de juiste kennis hebben en weten wat er van hen verwacht wordt. Denk hierbij aan kennis op zowel het gebied van expertise (e.g. crisismanagement of technisch incidentbeheer) als herstelprocessen. Het oefenen van incidenten is daarbij een belangrijk aspect om te toetsen of deze kennis beheerst wordt. Daarbij kunnen oefeningen gebruikt worden om ervaring op te doen met de technische herstelmaatregelen en herstelprocessen, en om eventuele tekortkomingen hierin te identificeren nog vóór een incident plaatsvindt.

Een ander belangrijk aspect zijn de relaties met andere organisaties. Ondanks dat herstelvermogen primair betrekking heeft op het herstel van de functionaliteit binnen de eigen organisatie, is het afstemmen met ketenpartners een onderdeel van het herstel. Bijvoorbeeld wanneer functionaliteiten afhangen van (ICT) diensten die geleverd worden door een externe leverancier. Het afstemmen met dergelijke ketenpartners kan vooraf worden geformaliseerd in contracten en/of SLAs en gedurende en na een incident zal er tussen ketenpartners moeten worden afgestemd.

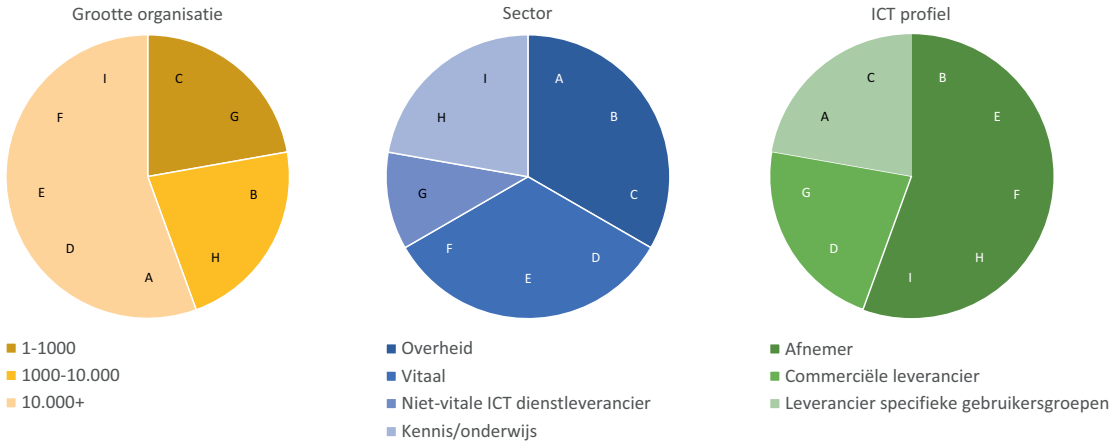
Ten slotte kan een organisatie ook samenwerken met andere organisaties welke niet directe leveranciers of afnemers zijn, bijvoorbeeld soortgelijke organisaties in dezelfde sector. Dit collectief herstelvermogen is de mate waarin organisaties gezamenlijk optrekken om hun herstelvermogen (beter) in te richten. De twee geïdentificeerde manieren waarop collectief herstelvermogen bedreven kan worden zijn: collectief leervermogen, bijv. informatiedeling tussen sectorpartners over bepaalde incidenten en advies richting de inrichting van het herstelproces); en collectief herstel, bijvoorbeeld de inrichting van sector-gezamenlijke uitwijkfaciliteiten.

Wat doen Nederlandse organisaties op het gebied van herstelvermogen?

Om inzicht te krijgen in de stand van zaken op het gebied van herstelvermogen zijn interviews afgenomen bij negen verschillende organisaties. Deze organisaties blijven anoniem en de bevindingen van de interviews zijn zo goed als mogelijk onherleidbaar naar specifieke organisaties en personen opgeschreven. In de komende paragrafen wordt er eerst een beknopt, geanonimiseerd overzicht gegeven van de (types) organisaties die bij dit onderzoek betrokken zijn geweest, waarna er wat dieper gekeken wordt naar de meest belangrijke bevindingen van dit onderzoek.

Selectie interviewkandidaten

Bij veel organisaties is herstelvermogen belegd bij meerdere personen met verschillende taken. Vanwege het verkennende karakter van dit onderzoek is er voor gekozen om inzichten te inventariseren bij personen met verschillende rollen en verantwoordelijkheden bij de organisaties, waaronder business continuity managers en information security officers. De negen betrokken organisaties zijn actief in verschillende sectoren: overheid, vitale dienstverlening, niet-vitale ICT-dienstverlening, en kennis/onderwijs. Vijf van de negen organisaties kunnen gekenmerkt worden als primair afnemer van ICT-diensten, twee organisaties worden gekenmerkt als commerciële ICT-dienstleverancier, en twee organi-



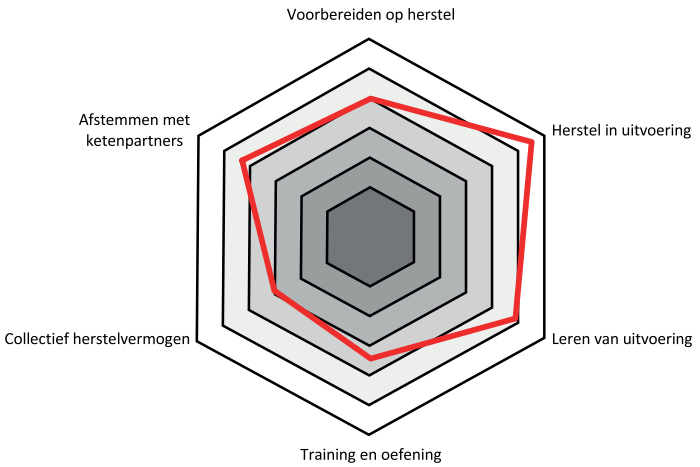
Figuur 3 - Categorisering van de geïnterviewde organisaties.

saties worden gekenmerkt als leverancier aan specifieke gebruikersgroepen (b.v. aan Rijksoverheid organisaties). De grootte van de organisaties varieert in omvang van minder dan 1.000 tot meer dan 10.000 medewerkers.

In figuur 3 staat de categorisering van de geïnterviewde organisaties grafisch weergegeven. Individuele organisaties worden hier aangegeven met de letters 'A' tot en met 'I'.

Status-quo herstelvermogen

Na een analyse van alle interviews is geconcludeerd dat herstelvermogen bij alle geïnterviewde organisaties is ingeregeld en al voor langere tijd wordt opgepakt in de vorm van een samenvoeging / integratie van business continuity management en cyber security. Het valt op dat de awareness en het commitment bij het management een belangrijke indicator voor goed ingericht herstelvermogen is. De organisaties waarbij het herstelvermogen slechts beperkt tot recht kwam gaven allen aan dat herstelvermogen niet door de gehele organisatie leeft. In deze gevallen wordt herstelvermogen vaak gezien als een 'feestje voor de ICT afdeling', terwijl herstel meer elementen raakt dan puur ICT. Door het gebrek aan awareness en commitment bij het hogere management zijn er bij deze organisaties onvoldoende mensen en middelen beschikbaar om herstelvermogen in de breedte op te kunnen pakken.
Een belangrijke drijfveer voor het management om zich te committeren aan herstelvermogen kan gekoppeld worden aan de mate waarin ICT van direct belang is voor de business continuity, maar ook specifieke richtlijnen vanuit wet- en regelgeving. Het herstelvermogen van een organisatie hangt hierbij ook sterk samen met het ICT-profiel van de organisatie. Vooral bij organisaties waarbij het primaire bedrijfsbelang sterk afhangt van ICT-continuïteit worden vergaande herstelmaatregelen getroffen.
Daarbij wordt ook opgemerkt dat de awareness bij het management (tijdelijk) kan opleven door recente (grote) incidenten bij eigen of vergelijkbare organisaties. De ransomware aanval op Universiteit Maastricht leidde tot vragen bij het management van veel van de geïnterviewde organisaties: 'kan dit ook bij ons gebeuren?'. Dergelijke situaties kwamen in de breedte van de geïnterviewde organisaties voor, ongeacht hoe goed het herstelvermogen is ingericht.
De algemene bevindingen die voortkomen uit de interviews zijn geïllustreerd in figuur 4. Dit radardiagram geeft weer in hoeverre het herstelvermogen van de organisaties zich gemiddeld gezien verhoudt tot de belangrijkste aspecten die eerder in dit artikel zijn beschreven. Daarmee geeft deze grafiek een eerste beeld bij de huidige stand van zaken op het gebied van herstelvermogen binnen Nederlandse organisaties. Wat opvalt uit deze grafiek is dat de gemiddelde organisatie goed scoort op het aspect 'herstel in uitvoering' . Voor 'voorbereiden op herstel', 'collectief herstelvermogen' en 'training en oefening' lijkt er nog de meeste ruimte voor verbetering te zijn.



Figuur 4 - Algemene bevindingen herstelvermogen. Hoe verder van het centrum verwijdert des te beter dit aspect er over het algemeen voor staat bij de geïnterviewde organisaties. Deze beoordeling is gebaseerd op een kwalitatieve analyse.

Een geconstateerde tekortkoming bij het voorbereiden op herstel is dat incidentscenario's slechts in beperkte mate periodiek worden bijgesteld. De meeste organisaties herzien deze scenario's pas zodra er een (grootschalig) incident plaatsvindt in de eigen organisatie of daarbuiten, zoals de Citrix-crisis of de ransomware aanval bij de Universiteit van Maastricht. Meerdere organisaties komen er bij deze incident-gedreven heroverweging achter dat sommige scenario's achterhaald zijn. Veelvoorkomende reden voor deze incident-gedreven aanpak is een gebrek aan toegewezen tijd en middelen om deze activiteit periodiek uit te voeren.
Op het gebied van collectief herstelvermogen komt er uit de interviews naar voren dat er vooral behoefte is, maar nog een beperkte implementatie. Vooral bij de vitale infrastructuur organisaties wordt hier al wel over nagedacht, bijvoorbeeld over de inrichting van gezamenlijke ICT-voorzieningen voor sectorpartners in geval van calamiteiten. Door een gebrek aan directe noodzaak en best-practices, maar ook vanwege juridische complicaties wordt hier nog geen concrete invulling aan gegeven. Daarnaast geven meerdere organisaties aan dat er behoefte is om van elkaar te leren op het gebied van herstelvermogen.

Alle organisaties geven aan dat herstel met enige regelmaat wordt beoefend. Er blijkt hier echter wel een terughoudendheid om risicovolle technische oefeningen uit te voeren, vanwege de lastig te voorspellen impact op de bedrijfsuitvoering. Hoewel eenvoudige technische maatregelen wel worden geoefend worden complexere technische herstelvoorzieningen nauwelijks getest.

Aanknopingspunten voor verbetering en vervolg

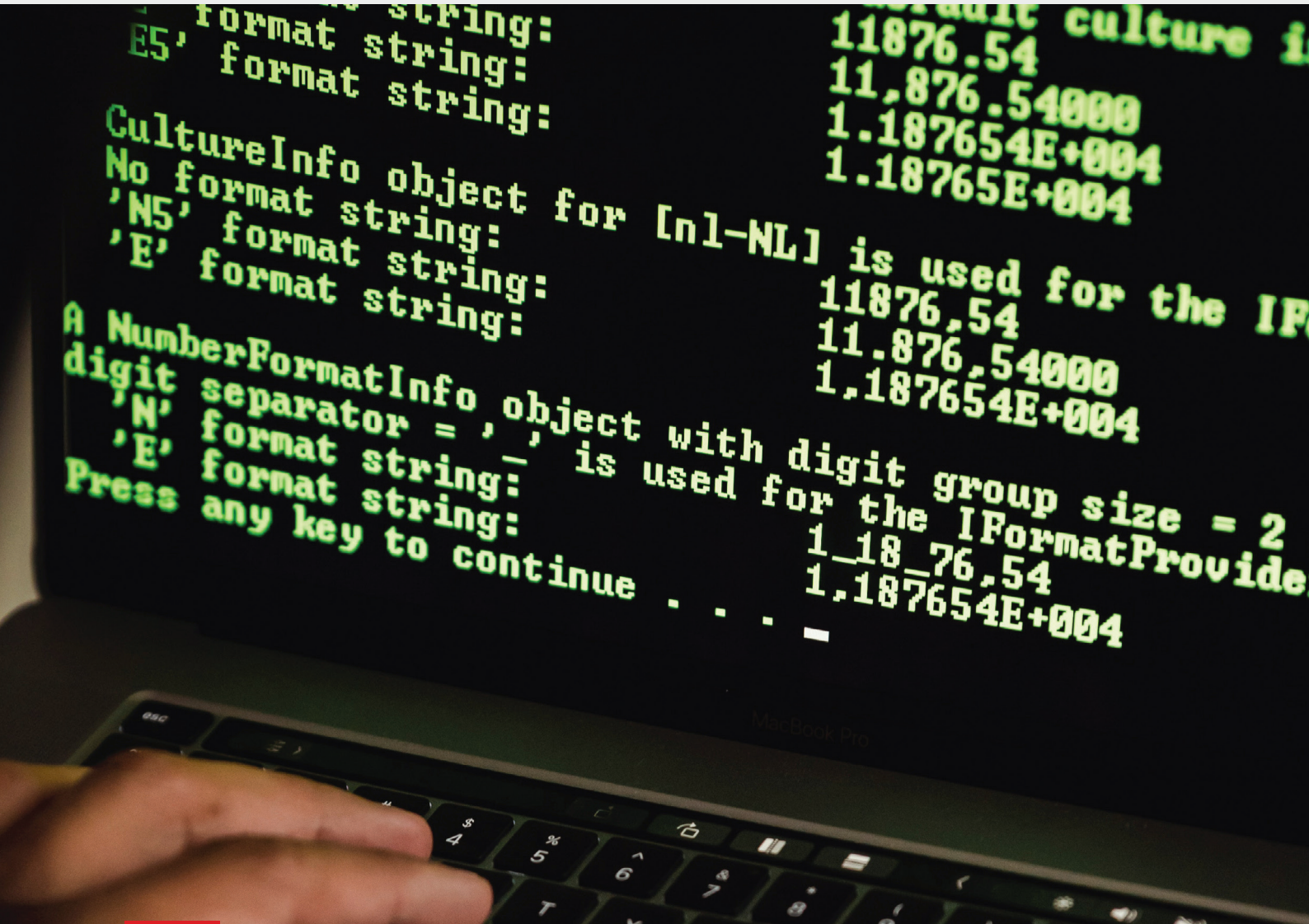
Aanvullend op de verbeteringen die organisaties voor hun eigen herstelvermogen doorvoeren, kunnen collectieve verbeteracties meerwaarde bieden. Het is bijvoorbeeld aannemelijk dat een organisatie minder aanleiding zal voelen om periodiek haar risico- en dreigingsprofielen aan te passen, indien dit gedaan wordt op basis van slechts de ervaringen vanuit die ene organisatie zelf. Indien de organisatie meer zicht krijgt op relevante ervaringen en getroffen maatregelen bij andere organisaties, dan ontstaat een meer accuraat dreigingsbeeld dat aanleiding kan zijn voor frequentere aanpassingen van het risico- en dreigingsprofiel. Het Cybersecuritybeeld Nederland (opgesteld door de NCTV in samenwerking met het NCSC) is een voorbeeld dat hieraan bijdraagt. Vooralsnog blijft het echter een uitdaging om een uniformere manier te vinden om relevante dreigingsinformatie op een vertrouwde wijze beschikbaar te maken voor andere organisaties, die voldoende gedetailleerd is om concreet toegepast te kunnen worden.

Het oefenen van realistische, grootschalige incidenten blijkt door individuele organisaties te worden ingeschat als te risicovol, hoewel het herstelvermogen zou kunnen verbeteren. Ook het concretiseren van collectief herstelvermogen zou volgens sommige geïnterviewde organisaties verbeterd kunnen worden. Wellicht dat het gebruik van collectieve (grootschalige) ICT testfaciliteiten, die dermate realistisch zijn dat ze als uitwijk faciliteit gebruikt zouden kunnen worden in geval van een calamiteit, een eerste stap zijn om aan deze tekortkoming tegemoet te komen. Voor een dergelijk (potentieel kostbaar) initiatief ter verbetering van collectief herstelvermogen is nog de vraag welke partijen bereid zijn om deze uitdaging als eerste op te pakken.

Conclusies en vervolgonderzoek

Dit artikel heeft een beknopte inzage gegeven in de huidige stand van zaken met betrekking tot herstelvermogen binnen Nederlandse organisaties. Er zijn hierbij een aantal belangrijke bevindingen verwoord over de rol die management awareness- en commitment speelt bij het herstelvermogen. Daarbij zijn er een aantal aanknopingspunten geschetst die het herstelvermogen van organisaties kunnen versterken.
Dit verkennende onderzoek heeft zich beperkt tot het herstelvermogen van de ICT functionaliteit van een select aantal organisaties. Het is de ambitie om dit verkennend onderzoek in de toekomst op twee manieren te verbreden. Ten eerste is gedurende het onderzoek het voorstel naar voren gekomen om de geïnventariseerde stand van zaken verder uit te werken naar self-assessments. Met deze self-assessments kunnen ook andere organisaties een inschatting maken over hoe hun herstelvermogen er voor staat en tips ontvangen voor verbetering. Daarnaast is voor veel organisaties ook OT (Operationele Technologie) van belang voor hun kernbedrijfsprocessen. Een inventarisatie van OT herstelvermogen is dan ook nodig om de stand van zaken op het gebied van herstelvermogen bij Nederlandse organisaties te completeren.

Auteur: Robert Metsemakers schrijft op persoonlijke titel en is als ervaren IT-auditor en informatiebeveiligings-expert beschikbaar voor security-advies en (algemene) schrijfopdrachten via robert.metsemakers@gmail.com.



BLOG

Wat spionnen je leren over threat intel analyseren

Nationale veiligheidsdiensten lijken in hun werk bij het maken van dreigingsanalyses op security-afdelingen. Uit hun praktijkervaring kunnen securityprofessionals daarom nuttige zaken leren.

CIA-logo in vloer hoofdkantoor.

In de film 'Fight Club' verkondigt hoofdrolspeler Brad Pitt de eerste Fight Club-regel: "You do not talk about Fight Club." Dit lijkt echter niet te gelden voor medewerkers van de Amerikaanse Secret Service. Bij het geven van een lezing op een securitycongres stellen ze zich steevast voor als: "Pete Puck, special agent of the Secret Service." Vaak dragen ze duidelijk zichtbaar een Secret Service-pin op het jasje van hun donkere pak. Ook een andere Amerikaanse veiligheidsdienst toont die voor mij onverwachte openheid. Op hun website (1) publiceert de CIA (Central Intelligence Agency) veel direct toepasbare documenten over het intelligence werk in de dagelijkse praktijk, de 'tradecraft'. Die tips en activiteiten, oorspronkelijk gericht op het verzamelen, verwerken en rapporteren van inlichtingen voor veiligheidsdiensten, zijn ook zeer bruikbaar voor securityprofessionals die werken met en aan (cyber) threat intelligence. Een interessant boek op diezelfde site is bijvoorbeeld 'Psychology of Intelligence Analysis' van Richards Heuer Jr. Drie opvallende zaken uit dit zeer lezenswaardige boek licht ik hieronder toe.

Geen mozaïek, maar medische diagnose

Het gaat niet om het verzamelen van zoveel mogelijk informatie en talloze metingen maar om wat je ermee doet. Het verschil in effectiviteit wordt gemaakt in hoe handig, snel en gericht je als analist de verzamelde dreigingsinformatie verwerkt tot 'actionable advice' voor de personen die erop moeten acteren. Bij het opstellen van een threat analyse ben je niet bezig met het leggen van een mozaïek. Het gaat er dus niet om eerst en uitputtend alle kleine stukjes te verzamelen om daarna pas de totale foto te (kunnen) zien. Bovendien heb je, anders dan bij een legpuzzel van striptekenaar Jan van Haasteren, geen deksel beschikbaar met daarop het totale eindresultaat. De informatiestukjes kunnen tot meerdere beelden leiden. Soms zijn er meerdere juiste uitkomsten tegelijk af te leiden uit dezelfde input. Bijvoorbeeld uit één verkiezing: (a) verkiezingskandidaat X heeft gefraudeerd en (b) zittende verkiezingskandidaat Y blijft (toch) niet in functie. Het maken van een threat analyse lijkt volgens Heuer meer op het stellen van een medische diagnose. Je moet niet alle, maar de juiste stukjes hebben en in de einddiagnose de bij de patiënt passende conclusie trekken. En op tijd, om de patiënt te laten overleven. Denk aan dr. House die bewust en behoorlijk eigenwijs niet alle symptomen onderzoekt, maar wel elke aflevering van de tv-serie de meest relevante eruit pikt.

Cognitieve dissonantie

Het is voor analisten moeilijk om nieuwe input te verwerken en deze te rijmen met eerder bestudeerd materiaal. Zeker als deze input in strijd lijkt met eerdere geanalyseerde informatie. "Dat kan in de praktijk wel zo zijn, maar het past niet in mijn zelf bedachte theorie", denk je dan. De nieuwe informatie klopt niet met het ontwikkelde beeld en wordt daarom veronachtzaamd door de analist. Met soms desastreuze gevolgen.
Sommige securitymedewerkers uiten als luis in de pels vaak hun eigen mening, die vrijwel altijd afwijkt van die van de rest van het team. De verleiding voor het management is dan groot die persoon weg te pesten. Of door het trainee-contract van een superkritische millennial niet te verlengen. Hoewel het wegwerken van deze neeschudders ogenschijnlijk de positieve teamspirit verbetert, houd je op den duur alleen gedweeë jaknikkers over, die de schaapsherder(in) prima volgen – maar die de voor hen onverwachte security dreigingen per definitie missen. Bedenk: zonder dwarsliggers kan de trein niet rijden.

Lees je rapport hardop

Geschreven en gesproken taal activeren verschillende neuronen in je brein. Het helpt soms om je tekst voor te lezen (tegen jezelf tijdens het thuiswerken) om de spinnenwebben op te ruimen en de complexiteit van de conclusie en de tekst te vereenvoudigen.

Referentie

(1) https://www.cia.gov/index.html

Auteur: Stijn Jans is CEO en oprichter van Intigriti, crowdsourced security platform.
Stijn is te bereiken via www.intigriti.com.

Continu testen door duizenden ethische hackers

De voordelen van crowdsourced security

Wanneer is een organisatie goed beveiligd tegen cybermisdrijven? Het is een vraagstuk waar security-experts dagelijks mee worstelen, zeker omdat er geen bevredigend antwoord op bestaat. In de dynamische en agile IT-wereld is het ontwikkelproces voortdurend: software wordt het hele jaar door bijgewerkt, nieuwe releases worden continu uitgerold. De traditionele manier van securitytests, vlak voor een nieuwe release of update, is hiervoor veel te kostbaar. Bovendien zijn zowel scope als beschikbare tijd vaak te beperkt. Crowdsourced security biedt uitkomst.

Crowdsourced security besteden hun beveiliging letterlijk uit aan 'het volk'. Mensen die, soms in dienst zijn bij een IT-bedrijf, maar het in elk geval leuk vinden om hun securitykennis zelfstandig, al dan niet als hobby, in de praktijk brengen. In de volksmond worden ze hackers genoemd, een term waar helaas een zweem van criminaliteit omheen hangt. Dat is de schuld van Hollywood: in films zijn hackers vaak asociale en onverzorgde figuren, vergroeid met hun bureau vol junkfood en energiedrankjes. Op de batterij monitors voor hun neus dansen steevast spannende groene letters in allerlei codeertalen.

De werkelijkheid is – gelukkig! - een stuk saaier: verreweg de meeste hackers zijn 'gewone' mensen, met een normale dagbesteding. Wél hebben ze een bovengemiddelde interesse in IT-security. En hoewel er natuurlijk ook kwaadwillende hackers tussen zitten, stellen veel anderen hun kennis en kunde juist in dienst van organisaties die behoefte hebben aan hun expertise. Deze ethische hackers gaan op uitnodiging van een bedrijf gestructureerd op zoek naar securitylekken, om zo de bedrijfsbeveiliging te verbeteren. Een helder verhaal – maar waarom kiezen zoveel organisaties dan nog steeds voor andere methoden?

Crowdsourced security versus penetration testing

We haalden het in de intro al even aan: penetration testing, pentest in het kort, is bij verreweg de meeste organisaties sinds jaar en dag dé manier om IT-infrastructuur te testen op zwakke plekken. Logisch, want lange tijd was het ook de beste manier. In een tijd van continu veranderende IT-assets is het echter niet meer voldoende. De belangrijkste verschillen tussen pentests en crowdsourced security op een rij:

Meer ogen zien meer kwetsbaarheden

Pentests worden in de regel uitgevoerd door een bescheiden team. De scope is beperkt: de experts werken een op voorhand overeengekomen programma af. Alhoewel ze stuk voor stuk vakmensen zijn, is hun expertise toch beperkt: ze zijn immers maar met een paar. Door een onbeperkt aantal ethische hackers met de benodigde en uiteenlopende expertise om hulp te vragen, zijn organisaties in staat om hun net veel wijder uit te werpen.

Oneindig testen

Door hun beperkte loopduur zijn pentests geknipt voor uitvoer vlak vóór een nieuwe release, maar zoals gezegd vinden updates tegenwoordig continu plaats. Omdat pentests ook nog eens momentopnamen zijn, zullen organisaties voortdurend achter de feiten aan blijven rennen. Veel verstandiger is het daarom om ethische hackers doorlopend naar kwetsbaarheden te laten zoeken.

Betaal voor tastbaar resultaat

Een ander belangrijk verschil schuilt in hoe organisaties hun securitybudget besteden. Bij pentests gaat het geld naar de handeling, maar is resultaat niet gegarandeerd. Dat is niet alleen zonde, maar zorgt ook voor een gevoel van schijnveiligheid. Dat er geen kwetsbaarheden gevonden worden, betekent namelijk niet dat ze er ook niet zijn. Bij crowdsourced security betalen organisaties pas als een zwakke plek is vastgesteld.

Van reactief naar proactief

Crowdsourced security is radicaal anders en betekent voor veel organisaties dat ze op een nieuwe manier over IT-beveiliging moeten gaan denken. Van reactief, naar proactief. Veel organisaties voeren pentesten uit omdat het nu eenmaal is wat ze kennen, maar ook omdat ze goed passen bij de traditionele watervalmethode van ontwikkelen. Men begint pas aan de volgende stap als de fase daarvoor volledig is afgesloten. Bovendien sluiten pentesten aan op wat wetgeving vereist: ze zijn een geijkte en relatief snelle weg naar compliance. Maar omdat scope en tijd beperkt zijn, kunnen kwetsbaarheden over het hoofd worden gezien. Organisaties die kiezen voor crowdsourced security, en bug bounty in het bijzonder, omarmen het idee om alle kwetsbaarheden voortdurend en definitief uit te bannen. Dat is ook nodig, want zoals beschreven laten steeds meer organisaties bij applicatieontwikkeling, of anders de leveranciers van hun software, de watervalmethode los. In plaats daarvan kiezen ze voor DevOps. Ontwikkelcycli zijn een stuk korter, een nieuwe functionaliteit wordt een stuk sneller opgeleverd. Door deze bovendien voortdurend te testen op kwetsbaarheden, is veel sneller te bepalen of een softwareconcept onveilig is.
Zo voorkomt u verspilling van kostbare tijd: developers krijgen het hele jaar door pakketjes met nuttige informatie, in plaats van periodiek en pas nadat een product nagenoeg is afgerond. Wanneer een lek lastminute moet worden gedicht, is dat dikwijls ook minder duurzaam dan wanneer het er al in de ontwerpfase kan worden uitgehaald. Op deze manier kunnen organisaties securityproblemen proactief, en met meer urgentie oppakken. Developers en security wachten niet langer af, maar zijn daar aanwezig waar het risico het grootst is.

Gestructureerde samenwerking

Het mag duidelijk zijn dat organisaties veel te winnen hebben bij het mobiliseren en activeren van de creativiteit van ethische hackers. Niet langer betalen ze security-experts voor tijd, zonder gegarandeerd resultaat en mét beperkte scope. In plaats daarvan besteden ze hun securitybudget aan resultaten en impact, en hebben ze een toekomstbestendige en schaalbare manier om de beveiliging van software en assets te verbeteren. De logische en voorstelbare volgende vraag luidt dan: waar te beginnen? Ethische hackers die willen helpen zijn er genoeg, maar het is goed voorstelbaar dat uw organisatie deze samenwerking gestructureerd, veilig en vertrouwd wil laten verlopen. Door te werken met een bug bounty platform volgt u alle tips waarmee de levendige community in een centraal overzicht komt. Ook is snel te zien hoe u er budgettair gezien voorstaat. Zorgen over de communicatie met ethische hackers zijn evenmin nodig: alle communicatie verloopt via het platform.

Intigriti: crowdsourced security platform

Wereldwijd is er een tiental bedrijven dat zich volledig toespitst op crowdsourced security. Een van die partijen is Intigriti, met het hoofdkantoor in België. CEO Stijn Jans: "Wij zijn begonnen vanuit onze overtuiging dat we met behulp van technologie en experts bedrijfsnetwerken veiliger kunnen maken. Inmiddels hebben we een wereldwijde community van meer dan 20.000 ethische hackers die deze visie onderschrijven. Samen zorgen wij voor een duurzame en schaalbare manier van security testing." Inti de Ceuckelaire, die de community aanstuurt en zelf ook ethisch hacker is, vult aan: "Dankzij de kennis en creativiteit van de mensen in onze community zijn we in staat direct impact te hebben op de security van bedrijven. Maar het werkt ook de andere kant op: dankzij de beloningen die bedrijven over hebben voor het aandragen van veiligheidslekken worden onze leden op een eerlijke manier beloond voor hun creativiteit."

In deze rubriek geven enkele iB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kun je sturen naar ibmagazine@pvib.nl.

Gelukkig, de feestdagen zijn voorbij!

Steeds vaker vinden grote hacks plaats in periodes dat veel mensen vrij zijn, zoals rond de kerstdagen. Zo hadden we wereldwijd eind 2019 en begin 2020 veel last van de Citrixkwetsbaarheid en van hackers die daar gebruik van maakten. Of in december jl. de FireEye/ Solarwinds inbraak (1). En niet alleen werkgerelateerde criminele activiteiten zijn een risico, privé is het net zo belangrijk om op te blijven letten in een periode waarin winkels dicht zijn en online shoppen een vlucht neemt (2).


Chris de Vries | Fook Hwa Tan | Lilian Knippenberg

Fook Hwa Tan

Normaliter is het altijd erg druk tijdens de kerstdagen en oud en nieuw door de vele borrels en feestjes zowel privé als zakelijk. Dit jaar is door COVID-19 en de daarbij behorende lockdown alles een stuk soberder geworden. Heb binnen de beperkingen nog wel met familie feest kunnen vieren, maar dat is niet te vergelijken met eerdere jaren.

Normaalgesproken is het bij Northwave rustig tijdens de feestdagen, maar dit jaar was het een erg druk uiteinde. Meerdere collega's hebben hard moeten doorwerken en de feestdagen moeten missen door incidenten in Duitsland. Het was topdrukte voor de criminelen, en dus ook voor ons! We hebben veel incidenten gezien afgelopen jaar, zoals Citrix, Microsoft Exchange Server, Zoom, Cisco Systems, Pulse VPN, Solarwinds Orion en andere. Ze dienden vaak als ingang bij organisaties voor cybercriminelen. Bij de meeste incidenten waar ons CERT was ingezet, begonnen de incidenten niet door een complexe aanval, maar vaak door een simpele Business Email Compromise (BEC), oftewel een phishingmail die een aanvaller toegang verleent tot het netwerk.

Na een lange periode van verkenning op het netwerk konden de criminelen toeslaan door een gebrek aan basis securitymaatregelen, zoals slechte monitoring op back-ups, basis bewustwording van medewerkers over phishing en het op tijd patchen van kwetsbaarheden. Ondanks de technologische vooruitgang, blijkt het voor veel organisaties nog erg moeilijk om de basis op orde te krijgen en te houden. En dan het moment van toeslaan. De feestdagen zijn vaak een periode waar IT-teams minimaal bezet zijn. Dus als op dat moment de aanval wordt ingezet, breng je een organisatie vrij snel tot wanhoop. Vooral in 2020, wanneer teams last hadden van coronamoeheid, is het dubbel moeilijk om je medewerkers gemotiveerd te houden. Ik hoop daarom dat in dit nieuwe jaar we allen opnieuw met nieuwe moed zorgdragen, dat medewerkers bewust blijven omgaan met informatie, basis securitymaatregelen zoals monitoring aanwezig is en security voor de gehele organisatie gemanaged wordt!

Lilian Knippenberg

De feestdagen is mijn favoriete tijd van het jaar. Gezelligheid met vrienden en familie, winters weer met kou en een zonnetje, binnen de verwarming een graadje lager en een extra dikke trui aan om het milieu wat te ontzien. Vol goede moed ga ik ook nu het nieuwe jaar in, ondanks of misschien wel dankzij de wereldwijde pandemie. In het afgelopen jaar kon er nog zoveel wel, zijn er toch weer stappen vooruit gezet op informatiebeveiligingsgebied en kon zo goed en zo kwaad als het ging de organisatie doordraaien. Ook stemt het mij hoopvol dat Nederland veel bewuster is van de mogelijkheid dat er onregelmatigheden plaatsvinden op bedrijfsnetwerken. De grote bekendheid die de hacks hebben gekregen en de rol van NCSC die snel reageerde en meer op de voorgrond treedt, geven een positief gevoel. Zo lang wij allen alert blijven en bewustzijn kweken bij collega's maken we het de cybercriminelen een stuk lastiger.

Chris de Vries

Een nieuw jaar, nieuwe kansen en goede voornemens. Wie kent dat gevoel niet of spreekt dat uit tegenover vrienden, familie en collegae? Maar in een pandemisch jaar krijgt dat toch een apart gevoel en een bijsmaak. Zeker als wij in Amerika zien wat de moderne media vermag (Trump en het Capitool) en weten welke oplichtingstrucs ons internet teistert. Wat een boze, slechte en vooral kwade wereld toch om ons heen.

Maar is dat enkel om ons heen? Moeten wij ook niet de hand in eigen boezem steken? Hoe fel reageren wij zelf, hoe kort is ons lontje, hoe weinig geduld tonen wij tijdens een 'lockdown' en hoe veilig handelen wij op het internet? Heel veel 'hacks' en inbraken kunnen voorkomen worden door iets meer rust te nemen, iets meer tijd voordat wij op de toetsen beginnen te tikken en het linkje even aanklikken. Wij als redacteuren zijn misschien (hoop ik) iets bewuster bezig en daarom willen wij ook proberen een voorbeeld te zijn. Daarom wens ik u een bezonnen, rustig en veilig, maar bovenal een gezond 2021 toe. Dat ons magazine ook in dit jaar uw leidraad en bron van informatie alsook plezier mag zijn. Jammer dat de feestdagen voorbij zijn!

Referenties

(1) https://www.computable.nl/artikel/nieuws/security/7107986/250449/-benelux-klanten-van-solar-winds-vrezen-hack.html

(2) https://nos.nl/artikel/2357984-waarschuwing-voor-valse-webshops-oplichters-hebben-nepsites-al-klaarstaan.html

Jaaroverzicht

Het bestuur in beeld

Scriptie

Voorwoord

Artikelen

(a) artikel (v) verslag (i) interview (o) opinie (b) blog (c) column

(a) artikel (v) verslag (i) interview (o) opinie (b) blog (c) column

COLOFON

IB is het huisorgaan van het Platform voor InformatieBeveiliging (PvIB) en bevat ontwikkelingen en achtergronden over onderwerpen op het gebied van informatiebeveiliging.

PvIB
Platform voor InformatieBeveiliging

HOOFDREDACTEUR
Nicole van Deursen

REDACTIE
Tom Bakker
Bianca Brooijmans
Maarten Hartsuijker
Lilian Knippenberg
Rachel Marbus
Fook Hwa Tan
Chris de Vries

BLADMANAGEMENT
MOS bv
Caroline Knobbe
Sam Dekkers
E ibmagazine@pvib.nl

ADVERTENTIE-ACQUISITIE
MOS bv
E acquisitie@mos-net.nl
T 033 247 34 00

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
VDR druk & print

UITGEVER
Platform voor Informatiebeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
E secretariaat@pvib.nl
W www.pvib.nl

ABONNEMENTEN
De abonnementsprijs in 2021 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

ABONNEMENTENADMINISTRATIE
Platform voor Informatiebeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
E secretariaat@pvib.nl

ISSN 1569-1063

COLUMN Berry

De meeste dromen zijn bedrog!

Ik heb in mijn vorige columns weleens geschreven over het misbruiken van cijfers om je doel te bereiken. Voordat ik begin te vertellen moeten jullie weten dat ik beslist niet in complottheorieën denk en dat ik een enorm vertrouwen heb in regering en regionaal gezag. Mijn vader wees mij er altijd op dat overheden en daaraan gelieerde instanties altijd gelijk hebben. Dus ik spreek met twee woorden tegen de agent die mij bekeurde omdat ik drie kilometer te hard reed, en glimlach als ik mijn belasting mag betalen. De laatste tijd heeft dat vertrouwen een beetje een deukje opgelopen. Mijn ergernis begon met de toeslagenaffaire waarin de overheid willens en wetens gezinnen onderuit schoffelde met list en bedrog. Ik ga daar nu niet verder op in; ik verwijs graag naar https://nl.wikipedia.org/wiki/Toeslagenaffaire.

Ik wil het graag over de beleidsvorming hebben van de coronacrisis. Het gaat te ver om alles te benoemen maar een aspect pik ik eruit, namelijk de soms nogal rommelige en tendentieuze berichtgeving. Mondkapjes helpen niets dus is het niet nodig deze verplicht te stellen, toch is per 1 december de wet aangenomen die ze verplicht stelt in openbare ruimtes. Vervelende ingrijpende besluiten worden vaak ingeleid met besmettingscijfers die niet altijd accuraat zijn door diverse computerstoringen bij de GGD. (Let wel: het enige dat de GGD's moeten doen is het aantal besmettingen doorgeven aan een centraal punt; ingewikkelde algoritmes doorlopen is niet nodig). We vermelden nu ook niet dat het aantal testen per dag vertienvoudigd is, en dat het dus niet vreemd is dat het aantal besmettingen stijgt.

Alle experts die in de diverse talkshows hun beste beentje voorzetten en het overheidsbeleid soms openlijk ter discussie stellen. Wie moeten we nu het eerst inenten, de ouderen (zoals ze in heel Europa doen)? Of de zorgmedewerkers, of toch eerst alle kinderen? Ik heb daar geen oordeel over, maar verbaas mij over de discussie. Waarom beginnen wij zo laat met vaccineren? Omdat het zorgvuldig moet. Ik ben het daar volledig mee eens, maar we hadden dit al maanden geleden kunnen voorbereiden. Alles moet natuurlijk goed geadministreerd worden, jawel door de eerdergenoemde rammelende computersystemen van de GGD.

Wij luisteren naar ministers en premiers die werkelijk hun uiterste best doen en ik ben er zeker van dat ze ons niet om de tuin willen leiden, maar waarom heb ik toch zo sterk het gevoel dat cijfers gemanipuleerd worden om beslissingen te ondersteunen? Waarom wordt het begrip zorgvuldigheid gebruikt om een blunder te verdoezelen? Waarom worden ministers gesteund die openlijk laten blijken zelf lak te hebben aan de door hen bedachte en gehandhaafde regels? Dit is ongeveer de droom die ik vannacht had.

Droom lekker verder,

Berry

TSTC

ICT en Security Trainingen

ADVANCE YOUR CAREER WITH SECURITY IN 2021

CSA - Certified SOC Analyst
GSEC - Giac Security Essentials
GPEN - Giac Penetration Tester
EDRP - Disaster Recovery Professional
EHF - Ethical Hacking Foundation
CND - Certified Network Defender v2
CEH - Certified Ethical Hacker v11
CPENT - Certified Penetration Testing Professional

Want security start bij mensen!!

TECHNICAL SECURITY TRAININGEN

CEH - Certified Ethical Hacker
CHFI - Computer Hacking Forensic Investigator
CPENT - Certified Penetration Testing Professional
SSCP - Systems Security Certified Professional
OSCP - Offensive Security Certified Professional

SECURITY MANAGEMENT TRAININGEN

CISSP - Certified Information Systems Security Professional
CISM - Certified Information Security Manager
CISA - Certified Information Systems Auditor
CRISC - Certified In Risk And Information Systems Control
C|CISO - Certified Chief Information Security Officer

PRIVACY TRAININGEN

CIPP/E - Certified Information Privacy Professional / Europe
CIPM - Certified Information Privacy Manager
CIPT - Certified Information Privacy Technologist
CDPO - Certified Data Protection Officer

CLOUD SECURITY TRAININGEN

CCSP - Certified Cloud Security Professional

ISO TRAININGEN

ISO 27001 - Foundation
ISO 27001 - Lead Implementer
ISO 27001 - Lead Auditor
ISO 27005 - Risk Manager
ISO 27701 – Privacy Management

www.tstc.nl

Onze trainingen zijn weer klassikaal of Live Online te volgen