SPECIAL BUSINESS CONTINUITY MANAGEMENT

INFORMATIEBEVEILIGING MAGAZINE

- Effectieve crisisbeheersing volgens Eelco Dykstra: ‘Denk aan de holy shit-factor’
- Cybercrises vragen om anticipatie en improvisatie
- Column – Help! Een incident!

JAARGANG 20 - 2020 - EDITIE 5

TSTC

ICT en Security Trainingen

NIEUW

GSEC - Giac Security Essentials
GPEN - Giac Penetration Tester
EDRP - Disaster Recovery Professional
EHF - Ethical Hacking Foundation

20% korting voor PVIB leden o.b.v. lidmaatschapsnummer op geselecteerde trainingen

Want security start bij mensen!!

Onze trainingen zijn weer klassikaal of Live Online te volgen

TSTC is jouw opleider op het gebied van IT, Security en Privacy

ISC2 certificeringen

- SSCP - Systems Security Certified Practitioner
- CISSP - Certified Information Systems Security Professional
- ISSAP - Information Systems Security Architecture Professional
- CSSLP - Certified Secure Software Lifecycle Professional
- CCSP - Certified Cloud Security Professional

ISACA certificeringen

- CISM - Certified Information Security Manager
- CISA - Certified Information Systems Auditor
- CRISC - Certified in Risk and Information Systems Control
- CGEIT - Certified in the Governance of Enterprise IT

PECB certificeringen

- ISO 27001 Lead Implementer
- ISO 27001 Lead Auditor
- ISO 27701 Privacy Lead Implementer
- CDPO Certified Data Protection Officer

EC-Council certificeringen

- CEH - Certified Ethical Hacker
- ECSA - Certified Security Analyst
- C|CISO - Certified Chief Information Security Officer
- CSA - Certified SOC Analyst
- CTIA - Certified Threat Intelligence Analyst
- CASE - Certified Application Security Engineer JAVA/.NET

Divers

- Linux LPIC 3 security
- Security+
- (Web)Application Security Assessment based on OWASP

www.tstc.nl

Business Continuity Management

Na de themanummers 'Privacy' dit jaar en vorig jaar 'Security architectuur', is het tijd om het thema 'Business Continuity Management (BCM) en Crisis Management' voor het voetlicht te brengen. En dat nu midden in de coronacrisis. Hoe actueel kun je zijn?

Toen ik begin dit jaar na de berichten uit China naar mijn boekenplank keek, zag ik het Pandemie Preparedness Pakket uit 2008 (voor de vogelgriep) staan met daarin allerlei materiaal zoals maatregelen die genomen moeten worden en scenario's over de impact (overbevolking ziekenhuizen, sluiten van scholen). Die genoemde maatregelen zijn nog steeds goed bruikbaar. Een groot verschil met toen was dat verondersteld werd dat een pandemie zo'n tien weken zou duren. Daar zitten we nu ruim boven. We zijn nu twaalf jaar verder en het lijkt wel of we weinig geleerd hebben. Het artikel van Lex Borger kijkt terug naar destijds. Verder in dit nummer artikelen die verschillende aspecten en invalshoeken van BCM en Crisismanagement aan de orde stellen. Het lijkt wel of het onderwerp verschuift naar het begrip resilience. Is het een nieuw buzzwoord? De definitie is niet altijd even duidelijk. Een aantal artikelen gaan hier nader op in.

Waarom gaat het bij bijna elke crisis weer mis? Eelco Dykstra deelt zijn ervaringen en welke problemen telkens terugkomen. Het artikel van Gert Kogenhop pakt het aspect van samenwerking aan om tot 'resilience' te komen. Er is nog steeds sprake van 'verzuiling' tussen disciplines die een rol spelen bij crises en BCM, waardoor men langs elkaar heen werkt en er geen centrale sturing is.
Een enquête over de Stand van Zaken van BCM in Nederland geeft het beeld dat er nog veel moet gebeuren. Naast het BCM-thema nog een vijftal artikelen over verschillende onderwerpen. Veel leesplezier!

Tom Bakker

IN DIT NUMMER

Auteurs: Tom Bakker is redactielid van iB-Magazine. Tom is bereikbaar via tombakker@pvib.nl. Sandra Kagie is freelance tekstschrijver (Sanscript Tekstproductie). Sandra is bereikbaar via info@sanscriptproducties.nl. Crisisexpert Eelco Dykstra, MD is internationaal crisis- en rampenexpert met een medische achtergrond. Dykstra is de drijvende kracht achter de internationale denktank Daily Impact Emergency Management (DIEM). Hij is te bereiken via eelco.dykstra@diem.nl.

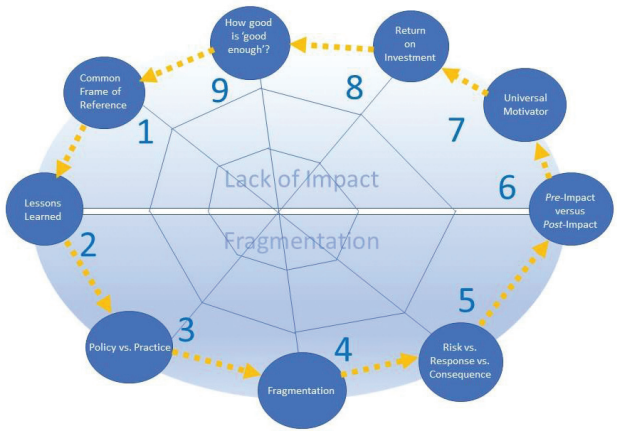
INTERVIEW

Effectieve crisisbeheersing volgens Eelco Dykstra:

‘Denk aan de holy shit-factor’

Zijn we gedoemd om pas te reageren nadat er iets kapot is gegaan? Een vraag die internationaal crisisexpert Eelco Dykstra weigert positief te beantwoorden. Zijn Amerikaanse collega’s daarentegen, met wie Dykstra in 2006 de aanpak van orkaan Katrina evalueerde, kwamen toen tot een volmondig ‘ja’. Mensen zijn van nature reactief: een weeffout in het menselijke ras, was de conclusie van de Amerikanen. Hierdoor lopen we in het geval van een crisis steeds weer tegen dezelfde obstakels aan. Omdat we niet leren van eerdere crises.

De sombere conclusie van zijn Amerikaanse collega's zette Dykstra aan het denken. Hoe krijg je mensen zover proactiever om te gaan met allerlei vormen van ellende die vanuit de toekomst op ons af komen? Welke obstakels staan ons in de weg om uit eigen beweging proactief te zijn en te leren van eerdere crises? Vragen die hij beantwoordt met het door hem ontwikkelde NUR-model, ofwel de Nine Universal Roadblocks. Negen obstakels waar we volgens Dykstra keer op keer tegenaan lopen wanneer we te maken hebben met een crisis. In een gesprek over moderne crisisbeheersing in zijn woonplaats Den Haag bespreken we met hem zijn 'lijst van frustratiepunten' zoals hij de negen roadblocks ook noemt.



The Nine Universal Roadblocks (NUR) Model™

Figuur 1 - Het 'Nine Universal Roadblocks' (NUR)-model.

We springen in het gesprek al snel naar roadblock 9: hoe goed is 'goed genoeg'? Een vraag die in het kader van crisismanagement volgens Dykstra veel te weinig wordt gesteld. Terwijl vooruitgang in moderne crisisbeheersing wat hem betreft juist afhangt van het stellen én beantwoorden van deze vraag. "De vraag dwingt je namelijk na te denken over wat je nu eigenlijk wil. En de vraag maakt het mogelijk resultaten van inspanningen kwantificeerbaar te maken", benadrukt Dykstra. "Welke uitkomst acht je wel of niet acceptabel? Waar neem je genoegen mee? Logische vragen die in het kader van crisismanagement echter maar weinig worden gesteld." En dat laatste heeft volgens de crisisexpert alles te maken met de angst om afgerekend te worden op het behaalde resultaat. Of liever gezegd op het niet-behaalde resultaat. "Je ziet het bij politici", geeft hij aan. "Zij willen niet afgerekend worden op resultaat, maar op hun intenties. Met als gevolg dat ze zich proberen te verschuilen achter uitspraken als 'honderd procent veiligheid bestaat niet'." Wanneer je als organisatie of bedrijf crisismanagement serieus neemt dan moet je volgens Dykstra vooraf overeenstemming bereiken en draagvlak creëren wat betreft de antwoorden op de volgende vragen:

- Welke resultaten willen we wel en niet? En wat accepteren we wel en niet?
- Hoeveel mag dat kosten?
- Wie moeten dat gaan doen?
- Hoe meten we resultaten?
- Wat zijn de gevolgen wanneer resultaten niet worden behaald?

"Bepaalde risico's zijn nu eenmaal niet te elimineren. Dat moeten we ons realiseren. En vervolgens is het belangrijk te weten hoe we om moeten gaan met een incident wanneer we ermee te maken krijgen. Het beantwoorden van bovenstaande vragen helpt daarbij."

Dwarsverbindingen centraal

Het NUR-model is volgens Dykstra toe te passen voor de analyse van problemen én bij de zoektocht naar oplossingen. "Overal waar dwarsverbindingen nodig of wenselijk zijn", benadrukt hij. Het leggen van dwarsverbindingen vormt wat hem betreft de kern van het model en dus de kern van effectief crisismanagement. Neem roadblock 3: afstand tussen beleid en praktijk. Van de negen obstakels, volgens Dykstra, waarschijnlijk de meest universele. Er wordt volgens hem namelijk het meest over geklaagd. Zowel door beleidsmakers als door de praktijkmensen. In zijn bijdrage aan het boek Grip op crisis (1) licht Dykstra de tegenstelling als volgt toe: "In het verleden heb ik wel eens aan beide kanten gevraagd wie nu als eerste op de andere zou moeten afstappen om de afstand tussen beleid en praktijk te verkleinen. Dat leverde geen verrassend resultaat op – de andere kant moest eerst maar eens bij hen komen kijken..." Als het gaat over dwarsverbindingen en het belang daarvan kun je niet heen om roadblock 4: versnippering – fragmentatie. "Waar we als klein land groot in zijn", verzucht de crisisexpert. "Gemeenten, provincies, waterschappen en dan ook nog eens veiligheidsregio's", somt hij op, waarbij vooral de veiligheidsregio's hem een doorn in het oog zijn. "Daar hebben we als Nederlanders toch geen enkele band mee. Niet emotioneel en ook niet vanuit historisch perspectief. Provincies hadden we al, waarom hebben we

Hoe goed is 'goed genoeg'? Een vraag die in het kader van crisismanagement veel te weinig wordt gesteld

het onderwerp veiligheid niet daar belegd?", vraagt hij zich af. Het volgende obstakel dat Dykstra in het kader van het belang van dwarsverbindingen wil benadrukken is roadblock 6: samenspel tussen vooraf en achteraf. "Samenspel tussen risicomanagement, gericht op preventie, en consequence management, gericht op recovery", licht hij toe. "Investeringen op deze vlakken die los van elkaar worden gedaan, leveren niet dat op wat je ervan verwacht. Leg ook hier dwarsverbindingen", geeft hij aan. Om vervolgens te verwijzen naar de Amerikaanse uitdrukking 'The time to repair your roof is when the sun is shining'. Probleem hier is dat geld moet worden uitgegeven en werk moet worden verzet voordat een probleem er is. De sense of urgency, zoals Dykstra het formuleert is er op dat moment nog niet. Terwijl dat gevoel van urgentie op het moment dat een crisis speelt en vlak daarna juist maximaal is. Reden voor Dykstra om in het geval van roadblock 5: concurrentie tussen risico, response en consequentie te pleiten voor het juiste evenwicht tussen de drie. En-en-en in plaats van of-of-of.

Businesscase voor resilience

Brengt ons bij de vraag aan de crisisexpert hoe je als securityprofessional governance en riskmanagement bij het bestuur op de agenda krijgt. Dykstra verwijst direct naar roadblock 8: rendement. "Je moet een businesscase maken voor het investeren in resilience, veerkracht/weerbaarheid", is zijn advies. "Dat je hier te maken hebt met een virtueel, niet-tastbaar, product en dito rendement maakt dit echter lastig." Wat investeerders terugkrijgen voor een dergelijke investering is volgens Dykstra lastig uit te leggen. En voor de woorden 'als het misgaat dan zijn de gevolgen minder erg dan wanneer je niet had geïnvesteerd', krijg je bij investeerders niet direct de handen op elkaar, zo weet hij uit eigen ervaring. Je moet wat hem betreft 'meer impact creëren' om te komen tot een succesvolle businesscase.
Handvatten die Dykstra hiervoor in het eerder genoemde boek Grip op crisis geeft, zijn:

- Bedenk dat als de directe schade zoveel is, de indirecte schade vele malen groter is;
- Visualiseer en bereken wat de uitval van essentiële voorzieningen betekent;
- Wat zijn de kosten van maatschappelijke onrust en ontwrichting;
- De rol van (her)verzekeraars.

Het NUR-model is volgens de crisisexpert heel breed toepasbaar. Op elke crisis die leidt tot de uitval van kritische infrastructuren. Aardbevingen en overstromingen, pandemieën, maar ook aanslagen en georganiseerde cyberaanvallen. "Wanneer je het model consequent toepast dan kun je het gebruiken als diagnostische tool voor je organisatie. Als thermometer om te weten hoe je ervoor staat op het vlak van moderne crisisbeheersing. Je ontwikkelt zo, ondanks de diverse stakeholders met ieder hun eigen agenda, een gemeenschappelijk referentiekader. En geleerde lessen worden continu in de praktijk gebracht", vat hij samen.

'Holy shit-factor'

Een belangrijke tip die Dykstra bedrijven en organisaties tot slot wil geven om te komen tot effectieve crisisbeheersing, heeft alles te maken met, zoals hij het formuleert, de 'holy shit-factor'. Vrij vertaald: wat betekent dit voor mij? Hij doelt hiermee op het belang om als organisatie medewerkers mee te nemen in een verhaal. Hen mede-eigenaar te maken van een probleem, maar veel belangrijker nog: mede-eigenaar van de zoektocht naar de oplossing. Om dit te bereiken heb je niet alleen experts nodig die medewerkers met vaak ingewikkelde verhandelingen waarschuwen of vertellen wat ze moeten doen. De impact van zo'n aanpak is volgens Dykstra namelijk niet diep genoeg. "Je moet medewerkers een verhaal in weten te trekken. Hen confronteren met wat hen daadwerkelijk te wachten staat. En daarvoor heb je verhalenvertellers nodig. Zij zijn namelijk door het schetsen van spannende 'reality-fiction'- scenario's in staat de 'holy shit-factor' te activeren. Waardoor medewerkers uiteindelijk zélf met de oplossing komen."

Referentie

(1) Grip op crisis: Van klassieke rampenbestrijding naar moderne crisisbeheersing, ISBN 978-90-9029456-8.

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Vervagende grenzen

De tijd gaat voort, de zomer is voorbij gevlogen. Stormen teisteren met meer regelmaat de kustplaats waar ik woon. De wind beukt tegen de ramen, ze klepperen en maken zacht piepende geluiden. Oude enkelglas ramen in houten sponningen met afgebladderde verf, eigenlijk wel toe aan een onderhoudsbeurt. Het leven verplaatst zich nog meer terug naar binnen. Daar, op een kleine vierkante meter staat mijn laptop op een piepklein tafeltje. Zeker nog tot en met het einde van dit jaar is die vierkante meter mijn werkruimte, de plek waar ik het leeuwendeel van de dag zit te tikken, bellen, Teamen (bestaat dit werkwoord al?) en peinzen.

Maar het is eigenlijk helemaal geen werkruimte. Het is een keukentafel. In mijn gezellige en kleine appartement. Het is mijn huis, mijn thuis. De plek waar ik mij helemaal privé kan voelen. Maar in toenemende mate voel ik me er niet meer zo fijn en vrij. Mijn thuis is een kleine werkgevangenis geworden waarin zakelijk en privé niet meer zo goed te scheiden zijn. Al mijn collega's komen met regelmaat virtueel over de vloer. Teams heeft een blurfunctie die op mijn laptop helaas niet werkt. Maar zelfs als ik mijn collega's mijzelf laat zien met een vage achtergrond, dan nog komen ze allemaal mijn huis in. Ik neem me voor om wat vaker virtuele meetings zonder beeld te doen. Maar ook dat is eigenlijk een lapje voor het bloeden.

Verwachtingen zijn ook verschoven. Werken vindt niet alleen primair thuis plaats, de uren waarin gewerkt wordt zijn ook aan het veranderen. De grenzen van de dag worden opgerekt en daarbij ook vaak impliciet aan anderen de verwachting dat zij daarin mee plooien. En nu zorgen juist die impliciete verwachtingen ervoor dat het zakelijk werkende leven nog meer plek opslokt in het privédomein. Het voelt niet prettig en ook ietwat ongezond. Waar de grenzen schuiven wordt het belangrijker om soms heel hard nee te zeggen en je eigen grenzen aan te geven. En dat is niet altijd even makkelijk.
Ik sprak er een tijd geleden al eens over met een vriendin. Zij had voor zichzelf een life-hack ontwikkeld om grenzen aan de dag te geven waardoor ze minder last had van vervagende privacy en invasie van werk in je privédomein. Elke ochtend, 20 minuten voor zij begint met werken, pakt ze haar tas in. Trekt haar jas aan, loopt naar buiten en stapt op de fiets. Dan fietst ze een rondje door het dorp. Komt weer thuis, hangt haar jas op, pakt laptop en telefoon uit de tas en gaat zitten werken. De werkdag ten einde gekomen, herhaalt dit ritueel zich opnieuw. En zo brengt ze duidelijke grenzen aan voor zichzelf. Nu de rest van de collega's nog.

Rachel

Auteur: Jelle Groenendaal is lector Risk Management & Cybersecurity aan de Haagse Hogeschool en adviseert als zelfstandig adviseur publieke en private organisaties over risico- en crisismanagement. Hij is bereikbaar via j.groenendaal@hhs.nl.

Cybercrises vragen om anticipatie en improvisatie

De ransomware-aanval op de Universiteit Maastricht (2019) en de wiperware-aanval op Maersk (2017) hebben pijnlijk aangetoond dat grote incidenten niet te voorkomen zijn en zelfs kunnen uitmonden in een cybercrisis. De mate waarin organisaties in staat zijn om de impact van cybercrises te beperken, wordt onder andere bepaald door de bedrijfscontinuïteit- en crisismanagement organisatie. Maar hoe richt je deze beheersmaatregelen adequaat in?

Het nieuwe Lectoraat Risk Management & Cybersecurity van de Haagse Hogeschool gaat deze en andere vragen op het snijvlak van risicomanagement en cybersecurity de komende vier jaar onderzoeken. In dit artikel geven we alvast een eerste reflectie op basis van een aantal bekende wetenschappelijke inzichten. De malware-aanval op de Universiteit Maastricht en de wiperware-aanval op scheepvaart- en transportgigant Maersk hebben onomstotelijk duidelijk gemaakt dat cyberincidenten dermate veel impact kunnen hebben op de bedrijfsvoering dat er gesproken kan worden van een cybercrisis. Een cybercrisis definiëren we als uitval, verstoring of misbruik van IT-systemen en/of diensten die het voortbestaan, integriteit en/of reputatie van de organisatie bedreigt en waarbij er onder (een perceptie van) tijdsdruk en onzekerheid besluiten genomen moeten worden. Naast grote impact op de organisatie, kan een cybercrisis een verstorende invloed hebben op maatschappelijke processen. In het uiterste geval zou een cybercrisis volgens de NCTV kunnen leiden tot maatschappelijke ontwrichting. Ter illustratie: door de aanval op Maersk raakte de Rotterdamse APM Terminals bijvoorbeeld volledig buiten bedrijf, waardoor schepen moesten uitwijken en er in de haven bijna een verkeersinfarct ontstond (1).

Impact beperken

De cyberweerbaarheid van organisaties wordt bepaald door hun vermogen om cyberincidenten te voorkomen en (als ze zich voordoen) de impact ervan te beperken. Nu partijen zoals de NCTV steeds nadrukkelijker stellen dat grote cyberincidenten niet voorkomen kunnen worden (2), moeten organisaties zich in toenemende mate gaan toeleggen op het treffen van maatregelen om de impact te beheersen. Bedrijfcontinuïteitsmanagement (BCM) en crisismanagement zijn twee beheersmaatregelen die daarvoor bedoeld zijn. BCM is het proces gericht op het beheersen van dreigingen die kunnen leiden tot verstoringen en daarmee tot het niet meer kunnen leveren van producten of diensten op aanvaardbare, vooraf vastgestelde niveaus (3). Hiertoe worden de dreigingen en belangrijkste organisatieprocessen in kaart gebracht en vervolgens bepaalt hoe de continuïteit in het geval van een verstoring gewaarborgd kan worden. Dit wordt beschreven in een zogeheten bedrijfscontinuïteitsplan waarin voor een aantal scenario's een handelingsperspectief wordt geschreven. Denk hierbij aan wat te doen bij de uitval een kritisch IT-systeem door een patch of bij de onbeschikbaarheid van een kantoorgebouw door brand. Crisismanagement kan gedefinieerd worden als het vermogen van organisaties om zich voor te bereiden en te reageren op een (cyber)crisis en daarvan te herstellen (3). Crisismanagement komt in beeld wanneer het bedrijfscontinuïteitsplan niet afdoende is of ontbreekt voor de situatie waarmee de organisatie geconfronteerd wordt. De huidige coronacrisis is een treffend voorbeeld: veel organisaties hadden geen rekening gehouden met een lockdown en daarmee de noodzaak om grote delen van het personeelsbestand thuis te kunnen laten werken. Een crisismanagementteam kan in dat geval besluiten om de capaciteit thuiswerkplekken uit te breiden en thuiswerken te faciliteren.

Noodzakelijk onderzoek naar BCM

Veel van de kennis die voor de inrichting, besturing en organisatie van informatiebeveiliging gebruikt wordt, is afkomstig uit (internationale) standaarden. Dit geldt ook voor BCM en crisismanagement. Denk aan de ISO 22301 of BCI 'Good Practice Guidelines' voor BCM en de BS 11200 of TS 17091 voor crisismanagement. Deze standaarden worden wereldwijd door vele organisaties gebruikt en zijn ontwikkeld door professionals die veel ervaring hebben in het vakgebied. Naar de werking en effectiviteit van deze standaarden is nog niet veel onderzoek verricht. Daarmee is tot op heden niet aangetoond dat het implementeren van dergelijke standaarden leidt tot een hogere continuïteit of beter beheerste (cyber)crisis. Empirisch onderzoek binnen organisaties naar het functioneren en de effectiviteit van BCM en cybercrisismanagement is schaars. Toegepast onderzoek is daarom noodzakelijk om te achterhalen in hoeverre en hoe organisaties zich adequaat kunnen voorbereiden en reageren op cybercrises.

Dat er eigenlijk nog maar weinig toegepast onderzoek gedaan is naar de werking en effectiviteit van BCM en cybercrisismanagement binnen organisaties, neemt niet weg dat er al een aantal voorlopige bevindingen kunnen worden gedaan op basis van bestaand onderzoek. In dit artikel geven we hiervan enkele voorbeelden.

BCM is in theorie vooral geschikt voorspelbare risico's (4). BCM is gebaseerd op de klassieke managementtheorie die veronderstelt dat de wereld en daarmee organisaties in grote mate voorspelbaar en (daardoor) beheersbaar zijn. Het instrumentarium van BCM is er dan ook op gericht om organisatieprocessen en (kenbare) risico's in kaart te brengen en vervolgens maatregelen te nemen die helpen om de continuïteit te waarborgen als zo'n vooraf geïdentificeerd risico zich opeens manifesteert. Voorbeelden van deze kenbare risico's zijn een bedrijfsgebouw dat tijdelijk

niet gebruikt kan worden door brand of een niet functionerend betalingssysteem door de uitval van een server.

Anticiperen op een cybercrisis

BCM kan bruikbaar zijn om organisaties voor te bereiden op een scenario waarbij producten of diensten door een cyberincident tijdelijk niet of niet op tijd geleverd kunnen worden. Zo kan er bijvoorbeeld een draaiboek worden gemaakt voor wat te doen bij een grootschalige ransomwarebesmetting of DDoS aanval. Hierbij zijn een aantal aandachtspunten van belang. Ten eerste moet bedacht worden dat veel bedrijfscontinuïteitsplannen handelingsperspectieven bevatten die uitgaan van de veronderstelling dat het netwerk en de reguliere communicatiemiddelen zoals e-mail en telefoon beschikbaar blijven tijdens een verstoring. Maersk heeft aangetoond dat een cyberincident kan leiden tot een complete uitval van het IT-netwerk en systemen. Daardoor kon er geen gebruik gemaakt worden van e-mail en telefonie (die afhankelijk zijn van het netwerk) met als gevolg dat het merendeel van de plannen niet uitgevoerd kon worden. Hetzelfde zou kunnen gebeuren wanneer een netwerk gecompromitteerd is en daardoor de communicatie niet meer te vertrouwen is. Ten tweede en voortbouwend op het vorige punt, is dat veel bedrijfscontinuïteitsplannen digitaal worden opgeslagen en bij een mogelijke uitval van het netwerk dus niet meer benaderd kunnen worden. Ten derde moet rekening gehouden worden met het risico dat back-ups besmet kunnen worden met kwaadaardige software die zich bijvoorbeeld drie maanden stilhoudt zodat er geen mogelijkheid meer bestaat om terug te gaan naar een schone versie (tenzij de back-ups nog langer teruggaan en/of er nog offline back-ups zijn gemaakt). Ten vierde moet bij een scenario van een grote ransomwarebesmetting rekening gehouden worden met de belasting voor de IT-organisatie om een groot aantal werkstations op te schonen en opnieuw in te spoelen.

De tweede bevinding is dat een planmatige respons die BCM kenmerkt alleen effectief kan zijn wanneer die respons met enige regelmaat beoefend en uitgevoerd wordt (5). De consequentie van deze bevinding is tweeledig. Ten eerste betekent het dat BCM vooral geschikt is voor (kleinere) risico's die zich met enige regelmaat manifesteren, zodat er een feedbackloop kan ontstaan tussen plan en uitvoering en de plannen niet verworden tot 'papieren tijgers'. Ten tweede betekent het dat BCM zich maar kan richten op een beperkt aantal risico's, omdat de tijd die nodig is om plannen te testen begrensd is. Een goede BCM organisatie beperkt zich daarom op een aantal meest voorkomende (kenbare) risico's en zorgt ervoor dat inzichten uit testen, oefeningen en echte incidenten verankerd worden in de plannen en trainingen voor personeel.

Snel veranderende omgeving

BCM kent echter ook een aantal beperkingen. De derde bevinding is dat BCM minder geschikt is voor organisatieomgevingen die aan veel verandering onderhevig zijn. BCM legt veel nadruk op het documenteren van organisatieprocessen en het vastleggen van een responsstrategie die past bij hoe de organisatie op papier beschreven is. In de praktijk blijkt echter dat die omschrijving vaak niet meer actueel is op het moment dat er een verstoring optreedt. IT-systemen zijn bijvoorbeeld uitgefaseerd of juist in productie genomen, bepaalde sleutelpersonen zijn door een reorganisatie niet meer werkzaam in de organisatie of een leverancier is vervangen. Hoewel in het bedrijfscontinuïteitsmanagementsysteem (BCMS) in de regel wordt opgenomen dat plannen jaarlijks herzien moeten worden of vaker bij grote veranderingen, lijkt de organisatiepraktijk weerbarstiger (4). Sommige organisaties en hun omgeving zijn zo aan verandering onderhevig, dat het ondoenlijk is om te allen tijde een actueel en diepgaand beeld te hebben van alle kritieke processen. In dergelijke omgevingen loopt BCM vaak achter de feiten aan en is veel van het voorbereidingswerk verspilde moeite.

Zwarte zwanen

Naast de kenbare, kleine risico's zijn er ook nog een aantal bedreigingen die zich niet vooraf laten kennen. Donald Rumsfeld noemde deze 'unknown unknowns', ofwel impactvolle, onvoorspelbare gebeurtenissen die per definitie buiten het bereik van risicobeheersing en dus BCM liggen. De vierde bevinding is dan ook dat BCM niet goed overweg kan met wat Nassim Nicholas Taleb 'zwarte zwanen' noemt. Eén van de eerste stappen van BCM is het identificeren van bedreigingen en bepalen in hoeverre deze dreigingen een risico voor de organisatie vormen. Grote, impactvolle gebeurtenissen laten zich echter niet altijd adequaat voorspellen. De huidige coronacrisis laat dit fraai zien. Grieppandemieën komen zo om de paar jaar voor, maar de huidige wereldwijde reactie met grootschalige lockdowns en reisrestricties zijn nog nooit eerder

vertoond. In de laatste vijf jaarrapportages van de Global Risk Rapportage van het World Economic Forum (WEF) - voor risicomanagers een belangrijke bron - stond infectieziekte dan ook niet in de top 10 van meest waarschijnlijke grote risico's. In de laatste editie van 2020 bungelde infectieziekte onderaan de ranglijst van risico's met grootste impact. Saillant detail: COVID-19 of corona komen helemaal niet voor in het op 15 januari 2020 gepubliceerde rapport (6).

Een belangrijke beperking van een planmatige respons is bovendien dat de plannen weinig houvast bieden wanneer de werkelijkheid anders is dan in het plan beschreven wordt. Als bij een cyberaanval de systemen veel langer platliggen dan van tevoren verwacht, of er treden onverwachte cascade-effecten op, zal de organisatie dus ter plekke inzicht moeten krijgen in het probleem en een responsstrategie moeten bepalen en uitvoeren. Dit is het domein van (cyber)crisismanagement.

Improviseren als een jazzmusicus

Crisismanagement helpt de organisatie om snel expertise en mandaat bij elkaar te brengen en (zodoende) betekenisvolle beslissingen te nemen. Crisismanagement speelt zich veelal op drie niveaus af: operationeel (bijvoorbeeld in het SOC of CERT), tactisch (hoofd CERT) en strategisch (CISO) (7). Hoewel naar cybercrisismanagement nauwelijks onderzoek is verricht, kunnen er wel op basis van de algemene literatuur over crisismanagement een aantal conclusies worden getrokken. Ten eerste blijkt uit onderzoek dat professionals onder crisisomstandigheden terugvallen op routinegedrag en daardoor doen wat ze altijd al deden (5). Een belangrijke aanbeveling is dan ook om de (cyber)crisisorganisatie zoveel mogelijk te laten aansluiten op de reguliere organisatie en van mensen tijdens crises geen contra-intuïtieve handelingen te verwachten c.q. te vragen. Dat mensen tijdens crises terugvallen op ingesleten gewoonten, verklaart waarom uit evaluaties vaak blijkt dat crisisdraaiboeken en specifieke crisisplannen niet of nauwelijks geraadpleegd zijn in de acute fase van crises. De waarde van dergelijke plannen zit hem dan ook vooral aan de 'voorkant': tijdens het opstellen maken ze experts en management bewust van hun rol, taken en verantwoordelijkheid tijdens een cybercrisis.

Uit de literatuur blijkt dat improvisatie tijdens crises onvermijdelijk is (8). In sommige gevallen zullen medewerkers namelijk geen routine hebben opgebouwd voor de situatie waarmee ze geconfronteerd worden of voldoet die routine simpelweg niet. Bij Maersk waren bijvoorbeeld ook verschillende vormen van improvisatie zichtbaar: bij een gebrek aan IT boekte de organisatie nieuwe orders in via WhatsApp en Gmail, bedacht het een offline systeem om containers te labelen en stampte het binnen enkele weken een totaal nieuw IT-netwerk uit de grond (9).

Improviseren heeft dikwijls een negatieve connotatie. Voor sommigen suggereert improvisatie dat de organisatie niet voorbereid was en beter voorbereid had kunnen zijn op een bepaalde verstoring. In de wetenschappelijke literatuur wordt er echter veel genuanceerder naar improvisatie gekeken. Improvisatie wordt gezien als een noodzakelijke vaardigheid van mensen en organisaties om adequaat te kunnen reageren op onverwachte kansen en bedreigingen (10). Het is een misvatting dat improvisatie geen voorbereiding vergt. In de wetenschappelijke literatuur wordt vaak de analogie van de jazzpianist gebruikt. Jazzpianisten kunnen pas improviseren – dat wil zeggen afwijken van de standaard – wanneer zij die standaard tot in de finesses beheersen (10). In de context van crisismanagement betekent dit bijvoorbeeld dat crisismanagementteams regelmatig 'standaard' crisisscenario's oefenen, maar ook de afwijkingen daarop. En leren strategische crisismanagementteams dat veel besluiten tijdens crises 'in de frontlinie' genomen worden en hoe zij die besluitvorming zo goed mogelijk kunnen faciliteren en waar nodig bijsturen.

Wees bewust van besluitvormingsvalkuilen

(Cyber)crises worden gekenmerkt door tijdsdruk, onzekerheid en de grote belangen die op het spel staan. Een derde conclusie is dat de literatuur laat zien dat professionals onder deze omstandigheden in de meeste gevallen adequate beslissingen nemen, maar ook vatbaar zijn voor besluitvormingsvalkuilen (5). Die valkuilen zijn van toepassing op ieder niveau – operationeel, tactisch en strategisch – al manifesteren ze zich soms op een andere manier. De betekenis voor de cybercrisismanagementpraktijk is dat crisismanagers bewust moeten zijn van deze valkuilen in hun eigen besluitvorming en die van hun ondergeschikten. Bekende valkuilen zijn de confirmatiebias (de neiging om een initieel gevormde hypothese te bevestigen door alle gekregen informatie als zodanig te interpreteren en vervolgens uitsluitend te zoeken naar aanwijzingen die de hypothese bekrachtigen) en gezonken kosten (de neiging om een taak die de eindfase nadert af te willen maken

Help mee bij het vormgeven van het onderzoeksprogramma

Moet het onderzoek zich de komende jaren vooral richten op supply-chain risico's en cascade-effecten? Of op de effectiviteit van security standaarden voor industrial control systems? Of zou het goed zijn als de kosten-baten van cyberinvesteringen beter wordt onderbouwd door middel van feiten? Geef je mening in de vragenlijst die het Lectoraat Risk Management en Cybersecurity heeft ontwikkeld. Deze vragenlijst is bedoeld om input vanuit het werkveld op te halen. De resultaten worden gebruikt bij het vormgeven van het vierjarige onderzoeksprogramma van het lectoraat. Het invullen van de vragenlijst kost slechts 5 minuten: https://bit.ly/2XHN7iP

omdat er veel tijd in heeft gezeten). Deze biases kunnen bijvoorbeeld optreden bij CERT professionals die bij een groot incident te lang een bepaalde hypothese proberen te bekrachtigen. Het is aan cybercrisismanagers om deze valkuilen te (h)erkennen en hier op te sturen.

Meer onderzoek nodig naar BCM

In dit artikel hebben we op basis van de wetenschappelijke literatuur enkele BCM en cybercrisismanagement inzichten beschreven. Wie de impact van cybercrises wil beperken, moet volgens de literatuur inzetten op anticipatie (BCM) en improvisatie – wat met behulp van crisismanagement kan worden gefaciliteerd en bijgestuurd. Velen vragen blijven echter nog onbeantwoord en meer toegepast onderzoek is nodig. Een paar voorbeelden: hoe zien effectieve BCM en cybercrisismanagementoefeningen eruit? Hoe ziet een robuuste cybercrisismanagementorganisatie eruit? Hoe kun je BCM slim automatiseren zonder concessies te doen aan de effectiviteit? In welke mate helpen besluitvormingsmodellen bij het voorkomen van besluitvormingsvalkuilen door cybercrisismanagementteams? Wat is de rol van de CISO in crisismanagement? Het lectoraat Risk Management & Cybersecurity hoopt deze en andere vragen de komende jaren samen met het werkveld te kunnen onderzoeken.

Referenties

(1) Van Duin, M. Maan, J. (2018). Cyberaanval op Maersk. Lessen uit crises en mini-crises 2017. Instituut Fysieke Veiligheid: Arnhem.

(2) NCTV (2020). Cybersecuritybeeld Nederland 2020.

(3) NVN-CEN/TS 17091: 2018. Crisismanagement – Handreiking voor het ontwikkelen van strategisch vermogen.

(4) Groenendaal, J. Helsloot, I. (in druk). Organizational Resilience: Shifting from a planning driven Business Continuity Management to Anticipated Improvisation. Journal of Business Continuity & Emergency Management.

(5) Groenendaal, J. Helsloot, I. (2016). The application of Naturalistic Decision Making (NDM) and other research: lessons for frontline commanders. Journal of Management and Organization, 22(2), 173.

(6) Van der Linden, L. (2020). Wat kunnen we met risicomanagement leren van virusinfecties die al dan niet uitgroeien van een pandemie. Genootschap voor Risicomanagement.

(7) Groenendaal, J. Helsloot, I. Scholtens, A. (2013). A critical examination of the assumptions regarding centralized coordination in large-scale emergency situations. Journal of Homeland Security and Emergency Management. 10(1), 113-115.

(8) www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

(9) Mendonca, D. Wallace, W.A. (2004). Studying organizationally-situated improvisation in response to extreme events. International Journal of Mass Emergencies and Disasters, 22(2), 5-30.

(10) Weick, K. E. (1998). Introductory essay – improvisation as a mindset for organizational analysis. Organization Science. 9(5), 543.

Help! Een incident!

Toen ik drie dagen door mijn proeftijd heen was, verloor ik mijn onbeveiligde USB-stick op de parkeerplaats van mijn net nieuwe werkgever. Mijn functietitel is 'sociaal psycholoog cybersecurity & compliance'… . I am not kidding you.

Ik help organisaties dus met het weerbaar maken van hun medewerkers tegen cyberdreigingen. Het voorkómen van de menselijke fout; je computer niet open laten staan, geen vertrouwelijke stukken mee naar buiten nemen, geen onbeveiligde USB-stick gebruiken, geen onbeveiligde USB-stick gebruiken, geen onbeveiligde USB-stick gebruiken… dat soort dingen. Je USB-stick niet verliezen staat niet eens in dat lijstje, want dat spreekt uiteraard voor zich.

Natuurlijk kan ik uitleggen waarom ik in die week nog één keer die USB-stick mee moest nemen, en wat er misging op de parkeerplaats. Maar het feit blijft dat er een incident was. Bij mijzelf, terwijl ik er door mijn functie de hele dag mee bezig ben. Kun je nagaan hoe dat is voor mensen wiens core business heel ergens anders ligt. De laptop blijft soms even in de auto liggen omdat we er niet mee willen sjouwen, we laten een bezoeker onbegeleid naar de uitgang lopen omdat we te laat zijn voor de volgende meeting, we mailen een bestand even snel naar onze privémail om er 's avonds verder aan te werken.

Aan ons informatiebeveiligers de complexe taak die incidenten te beperken. Hoe langer ik in dit vak werk, hoe duidelijker het mij wordt dat deze taak bestaat uit twee subtaken. Ten eerste natuurlijk incidenten proberen te voorkomen. Maar hoe hard we ook ons best doen, we kunnen incidenten nou eenmaal niet 100% voor zijn. Daarom is onze tweede subtaak minstens zo belangrijk: de impact van incidenten beperken.

Willen we in staat zijn de impact van incidenten te beperken, zullen we in ieder geval zo snel mogelijk moeten weten dat er een incident is (geweest). Dat klinkt logisch, toch gaat het in de praktijk vaak anders. Juist doordat we erop hameren dat medewerkers veilig moeten werken, kan er voor hen een drempel ontstaan om te melden dat er iets mis is gegaan. Dan kan men kiezen voor zwijgen en hopen dat het voorbij gaat. Niet wat je als informatiebeveiliger wil, want als het níet voorbij gaat, ben je er laat bij. Soms te laat.

Dus, werk aan het creëren van openheid! Vertel medewerkers wat je van ze verwacht als het toch misgaat. Vertel ze dat het kan gebeuren. En dat je het wilt weten. Dat je liever drie keer te vaak wordt gebeld dan één keer te weinig. Dat het erbij hoort. Dat het niet stom is en het iedereen kan gebeuren. Maar dat ze wel de verplichting hebben om het te melden.

Dus zo klopte ik, drie dagen na het verstrijken van mijn proeftijd, aan bij onze Information Security Officer. Die me met een grote grijns complimenteerde met mijn openheid. Hij had namelijk de USB-stick zelf gevonden en was vooral benieuwd hoe ik zou handelen na een fout. Fieuw, toch een klein beetje geslaagd…

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.

Auteurs: Ellen Joyce Dijkema is Senior Manager Business Improvement bij BDO Advisory. Zij is bereikbaar via ellen.joyce.dijkema@bdo.nl.
Erie Berhitu is Manager Cybersecurity & Business Continuity bij BDO Advisory. Zij is bereikbaar via Erie.berhitu@bdo.nl.

Never waste a good crisis

Naar antifragiliteit in bedrijfsvoering en supply chain

2020 is vooralsnog een 'interessant' jaar gebleken voor organisaties en hun toeleveringsketens. Een dreigende handelsoorlog tussen de VS en China, de naderende post-Brexit economie en de coronacrisis zetten organisaties er toe aan om hun bedrijfsmodellen drastisch te herzien. Met name de coronacrisis zorgt ervoor dat iedere schakel uit de toeleveringsketen onder druk komt te staan. In het kader van 'never waste a good crisis' kunnen de huidige perikelen ook worden gezien als kans om te leren.

Bedrijfscontinuïteit maakt net als de vertrouwelijkheids- en integriteitsaspecten van informatiebeveiliging steeds vaker integraal onderdeel uit van risicomanagement. Hiermee lijken zowel informatiebeveiliging als continuïteit eindelijk de strategische aanhaakpunten te hebben gevonden om bedrijfsbreed op strategisch niveau te mogen opereren. De coronacrisis heeft aangetoond dat continuïteitsplannen die bedrijven op de plank hebben liggen, niet altijd specifiek genoeg zijn voor iedere situatie. Of juist te specifiek waren gericht op scenario's die – tot nu toe – niet hebben gespeeld. Terwijl scenario's waar wél al veel eerder tegen zou moeten zijn opgetreden, te weinig aandacht hebben gehad. Waaruit weer blijkt dat het beheersen van de bedrijfscontinuïteit niet is te vatten in een 'one-size-fits-all'-scenario. Het vergt inzicht in de grote diversiteit aan risico's voor de continuïteit in allerlei organisatieonderdelen en -aspecten zoals processen, mensen, middelen, leveranciers en systemen. Pas als daar een goed overzicht van bestaat, kunnen passende continuïteitsmaatregelen worden bepaald. Dat is best wat werk – maar is nodig, én levert veel inzicht op in waar de organisatie nou eigenlijk om draait.

Verbeterslag

Net als bij het risicomanagement dat wordt gedaan om 'in control' te komen, zal het continuïteitsmanagement een forse verbeterslag moeten doorgaan om óók van enige beheersing terzake te kunnen spreken. En dan gaat het om meer dan alleen denken in scenario's. Want er zal ook aandacht moeten zijn voor het trainen van medewerkers, het periodiek testen en aanpassen van plannen, en – wellicht het belangrijkste aspect – het blijvend herhalen van alle bovengenoemde stappen om continu te streven naar verbetering en veranderingen binnen en buiten de organisatie soepeltjes te verwerken in de continuïteitsplannen.
Dus kort en goed: bedrijfscontinuïteit als continu proces vergt een consistente, proactieve en procesmatige aanpak waarbij tenminste aandacht wordt besteed aan:

- Het analyseren van risico's en de gevolgen voor de bedrijfsdoelstellingen;
- Implementatie van maatregelen en procedures om risico's te beheersen;
- Het identificeren van verschillende dreigingsscenario's;
- Business Impact Analyses om de belangrijkste risico's en aspecten bij crises in kaart te brengen;
- Het identificeren en implementeren van algemene herstelstrategieën;
- Identificatie van calamiteitsscenario's;
- Oefenen met en testen van geplande procedures en plannen;
- Herhaald evalueren van het risicomanagement en de continuïteitsacitviteiten.

Supply Chain Management

Een belangrijk aspect voor veel organisaties in relatie tot continuïteit betreft de leveringsketen, ofwel de supply chain. Het specifiek als apart onderdeel van de bedrijfsvoering beheren van supply chains is in de voorbije jaren steeds belangrijker geworden voor het concurrentievermogen van veel bedrijven. Het mondiale karakter van de toeleveringsketen maakt deze ook steeds kwetsbaarder voor risico's voor de bedrijfscontinuïteit. Hoe langer en complexer de keten, des te meer kans op fouten en afbreuk en des te kleiner de foutmarge voor het opvangen van

vertragingen en verstoringen. De focus die geruime tijd heeft gelegen op supply chain-optimalisatie om kosten te minimaliseren, heeft buffers verminderd. Het opvangen van vertragingen en verstoringen wordt daardoor steeds moeilijker. De coronacrisis heeft veel bedrijven doen inzien hoe kwetsbaar ze daadwerkelijk zijn (geworden) voor een onderbreking in de wereldwijde, zoveel gecompliceerde supply chain. De afgelopen periode is gebleken dat goedkope leveranciers met veelal lange doorloop- en levertijden uiteindelijk minder betrouwbaar of flexibel zijn dan gewenst. De economische risico's die hieruit voortvloeien, zijn zeer reëel en zijn merkbaar in zowat alle sectoren.

Zoeken naar zekerheidsequivalenten

Lange tijd werd voornamelijk gekeken naar efficiënte supply chains en lage kosten. Dit lijken gelukkig niet langer de (enige) dimensies waarop waardeketens worden beoordeeld. Het ligt voor de hand dat in de nasleep van de coronacrisis veel bewuster naar risico's wordt gekeken. We zien nu meer de noodzaak om vanwege de risico's de sourcingstrategie aan te passen, door bijvoorbeeld productie of inkoop beter te spreiden, leveranciers dichter bij huis te zoeken (`nearshoring') en leverancierskwalificaties anders te definiëren.

Door de toegenomen risico-aversie zijn organisaties nu meer gericht op zekerheid en proberen zij een buffer of voorraad aan te leggen of alternatieve leveringsmogelijkheden te zoeken. `Just-in-time'-leveringen worden vaker vervangen door een ruimere tijdsplanning. Sommige organisaties sourcen belangrijke componenten bij meerdere leveranciers; dat houdt die niet alleen scherp maar zorgt ook voor redundantie die de afbreukrisico's aanzienlijk terugbrengt. `Total cost of ownership' krijgt zodoende hernieuwde aandacht, waarbij ook de kosten van vertraagde en ontbrekende leveringen in ogenschouw moeten worden genomen.

Dit geldt ook zeker voor de IT-supply chain. Soms kent een organisatie nog wel alle of bijna alle IT-dienstenleveranciers. Maar slechts weinig organisaties kennen ook de leveranciers van die leveranciers. Het is daardoor lastig om te weten hoe de IT-ketens in elkaar zitten, en nog lastiger om erachter te komen hoe bijvoorbeeld de informatiebeveiliging van de ketens zijn geregeld. Wie kent er niet het geval Diginotar? Daar liet een IT-onderonderaannemer een enkel steekje vallen. Einde Diginotar. Misschien loopt zoiets bij uw organisatie niet zo snel uit de hand, maar hoe weet u dat eigenlijk?

Ken de supply chain

De afgelopen periode hebben veel ondernemers ad hoc op situaties ingespeeld. Hierdoor zijn een aantal gaten in de zichtbaarheid en betrouwbaarheid van de supply chain blootgelegd, maar wat zo ad hoc is gevonden, geeft te denken dat er wellicht meer is. Daarom is het nu een goed moment om de supply chain helemaal te evalueren en de impact van eventuele risico's op de bedrijfsvoering te beoordelen. Uitzonderingen daargelaten, zal blijken dat de supply chain robuuster en wendbaarder moet. Daarvoor zijn zes strategieën beschikbaar:

- **Houd dagelijks veranderingen in de vraag in de gaten om goed gevoel te houden bij de benodigde producten en voorraden.** Uit de dagelijkse veranderingen komen de eerste signalen voort dat er misschien `iets' aan de hand is. Bedenk daarbij echter wel dat schommelingen ook gewoon dat kunnen zijn. Niet iedere afwijking is het eerste signaal van problemen; soms is er niks. Maar zonder te kijken, weet u niet dat en of er iets aan de hand is. Voor zover het gegevensstromen van en naar de leveranciers en afnemers betreft, zijn tegenwoordig uitstekende tools beschikbaar om allerlei patronen te ontdekken – en de uitzonderingen daarop;
- **Communiceer met de belangrijkste leveranciers over eisen en wensen – wederzijds.** Spreek ook eens met afnemers, of die wellicht wensen hebben waar u uit service-oogpunt makkelijk op in kunt spelen;
- **Wees een transparante partner,** maak goede afspraken en deel informatie, zodat uw leveranciers tijdig kunnen inspelen op uw variabele behoeften. Werken in de keten betekent ook samenwerken;
- **Geef prioriteit aan (de juiste) klanten en producten.** Niet alle producten hoeven even snel bij alle afnemers te liggen, en wat kost dat wel niet? Beter is te weten wat de meeste kritische afnemers zijn, waar de beste (belangrijkste) marges worden gehaald en waar dus de meeste aandacht aan moet worden gegeven. Weet welke klanten en producten het betreft;
- **Focus op continuïteitsmaatregelen voor die klanten of producten met de hoogste marges** en investeer werkkapitaal om de winstgevendheid te maximaliseren, verlies van vitale klanten te voorkomen en reputatierisico's te minimaliseren;
- **Beperk leveranciersrisico's.** Maak een inschatting van de mogelijke toekomstige toeleveringsketen, inclusief manieren om leveranciers te diversifiëren, en beoordeel het kosten-batenvoordeel van onder andere het continu onderhouden van dubbele faciliteiten of routes vanuit de `total-cost-of-ownership'-gedachte inclusief de kosten

Optimale voorbereiding zodat u een toekomstige crisis het hoofd kunt bieden

van onderbrekingen. De coronacrisis heeft de noodzaak aangetoond om goed te diversifiëren om verstoringen van kritische componenten te beperken en wendbaarheid te vergroten. Dit geldt ook voor IT. De meeste IT-dienstenleveranciers werken met onder- en zelfs onder-onderaannemers. Daar kan nog wel eens wat misgaan. Weet wat waar gebeurt. Neem ook maatregelen als het niet overal even goed geregeld is met informatiebeveiliging;

- **Evalueer de gehele supply chain.** Zijn leveranciers, afnemers, productiefaciliteiten en magazijnen op de juiste plaatsen gevestigd? Zijn er veranderingen die u moet overwegen gezien het kritieke belang voor producten en de mogelijkheid voor verstoring? Hierbij geldt ook dat die bovengenoemde onder-onderaannemers weleens in een land opereren waar de organisatie liever niet mee te maken wil (of mag) hebben. Zonder inzicht in wat nou uiteindelijk waar gebeurt, zal de organisatie daar pas te laat achter komen;
- **Kies de verbeteracties met het meeste rendement voor de korte en lange termijn.** Gebruik hierbij nieuwe technologieën die het beheer van netwerken van leveranciers vergemakkelijken waardoor signalen van verstoring sneller doorkomen en zo snel mogelijk kan worden ingegrepen.

Verhogen van antifragiliteit

Maar hoe bereidt u zich dan optimaal voor zodat u een toekomstige crisis het hoofd kunt bieden? Een belangrijke factor hierbij is het nastreven van antifragiliteit. Antifragiliteit staat voor het vermogen van een organisatie om sterker te kunnen worden van tegenslagen. De optiehandelaar, wiskundige en filosoof Nassim Taleb argumenteert dat men te veel naar de wereld kijkt als voorspelbare plek. We hebben de neiging optimistisch te zijn en niet uit te gaan van onverwachte gebeurtenissen. Op het eerste gezicht geen slechte eigenschap. Tot zich een totaal onverwachte gebeurtenis voordoet. Dan blijkt toch dat veel organisaties niet veel meer kunnen doen dan dweilen en de kraan dichten, meestal in die volgorde. Of zolang het nog niet zo erg lekt, tegen steeds hogere kosten blijven dweilen en klagen dat de waterrekening zo hoog wordt, daar zou de overheid toch iets aan moeten doen.

Taleb stelt dat robuuste organisaties beter bestand zijn tegen onverwachte gebeurtenissen. Onder meer door wendbaar te zijn en snel van koers te kunnen veranderen waar nodig, door te diversifiëren in producten, diensten en grondstoffen, en door te experimenteren en innoveren op het gebied van mensen, producten en technologie. Wie continu in beweging is, kan snel omschakelen naar verdedigen en voorkomen dat iedereen er maar een beetje bij staat als de calamiteit vrij komt voor de keeper. En: 'train like you fight, then you'll fight like you train'. Dat geeft zelfvertrouwen dat áls er wat gebeurt, het niet exact hetzelfde zal zijn als in een getraind scenario maar men toch voldoende voorbereid is om er zonder al te veel schade doorheen te komen.

Maar bovenal zijn antifragiele organisaties degenen die zelfs beter worden van tegenslagen; ze komen sterker uit de crisis dan ze waren. Dit vergt veel inzicht in de huidige organisatie en behalve dat innovatie continu doorgaat, ook inzicht in waar innovaties nog net niet kunnen – totdat een crisis barrières wegneemt. Onder druk wordt alles vloeibaar, dus zorg dan actief vooruitgang te kunnen boetseren. Als dit aansluit op een continu bewustzijn van de omgeving en de veranderingen daarin, dan komen we al dichtbij de agile organisatie die zo vaak wordt gewenst. De organisatie is dan niet alleen agile in het afpakken van de bal en terugnemen van het initiatief – robuust – maar kan dan direct terreinwinst boeken – de tactieken waren al geoefend en kunnen nu dan eindelijk worden ingezet. Welke ideeën hebt u op de plank om robuuster en bovendien antifragiel te kunnen optreden in de supply chain?

Dieper inzicht

Betekent dit dat u per direct antifragiel moet worden om een toekomstige crisis het hoofd te kunnen bieden? Zeker niet. Maar, het is verstandig dieper inzicht te krijgen in enerzijds uw vitale systemen en processen en anderzijds de impact die een onderbreking van de continuïteit met zich meebrengt, zodat u de bedrijfsvoering en leveringsketens continu robuust kunt houden – én wendbaar de toekomst in kunt gaan. 'Never waste a good crisis', want wie weet komen u en uw leveranciers er sterker uit.

Auteur: Gert Kogenhop is directeur van bcm+, een bedrijf dat is gespecialiseerd in training, consultancy en implementatie van business continuity-managementsystemen conform de norm ISO 22301. Hij is voorzitter van Business Continuity Management en Crisismanagement normcommissie bij NEN. Gert is bereikbaar via gk@bcmplus.nl.

CMT, CSIRT, BCMT, de rollen en verantwoordelijkheden

Het aantal cyber security incidenten neemt eerder toe dan af. Kleine, maar ook grote, gerenommeerde organisaties worden getroffen. In eigen land staat ons het ransomware incident bij de Universiteit Maastricht nog helder voor de geest en in de zomer was Garmin volop in het nieuws en zij zijn zeker niet de enigen die dit hebben ervaren. De afhankelijkheid van IT of ICT is enorm, eigenlijk onaanvaardbaar groot.

De harde realiteit is dat bijna niemand alternatieven heeft, bijvoorbeeld een handmatige wijze van werken, in situaties waarbij applicaties, het netwerk of internet niet beschikbaar of bereikbaar zijn, bestanden 'verdwenen' zijn of gecompromitteerd. In ernstige gevallen leidt dit tot een crisissituatie waarbij de samenwerking tussen verschillende disciplines in de (tijdelijke crisis) organisatie van doorslaggevend belang is bij het oplossen van het probleem, adequate reactie en schadebeperking, zowel organisatorisch, financieel alsook met betrekking tot de reputatie.

Elke organisatie wordt blootgesteld aan risico's. Velen zijn vergelijkbaar, zoals ICT-uitval, een bedrijfsbrand, problemen met gas, water en elektra of extreem weer. Anderen zijn specifiek, bijvoorbeeld als gevolg van wat bedrijven of organisaties doen: zoals de chemische industrie, softwareontwikkeling, een bouwbedrijf, datacenter, gemeente of bakkerij. Ook waar organisaties gevestigd zijn maakt een verschil: in de buurt van een luchthaven of naast een rivier, dijk of dam. Of de buurman is bijvoorbeeld een chemische fabriek of een olie-, opslag- of distributielocatie. Risk Management, organisational en operational, is een must en over het algemeen wordt dit redelijk goed beheerst en beheerd (gemanaged). Deze aanpak bestaat uit een reeks processen en procedures die de besluitvorming en prestaties ondersteunen en verbeteren. Het geeft een geïntegreerd beeld van hoe goed een organisatie haar specifieke risico set managet. De wereld en heel specifiek onze (zakelijke) omgeving, verandert in een snel tempo, dus we moeten allemaal voortdurend onze ogen op de bal houden. Voorbeelden zijn de gevolgen van klimaatverandering, Brexit, de handelsoorlog VS versus China, COVID-19 en de niet echt gunstige ontwikkelingen op cybersecuritygebied.

Iedereen afhankelijk van ICT

Tegenwoordig is iedereen afhankelijk van informatietechnologie, of we het nu leuk vinden of niet, en we hebben deze situatie zelf gecreëerd. Als gevolg daarvan zijn informatiebeveiliging en gegevensbescherming belangrijke elementen waar aandacht aan moet worden besteed. De EU-richtlijn 'Concerning measures for a high common level of security of network and information systems across the Union' en de 'General Data Protection Regulation' (GDPR) zijn belangrijke drijfveren voor alle ICT-gerelateerde disciplines. ICT-afhankelijkheid maakt organisaties kwetsbaar en we kunnen niet wegkijken en doen of het ons niet zal raken. ICT-uitval, niet alleen technisch falen, maar ook niet beschikbaar zijn van applicaties, gegevensbestanden, netwerken en toegang tot internet als gevolg van cybercriminaliteit, veroorzaakt een enorme verstoring en kan voor veel organisaties zelfs fataal zijn. Een kwestie die 25 jaar geleden nauwelijks bestond.

Organisaties kunnen worden geconfronteerd met een crisissituatie als gevolg van een ernstige verstoring, dus Crisis Management en Business Continuity Management zijn voorwaarden voor een goed gemanagede organisatie en in sommige landen zijn deze zelfs verplicht. Onvoorbereid zijn is niet acceptabel en 'We kijken wel als er wat gebeurt' is onmogelijk, onverantwoordelijk en wordt zeker niet beschouwd als een 'good business practice'.

Wat is Business Resilience?

Organisaties moeten stabiel, robuust en tegelijkertijd veerkrachtig (resilient) en wendbaar (agile) zijn. Enige tijd geleden is de term Organisational Resilience geïntroduceerd, hoewel er nog geen overeenstemming is over hoe deze te definiëren. Gezien de complexiteit van het verband tussen onder meer resilience, risico en business continuity management is het verstandig om met resilience te beginnen, omdat dit een soort overkoepelend karakter heeft. Als het gaat over resilience, of vertaald weerstandsvermogen (weerbaarheid) en veerkracht, dan moet deze wel in de juiste context geplaatst worden. Hieronder een aantal definities die voor het behoud van originaliteit in het Engels zijn.

- **Psychological resilience** is the ability to mentally or emotionally cope with a crisis or to return to pre-crisis status quickly.
- **Computer networking resilience** is the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.
- **Material science resilience** is the ability of a material to absorb energy when it is deformed elastically, and release that energy upon unloading.
- **Organisational resilience (ISO 22316:2017)** is the ability of an organization to absorb and adapt in a changing environment.
- **Organisational resilience (BS65000:2014)** is the ability of an organisation to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper

Als we vertrekken vanuit de laatste definitie, die iets specifieker is dan de ISO 22316, dan is nog niet geheel duidelijk waar risico en business continuity management passen. Het Security and Continuity (SECO) Institute heeft hieraan een

vervolg gegeven en een aantal disciplines samengebracht in wat zij noemen Business Resilience. De definitie daarvan, voortbordurend op de British Standard luidt:
`Business Resilience is the ability of an organisation to anticipate, prepare for, detect, respond and adapt to substantial change and sudden disruptions in order to survive and prosper by integrating management systems that build resilience, and develop capabilities for an effective risk response that safeguards the interests of key interested parties and restores the organization's capabilities.'
Business Resilience is de integratie van een aantal disciplines of expertisegebieden gecombineerd in een gezamenlijke inspanning om de toekomst van een organisatie veilig te stellen in de continu veranderende omgeving waarin deze opereert, de veerkracht van uw organisatie op het moment van een ernstige verstoring. Het gaat hier over het combineren van Risk Management (RM), Information Security & Data Protection (IS & DP), Business Continuity Management (BCM) en Crisis Management (CM) op het juiste niveau, met als doel een optimale uitvoering van de elementen te garanderen. Het is absoluut een uitdaging om de verschillende expertisegebieden zo goed mogelijk te laten samensmelten, terwijl iedereen nog steeds in staat moet zijn onafhankelijk te werken. En wie is vervolgens de eigenaar van dit proces? Voor veel organisaties is dit onbekend terrein. Er moet aandacht worden besteed aan samenwerking, informatie-uitwisseling en het juiste niveau van (systeem)integratie.
Deze definitie van Business Resilience is essentieel voor het opbouwen van een veerkrachtige organisatie, want wat de doelen en doelstellingen ook zijn, dit is de kern van elk bedrijf. `Hoe' en `Waarom' elementen werden toegevoegd aan de British Standard definitie en de belangrijke term 'detect' werd toegevoegd, daar dit een `must have' is voor mensen die werkzaam zijn in Information Security. Bij SECO Institute werd het woord 'substantial' in dit geval als een betere match ervaren dan 'incremental'.
De belangrijkste redenen voor het combineren van deze vijf expertisegebieden zijn:

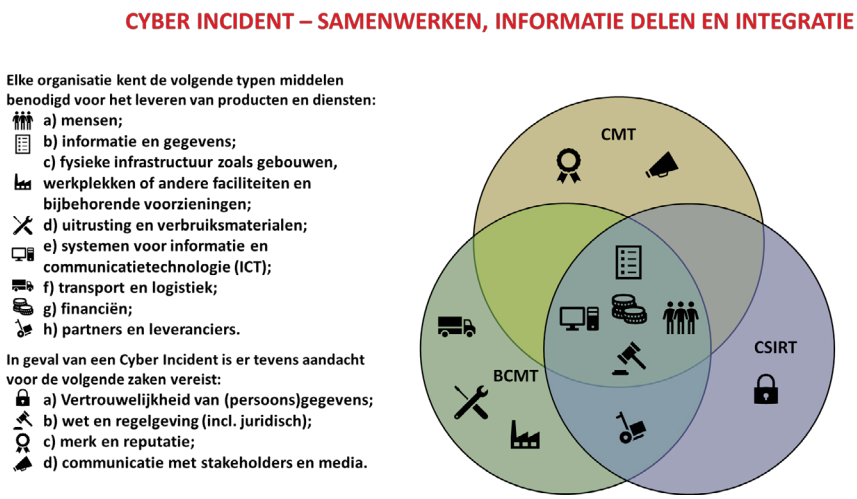
- Deze gecombineerde gebieden hebben al een gemeenschappelijk doelstelling: het beschermen van de kroonjuwelen van de organisatie en het veiligstellen van de toekomst;
- Het koppelen van de inspanningen is een kwestie van consistentie en coördinatie door afstemming, met tal van synergiemogelijkheden;
- De professionals die werkzaam zijn in deze vijf expertisegebieden zullen veel effectiever en efficiënter kunnen functioneren, terwijl zij nog steeds in staat zijn om onafhankelijk te werken en zij hun onpartijdigheid kunnen behouden voor die zaken waarvoor dit vereist is.

De kern van een resilient organisatie

Uiteraard kunnen er andere elementen aan Business Resilience worden toegevoegd, bijvoorbeeld op basis van het feit dat organisaties zich in een specifieke branche bevinden. Zo moeten bijvoorbeeld banken rekening houden met specifieke wet- en regelgeving en eisen vanuit De Nederlandsche Bank en andere toezichthouders (bijvoorbeeld EU-regelgeving en Bazel-akkoorden). In de voedselindustrie zijn er specifieke kwaliteit en `food safety manufacturing' regelingen (bijvoorbeeld BRC, IFS en ISO 22000) en `product fraud' elementen die kunnen worden toegevoegd voor een optimale invulling. In de chemiesector zijn er veel lokale eisen, bijvoorbeeld vanuit OSHA.
Vanuit dit perspectief kan Business Resilience gezien worden als een soort `Joint Crisis Fighter', zoals de JSF, de nieuwe 'Joint Strike Fighter' (de F-35), die zowel informatie sneller kan verzamelen als delen dan welk ander vliegtuig dan ook. Vanzelfsprekend dien je voorzichtig om te gaan met vergelijkingen, maar het verzamelen en delen van informatie is wel in de kern van een resilient organisatie.

Samenwerken, informatie delen en integratie

Het verzamelen en delen van informatie tijdens bijvoorbeeld een cyberincident, de inspanningen tijdens de samenwerking tussen het Crisis Management Team (CMT), het Cyber Security Incident Response Team (CSIRT) en het Business Continuity Management Team (BCMT), zijn cruciaal en van het grootste belang, net als tijdens elke andere vorm van verstoring die van invloed is op de levering van geprioriteerde producten en diensten. In de ISO 22301:2019 Business Continuity Management Systems – Requirements (hoofdstuk 8.3.4) standaard is een lijst opgenomen van soorten benodigde middelen, die ten minste moeten worden bepaald om geselecteerde strategieën te implementeren. Zie figuur 1.



Figuur 1 – Samenwerken, informatie delen en integratie.

Bij het over elkaar leggen van deze elementen en daaraan gerelateerde activiteiten over de drie teams die betrokken zijn bij een cyberincident, CMT, CSIRT en BCMT is het duidelijk dat er elementen en middelen zijn die team-specifiek zijn. Zoals merk, reputatie en communicatie met belanghebbenden en media, die worden beheerd door de CMT. Beveiliging van (persoonlijke) informatie/gegevens worden beheerd door de CSIRT en middelen gerelateerde activiteiten met betrekking tot de fysieke infrastructuur, zoals gebouwen, werkplekken of andere faciliteiten en bijbehorende voorzieningen, uitrusting en verbruiksmaterialen plus transport en logistiek worden beheerd door de BCMT. Alles in overeenstemming met hetgeen hiervoor vermeld over de behoefte, en vaak zelfs een vereiste, om zelfstandig, onafhankelijk en onpartijdig zaken uit te kunnen voeren.
Het is echter compleet duidelijk dat alle andere middelen, en met name zaken als het voldoen aan wet- en regelgeving, betrokkenheid van alle teams vereisen, maar in de meeste gevallen met een ander doel. Dit wordt duidelijk wanneer het gaat om de informatiebehoefte. Zo is informatie over het cyberincident voor het CMT van het grootste belang om het ernstniveau te bepalen en om onder meer vast te stellen wat te communiceren aan wie, rekening houdend met wederom fungerende wet- en regelgeving en mogelijke specifieke voorschriften die van toepassing zijn. Voor het CSIRT is informatie een vereiste voor het proces van detecteren en adequaat reageren, daar hier hun specifieke verantwoordelijkheid ligt tijdens een cyberincident. Het BCMT heeft informatie nodig om de situatie te beoordelen en het juiste scenario uit te voeren om de levering van producten en/of diensten op aanvaardbare vooraf gedefinieerde niveaus voort te kunnen zetten. Het is duidelijk dat het interpreteren en gebruiken van alle gedeelde middelen en elementen nog steeds een specifieke teaminspanning is op basis van hun specifieke vereisten, maar de beschikbaarheid van één unieke set van elk op één plaats is een voorwaarde voor een succesvolle reactie in het geval van, in dit voorbeeld, een cyberincident. Samenwerken, informatie delen en integratie zijn de sleutelwoorden en tegelijkertijd uitdagingen, zie figuur 1.

Business Resilience Management Systeem

Op basis van de 'wens' om een gedegen bedrijfsbeleid te voeren en onder alle omstandigheden de controle te kunnen (blijven) behouden, dus inclusief adequaat reageren tijdens een incident, dienen de genoemde vakgebieden te worden samengebracht in één managementsysteem, het Business Resilience Management Systeem.

Veel organisaties bevinden zich nog in de ontwikkelingsfase als het gaat om het implementeren van een Business Resilience Management aanpak

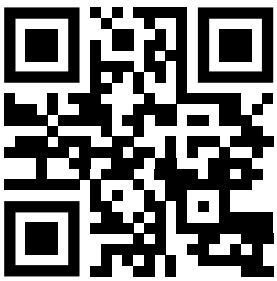
Elke organisatie dient een verantwoordelijke functionaris aan te stellen, waarbij de titel niet van het grootste belang is (Manager, Officer, Hoofd of Coördinator bijvoorbeeld) voor het beheer van de Business Resilience inspanning. Deze functionaris is automatisch de eigenaar van het Business Resilience proces. Optimaal is het wanneer deze functionaris rechtstreeks rapporteert aan het juiste C-level in de organisatie. Dit is eigenlijk een voorwaarde voor een succesvolle implementatie en uitvoering, maar wellicht voor menig organisatie nog niet volledig duidelijk. Een sponsor op C-level is wel het minste en wie dat dan moet zijn hangt af van het soort bedrijf. Voor een bank of verzekeraar ligt dit vaak op het bordje van de Chief Information Officer of Chief Risk Officer, terwijl dit in de maak- of bijvoorbeeld voedingsindustrie, waar dit soort functies op een ander niveau opereren, de Chief Financial Officer of Chief Operating Officer blijkt te zijn.

Uitdaging

Veel organisaties bevinden zich nog in de ontwikkelingsfase als het gaat om het implementeren van een Business Resilience Management aanpak en slechts een enkeling heeft een managementsysteem ingericht. Het volwassenheidsniveau is daardoor nog steeds laag en een uitspraak als "Business Resilience is ingebed in de manier waarop we hier werken" lijkt een brug te ver voor velen. Business Resilience is nog steeds een relatief jong vakgebied en organisaties zijn op zoek naar richting, ondersteuning en 'best practices' om hun inspanningen te verbeteren en de organisatie verder te brengen. Het implementeren van Business Resilience Management en het creëren van een managementsysteem in elke organisatie met silo's, eilandjes en koninkrijkjes, waarin de vijf expertisegebieden zijn gevestigd, is voor alle betrokkenen een uitdaging. Om in dit geval gebruik te maken van de kracht van herhaling hier nogmaals één van de redenen om dit te doen: de professionals die werkzaam zijn in deze vijf expertisegebieden zullen veel effectiever en efficiënter kunnen functioneren, terwijl zij nog steeds in staat zijn om onafhankelijk te werken en hun onpartijdigheid kunnen behouden voor die zaken waarvoor dit vereist is. Een fantastische uitdaging voor de Business Resilience functionaris.

Uit een recent onderzoek onder deelnemers aan een webinar over dit onderwerp komt naar voren dat ongeveer 40% al op de één of andere manier bezig is om deze vijf vakgebieden met elkaar te verbinden of zelfs 'volledige' integratie nastreeft zoals hier bedoeld. Op de vraag of men dit een goede ontwikkeling vindt, reageert nagenoeg iedereen: "Dit is de toekomst, daar is geen twijfel over mogelijk". Waarvan akte.

COLUMN Berry



Bekijk deze video

Verkiezingen, hoe moet dat nu?

We leven in een rare maatschappij op dit moment. Een onzichtbare vijand waart rond die pas zichtbaar wordt als je ermee besmet raakt. Ik noem de naam niet, want die horen we vaak genoeg. Wat natuurlijk in deze barre tijden wel altijd doorgang moet vinden zijn de verkiezingen. Stemhokjes zijn natuurlijk beslist uit den boze en dus worden we min of meer gedwongen om verfoeide websites te openen waar je kunt stemmen.

Normaliter worden belangrijke stemmingen gedaan op bijvoorbeeld partijcongressen, maar die kunnen ook de nodige verwarring geven. Graag verwijs ik kortheidshalve naar het partijcongres van het CDA in 2011 waar op de uitzetting van Mauro kon worden gestemd. Chaos alom en als je chagrijnig bent raad ik u dit filmpje aan (https://bit.ly/3kepDuw). Geweldig leuk en vermakelijk, maar het lijkt erop dat het CDA patent heeft op rommelachtige verkiezingen, want ook bij de verkiezingen van de partijleider van het CDA wordt sterk getwijfeld aan de uitslag. De eerste ronde moest helemaal worden overgedaan omdat een ethical hacker aantoonde dat het eenvoudig was om de verkiezingsuitslag te beïnvloeden. Inmiddels zijn alle rondes geweest en blijkt de winnaar met een miniem verschil te hebben gewonnen. Het verschil in het aantal stemmen was zeer beperkt, maar werd zowel door de winnaar als de verliezer geaccepteerd. Toch ontstaan er nu wat twijfels, omdat onder andere de echtgenote van Tweede Kamerlid Pieter Omtzigt na het stemmen op haar man, een pop-up kreeg en bedankt werd voor haar stem op de tegenstander. Er zouden meerdere mensen een verkeerd pop-upje hebben gehad. Zou allemaal kunnen, maar de notaris is er zeker van dat alles goed is gegaan en dus is dat zo.

Bewust gebruik ik dit voorbeeld omdat deze verkiezingen natuurlijk helemaal nergens over gaan, maar op 3 november staan de verkiezingen in Amerika op de planning. Met een president die voorzichtig gezegd redelijk onvoorspelbaar is. Die al verschillende dreigementen heeft geuit over de wijze waarop gestemd wordt. Het is maar de vraag of de verkiezingen op deze datum doorgang vinden.

Ergens in januari vindt de inauguratie plaats van de nieuwe president. Het verkiezingsstelsel is erg complex en Russische inmenging is niet ondenkbaar. Trump won de verkiezingen in 2016 ondanks het feit dat hij miljoenen minder stemmen kreeg dan Clinton. Ik verwacht dat de discussies over de einduitslag op 4 november zullen gaan beginnen en het is de vraag of er een duidelijke winnaar komt van die discussies. Tegen de tijd dat dit onvolprezen blad op de deurmat valt, is wel bekend of de CDA-verkiezingen eerlijk zijn verlopen.

Berry

Auteurs: Lex Borger is security architect, docent bij Tesorion en oud-hoofdredacteur van iB-magazine. Lex is bereikbaar via lex.borger@tesorion.nl. Ewout de Roos is security consultant bij Tesorion. Ewout is bereikbaar via ewout.deroos@tesorion.nl.

COVID-19 als BCM booster

In een eerdere uitgave van dit blad stond een artikel over het omgaan met de gevolgen van een pandemie (1). De directe aanleiding voor dat artikel was de dreiging van een uitbraak van de vogelgriep (H5N1) in die tijd, met een terugblik op de SARS-epidemie in 2003. Beide epidemieën hebben het niet gehaald tot de status 'pandemie'. Profetisch meldde Henk Zellenrath in zijn artikel dat 'het een kwestie van tijd is voordat de bom barst.'

Dit leek al in 2009-2010 het geval met de varkensgriep (ook bekend als H1N1 of swine flu). Ondanks een officiële pandemiestatus kon deze uitbraak niet herkend worden boven de normale seizoensgriepcijfers. En het bleef 'tegenvallen': een uitbraak van MERS die in 2012 begon en nog steeds voortduurt, heeft moeite een epidemie genoemd te worden. Tussen 2013 en 2016 woedde een Ebola-epidemie in Afrika. Voor Europa heeft dit weinig gevolgen. Het leek wel of het pandemiescenario in een BCM-impactanalyse meer een theoretische oefening was dan een serieuze dreiging.

Klapper

En toen kwam de klapper, helemaal uit het niets. Vanuit Wuhan kwam eind 2019 een nieuw coronavirus, SARS-CoV-2, die bij mensen een ziekte veroorzaakt, COVID-19, die het in een paar maanden tijd tot 'pandemie'-status brengt. Wereldwijd leidt COVID-19 tot een enorme belasting van de gezondheidszorg, in haar wielen gevolgd door een gigantische economische schade. De cijfers zijn hoog (in augustus 2020 al meer dan 20 miljoen besmettingen en meer dan 700 duizend doden). De maatregelen zeer ingrijpend: reisverboden, gedwongen sluitingen, verplichte quarantaines, thuiswerken, afstand houden en mondkapjes dragen zijn het 'nieuwe normaal'. In hoeverre was de COVID-19 pandemie te voorzien? Niet. Het was te verwachten, maar dat is iets anders. Was de impact te voorzien? Dat zeker wel. En er is geen mooiere manier om dat te illustreren dan met quotes uit het artikel van Henk Zellenrath:

'Een pandemie is echter maar één van de vele mogelijke groot-

schalige calamiteiten die u kunnen treffen zonder dat u daar iets aan kunt doen. Denk eens aan een gifwolk in de Botlek, of aan Tsjernobyl. Ook kunt u dichtbij huis blijven en eens nadenken over gevolgen waar u geen invloed op uit kunt oefenen zoals 'just in time' toelevering. Heeft u wel eens gevraagd wat uw vitale leveranciers aan BCP hebben gedaan? Is het onderwerp onderdeel van een Service Level Agreement? De lijst mogelijke calamiteiten is eindeloos lang.'

'Veel van pandemieachtige rampen zijn geen calamiteit in de traditionele zin van het woord zoals die tot heden binnen BCP vaak wordt gebruikt. Een calamiteit is een onverwachte gebeurtenis. H5N1 en vele andere rampen kan men echter al een aantal jaren vooraf aan zien komen. Nu komen ze alleen ineens snel dichterbij. Dus onverwacht is het niet echt. U kunt het wat dat betreft vergelijken met het Y2K-syndroom van rond de eeuwwisseling.' 'Medewerkers worden besmet en besmetten op hun beurt weer anderen, leveranciers kunnen niet aan hun verplichtingen voldoen en beroepen zich op overmacht. Uw klanten laten niets van zich horen of annuleren hun orders. Afhankelijk van het (doem)scenario dat u schetst kan een dergelijke gebeurtenis leiden tot een totale ontwrichting van de maatschappij. De gezondheidszorg werkt niet of zeer gebrekkig, beveiliging functioneert niet meer.' 'Ervaring leert verder, zoals recentelijk de gevolgen in New Orleans als resultaat van de orkaan Katrina, dat binnen zeer korte tijd na het wegvallen van het openbaar gezag de eerste plunderingen een feit zijn.'

Pandemiescenario

Uit deze teksten blijkt dat COVID-19 zich goed gehouden heeft aan het pandemiescenario zoals dat in 2006 voorzien werd. Zellenrath heeft het over een aantal aspecten die ingevuld moeten worden, wil een BCP van nut zijn: business continuity beleid en een duidelijke scope. Bij een pandemie is het juist belangrijk om die scope goed in de gaten te houden, want het scenario voor een pandemie wijkt af van vele andere calamiteitsscenario's, in maatregelen die buiten de bedrijfsscope genomen worden en de impact die het veroorzaakt:

- Er zullen nationaal en internationaal maatregelen genomen worden om de pandemie te beperken;
- Er kunnen van overheidswege dwingende maatregelen komen voor je bedrijf;
- Een pandemie zal ook je klanten, partners en concurrenten treffen.

Dit maakt dat plannen voor een pandemie meer een 'best effort'-karakter zullen hebben, in plaats van continuïteitsgaranties te leveren. Toch beveelt Zellenrath aan dezelfde methodiek te gebruiken voor het maken van de pandemieplannen. Wat betreft de pandemie hebben deze plannen als hoofddoel:

- Voorzien in het welzijn van medewerkers. Die heb je nodig om vitale processen op te starten en gaande te houden. Tegelijkertijd zijn ze mogelijk een besmettingsbron. Contactbeperking onderling is dus noodzakelijk, anders is er niet voldoende personeel over. (In termen van deze tijd: thuiswerken, afstand houden, drukte vermijden en mondkapjes dragen).
- Zo spoedig mogelijk de draad weer kunnen oppakken. Hier hoort ook bij het contact houden met je relaties door de pandemie heen, waarbij je kunt kijken hoe je hen zou kunnen helpen.

Calamiteitscenario's

BCM is de capaciteit in een organisatie om te kunnen omgaan met een crisis die voortkomt uit een calamiteit. Calamiteiten zijn incidenten met een lage kans van voorkomen, die potentieel veel impact hebben op de organisatie en waar moeilijk preventief tegen te beschermen is. Wat je daarom preventief doet, is de mogelijke calamiteitscenario's inventariseren en plannen hoe je in het geval van het voordoen van zo'n scenario een crisis zou aanpakken.

Omdat dit potentieel veel verschillende scenario's zijn, en je niet in detail alles wilt plannen, is het zaak om de plannen algemeen en flexibel te houden. In het algemeen bevatten BCM-plannen voor elke fase: vóór, tijdens en na een crisis. Hiervoor kent BCM het BCP (Business Continuity Plan) om de scope te bepalen (beleid, systemen, calamiteiten), verschillende CMPs (Crisis Management Plannen) voor de aanpak van calamiteiten bij een crisis, en het DRP (Disaster Recovery Plan) voor de terugkeer naar normaal ná de crisis.

Het BCP zal veelal een aantal basisprocessen van algemeen nut voor de organisatie specificeren die op orde horen te zijn, zoals een recente BIA (Business Impact Analyse), incident managementproces, (IT-)asset managementproces en een communicatieplan. Omdat een crisis zeldzaam is, kun je je voorstellen dat het meest gebruikte plan in een organisatie het BCP is. CMPs en het DRP worden niet vaak in crisissituaties uitgevoerd, wat het nodig maakt deze regelmatig te oefenen, zeker jaarlijks. Ook dat is in het BCP geregeld.

Een BCP moet passen op en meegroeien met het volwassenheidsniveau van de organisatie. Initieel zal BCM zich alleen richten op de kritieke bedrijfsprocessen en de belangrijkste externe afhankelijkheden en zullen de plannen een hoog abstractieniveau hebben. Naarmate er meer geoefend wordt, zal BCM zich meer ontwikkelen, worden de plannen specifieker en het vertrouwen van de organisatie in de plannen groter.

Pandemie-specifieke maatregelen

Het is heel nuttig om BCM niet alleen binnen het bedrijf te oefenen. Externe afhankelijkheden kun je gezamenlijk oefenen, met je leveranciers en afnemers, binnen je sector of nog breder. Hierbij wordt samenwerking in crisissituaties goed beproefd, iets wat bij een echte crisis vlekkeloos moet werken.

In de rest van het artikel geeft Zellenrath een overzicht van maatregelen zoals die in het BCP, in het relevante CMP voor de aanpak van een pandemiecrisis, en in het DRP kunnen worden opgenomen. Hij constateert al dat de pandemiespecifieke maatregelen vooral in het BCP komen. Een paar opvallende zaken:

- Inventariseer de noodzakelijke (IT-)middelen tijdens de crisis. Hij noemt hier de IT-capaciteit in het algemeen, thuiswerken en videoconferencing. (In 2006 was videoconferencing nog iets dat je apart opzette, nu hebben we simpelweg Teams, WebEx en Zoom);
- Neem de mogelijke sociale gevolgen voor je medewerkers op in je plannen. Ze moeten mogelijk thuiswerken omdat scholen en kinderopvang gesloten zijn of openbaar vervoer niet rijdt;
- Reken op een verzuim van 25%. Regel op basis hiervan vervangbaarheid van medewerkers;
- Vermijd concentraties van medewerkers op kantoor. Bereid de BHV voor met kennis over ziekteverschijnselen en beschermende kleding. (Dit punt is rechts ingehaald door massaal thuiswerken);
- Calamiteitsmaatregelen opnemen in SLA's;
- Inventariseer de risico's van 'just-in-time'-leveringen in jouw logistieke ketens;
- Onderzoek alternatieven voor het nakomen van verplichtingen bij calamiteiten. Denk hierbij vooral aan hulp vragen of bieden aan 'bevriende' organisaties;
- Houd rekening met de impact op economische gevolgen van de pandemie. Kunnen jij en je debiteuren aan hun verplichtingen voldoen? Heb je je geld voor andere zaken nodig?

Zo kun je aan de hand van het artikel al toetsen hoe pandemie-proof de BCM-capability van jouw organisatie is; door te beschouwen hoe een pandemie als calamiteitsscenario in het BCP opgenomen is. Een crisis als gevolg van een

pandemie heeft binnen de organisatie niet alleen impact door de absentie van mensen door ziekte, maar zoals we zagen ook door de gevolgen van overheidsmaatregelen op mensen, het veranderde gebruik en beheer van IT-middelen. En al je ketenpartners zullen dezelfde impact ook voelen, wat zowel de toevoer- als afvoerketen onder druk zal zetten. Elke afhankelijkheid van die keten vertaalt zich in potentiële impact op jouw organisatie, zowel logistiek en financieel. Je ketenpartners kunnen wellicht niet leveren of afnemen, of jouw bedrijf kan dat juist niet. Dit zou je daarin terug willen zien.

Paradoxen

Eén aspect dat voor andere crises geldt, is bij een pandemie-crisis minder aanwezig. Doorgaans heeft een crisis naast financiële gevolgen ook een negatieve impact op de geloofwaardigheid en reputatie van de organisatie. Bij een pandemie is dit minimaal, doordat de crisis zo breed gevoeld wordt. Als we naar de huidige crisis kijken, dan zien we dat bijna de hele maatschappij onder druk staat van de crisis, wat doorwerkt als economische krimp voor de hele samenleving. En paradoxaal zijn er ook organisaties die juist welvaren bij een pandemie, omdat de vraag naar hun producten of diensten juist stijgt of omdat ze flexibel genoeg waren om snel in te springen op nieuwe vraag uit de markt. Zoals bedrijven die mondkapjes gingen leveren of (onderdelen voor) beademingsapparatuur.

Ervaring rijker

We hadden voor de COVID-19 crisis al zeker genoeg kennis om business continuity goed op orde te hebben. Echte ervaring was er nog niet. Nog niet eerder tijdens het IT-tijdperk kwam een pandemie zo snel op en had die pandemie zo een grote impact op de samenleving. Met deze ervaring rijker is onze bewustwording gegroeid en kunnen we een boost geven aan de BCM-capaciteit in de organisatie. Deze boost zal er voor zorgen dat met name communicatieverantwoordelijkheden en ketenafhankelijkheden goed in beeld zijn, de organisatie zich flexibeler zal kunnen opstellen met meer ruimte voor creativiteit. En bij organisaties die hier goed uitkomen worden just-in-time delivery strategieën en de financiële noodbuffers waarschijnlijk nog eens goed onder de loep genomen.

Referentie

(1) Henk Zellenrath (2006, juli). 'Pandemie' en Business Continuity Planning. Informatiebeveiliging, p. 44-47.

Rectificaties

In iB-4 waren bij het artikel van Kimberly Hengst over 'Best practices in cloud incident handling' de referenties naar de bronnen weggevallen. Daarom publiceren we ze hieronder alsnog.

(1) www.telegraaf.nl/nieuws/2785226/pathe-voor-19-miljoen-euro-opgelicht-door-nepmails
(2) www.forbes.com/sites/leemathews/2019/06/09/toyota-parts-supplier-hit-by-$37-million-email-scam
(3) www.ad.nl/enschede/cybercriminelen-lichten-rijksmuseum-twenthe-op-voor-2-9-miljoen~a3a0b6ab/
(4) P. Cichonski, T. Millar, T. Grance and K. Scarfone, 'Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology', NIST Special Publication, vol. 800, no. 61, pp. 1--79, 2012.
(5) K. Hengst, 'Best Practices in Cloud Incident Handling', 7 February 2020, http://essay.utwente.nl/80630/.

In iB-4 is bij het artikel van Tim Janssen 'Met een SSI behoudt de gebruiker regie over zijn eigen data' de bedrijfsnaam niet goed vermeld. De correcte naam van het bedrijf is Visma Connect. Tim Janssen is werkzaam bij Visma Connect en is bereikbaar via tim.janssen@visma.com.

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

Securitylessen van mijn vader

Vier dingen die ik spelenderwijs van mijn vader leerde zijn ook toepasbaar in het securitywerkveld.

Slalommen op je fiets is leuk en nog leuker als je het doet in een haven. Zorg wel dat de aansluitende trapper omhoog is als je op de kade een vrije bolder aan de waterkant wilt passeren. Anders val je met fiets en al in het water en wordt je vader (hij bedoelde: mijn opa) zeer boos. Met andere woorden: als je software automatisch periodiek het bestand -waar je aan werkt- opslaat, maak dan aan het begin van elke werksessie een veiligheidskopie. Met bijvoorbeeld een volgnummer in de naam. Zodat je weggooi-actie in je afstudeerwerkstuk, de onherstelbare nieuwe sortering in een spreadsheet of de moeilijke Photoshop-operatie niet meteen onbedoeld wordt opgeslagen in de enige versie van je bestand. Sommige mensen zijn fanatiek met back-ups en kopiëren elk uur hun hele harde schijf naar een extern exemplaar. Als je de leesbaarheid van deze kopie nooit controleert, wees dan bij een ransomware infectie niet verbaasd als de malware ook die volledige kopie van een uur geleden heeft besmet. Bij back-ups met magnetische tapes hanteert men het grootvader-vader-zoon-principe. Zodat er dus altijd twee generaties back-ups aanwezig zijn, met enige tijd ertussen en waarbij de restore-mogelijkheid regelmatig wordt getest. Dat is nog steeds een goed idee.

2 Een steen maakt een grappig geluid op een Duitse staalhelm. Afgevuurd met een katapult is de energie van de steen groter en het geluid harder. Je kunt na enige oefening zelfs een staalhelm van het dak van het schuurtje af schieten. Doe dit niet terwijl je er recht onder staat, want zo'n vallende helm geeft door zijn scherpe rand rondom een flinke snijwond in je hoofd en leidt tot behoorlijk veel bloedverlies. Stel je hebt een algoritme bedacht om gegevens te anonimiseren door de naam van klant 1 te koppelen aan het adres van klant 2 en de woonplaats van klant 3. Met een geanonimiseerde productiedatabase kan de business niet werken. Pas daarom je anonimiseer-programma niet toe op de live productiedatabase, maar maak daarvan eerst een kopie. Als het algoritme afdoende anonimiseert, is het immers niet eenvoudig terug te draaien. Anders kan iemand met inzage in het volledige bestand (een tester of zo, ik noem maar iets) dat immers ook gemakkelijk doen!

3 Mijn vader verkocht verzekeringen en ontving als tussenpersoon alle schademeldingen in onze buurt. Daardoor had ik reeds als kind over al die gebeurtenissen toegang tot actuele threat intelligence, die mijn vader tijdens het spelen, bij de dagelijkse net-uit-school-thee of aan de eettafel met gedetailleerde voorbeelden zeer actionable maakte voor mij.
Hij deed me voor hoe je het beste achterstevoren op je fiets kunt rijden. Alles is andersom: links en rechts op het stuur zijn verwisseld en je terugtraprem gaat naar voor. Verder zit het ongemakkelijk, dus je kunt het niet goed lang aan een stuk doen. En je ziet niet waar je heengaat, zoals bij reverse engineering van malware. Toch was hij zuinig op zijn fiets die hij na gebruik ook telkens (en afgesloten) in het schuurtje stalde. Laat terwijl je binnen bent bij het stallen van je fiets niet je complete sleutelbos aan de buitenkant in het slot steken. Een inbreker kan jou namelijk met je eigen sleutels opsluiten en rustig het hele huis leegroven. En omdat er dan geen braaksporen zijn, wordt de diefstal niet gedekt door de verzekering. Het gaat er dus niet om óf je verzekerd bent, bijvoorbeeld tegen computercriminaliteit en malware, maar wat de precieze definitie van de dekking in de polis is. En dat, wanneer je al je wachtwoorden opslaat in één passwordmanager, het noodzakelijk is om dat ene wachtwoord van dat programma uitstekend te beveiligen. Dus niet al je sleutels of eieren in één mandje bewaren, want dan kun je ze allemaal tegelijk kwijtraken. Overigens: als je een wachtwoordsysteem gebruikt met overal 'pietjepuk-2020' gevolgd door FB, LI, WA voor respectievelijk Facebook, Linkedin en Whatsapp heb je weliswaar overal andere wachtwoorden die je gemakkelijk kunt onthouden, maar loop je toch een risico. Iemand die één wachtwoord van je onderschept, kan daarmee gemakkelijk de andere wachtwoorden raden. En de eigenaar van de app, website of applicatie (bij connectie via internet) waar je een wachtwoord aanmaakt, hoeft deze niet eens te onderscheppen. Je geeft hem/haar bij het registeren immers dat wachtwoord zelf. Dat jij op het invoerscherm sterretjes ziet, betekent niet dat de ontvanger het niet kan lezen en onversleuteld opslaan in een wachtwoordentabel.

4 Mijn laatste voorbeeld gaat over communicatie. Mijn vader leerde me dat lezen leuk en nuttig is, omdat je jezelf er altijd (bij regen en zonneschijn) mee kunt vermaken en dat je er vrijwel alles mee kunt leren. Hij deelde zijn praktijkkennis (zie hiervoor) en schonk me verder aandacht, tijd en liefde en werd zo mijn trusted advisor. Als hij iets zei, geloofde ik dat direct. Toen we een keer tijdens een boswandeling een weiland omringd door schrikdraad zagen, wist ik al genoeg door het lezen van het waarschuwingsbord. Mijn vader vertelde me dat je niet aan het draad moest komen en zeker niet met natte handen, bijvoorbeeld na het zwemmen.
Later leerde ik tijdens mijn NLP-studie dat ik zowel in de visuele (lezers, kijkers) als de auditieve (luisteraars, toehoorders) groep viel, qua geprefereerde communicatiestijlen. En op die NLP-voorkeur representatiesystemen moet je inspelen om je security awareness boodschap goed over te laten komen bij je doelgroep(en).

Door bovengenoemde lessen bleef ik gelukkig buiten de derde groep mensen, die communicatie over security zelfs niet wil geloven als het duidelijk is opgeschreven en met grafieken en schema's is toegelicht. En ook niet wil luisteren als een betrouwbaar iemand geduldig en met aansprekende (!) voorbeelden de risico's in een presentatie uitlegt. Neen, deze laatste groep (de voelers) kan dat iets op securitygebied géén goed idee is helaas alleen ontdekken door zelf op het schrikdraad te plassen.

Auteurs: Joop Franke (Hon) FBCI is certified BC-professional en eigenaar van BCxPert. Joop is te bereiken via info@bcxpert.nl & www.bcxpert.nl of Linkedin http://linkedin.com/in/joopfranke. Tom Bakker RI RE CISM CISA is redactielid van iB-magazine. Tom is te bereiken via tombakker@pvib.nl.

De stand van zaken van BCM in Nederland

Op 9 juni 2020 is een enquête gepubliceerd met het doel na te gaan hoe BCM in Nederlandse organisaties is ingevoerd. Dit verslag is het resultaat van de enquête tot 1 september 2020 en is 34 maal ingevuld.

De enquête is bekend gemaakt via LinkedIn, Twitter, verzoek aan provincies en gemeenten en delen door anderen in ons netwerk en persoonlijke uitnodigingen. We hebben niet het bereik gevonden waarop we hadden gehoopt. De reden hiervoor is ons niet bekend. Daarom blijft de enquête nog openstaan en wanneer er daartoe aanleiding is worden de resultaten bijgesteld.

Met 34 ingevulde enquêtes moeten we voorzichtig zijn met het trekken van (harde) conclusies. Toch kunnen we er wat mee en zullen we een aantal vragen en antwoorden met een toelichting weergeven.

Wat is Business Continuity Management?

We hebben dit als volgt omschreven:
"Business Continuity Management is het geheel aan samenhangende activiteiten dat erop is gericht dat een organisatie in beeld heeft welke bedreigingen, risico's er op een organisatie rusten en welke (gevolg) schade deze kunnen veroorzaken als bedreigingen manifest worden" De aard van de bedreigingen worden geïnventariseerd door middel van het uitvoeren van een Bedreigingen en Kwetsbaarheid analyse, de (gevolg) schade wordt in beeld gebracht door middelen van het uitvoeren van een Business Impact analyse. Het beeld van bedreigingen kan zeer divers zijn en overal in de organisatie aanwezig zijn. Sleutelwoord in Business Continuity Management is dan ook 'samenwerken"! Om het manifest worden van bedreigingen, risico's te kunnen beperken stelt een organisatie nadat het bedreigingenbeeld is vastgelegd een Preventieplan op met het doel geconstateerde bedreigingen, risico's te kunnen gaan beheersen. Op basis van een (gevolg) schadebeeld: bedreigingen zijn manifest geworden, stelt een organisatie een repressieplan BCP (Business Continuity Plan) op waarin de volgende plannen zijn opgenomen:

1. Bedrijfshulpverleningsplan met als doel: op het moment van manifest worden van de bedreiging / het risico; de veiligheid van bezoekers en medewerkers te waarborgen;
2. Een crisismanagement- en crisiscommunicatieplan om na het manifest worden van een bedreiging/risico de gevolgen en reputatieschade te kunnen beheersen;
3. Herstel ('recovery') plannen; vaak maatwerk afgestemd op de aard en omvang van de organisatie.

Veel bekende plannen van het onder 3 genoemde zijn: IT -, Werkplek uitwijk maar ook plannen waarmee ernstige informatiebeveiligingsincidenten kunnen worden beheerst.

Het algemene beeld van de enquête

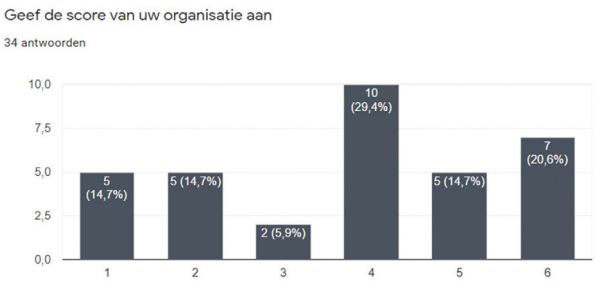
Verschillende sectoren hebben deelgenomen aan de enquête. Van organisaties die de enquête hebben ingevuld had het merendeel (70,6%) meer dan 1000 medewerkers. Het zou erop kunnen duiden dat in kleinere organisaties BCM nog niet echt zijn plaats heeft gevonden. Vanuit de bank & verzekeringssector hadden we ook wat meer deelname verwacht evenals van Gemeenten en Provincies. Van diegenen die de enquête hebben ingevuld hebben we een aantal enquêtevragen in dit verslag opgenomen en voorzien van een toelichting.

Vraag: Is er op strategisch niveau een proceseigenaar benoemd?
Om het BCM-proces goed in een organisatie verankert te krijgen moet er op strategisch niveau voldoende aandacht en draagvlak zijn. Dit kan worden bewerkstelligd door op strategisch niveau een BCM-proceseigenaar te benoemen die eindverantwoordelijk is voor de werking en de resultaten van het proces. Uitwerking van de BCM-activiteiten worden door de proceseigenaar gedelegeerd naar een BCM-groep op tactisch en operationeel niveau. Gelukkig zien we dat bij de meeste organisaties een proceseigenaar is benoemd (82%). Daar waar dat niet het geval is kun je, je afvragen "voor wie doe je het dan?"

Vraag: Is het budget toereikend voor het BCM-proces?
Elk proces heeft een budget te besteden. Dit geldt ook voor het BCM-proces. Jaarlijks dient bij de budgetronde door de BCM-groep op tactisch niveau een opgave worden gemaakt voor het nodige budget voor o.a. onderhoud van het proces, plannen, maatregelen, testen en oefenen. Organisaties waar het budget toereikend (62%) is, mogen zich gelukkig prijzen, terwijl bij organisaties waar dit niet het geval is het een 'survival of the fittest' wordt.

Vraag: In onze organisatie wordt in silo's gewerkt
Om BCM een succes te laten zijn in de organisatie is, zoals hiervoor al geschreven, samenwerking in een organisatie van enorm belang. Indien samenwerking ontbreekt dan zal dit direct ten koste gaan van de kwaliteit van het Business Continuity Management Proces en de producten, plannen die dit proces voortbrengt. Als binnen organisaties het beeld is zoals in figuur 1 is aangegeven, dat is dat zeer verontrustend. Advies aan deze organisaties is dan ook: ga samenwerken! Organiseer het proces zodanig dat bekend is wie waarvoor verantwoordelijk is en breng dit in uiting in een BCM-organogram. Om silowerking te voorkomen zal er vaak eerst een bewustwordingscampagne moeten worden uitgevoerd.

Vraag: Is er BCM-beleid opgesteld?
Doel van beleid is dat in dit geval richting wordt gegeven aan



Figuur 1: 1= helemaal mee eens, 6=helemaal mee oneens

Business Continuity Management in een organisatie. Hiermee kan ook worden voorkomen dat silo werking blijft plaatsvinden. De meeste organisaties die de enquête hebben ingevuld hebben een BCM-beleid opgesteld (88%). Een advies aan organisaties die dit nog niet hebben gedaan is om alsnog beleid te gaan opstellen. Zonder beleid ligt silo werking ook hier weer op de loer en mogelijk dat het proces zich niet in de juiste richting begeeft.

Vraag: Worden er periodiek Bedreigingen en Kwetsbaarheid analyse uitgevoerd?

Eén van de stappen uit het Business Continuity Management proces en één van de belangrijkste pijlers voor het Business Continuity Plan (BCP), is het periodiek uitvoeren van een Bedreigingen en Kwetsbaarheid analyse. Als deze stelselmatig goed wordt uitgevoerd met alle betrokkenen in de organisatie dan krijgt de organisatie de beschikking over het totale bedreigingenbeeld dat op de organisatie van toepassing is en kan proactief gekeken worden naar preventieve maatregelen waar dat nodig is. Als het bedreigingenbeeld niet bekend of onvolledig is, is het zeer goed mogelijk dat een organisatie plotseling wordt geconfronteerd met een dan onverwachte maar waarschijnlijk zeer ongewenste gebeurtenis. We zien bij de meeste organisatie de Bedreigingen en Kwetsbaarheid analyse periodiek wordt uitgevoerd. Aan de organisaties die dit niet doen of nog niet gedaan hebben (15%) is toch wel het advies dit zo snel mogelijk te doen.

Vraag: Worden er periodiek een Business Impact Analyse uitgevoerd?

Een tweede belangrijke pijler die informatie levert voor het opstellen van het Business Continuity Plan (BCP) is het periodiek uitvoeren van Business Impact Analyse (BIA). Uitkomsten van een BIA stelt een organisatie in staat om vroegtijdig maatregelen te kunnen invoeren en plannen te kunnen opstellen om gevolgschade die in de BIA wordt geïnventariseerd te kunnen gaan beheersen. Met de uitkomsten van een BIA kan een organisatie een kosten- baten analyse maken voor wat betreft het realiseren van gevolgschade-beperkende maatregelen. Bij veel organisaties die de enquête hebben ingevuld wordt de BIA jaarlijks uitgevoerd (41%) maar ook als er zich wijzigingen voordoen in processen, gebouwen, bedrijfsmiddelen, wetsaanpassingen etc. (29%). Zonder het uitvoeren van een BIA (20%) zal het moeilijk, zo niet onmogelijk zijn om maatregelen te treffen om gevolgschade te kunnen beheersen zodra een bedreiging, risico manifest wordt.

Vraag: Wat is de gemiddelde testfrequentie van het BCP of delen ervan?

Doel van het testen, toepassen van het BCP is om de werking aan te tonen van de maatregelen en de plannen die door het BCM-proces zijn voortgebracht. Als er niet periodiek wordt getest dan zal dit in geval een bedreiging manifest wordt voor een organisatie vérstrekkende gevolgen hebben om dat de maatregelen/plannen niet werken en 'kapitaalvernietiging' van alle inzet en investering in maatregelen op de loer ligt. Verder kan het voor de organisatie grote reputatieschade met zich meebrengen. De meeste testen jaarlijks (50%) dan wel halfjaarlijks (27%). Op de vervolgvraag wat er dan getest wordt valt op dat vaak BHV (ontruiming) en back-up & recovery testen worden genoemd. Blijkbaar is het toch nog steeds voornamelijk een ICT-aangelegenheid naast de verplichting tot ontruimingsoefeningen.

Vraag: Wordt er een jaarlijkse testkalender opgesteld?

Om te voorkomen dat er onvoldoende periodiek/tijdig wordt getest en geoefend met het BCP, is het advies om een jaarlijkse testkalender op te stellen. Dit gebeurt in samenwerking met de planeigenaren. Op deze wijze weet de organisatie wanneer er testen/oefeningen gepland staan en dan ook volgens deze planning uitgevoerd moeten worden. Bij toepassen van de testkalender geldt: "Comply or Explain" Voer de testen uit op de geplande datum of leg uit waarom dit niet is gebeurd. Een ruime meerderheid van de organisatie geeft aan dat een jaarlijkse testkalender wordt opgesteld (71%).

Vraag: Wordt deze testkalender geaccordeerd door lid van het strategisch management?

Voor draagvlak en betrokkenheid bij het testen van het BCP is het zeer gewenst dat de testkalender geaccordeerd wordt door een lid van het strategisch management of de BCM-proceseigenaar. Deze laat dan direct zien dat testen noodzakelijk is. Bij de meeste organisatie wordt de testkalender dan ook bevestigd (79%).

Vraag: Worden testen altijd volgens de testkalender uitgevoerd?
Het is van groot belang dat testen die genoemd staan in de testkalender ook tijdig worden uitgevoerd. Voorkomen moet worden dat testen op het laatste moment gecanceld gaan worden. Toepassen van een testkalender vraagt dan ook de bijbehorende discipline. Uit de enquête blijkt dat bij de meeste organisaties de testen in overeenstemming met de testkalender worden uitgevoerd (63%). Bij organisaties waar dit niet gebeurt kan dat betekenen dat omissies in de maatregelen of plannen te laat worden opgemerkt of dat in het slechtste geval blijkt dat de maatregelen en de plannen tijdens een calamiteit niet werken.

Vraag: Wordt er voor elke test een testplan gemaakt?
Doel van testen van het BCP: periodiek de ingevoerde maatregelen en bijbehorende plannen op werking te toetsen en hier aan de BCM-proceseigenaar zekerheid te geven over de werking van het BCP.
Het is aan te bevelen voor elke test een plan op te stellen waarin beschreven: 1. de doelstelling en 2. de KPI's. Bij de evaluatie: toetsing van de afwijking van het resultaat ten opzichte van de KPI's. Uit de enquête blijkt dat het merendeel van de organisaties een testplan maakt (71%).

Vraag: Hoe vindt u dat het proces wordt beheerd, periodieke audits, certificering, onderhoud BCP?
BCM is een proces net als andere processen in een organisatie. Veel processen in een organisatie worden onderworpen aan audits die vervolgens weer van belang kunnen zijn voor certificering. Voor het BCP moet een onderhoudskalender worden opgesteld en worden bewaakt zodat het BCP en bijbehorende maatregelen op actualiteit kunnen worden getoetst. Organisaties die gecertificeerd zijn (27%) zullen hier strikt de hand aan houden anders lopen zij het risico dat op enig moment het certificaat wordt ingetrokken. Als een dergelijk certificaat werd gecommuniceerd naar 'stakeholders' dan kan dat reputatieschade tot gevolg hebben wanneer de 'stakeholders' merken dat het certificaat is ingetrokken. Toch zien we het beheer van het BCM-proces in sommige organisaties varieert van Kan beter en Slecht tot Zeer Slecht (samen 41%). Hier is het risico aanwezig dat het BCM-proces op enig moment totaal niet meer functioneert en er enorme kapitaalvernietiging optreedt.

Vraag: Hoe waardeert u het BCM-proces binnen uw organisatie?
Wat hier ook opvalt is het aantal waarderingen van Kan Beter, Slecht en Zeer Slecht (41%). Als oorzaken/redenen werden hiervoor aangegeven o.a.:

- Te veel werk voor een te beperkte hoeveelheid beschikbare resources
- Binnen de organisatie geen oog voor, ad hoc organisatie
- Onvoldoende commitment bij Raad van Bestuur en Management
- BCM is alleen in de PDC-organisatie geborgd. (ICT en Facilitair bedrijf)
- Niet de hoogste prioriteit, dagelijkse business staat voorop.
- Bewustwording en draagvlak
- Heeft nog meer gewenning nodig
- Geen aandacht en geen erkenning hiervoor
- Communicatie: "onbekend maakt onbemind"

Organisaties met een zeer goed of goed beoordeling (59%) gaven de volgende redenen:

- Er is voldoende aandacht en we testen regelmatig de procedures;
- Succesvol omdat het crisis proces zeer goed werkt en op ieder niveau functionarissen zijn benoemd (strategisch, tactisch, operationeel);
- Management commitment, budget, resources, BCM-organisatie, beleid, goede borging in organisatie door veel draagvlak, ondersteunende software, pragmatisch ingericht, Ingebed in de bedrijfsvoering;
- ISO22301 gecertificeerd BCM-team aangesteld;
- Interesse toezichthouder. Crises. Near misses;
- Support van moederbedrijf.

Tot slot

- BCM is een MANAGEMENT-proces
- Het BCM-proces levert toegevoegde waarde aan de organisatie
- Het BCM-proces helpt de strategische doelen te kunnen bereiken ook in onzekere tijden
- BCM is van elke afdeling, van elke laag in de organisatie
- BCM is er voor iedereen die betrokken is bij uw organisatie
- BCM is een vak, een professie!
- BCM is vooral mensenwerk!
- BCM is waar mensen samenwerken, het is geen individuele opdracht
- BCM is een samenspel van activiteiten

Als je je herkent in de resultaten van de enquête dan heb je wel ideeën wat er moet gebeuren of je weet dat je het goed hebt aangepakt.

Voor de gedetailleerde rapportage van de resultaten verwijzen we je naar:
https://www.bcm-nl-incidents.eu/bcm-enquete.html

Auteur Jan Martijn Broekhof is managing director van Nederlands security SaaS vendor Guardian360. Jan Martijn is bereikbaar via jm.broekhof@guardian360.nl.

Moeten ook MKB IT-dienstverleners er nu echt aan gaan geloven?

Pas recent werd duidelijk dat een rechter in 2018 een vonnis heeft gewezen waarin een IT-dienstverlener de kosten grotendeels moest vergoeden die het gevolg waren van schade door een ransomware infectie. In de dagen nadat het vonnis bekend werd ontstonden verschillende discussies op LinkedIn en sites als Security.nl. De meningen liepen sterk uiteen: voor sommigen was het een onbegrijpelijke uitspraak, anderen verzuchtten dat er nu eindelijk eens opgetreden werd.

Wat was er aan de hand? Doordat er op afstand op een RDP-server ingelogd kon worden met eenvoudig te achterhalen credentials, is het de criminelen gelukt om ransomware in het netwerk actief te maken, waardoor bestanden onbeschikbaar werden. De back-upvoorzieningen waren niet afdoende ingericht waardoor de klant zich genoodzaakt voelde om bitcoins te betalen om de bestanden weer terug te krijgen. Omdat de partijen in de ogen van de rechter beiden schuldig zijn aan het ontstaan van deze situatie, heeft de rechter geoordeeld dat de IT-dienstverlener twee derde van de financiële schade voor zijn rekening moest nemen. Deze kosten voor onderzoek en herstel worden daarnaast nog verhoogd omdat de IT-dienstverlener ook de proceskosten van zijn klant moet vergoeden.

Zorgplicht IT-dienstverlener

Wat de uitspraak mede interessant maakt, is dat de rechter een uitspraak gedaan heeft die deels gebaseerd is op de zorgplicht die een IT-dienstverlener heeft en de verwachtingen die een klant ten aanzien van informatiebeveiliging mag hebben. Ondanks dat er geen wettelijke verplichtingen zijn, mag een klant wel een bepaald basisniveau van beveiliging van zijn IT-dienstverlener verwachten. Saillant detail is dat de IT-dienstverlener wel heeft aangegeven bij zijn klant dat er zwakke wachtwoorden gebruikt werden. Maar omdat men dat onhandig vond, koos de klant ervoor deze niet sterker te maken. De rechter verwijt de IT-dienstverlener dat hij niet meer indringend en herhaaldelijk gewaarschuwd heeft. De rechter stelde ook dat de IT-dienstverlener de opdracht had kunnen weigeren omdat het simpelweg niet mogelijk was om een nieuw netwerk aan te leggen en te beheren dat aan de basisveiligheidseisen voldoet.

Precedent geschapen?

Wat ikzelf interessant vind aan deze zaak is, dat een IT-dienstverlener aansprakelijk gesteld is voor schade, terwijl de klant de IT-middelen niet veilig genoeg gebruikt heeft. Volgens de rechter mag een klant een bepaald basisniveau van beveiliging verwachten van zijn IT-dienstverlener en is het de plicht van de IT-dienstverlener om de klant indringend en herhaaldelijk te waarschuwen wanneer hij beveiligingsadviezen niet opvolgt.

Het voelt een beetje alsof een autoverkoper niet alleen moet controleren dat een klant een rijbewijs heeft, maar ook herhaaldelijk moet benadrukken dat hij niet te hard moet rijden, niet te veel alcohol moet drinken en om zijn verlichting moet denken. Tegelijkertijd vind ik het een positieve ontwikkeling dat IT-dienstverleners meer zorg gaan dragen voor hun klanten. Elk bedrijf is tegenwoordig een automatiseringsbedrijf; zonder IT staat alles stil. En laten de meeste klanten nou weinig tot geen verstand hebben van IT, anders hadden ze de IT-dienstverlener helemaal niet nodig, toch? De metafoor met de auto gaat hier dan weer op. Als automobilist vind je het heel normaal dat je met een geldig rijbewijs de weg op gaat, dat je verzekerd bent en dat je je auto regelmatig laat onderhouden en APK-keuren.

Wetgeving en brancherichtlijnen

Belangrijk detail is echter wel dat er veel wetgeving is rondom autorijden. Zonder rijbewijs of APK-keuring mag je niet eens de weg op. Bij het gebruik van IT-middelen en afnemen van IT-diensten is deze wetgeving er nog niet. Maar die zit er wel aan te komen. Er ligt namelijk een wetsvoorstel op Europees niveau klaar met de naam: Uitvoeringswet Cyberbeveiligingsverordening. Deze verordening biedt een Europees kader voor cyberbeveiligingscertificering voor ICT-producten, ICT-diensten en ICT-processen die gelden in de hele EU. Hoewel de certificering in beginsel nog vrijwillig is, verwacht ik wel dat afnemers steeds meer naar dit certificaat zullen gaan vragen, net zoals gebeurd is met de ISO 27001. Zodra het certificaat vaak genoeg verlangd wordt, zullen steeds meer rechters van mening zijn dat het voldoen aan bepaalde standaarden simpelweg van de IT-dienstverlener verwacht mag worden, ondanks dat het misschien nog geen geldende wetgeving is.

Risicobeheersing

Ook voor de IT-dienstverleners die het MKB bedienen geldt dat zij hun eigen risicobeheersing steeds beter op orde moeten krijgen, willen ze ongeschonden door juridische procedures komen. Dit zal helaas wel als gevolg hebben dat IT-dienstverleners nog meer tijd kwijt zijn aan het administreren en minder tijd overhouden voor daadwerkelijk ondersteunen van hun klanten. Wat dit met de tarieven gaat doen zal de tijd uitwijzen, maar ik verwacht dat IT-dienstverleners alleen kunnen overleven door nauw samen te gaan werken met andere IT-dienstverleners of zich over te laten nemen door een grotere partij.

Binnen Cyberveilig Nederland wordt ook nagedacht over het borgen van kwaliteit door informatiebeveiligers. Welke kwaliteit mag een klant verwachten van een bij de brancheverenging aangesloten bedrijf? Ik zou de IT-dienstverleners willen adviseren om die ontwikkeling nauwlettend in de gaten te houden. Informatiebeveiliging is niet alleen een essentieel element binnen hun dienstverlening, deze component zal in de komende jaren alleen maar zwaarder gaan wegen.

Referenties

(1) Bron: https://uitspraken.rechtspraak.nl/inziendocument?id=-ECLI:NL:RBAMS:2018:10124

(2) Bron: www.security.nl/posting/660081/It-bedrijf+moet+schade+door+ransomware+bij+klant+grotendeels+vergoeden

(3) Bron: www.internetconsultatie.nl/uitvoeringswetcyberbeveiligingsverordening

(4) Bron: https://cyberveilignederland.nl/kwaliteit-transparantie/

Auteurs: Marc de Jong Luneau is commercieel directeur en senior strategisch adviseur security bij Northwave. Pim Takkenberg is directeur cyber security van Northwave. Marc is bereikbaar via: marc.d.jongluneau@northwave.nl. Pim is bereikbaar via: pim.takkenberg@northwave.nl.

Cyber resilience en de lessen van het incident

Deel 2: Van wake-up call naar resilience roadmap

In het eerste artikel in deze reeks (iB-Magazine, jaargang 20, editie 4, pagina 42-45) maakten we kennis met Stock Foundation BV (fictieve naam, waargebeurd verhaal). Dit bedrijf werd in maart van vorig jaar voor het eerst binnengedrongen door een zogenaamde 'initial access broker'. Vervolgens volgde in mei 2019 een omvangrijke ransomware-aanval. Het bedrijf kwam volledig stil te liggen. Criminelen maakten daarbij een bedrag van drie cijfers buit. In Bitcoin welteverstaan.

Northwave hielp bij de incident response en recovery en later met een cybersecurity roadmap met als doel meer stabiliteit en weerbaarheid in de toekomst. We analyseerden in het eerste artikel dit incident op basis van de Unified Kill Chain, het MITRE ATT&CK framework en enkele andere modellen.

Dit gecombineerde model deelt cyberaanvallen op in achttien unieke stappen binnen drie fasen. De opties om binnen te komen (IN), het raakvlak uit te breiden (THROUGH) en ook verschillende routes naar het creëren van impact (OUT). In de rest van het artikel verdiepten we dit perspectief om te komen tot een evaluatie van het incident en een aantal constateringen ten aanzien van wat Stock Foundation zou kunnen doen om zich in de toekomst beter te kunnen weren.

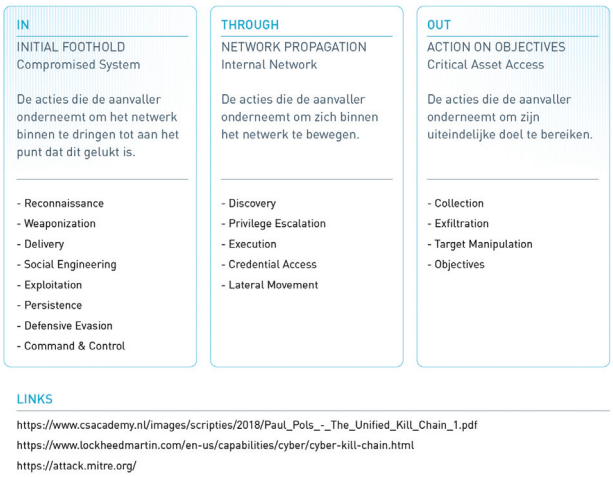
Voortschrijdend inzicht, dank aan de lezers

Aanvankelijk was de insteek van deze reeks om door de bril van incident response te kijken naar nog twee andere vaak voorkomende situaties. In gesprek met een aantal lezers naar aanleiding van het eerste artikel, hebben we echter besloten om in dit tweede en derde artikel in te zoomen op de aanpak die Stock Foundation volgde naar aanleiding van dit specifieke incident. Dit in plaats van een diepere analyse van meerdere dreigingen.

Het management van Stock Foundation is naar eigen zeggen behoorlijk ruw wakker geschud door dit incident. In de letterlijke woorden van de CEO in een mail aan het management (met goedkeuring hier gebruikt):

"… Ik realiseer me hierdoor hoe afhankelijk we zijn geworden. Tevens zijn we verbonden met een uitgebreid netwerk van stakeholders: leveranciers, klanten, partners en medewerkers. Ook daar hebben we verantwoordelijkheid te nemen. Daarbij heb ik jullie hulp nodig."

Wat de CEO wil, zijn snelle, praktische maar wel structurele verbeteringen. Hoewel wij zien dat dezelfde groep een slachtoffer meestal niet meteen nogmaals aanvalt, is de urgentie voelbaar dat men niet door een andere manier in dezelfde situatie gebracht wil worden. De concrete vraag is



Afbeelding 1 - Unified Cyber Kill Chain.

dan ook: "Wat moet de komende zes maanden onze (cyber resilience) roadmap zijn?"
De opdracht die wij op ons nemen, is om niet alleen informatie en systemen beter te beschermen, maar ook te borgen dat de organisatie goed kan omgaan met verstoringen. Bij de onderneming zelf, maar ook in de supply chains van de onderneming.

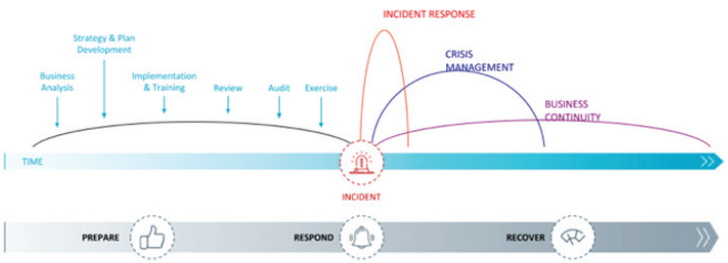
Pragmatisch risico's analyseren

De eerste stap is het beter op de radar krijgen van de security risico's. Juist ook binnen het bedrijf. De organisatie wil meters maken, dus kiest ze voor analyse op basis van alleen de meest prominente cyberdreigingen. Deze keuze geeft ons misschien geen allesomvattend beeld, maar wel een adequaat uitgangspunt.
Naast ransomware zijn er nog twee categorieën die veel schade aanrichten en regelmatig voorkomen. In goed Nederlands: Business E-mail Compromise en Insider threats (verzamelnaam voor onbedoelde of gerichte 'aanvallen' van binnenuit).
We inventariseren de risico's in een workshop met het management van Stock Foundation. Welke bedrijfsprocessen staan op het spel als we door zo'n dreiging geraakt worden? Waar loopt intellectueel eigendom of andere kritische data gevaar? Hoe zit het met privacy compliance als dit gebeurt? Wat gebeurt er als een leverancier de levering staakt vanwege zo'n incident of een klant niet meer kan afnemen? Wat is de financiële schade dan?
De sessie zorgt, behalve voor besef en bewustzijn, vooral ook voor betrokkenheid. De concrete en ook kwetsbare vraag om hulp die de CEO eerder deed, wordt nu breed beantwoord. Daardoor ontstaat een duidelijker beeld van datgene dat de organisatie al doet. Dat overzicht ontbrak tot nu toe. Op basis van de risico's en bestaande maatregelen maken we nu een overzicht van wat ons nog te doen staat. De contouren van de cyber resilience roadmap dienen zich in deze sessie dus al aan. Bovendien: daar waar de crisis bij een aantal mensen toch een machteloos gevoel had achtergelaten, krijgen meer managers nu ook zelfvertrouwen in nut en noodzaak van hun bijdrage. Dat gaat ons helpen in het doorvoeren van maatregelen.

Wat is resilience?

Waar we met Stock Foundation aan werken, vatten wij vaak samen in de term (cyber) resilience. Zoals met elke term zijn er allerlei definities en interpretaties in omloop.
Het NCSC leverde bij het 'Cybersecurity Beeld' in 2019 en in 2020 onomwonden het advies aan de Nederlandse publieke en private sector om meer te investeren in weerbaarheid tegen digitale risico's. Een digitaal risico is de kans dat een cyberincident zich voordoet en de impact daarvan, beide in relatie tot het niveau van de actuele weerbaarheid. Maar wat is die weerbaarheid of resilience eigenlijk? Het NCSC zegt het als volgt:
"Weerbaarheid: het vermogen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken."
Als je een compleet plan wilt opzetten en uitvoeren, is het vaak praktisch om een model als uitgangspunt te nemen voor het structureren van doelstellingen en activiteiten.
Onderstaand model geeft context aan de definitie en zet de benodigde 'vaardigheden' in een tijdlijn van het incident. Zo wordt benadrukt op welk moment welke aspecten van resilience gevraagd zijn. Dit helpt vooral bij het aan het management toelichten (budgetverantwoording) van de relevantie van delen van het plan en het duiden van de onderlinge samenhang.

In dit model zijn Incident Response (CSIRT), Crisis Management en Business Continuity Management de drie pijlers van veerkracht. De inhoudelijke kwaliteit en samenhang van die drie gebieden laten zich goed aansturen met behulp van een cyclisch kwaliteitsmanagementsysteem (PDCA). Regelmatig oefenen is een uitste-



Afbeelding 2 – Veerkracht bij cyberincidenten.

kende manier om opzet, bestaan en werking vast te stellen en om gewoon beter te worden in wat je doet. We gaan hier in het derde artikel verder op in.

Resilience roadmap

Tot zover de theorie. Terug naar Stock Foundation. Met de incidentevaluatie, de analyse van risico's op basis van andere relevante dreigingen en een verdere verkenning binnen Stock Foundation trekken we een aantal belangrijke conclusies die concreet vormgeven aan een roadmap en de uitvoering daarvan. Er wordt op allerlei terreinen hard gewerkt. Dat leidt tot de volgende resultaten na zes maanden:

- **Er was niets georganiseerd.** Maatregelen die er zijn, zijn met de beste intenties, ad hoc tot stand gebracht. Overzicht ontbreekt evenals duidelijke taken en rollen. De CEO stelt een stuurgroep in met een mandaat voor het uitvoeren van de roadmap. De stuurgroep zal daarnaast een meer permanente organisatievorm voorstellen aan het bestuur;
- **Stock Foundation vertrouwde volledig op haar IT-leverancier,** maar controleerde deze niet. We weten niet of veiligheid, betrouwbaarheid en continuïteit van de IT goed geborgd zijn. Uit het incident blijkt dat aanvallen die deels gebruik maken van bekende kwetsbaarheden en tools niet werden opgemerkt. Als onderdeel van de Incident Response was al een Endpoint Detection & Response (EDR) oplossing uitgerold (eset) en verbonden met het SOC van Northwave. Stock Foundation besluit dit nu uit te breiden en ook netwerk, applicaties en threat intelligence bronnen te gaan monitoren om aanvallers voor te zijn. Daarnaast worden een aantal security testen gedaan en wordt er met de IT-leverancier een Rapid Response Plan toegevoegd aan het Service Level Agreement. Dat plan zal eens per zes maanden geoefend gaan worden samen met de IT-leverancier;
- **Stock Foundation kende niet alle afhankelijkheden in haar bedrijfsvoering.** Managers van verschillende afdelingen krijgen opdracht om dit te inventariseren en met de teams meteen implementeerbare oplossingen te bedenken en afspraken te maken om de continuïteit van die processen beter te beschermen. Zo ontstaat er een heel pragmatische eerste versie van een Business Continuity Management structuur die op vele gebieden meteen al effect heeft. De top van het bedrijf gaat in gesprek met de belangrijkste klanten en leveranciers om het met hen te hebben over de onderlinge afhankelijkheden. Daarbij wordt het incident steeds als sprekend voorbeeld gebruikt. Relaties van de onderneming reageren zeer positief op de gesprekken. In de supply chain ontstaat nu ook meer bewustzijn;
- **Het ontbrak bij Stock Foundation aan een crisismanagementstructuur.** De CEO stelt een Crisis Management Team (CMT) samen met zichzelf aan het hoofd. Er wordt in een workshop en op basis van de incidentevaluatie een eerste versie van een crisisplan opgesteld. Ook wordt een 'out of band' communicatieplatform (CrisisSuite) ingericht, dat zal dienen als toolkit en Document Management System voor Crisis Management en Business Continuity Management. Dat heeft als groot voordeel dat niet alleen zorgvuldig gelogd kan worden, bijvoorbeeld tijdens oefeningen, maar ook dat benodigde plannen en documenten veilig zijn opgeslagen en communicatie altijd kan plaatsvinden los van de eigen IT-infrastructuur. Het CMT oefent in de eerste twee maanden twee keer en vervolgens na vier maanden nog eens. Daarna gaat het CMT elk half jaar oefenen.

Van resilience roadmap naar digital journey

We hebben in dit tweede deel gezien hoe Stock Foundation is opgestaan na een fors incident en die ervaring heeft omgezet naar een aantal concrete en snelle verbeteringen: er zijn stappen gemaakt in het beter aansturen van de beveiliging (business). Er is binnen de IT een veel betere positie ten aanzien van detectie en response (bytes). Medewerkers zijn bewuster en vaardiger, waardoor ze beter in staat zijn hun rol te pakken bij het beschermen van informatie (behaviour).
Mooie eerste resultaten. Maar digitalisering is een constante reis met vele variabelen en een hoop dynamiek. Daarom besteden we in het laatste deel van deze reeks aandacht aan het vraagstuk: 'Hoe bewaren we bij Stock Foundation de veerkracht op de lange termijn?'

BE PREPARED!

Hoe toepasselijk is momenteel dit themanummer 'Business Continuity Management'. Als ik vorig jaar rond deze tijd had gezegd dat een pandemie onze gezondheidzorg en economie wereldwijd in de greep zouden hebben, dan hadden velen mij voor gek verklaard. Het scenario pandemie binnen BCM is momenteel uiterst relevant en geeft maar weer aan dat het telkens belangrijk is om voorbereid te zijn op calamiteiten die de bedrijfsvoering in jouw keten kunnen verstoren.

Het vakgebied van BCM vergt meer dan de veelal genoemde jaarlijkse uitwijktest en is in combinatie met cyber resilience uitermate interessant en boeiend. Als voormalig CISO, waarnemend CIO en BCM-programmamanager bij een grote financiële instelling ben ik bekend met ook de niet-technische kant van BCM (en cyber resilience). Deze kant van de medaille moet je wel als voorzijde van de medaille zien. Hier draait het om. Dit zijn veelal de onderdelen waar de grootste uitdagingen zitten. Uiteraard is techniek ook belangrijk, maar is vaak beter 'kneedbaar' dan onderdelen als organisatie, governance, processen of de mens zelf. Als je erin slaagt om op evenwichtige en risicogebaseerde wijze deze onderdelen samen met de technologie op een hoger niveau te tillen en een 'sluitend' PDCA-cyclus hebt bewerkstelligd, dan heb je oprecht de medaille gewonnen. Het is natuurlijk geen wedstrijd, maar wel een prestatie op zich. En tijd om achterover te leunen is er niet, want je moet blijven oefenen, leren en verbeteren om als organisatie voorbereid te blijven.

Wat interessant is om te zien is dat veranderbereidheid en verandercapaciteit tijdens de corona crisissituatie aanzienlijk hoger is dan gedurende business as usual. Het in Nederland veelal toegepaste 'poldermodel' wordt tijdelijk losgelaten en er worden daadwerkelijk op korte termijn knopen doorgehakt en zaken gerealiseerd. De organisatie hoef je niet te overtuigen over de noodzaak of what's in it for me? Prioriteiten stellen en snel besluiten nemen zijn voor diverse organisaties equivalent geweest aan de keuze wel of niet overleven. Ingrediënten waar menig projectmanager jaloers op zal zijn om zijn reguliere project af te kunnen ronden en zich terecht afvraagt welke randvoorwaarden, doelen en/of stakeholders hij beter had moeten afhechten. Voorbeelden als basisonderwijs op afstand of het mogelijk maken van remote onderhoud van wafersteppers waren normaliter niet bespreekbaar geweest en op korte termijn gerealiseerd. Als BCM-programmamanager heb ik indertijd alle leden van de Raad van Bestuur een koffiemok gegeven met daarop de confronterende tekst 'The only thing harder than preparing for a disaster is explaining why you didn't!' Een dergelijke mok is, als eenmaal die pandemie zoals COVID-19 een feit is, niet meer nodig en hoop ik dat je ondertussen niet aan jouw stakeholders hebt moeten uitleggen dat je onvoldoende voorbereid was.

Als consultant, auditor, project- of interimmanager (con4RM), bestuurder bij een coöperatie (Composit), bestuurslid bij PvIB en 'geestelijk vader' achter het NBA-LIO volwassenheidsmodel IB (1), ben ik dagelijks bezig met informatie risicomanagement (IRM), compliancy, security, privacy en BCM. Ik ben betrokken (geweest) bij vele vraagstukken, projecten, programma's of 'crash acties' om er uiteindelijk voor te zorgen dat informatierisico's (beter) worden beheerst. Deze problematiek is weerbarstig en de komende jaren zal de vraag naar helder inzicht en tijdige stuurinformatie toenemen om het management te kunnen faciliteren in het kunnen nemen van hun verantwoordelijkheid en de uitvoering van de daarbij horende IRM-taken. Learning by doing klinkt wellicht experimenteel, maar is naar mijn mening de beste manier om gecontroleerde vooruitgang te boeken. Daarbij hoort ook leren van fouten en leren van andere organisaties. Hiervoor biedt PvIB een prima (netwerk)platform. Oftewel: Be prepared en bezoek onze (virtuele) evenementen.

Robert Warmoeskerken

[1] Behandeld in vorige editie iB-4.

Auteurs Dr. Milena Kooij-Janic, Senior Consultant Responsible AI, TNO en is bereikbaar via milena.kooij@tno.nl. Drs. Hans van Vlaanderen, Managing Director, ZorgTTP en is bereikbaar via hans.van.vlaanderen@zorgttp.nl

Betere gezondheidszorg door privacy vriendelijk data analyseren met Multi-Party Computation

Slimme algoritmes kunnen helpen om de gezondheidszorg te verbeteren. Door risicofactoren in kaart te brengen die een rol spelen bij het ontstaan en beloop van ziektes, kunnen nieuwe behandelingen worden ontwikkeld. Om dergelijke algoritmes te trainen is een grote hoeveelheid data nodig, vaak afkomstig uit meerdere databronnen. Het combineren van die data op individueel niveau om 'patient journeys' in kaart te brengen is in de praktijk problematisch; zowel juridisch als technisch.

De Algemene Verordening Gegevensbescherming (AVG) vereist een grondslag voor het verwerken van tot de persoon herleidbare gezondheidsgegevens. Voor afzonderlijke dataverzamelingen is die aanwezig. Daarnaast kan voor het combineren van dataverzamelingen voor wetenschappelijk onderzoek een beroep worden gedaan op de AVG uitzonderingsbepaling voor wetenschappelijk onderzoek en statistiek. In de praktijk is dit echter het punt waarop koppeltrajecten vertraging oplopen of verzanden in juridische discussies over grondslagen en de praktische implicaties van het verkrijgen van toestemming van de betrokkenen. Is er bijvoorbeeld sprake van een gerechtvaardigd belang voor het combineren van de data?

Decentraal en veilig met wiskundige zekerheid

Naast de juridische hobbels zijn er ook technische uitdagingen om de data op veilige en inhoudelijk betekenisvolle wijze te koppelen. Daarbij dienen noodzaak, proportionaliteit en subsidiariteit overwogen te worden: de verwerkingsdoelen met zo min mogelijk persoonsgegevens bereiken, zodat inbreuk op privacy minimaal is. Gelukkig staat de techniek niet stil. De afgelopen jaren zijn we getuige van een snelle ontwikkeling van cryptografische technieken die het mogelijk maken om berekeningen uit te voeren met vercijferde data. Deze set van verschillende cryptografische technieken, bekend onder verzamelnaam Multi-Party Computation (MPC), stelt partijen in staat gezamenlijk aan data te rekenen alsof ze een gedeelde database hebben. Dat wil zeggen dat het mogelijk is machine learning algoritmes te trainen met een verrijkte dataset, gecombineerd uit meerdere databronnen, waarbij de gegevens van elke partij vercijferd blijven. Daardoor krijgt geen andere partij

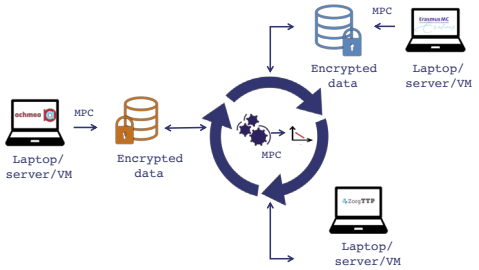
inzicht in de originele data en wordt alleen het afgesproken resultaat van het machine learning model gedeeld. Deze werkwijze sluit aan bij het Personal Health Train (PHT) concept bij welke het voorkomen van dataduplicatie in gecentraliseerde silo's een belangrijk uitgangspunt is. MPC kan bovendien een belangrijke bijdrage leveren aan het oplossen van het vraagstuk van verticaal gepartitioneerde data waarvoor binnen de PHT nog geen goede oplossing bestaat. Hoewel MPC-technieken al decennia bestaan, zijn ze de laatste tijd door steeds efficiëntere algoritmes dusdanig versneld dat ze klaar zijn voor toepassing in de praktijk. Er bestaat echter geen kant en klare oplossing. De keuze voor een specifieke technologische configuratie hangt af van use-case specifieke randvoorwaarden zoals; aantal betrokken partijen (dataeigenaren), hoeveelheid gegevens, aard van berekeningen (vermenigvuldigingen of optellingen) en mate van vertrouwen tussen partijen (berekeningen met wiskundige privacybescherming duren langer).

Voorspelmodel voor patiënten met hartfalen

Momenteel werkt TNO in de context van het Europees onderzoeksproject BigMedilytics samen met Achmea, Erasmus MC (en ZorgTTP) aan een dergelijke oplossing in een pilot gericht op patiënten met hartfalen. Het doel van de pilot is de factoren te identificeren die bijdragen aan risico's op hartfalen. Zo wordt gezocht of er een correlatie bestaat tussen het aantal heropnamedagen en mogelijk belangrijke factoren zoals leefstijl of comorbiditeit. De geleerde correlatie zou gebruikt kunnen worden om gepersonaliseerde, patiënt-specifieke interventies te ontwikkelen. Hoe meer relevante gegevens per patiënt beschikbaar zijn, des te meer kan geleerd worden over factoren die mogelijk de heropnamedagen beïnvloeden, door inzet van machine learning technieken. Erasmus MC en Achmea beschikken over complementaire gegevens betreffende patiënten met hartfalen. Zo beschikt Erasmus MC over de uitgebreide leefstijlgegevens van bewoners van de wijk Ommoord. Achmea heeft o.a. gegevens over medicijngebruik, tandarts-, huisarts- en ziekenhuisbehandelingen. In de pilot wordt gebruik gemaakt van synthetische data. Als met echte patiëntgegevens gewerkt zou worden, dan kan beroep gedaan worden op de uitzonderingsgrond die de AVG biedt om gegevens ten behoeve van wetenschappelijk gezondheidsonderzoek te mogen verwerken.

Oplossing met een helpende partij

Hoewel er MPC-protocollen met slechts 2 deelnemende partijen mogelijk zijn, is er in dit project voor een protocol met 3 partijen gekozen. In een protocol met drie partijen is de berekening sneller. De andere reden is governance, de betrokken partijen zijn gewend om de gegevens door een vertrouwde derde partij te laten verwerken. De drie partijen sluiten een verwerkersovereenkomst af met elkaar voor het combineren van de data via de MPC-oplossing. In deze overeenkomst wordt vastgelegd welke berekening op welke data wordt uitgevoerd, en aan welke partij(en) het resultaat bekend wordt gemaakt. Dit wordt vervolgens technisch afgedwongen met het cryptografisch protocol. Bij iedere deelnemende partij wordt een server geïmplementeerd waarop de ontwikkelde MPC-applicatie op geïnstalleerd wordt. De servers van Achmea en Erasmus MC versleutelen de data om vervolgens een interactief rekenprotocol te starten met de servers van Achmea, Erasmus MC en ZorgTTP. In het protocol worden (versleutelde) data uitgewisseld en berekeningen gedaan op versleutelde data.



Veilig data koppelen

De MPC-oplossing bestaat uit twee delen: de zogeheten secure inner join en de secure lasso regressie. In de eerste stap wordt bepaald welke data gekoppeld kan worden; patiënten die in beide datasets voorkomen. Het berekenen van de overlap met MPC zorgt ervoor dat geen van de partijen te weten komt welke patiënten in de overlap voorkomen, waardoor hun identiteit wordt beschermd. Alleen de grootte van de overlap wordt gedeeld. De tweede stap is het uitvoeren van de secure machine learning. Er wordt gebruik gemaakt van secret sharing, waarbij de data met wiskundige zekerheid zó is opgedeeld, dat geen nieuwe informatie over data wordt onthuld. Alleen het eindresultaat wordt geopenbaard. Bij de hiervoor beschreven oplossing is directe en indirecte herleiding van personen redelijkerwijs uitgesloten. Dit is niet voor iedere MPC-oplossing het geval. Dat maakt dat MPC-oplossing altijd in de specifieke context geëvalueerd moet worden op mate van herleidbaarheid. De opzet heeft de potentie om in de context van de AVG de huidige moeizame totstandkoming van koppelingen te doorbreken. Daarmee kan een belangrijke angel uit de juridische discussie over datakoppelingen worden gehaald. MPC voegt daarbij waarde toe als een technologie waarmee wordt aangetoond dat passende waarborgen zijn getroffen om de privacy van de betrokkenen te waarborgen.

The BigMedilytics project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 780495.

Auteur: Maurice Derogee is werkzaam als ISO bij Servicepunt71. Maurice is bereikbaar via m.derogee@servicepunt71.nl.

Due diligence en Due care

Vanuit het rijk zijn er vele handreikingen, richtlijnen en kaders waarnaar wij ons kunnen richten, of die wij wettelijk moeten volgen. Zo zijn deze handreikingen en kaders voor de lokale overheid gebaseerd op de code voor informatiebeveiliging (NEN/ISO 27001 en 27002 de maatregelen), en worden de BIO genoemd. BIO staat voor Baseline Informatieveiligheid Overheid. Deze handreikingen (best practises) worden aangeleverd door de IBD (Informatiebeveiligingsdienst) als onderdeel van de VNG (Vereniging Nederlandse Gemeenten).

Met BIO kunnen we per onderwerp (organisatie, personeel, gebouwen, systemen) in kaart brengen wat er al is of wat er nog verbeterd of gestart moet worden om zo een goede beveiligingsorganisatie op te zetten. Er is door het kabinet veel gesproken over vermindering van de regeldruk maar hiervan is eigenlijk weinig terechtgekomen. In 1980 waren er nog 1100 wetten, anno 2020 zijn er 2500 wetten en circa 140.000 wetsartikelen. Hierbij opgeteld dan nog de AMvB's (Algemene Maatregel van Bestuur) per gemeente. Als we dan de impact hiervan op het bedrijfsleven bekijken in de zin van 'wat kost het het bedrijfsleven om aan al de relevante wetten en regels te kunnen voldoen', dan komen we uit op een bedrag van 9,5 miljard. De kosten voor de overheid om aan deze regels te voldoen zijn dan ook fors.
Dit houdt mij en mijn collega's flink aan de slag om alles volgens het boekje te willen doen. Hier worden wij door jaarlijkse audits en zelfevaluaties (de ENSIA ofwel Eenduidige Normatiek Single Information Audit) op getoetst. De ENSIA is specifiek voor bepaalde onderwerpen zoals SUWI, DigiD, BAG, BRO, BGT, Informatiebeveiliging en wordt gerapporteerd naar de toezichthouders Rijk.

Informatiebeveiliging niet sexy

Deze beknopte inleiding in de gemeentewereld leidt tot mijn vraagstelling. Is een gemeentelijke organisatie of samenwerkingsverband wel echt in staat dit zelf te organiseren op de juiste wijze? Ik doel hierbij niet op deskundigheid, want die is er. Al merk ik zelf dat dit beeld niet erg leeft buiten de gemeenten, of zelfs het rijk. Je merkt zelfs vaak verbazing als je in een gesprek met een externe partij blijk geeft van inhoudelijke en gedegen vakkennis. "Waar ligt dit dan aan?", vraag ik mij af. Deels kan ik het wel verklaren. Een gemeente is een politiek gedreven organisatie en hier liggen de doelen toch anders dan bij een onderneming in de commerciële wereld. Informatiebeveiliging is nu eenmaal geen sexy onderwerp, en wordt eerder als belemmering gezien dan een kwaliteitsverhogende discipline. De BIO is gebaseerd op een risico analyse die kwalitatief is. Ofwel het is deels te bepalen door het soort gegevens dat in bijvoorbeeld een informatiesysteem wordt gebruikt, ofwel het is deels te bepalen op het gevoel van de eigenaar van deze gegevens. Het is dus lastig aan te geven wat de kosten en baten zullen zijn van een mitigerende maatregel. Ook schrijven al de richtlijnen, wetten en regels niets over het verplicht hebben van een budget voor de beveiliging van de gegevens ofwel een informatiebeveiligingsbudget.

Een software-ontwikkelaar zal dit commercieel gezien op een kwantitatieve manier aanpakken. Hierbij worden wel alle kostenaspecten meegenomen en is er inzicht in de totale kosten van een te nemen maatregel. Dat kan vervolgens afgezet worden tegen het risico en de kosten als dit risico zich daadwerkelijk voordoet, dus ook wat dit jaarlijks zou betekenen (de JSV ofwel Jaarlijkse Schade Verwachting). Dan kun je dus de vraag 'wat levert het ons op' van de algemeen directeur beantwoorden.
Wat ik vooral zie, is dat de lokale overheid hard werkt aan de digitalisering en veel moderne technieken en diensten omarmt. In de coronatijd blijkt dit wel. De gemeenten draaien door op afstand en weten al hun dienstverlening feitelijk prima voort te zetten. Eigenlijk net zo goed als het bedrijfsleven dit doet in de dienstverlening. Hier kom ik dus weer terug op het beeld over de gemeenten en de vraag of zij dit allemaal zelf wel kunnen.

Paarse krokodil

Veelal zie je dat er bij de grotere gemeenten een goede organisatie is opgebouwd voor informatiebeveiliging en privacy. Maar ook daar hoor ik dezelfde geluiden over maatregelen en bijbehorende kosten. Uitbesteden wordt dan ook vaak gekozen. Op zich niet vreemd, want zoals eerder beschreven, hebben mensen een gefixeerd beeld van de overheid en ook hierdoor is het lastig gespecialiseerd personeel in voldoende mate te werven. En als je het geluk hebt dit wel voor elkaar te krijgen dan is het een kunst ze ook te houden. We kennen allemaal wel het reclamefilmpje van de paarse krokodil dat helaas ook wel slaat op de snelheid waarmee de zaken lopen binnen een gemeente. Dus huren veel gemeentes personeel in, maar daar komen vanuit de maatschappij weer negatieve reacties op: te veel kosten aan inhuur. Immers als je alles zelf wilt organiseren als gemeente, dan heb je heel specialistische mensen nodig die bijvoorbeeld: de netwerkbeveiliging op orde brengen, de firewalls beheren (24x7x365!), web- en e-mailsecurity op orde brengen, architectuur beheren en bewaken, een SOC/SIEM-service leveren, Incident Response Teams. Dit is dus nauwelijks als geheel te organiseren zonder bepaalde zaken uit te besteden aan specialistische partijen. En dit gaat uiteindelijk op voor ICT als geheel. Vanuit de overheid is er dan ook een aanbesteding gedaan voor een gezamenlijke dienstverlening op het gebied van onder andere informatiebeveiliging, ofwel GGI (Gezamenlijke Gemeentelijke Infrastructuur). Effectief gezien dus: schaalvoordeel halen en goedkoper je maatregelen realiseren bij diezelfde marktpartijen, als waar je als

individuele gemeente op was uitgekomen, en op een manier die dan ook hetzelfde is als bij de andere deelnemers.
Maar net als het niet verplicht hebben van een beveiligingsbudget, is ook hier geen verplichting om daaraan mee te doen. Vaak zie je dan toch een situatie ontstaan waarbij er zaken bij diverse partijen zijn belegd en dat deze partijen, om als geheel effectief te zijn, goed moeten samenwerken en ook goed moeten worden aangestuurd.

Due diligence en Due care

Er zijn twee soorten aanbieders. De ene is gespecialiseerd in dienstverlening aan de overheidswereld en weet goed hoe de processen daar werken. De ander biedt generieke diensten en specialismen die binnen elke bedrijfsomgeving kunnen worden ingezet. Deze aanbieders voeren uit wat er wordt gevraagd (binnen de kaders van de afspraken) en je zult dan dus zelf goed moeten weten of wat je vraagt wel het juiste is. Een regie-organisatie kan dan niet zonder mensen met technische kennis op de uitbestede specialismen. Je mag alleen al vanwege de verantwoordelijkheden, die je toegewezen zijn, niet blind vertrouwen op externe partijen.

De overheidsbezuinigingen – en dan met name aangaande de ICT – betekenen vaak echter bezuiniging op menskracht. Dan houd je als gemeente uiteindelijk al snel enkel jouw CISO en misschien jouw ISO(`s) over en hopelijk jouw Privacy Officer naast de verplichte FG. Je bent dan vooral bezig met het managen van contracten en het invullen van je maatregelen met informatie die de externe partijen jou moeten aanleveren. En hoe controleer je of alles echt gaat, zoals beweerd?

Je bent als (gemeentelijke!) organisatie verplicht om gedegen onderzoek te verrichten en op een goede manier zorg te dragen voor de (persoons)gegevens die je onder je hebt. Je kunt hierbij verantwoordelijkheid niet delegeren. Due diligence en Due care. Dus als je het beheer van een informatiesysteem en de betrokken gegevens uitbesteedt, zul je gedegen onderzoek moeten doen of de beoogde partij voldoende maatregelen heeft genomen en haar organisatie op orde heeft, die passen bij het beveiligingsniveau van de betrokken gegevens. De opdrachtnemer zal dan moeten zorgen dat het benodigde niveau geleverd wordt en op peil blijft. Gaat het mis, dan zal er door bijvoorbeeld de Autoriteit Persoonsgegevens (AP) worden gekeken naar deze omgeving en die zal dus toetsen of er voldoende is gedaan om te voorkomen dat het mis zou kunnen gaan. Is dit niet in orde dan zal dit bepalend zijn voor de hoogte van een opgelegde boete.

Slachtoffer betaalt zelf

Hier ontstaat dan gelijk het probleem (althans, zoals ik het zie). Stel dat er een claim wordt gelegd bij de leverancier van de dienst omdat deze volgens de gemeente oorzaak is geweest van het incident en de opgelegde boete. Dit zal uiteindelijk een rechter worden voorgelegd. Stel verder dat blijkt dat het incident is veroorzaakt omdat de gemeente heeft geëist van de leverancier dat het wachtwoord voor het aanmelden eraf moest omdat dit veel te lastig werd gevonden. En dat de leverancier hierop meerdere malen heeft aangegeven dat dit onverstandig was, maar uiteindelijk onder druk toch heeft ingestemd en dat dat uiteindelijk de oorzaak bleek van het incident. Dan zal de leverancier een deel van de boete moeten gaan betalen vanwege het feit dat ze dit hadden moeten weigeren, ongeacht de gevolgen. De gemeente zal zelf nog steeds het grootste deel voor haar rekening krijgen vanwege de verantwoordelijkheid, maar ook vanwege … het gebrek aan kennis?

De externe partij had niet mogen zwichten en betaalt daar de prijs voor. De gemeente betaalt eigenlijk niets, immers zij werken met gemeenschapsgeld. Dus feitelijk betaalt de ingezetene van de betrokken gemeente. Dus het slachtoffer (de burger wiens gegevens zijn gelekt) betaalt zelf en zal mogelijk nog meer betalen in persoon doordat zijn of haar identiteit wordt misbruikt door een crimineel die de gegevens online ontdekte. De zogenoemde afgeleide schade.

Zou dit dan voldoende grond zijn om een gemeente wettelijk te verplichten de zaken intern volledig en in praktijk bewezen op orde te hebben en zelfs als voorbeeld te dienen? Immers een gemeente heeft een schat aan gegevens en informatie onder zich. En uiteraard kost het de gemeente haar reputatie zodra het goed misgaat. Maar dan nog zal een burger niet kunnen beslissen om zijn paspoort of rijbewijs bij een andere gemeente te halen (omdat die van zijn of haar woonplaats niet te vertrouwen is). En de boetes dan? Een commercieel bedrijf kan het de kop kosten. Een gemeente feitelijk dus niet. Het zal politiek niet lekker worden ontvangen en er zullen mensen vertrekken. Ook zal er onderzoek worden gedaan en verbeteringen worden voorgesteld of zelfs bevolen. Maar uiteindelijk draait alles door. Rechtsongelijkheid zou je zo denken. En feitelijk ervaar ik dat ook zo.

De gemeenten moeten bezuinigen op het ambtelijk apparaat

Zou je dus moeten concluderen dat een gemeente anders wordt benaderd vanwege een lager kennisniveau in vergelijking tot een commercieel bedrijf? Of omdat het nu eenmaal een ambtelijk en politiek apparaat betreft waar alles nog gaat op een manier die al jaren zo is? Dit naast alle moderne ambities die de overheid heeft met bijbehorende wettelijke verplichtingen en de forse verantwoordelijkheden. Het doet je afvragen of het niet tijd wordt voor een modernere organisatiestructuur. Als ware het een commercieel bedrijf. De Wet Normalisatie Ambtelijk Personeel (WNRA) is er al een begin voor.

Gemeente als commercieel dienstverlener

Het politieke element zal blijven. Dit is nu eenmaal het kenmerk. Maar politiek zorgt ook voor tegenstrijdige belangen. Zoals in dit artikel beschreven moeten de gemeenten bezuinigen op het ambtelijk apparaat. Zo ontstond in 1992 discussie rond het aantal ambtenaren. Het rijk zou het met 7.000 ambtenaren minder moeten doen. Per 1 januari 1997 moesten de werktijden worden aangepast en werd de werkweek van 40 uur naar 36 uur teruggebracht. Net als de beloofde vermindering van de regeldruk is ook hier tot op de dag van vandaag nog steeds discussie over.
De regio waarin ik werkzaam ben is hier uiteraard ook mee bezig geweest. Zo is ook het Servicepunt71 op 1 januari 2012 ontstaan als dienstverlener voor de deelnemers en eigenaren (de betreffende regiogemeenten). De deelnemers hebben hun personeelsbestand ingekrompen en deze mensen zijn samengekomen in het Servicepunt. Op zich beschouwd leidde dit tot een tweeledig effect. De gemeenten hebben het aantal ambtenaren teruggebracht en met het Servicepunt71 hebben de kleinere gemeenten in het samenwerkingsverband tevens ineens meer specialismen tot hun beschikking en dus ook continuïteit in hun dienstverlening gekregen. Zo ontstond dus een gespecialiseerde lokale overheid dienstverlener.
Maar ook hier was er al sprake van uitbesteding van netwerkdiensten door een tekort aan interne specialisten. Anno nu heeft dit door verdere bezuinigingen - en moeite om gespecialiseerd technisch personeel te werven - geleid tot volledige uitbesteding van de ICT-dienstverlening op de Servicedesk na. Servicepunt71 werd dus een regievoerende organisatie.

Hoe wordt dit een moderne organisatie die enerzijds politiek gedreven moet zijn (en is) en anderzijds functioneert als een commerciële dienstverlener? Is dit een haalbaar scenario gezien de specifieke taken die een gemeente uitvoert met specifiek voor de gemeente gebouwde informatiesystemen door gespecialiseerde dienstverleners?
Net voor de deadline van dit artikel publiceerde de Rijksoverheid een notitie over de *Digitale overheid in het post-coronatijdperk*, getiteld: *Dichterbij door digitalisering* (1). Over actualiteit gesproken, ik ga mij er in verdiepen en kom wellicht daar later op terug.

Referentie

(1) Dichterbij door digitalisering:
www.rijksoverheid.nl/documenten/rapporten/2020/08/20/dichterbij-door-digitalisering

Auteur: Michiel Steltman is woordvoerder van Online Trust Coalitie en bereikbaar via info@onlinetrustcoalitie.nl. Evert van Zanten is bestuurslid PvIB en bereikbaar via evertvz@nnextsecure.com.

Online Trust Coalitie: op weg naar vertrouwen in de cloud

Continuïteit van de business is afhankelijk van infrastructuren die door derden worden aangeboden. Als je dat goed wil managen, wil je de zekerheid dat jouw dienstverlener die kan bieden en vooral ook vertrouwen. Hoe dit in Nederland en Europa concreet vorm moet krijgen is het grote vraagstuk waar de Online Trust Coalitie (OTC) zich op heeft gestort. Waarom werkt de traditionele manier van denken over continuïteit en zekerheden niet in de nieuwe informatiewaardeketen?

Uit recent onderzoek van de DHPA (1) blijkt dat 75% van de Nederlandse mkb-ondernemers één of meer clouddiensten gebruikt. En over twee jaar is er volgens de onderzoekers geen bedrijf meer te vinden dat IT nog volledig in eigen beheer organiseert. De coronacrisis, met daarbij het massale thuiswerken, versnelt die ontwikkeling. We zijn steeds meer afhankelijk van de cloud. Ook de Europese commissie herkent het groeiend belang van clouddiensten voor innovatie en digitalisering. Zij zet stevig in op ontwikkeling en gebruik van clouddiensten van Europese bodem, mede vanuit de wens voor meer autonomie.

Om clouddiensten te gebruiken heb je alleen een internet-aansluiting en een creditcard nodig. Maar voor de doorsnee afnemer is het een stuk minder eenvoudig om zekerheid te krijgen dat het met die cloud goed zit. Vaak worden simpele vragen gesteld zoals 'is het veilig', of 'waar staat mijn data'. Maar zekerheid gaat om het hele pakket: vertrouwelijkheid, informatiebeveiliging, beschikbaarheid en continuïteit, integriteit en uiteraard ook conformiteit met de AVG. Daar komt bij dat de afnemer zelf ook het een en ander moet doen om de bekende CIA-triade plus de wettelijke conformiteit van het geheel met de wet te borgen. Vaak is onvoldoende

duidelijk wat dat dan inhoudt. Nog ingewikkelder wordt het als de afgenomen clouddiensten worden gebruikt als onderdeel van eigen onlinediensten, iets dat bij digitalisering volop gebeurt. De afnemer wordt dan onderdeel van een keten en heeft te maken met vragen zowel als doorgeven en aggregeren van zekerheden naar 'boven'.

Welke clouddienst is geschikt?

Aanbieders van clouddiensten beloven zonder uitzondering dat die zaken bij hen prima geregeld zijn. In de meeste gevallen is dat ook zo. Toch gaan afnemers, zeker de grotere, er in de praktijk niet altijd van uit dat de claims, verklaringen of certificaten van providers voldoende zekerheid geven. Dat komt omdat managementsystemen en certificaten ontworpen en bedoeld zijn om de aanbieder, en niet afnemers zekerheid te geven. Daarom is het erg ingewikkeld en duur voor afnemers om te kunnen beoordelen of een clouddienst geschikt is voor hun situatie, en of die past bij hun risicoprofiel. Deze kwestie wordt nog urgenter doordat het Europese Hof onlangs het Privacy Shield (2) ongeldig heeft verklaard. Afnemers van clouddiensten kunnen er niet langer op rekenen dat in ketens waarin Amerikaanse aanbieders zijn betrokken hun data conform de Europese privacywet wordt beschermd. Afnemers constateren daardoor dat de claims van hun leveranciers en hun auditors niet helemaal juist bleken te zijn, los van wiens schuld dat is. Tot overmaat van ramp leggen de Europese en Nederlandse privacy-autoriteiten dat probleem volledig bij de afnemers neer. Met het advies om uit te zoeken bij wie en waar data terecht kan komen en hoe het met de wetgeving bij die bedrijven en landen is geregeld. Bij twijfel moeten ze het gebruik van die diensten zelfs onmiddellijk stoppen.

Die verplichting om dit alles voor de tientallen clouddiensten die een gemiddeld bedrijf gebruikt uit te zoeken, te controleren en te regelen, en de oproep om clouddiensten bij twijfel dan niet meer te gebruiken, zijn onuitvoerbaar. Het CIO Platform Nederland, een samenwerking van onder andere IT-managers van 130 grote organisaties, stelde vorig jaar in een brandbrief aan de privacy-autoriteiten dat het auditen van clouddiensten en hun leverancierketens ondoenlijk is. Zeker als dit ook nog eens periodiek herhaald zou moeten worden. Daarbij komt dat het idee dat bedrijven zomaar de stekker uit hun clouddiensten kunnen trekken volstrekt onrealistisch is.

Cloud is een buitenbeentje

Het onderliggende probleem is dat 'de cloud' een buitenbeentje is in de AVG, maar ook in de praktijk van certificeringen. Beiden gaan uit van het COBIT-model dat stamt uit de periode voor de cloud. Afnemers hebben dan zelf de volledige regie over hun IT, want computers en software werden gekocht en beheerd binnen de eigen organisatie. Of hooguit door ingehuurde leveranciers, maar daardoor nog steeds onder eigen regie. Inmiddels bestaat de digitale economie uit een omgekeerde keten van control. Niet de afnemer maar de aanbieder bepaalt de functionaliteit, de beveiliging, privacy en andere eigenschappen van een clouddienst. De afnemer heeft slechts de keuze: is een dienst wel of niet geschikt. En moet deze afweging maken op basis van moeilijk toegankelijke of onvolledige informatie; informatie die daar eigenlijk niet voor is bedoeld. En zonder hulp van de privacy-autoriteiten. Kortom, de vermeende top-down regie over onlineketens is fictie en afnemers krijgen die regie ook niet meer terug.

Zekerheid

Ruim twintig organisaties vanuit de overheid, bedrijfsleven en wetenschap hebben dit probleem herkend en zijn gestart met de Online Trust Coalitie (OTC). De OTC wil laagdrempelige, standaardmethoden ontwikkelen die de afnemers van clouddiensten duidelijkheid geven over de betrouwbaarheid en veiligheid, en die voor aanbieders eenvoudig te hanteren zijn. De essentie is dus niet de betrouwbaarheid zelf, zoals ontwikkelen van het zoveelste framework, maar het zorgen voor de betere methoden en informatie over betrouwbaarheid in digitale ketens. Deelnemers in de OTC zijn momenteel betrokken in Europese werkgroepen rond certificering en er zijn contacten gelegd met het Duitse project Gaia-X (4). Later dit jaar publiceert de OTC een whitepaper met aanbevelingen voor relevante stakeholders.

Goede methoden om afnemers zekerheid te geven over de betrouwbaarheid van clouddiensten maakt het gebruik ervan, en daarmee digitalisering, laagdrempeliger. Dat is hard nodig voor de ambitie van Nederland om digitale koploper in Europa te worden.

De Online Trust Coalitie roept organisaties op om deel te nemen en met elkaar de digitale economie van Nederland in de internationale context te versterken. Aanmelden kan via: info@ onlinetrustcoalitie.nl

Referenties

(1) www.trustedcloudexperts.nl/driekwart-van-nl-bedrijfsleven-heeft-saas-applicaties/

(2) Het EU-U.S. Privacy Shield is een overeenkomst tussen het Amerikaanse ministerie van Economische Zaken en de Europese Commissie over de uitwisseling van persoonsgegevens tussen bedrijven in de EU en de VS.

(3) https://ecp.nl/timeline/lancering-otc/

(4) www.dhpa.nl/gaia-x/

Auteur: Joost Geerts volgde een opleiding Automotive Engineering aan de Hogeschool van Arnhem en Nijmegen en studeerde onlangs succesvol met zijn scriptie voor BRACE. Hij werkt als Diagnostic Engineer bij Tobroco Giant in Oisterwijk. Joost is bereikbaar via: joostgeerts@hotmail.com

Hacker gehackt

'Onderzoek naar manipulatie van wettelijk verplichte systemen binnen professionele mobiliteitsbranche'

De professionele mobiliteitsbranche is onderhevig aan vele vormen van wetten en regelgeving. Fabrikanten implementeren technisch complexe systemen in hun voertuigen, zoals een tachograaf, om aan de strenge eisen te voldoen. Verkeersdeelnemers en transportbedrijven ervaren vaak ongemakken en hoge kosten door het gebruik van deze systemen, waardoor zij in de verleiding komen deze systemen te manipuleren. Hierdoor wordt steeds meer van handhavende instellingen en hun inspecteurs gevraagd.

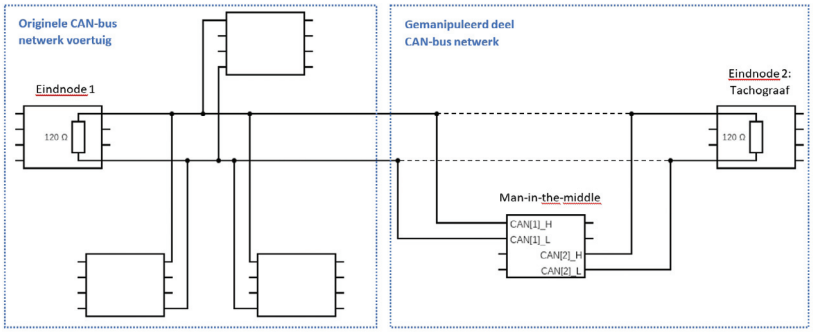
Om deze handhavende instellingen meer handvatten te bieden, is onderzoek gedaan naar de wijze waarop deze systemen in de praktijk worden gemanipuleerd. Doelstelling is om de handhavers te voorzien van methoden en gereedschappen in de bestrijding van deze vorm van fraude. De hieruit volgende onderzoeksvraag luidt: Wat is voor handhavende inspecteurs een geschikte methode om manipulatie van wettelijk verplichte systemen vast te stellen en te verifiëren? Om een bevredigend antwoord op deze vraag te verkrijgen, is het onderzoek opgedeeld in drie afzonderlijke fasen. De analysefase geeft inzicht in beweegredenen en, door fraudeurs toegepaste, methodieken. In de onderzoeksfase is technisch onderzoek verricht naar een relevant, manipulerend device door reverse engineering van hardware. In de verificatiefase zijn bevindingen uit de onderzoeksfase gebruikt om een testmethode te ontwikkelen.

Beweegredenen fraudeurs

Om inzicht te vergaren in de beweegredenen en handelswijzen van fraudeurs, is in de analysefase een objectieve benadering opgesteld. Hierbij is gebruik gemaakt van een combinatie van wetenschappelijke theorieën en risicoanalyses middels de SAE/ISO-21434 cybersecurity standaard (1). Deze benadering koppelt beweegredenen van fraudeurs aan voertuigsystemen die interessant kunnen zijn voor manipulatie.

Een wetenschappelijk model om onderzoek naar beweegredenen van fraude te doen, is de Fraud Diamond Theory (FDT) (2). Volgens dit model dienen ten minste vier elementen aanwezig te zijn alvorens mensen overgaan op het initiëren van frauduleuze acties. Deze elementen zijn: ondervonden druk, waargenomen kans, rationalisatie en bekwaamheid. Hierbij lijkt het element 'ondervonden druk' het zwaarst te wegen. Mogelijke vormen van ondervonden druk zijn sociale, politieke, persoonlijke, financiële en werkgerelateerde druk. Daarnaast kunnen gezondheidskwesties, verslaving en hebzucht een belangrijke rol spelen. In 95% van alle onderzochte gevallen van fraude is er sprake van een vorm van financiële druk (3). In dit onderzoek lijkt dit ook de belangrijkste drijfveer voor de fraudeurs.

In het onderzoek naar beweegredenen en methoden van fraudeurs is onderscheid gemaakt tussen de ontwikkelaar en eindgebruiker van de manipulatie. Er is een belangrijke wisselwerking tussen deze twee groepen. Elementen binnen de FDT kunnen per groep verschillen. Het belangrijkste element 'ondervonden druk' lijkt bij deze verschillende groepen, gelijk te zijn. Namelijk financiële druk.



Afbeelding 1 - CAN-netwerk.

Tachograaffraude

Nadat inzicht is verkregen in de motivaties van fraudeurs, is bekeken welke systemen relevant kunnen zijn voor manipulatie. Er is een lijst opgesteld met negenentwintig voertuigsystemen. Aan de hand van een eenvoudige waarschijnlijkheids- en impactanalyse is een selectie gemaakt met potentieel interessante systemen voor manipulatie. De systemen in deze selectie hebben een uitgebreidere impactanalyse ondergaan. Hierbij is, per manipulatie, bekeken wat het potentieel gewin is voor de fraudeur en wat de potentiële, maatschappelijke schade is die de manipulatie tot gevolg zou hebben. Uit deze analyse volgen de vier meest relevante, potentiële manipulaties. Dit blijken manipulaties te zijn met betrekking tot alcoholslot, emissiesystemen en tachograaf.

Aan de hand van de SAE/ISO 21434 standaard zijn uitgebreide risico- en attack surface analyses uitgevoerd. Ieder systeem is onderverdeeld in afzonderlijke items. Per item is bekeken welke schade en bedreigingen kunnen ontstaan wanneer manipulatie wordt geïnitieerd. Uiteindelijk zijn aan de hand van impact- en waarschijnlijkheidsanalyses, risicofactoren bepaald. Aan de hand van deze risicofactoren is bepaald welk systeem, of systemen, het meest relevant zijn voor verder onderzoek. Aan de hand van de risicoanalyses is gebleken dat tachograaffraude de meest relevante vorm van manipulatie is binnen de gestelde kaders. Tijdens de onderzoeksfase is een samenwerking met de Inspectie van Leefomgeving en Transport (ILT) (4) aangegaan om zodoende relevante input en onderzoeksmateriaal te bemachtigen. Middels deze samenwerking zijn we in het bezit gekomen van een gemanipuleerd tachograafsysteem. Hiervan was bekend dat de manipulatie geschiedde met behulp van een USB-dongel, die gedetailleerd is onderzocht. Technische details over de werking van de manipulatie waren op voorhand onbekend. Evenals de aansluiting van de USB-dongel op het elektrische systeem van het voertuig. Er werd verondersteld dat deze USB-dongel een regelsysteem bevatte die de manipulatie van de tachograaf realiseerde. De manipulatie werd geactiveerd op verzoek van de chauffeur door de pedalen van het voertuig in een zekere volgorde te bedienen. Uitgebreid technisch onderzoek en reverse engineering van de USB-dongel heeft uitgewezen dat de complexiteit van manipuleren door het device, buitengewoon hoog is. Omdat niet alle relevante onderdelen van het tachograafsysteem in beslag zijn genomen, blijft het enigszins speculatief hoe de gedetailleerde werking van de manipulatie plaats heeft gevonden.

Man-in-the-middle-aanval

Desondanks zijn gedurende het technisch onderzoek vele interessante aanknopingspunten gevonden. Conclusies uit dit technisch onderzoek zijn dat de dongel inderdaad voorzien is van een regelsysteem. Dit regelsysteem is verbonden met het CAN-bus netwerk van het voertuig, waardoor het voertuigdata kan ontvangen en gemanipuleerde data op het netwerk kan plaatsen. Standen van de pedalen, om de manipulatie te activeren, worden via dit netwerk verkregen. Voornaamste conclusie uit het onderzoek is dat de manipulatie hoofdzakelijk geschiedt door middel van een 'man-in-the-middle' aanval, zoals inzichtelijk gemaakt in figuur 1.

Hierbij is de USB-dongel continu verbonden met het voertuignetwerk. Wanneer manipulatie wordt geïnitieerd, wordt de dongel in serie geschakeld in het netwerk en deelt deze het netwerk op in twee afzonderlijke lussen. De dongel onderschept datacommunicatie tussen beide lussen, geeft boodschappen door en kan relevante data gemanipuleerd op het netwerk plaatsen. Om de bevindingen uit de onderzoeksfase te verifiëren, is een testopstelling ontworpen. Voornaamste eis aan de opstelling is dat de manipulerende USB-dongel getest kan worden. Andere eisen aan de opstelling zijn dat deze uit te breiden moet zijn voor andere, toekomstige manipulaties van het tachograafsysteem. Hiermee kan het in de toekomst toegepast worden als trainings- en demonstratiemateriaal. Het ontwerp bevat onder andere twee afzonderlijke CAN-bus netwerken, een programmeer-

bare voertuig-ECU, aansluitingen voor tachograafunit, een programmeerbaar microcontrollerbord en een ECU-simulator die sensor- en actuatorwaarden kan simuleren en op het voertuignetwerk kan plaatsen. Noodzakelijke componenten zijn verzameld en verwerkt in een prototype testopstelling.

CAN-bus communicatieprotocol

Zware voertuigen, waaronder trucks, maken gebruik van het SAE J1939 CAN-bus communicatieprotocol. Dit omvat een set standaarden die omschrijft hoe ECU's via het CAN-bus-netwerk met elkaar communiceren (5). Het zou voor fraudeurs een logische methode zijn geweest om voertuigsignalen en parameters te achterhalen middels dit protocol. Om die reden is verkozen deze standaard te bestuderen en, met behulp van deze informatie, de pedaalstanden te simuleren. De potentiometers van de ECU simulator simuleren de pedaalstanden en worden op het netwerk geplaatst Deze berichten worden door de programmeerbare voertuig ECU ontvangen. Er is een algoritme geschreven om deze databerichten te ontvangen en vervolgens, in gestandaardiseerd J1939 formaat, terug te plaatsen op het CAN-bus netwerk. Simuleren van de pedaalstanden zou het manipulerende device moeten activeren.

Gedetailleerd inzicht

Instructies van het manipulerende apparaat, in de vorm van firmware of broncode, zijn niet beschikbaar tijdens dit onderzoek. Deze instructies bevatten de exacte randvoorwaarden die het regelsysteem bevat voor activering van de manipulatie. Hoewel bekend is dat de manipulatie wordt getriggerd middels het bedienen van de pedalen, kan de frauderende programmeur talloze randvoorwaarden hebben gesteld voor activering. Verkrijgen en analyseren van firmware instructies valt buiten de projectkaders, waardoor zelfstandig gespeculeerd moet worden over mogelijke randvoorwaarden. Om deze reden is een uitgebreide lijst met randvoorwaarden opgesteld en een methode ontwikkeld om deze in J1939 CAN-bus netwerkberichten te verwerken. Ondanks dat het manipulerende device niet geactiveerd kon worden, is er een bruikbare testmethode en -opstelling ontwikkeld. Hierbij is vastgesteld dat verzonden data door het manipulerende device wordt ontvangen. De ontwikkelde opstelling en methode bieden voldoende perspectief voor aanvullend onderzoek.

Dit onderzoek heeft gedetailleerd inzicht opgeleverd in de werk- en denkwijzen van manipulatoren van voertuigsystemen. Belangrijkste kwetsbaarheden die uitgebuit worden zijn de, in onvoldoende mate beveiligde, toegang tot voertuignetwerken en firmware van besturingssystemen. Beveiliging van voertuignetwerken reikt niet verder dan geheimhouding door fabrikanten. Deze vorm van 'security through obscurity' is door reverse engineering van de CAN-bus relatief eenvoudig te omzeilen. Daarnaast is gebleken dat de onderzochte tachograafmanipulatie aan hoge complexiteit onderhevig is. Hierdoor is het onrealistisch gebleken een onweerlegbare methode te ontwikkelen, waarmee handhavers dergelijke tachograafmanipulaties kunnen vaststellen en verifiëren. Desondanks heeft het onderzoek een aantal praktische aanbevelingen voor handhavende inspecteurs opgeleverd die toepasbaar zijn bij wegcontroles. De onderzochte 'man-in-the-middle' aanval laat een kenmerkend spoor achter dat meetbaar is voor inspecteurs. Andere, praktische aanbevelingen zijn het doormeten van verdachte stekkers binnen de cabine en inspecteurs uitrusten met CAN-dataloggers. Door data van het voertuignetwerk te loggen tijdens een actieve tachograafmanipulatie, kan waardevolle informatie worden verkregen die als input kan dienen voor verder onderzoek.

Het onderzoek heeft een ontwerp voor een testopstelling opgeleverd. Op basis hiervan is een prototype gebouwd dat uitgebouwd dient te worden naar het ontwerpmodel. In dat geval kunnen aanvullende tests met verschillende randvoorwaarden worden uitgevoerd, hetgeen kans op activatie van het manipulerende device vergroot. Het ontwerp biedt daarnaast voldoende mogelijkheden voor het testen van alternatieve systeemmanipulaties. In de ISO/SAE 21434 standaard wordt de attack feasibility van aanvallen, rechtstreeks op het CAN-bus netwerk, laag geacht. Motivatie hiervoor is dat dit fysieke toegang tot het voertuig vereist en niet heel waarschijnlijk wordt geacht. Het lijkt erop dat de standaard voornamelijk rekening houdt met aanvallen van buiten het voertuig door onbevoegden. Uit dit onderzoek blijkt echter dat voertuigeigenaren voldoende druk kunnen ondervinden hun eigen voertuigsystemen te manipuleren. Deze benadering door de standaard zou heroverwogen kunnen worden.

Referenties

(1) Society of Automotive Engineers International (SAE). (2020). Road Vehicles - Cyber Security Engineering ISO/SEA DIS 21434. Geneva, Switzerland: ISO/SAE International 2020

(2) ABDULLAHI, R. (2015). Fraud Triangle Theory and Fraud Diamond Theory. Understanding the Convergent and Divergent For Future Research . Terengganu, Malaysia: Universiti Sultan Zainal Abidin.

(3) Lister, L. M. (2007). A practical approach to fraud risk. Lake Mary, Florida, USA: Institute of Internal Auditors, Inc.

(4) Inspectie Leefomgeving en Transport. (z.d.). Over de ILT. Opgehaald van: ILenT.nl https://www.ilent.nl/over-ilt

(5) Society of Automotive Engineers. (1998). J1939 DA - Digital Annex of Serial Control and Communication. Warrendale: Society of Automotive Engineers

In deze rubriek geven iB-redacteuren Chris de Vries en Maarten Hartsuijker 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.

Privacy en het testsucces van GGD's

Momenteel worden we door de GGD's en het RIVM (en onze persoonlijke omgeving) gestimuleerd om ons bij corona-klachten te laten testen. Er wordt zelfs zoveel getest dat de verwerkingscapaciteit tekortschiet. Met het testsucces ontstaat er een enorme dataverzameling. Moeten we ons zorgen maken over de veiligheid van deze data? Hoe zit het met de privacy van de daar opgeslagen systemen? Kunnen we gebruik maken van ons verwijderingsrecht?

De afgelopen maanden hebben we gezien dat verschillende in de haast opgezette corona-gerelateerde systemen met datalekken te kampen hebben gehad. Als je je persoonlijke gegevens wilt beschermen, doe je er dus goed aan om ze te laten verwijderen zodra ze hun doel hebben gediend. Maar mag dit ook? Via een speurtocht langs het RIVM en de landelijke GGD-GHOR kom ik uit bij de lokale GGD die er verantwoordelijk voor zou moeten zijn, maar er in de weken voor deze AHN geen eenduidig antwoord op kon geven.

Geen bewaarplicht

Op de verwerking van de coronagegevens zijn meerdere wetten van toepassing. Zo heeft de Wet Publieke Gezondheid geen bewaarplicht, maar de plicht om gegevens maximaal 5 jaar te bewaren (eigenlijk een verwijderplicht). De GGD zet dit om in 'wij bewaren coronagegevens 5 jaar' (1). Je kunt je afvragen of het hanteren van de maximaal toegestane termijn langer dan noodzakelijk (AVG) is. Het ontbreken van antwoorden en het hanteren van maximale bewaartermijnen voeden niet het vertrouwen dat nodig is voor een maatschappelijk belangrijke systeem als dit. En dat is jammer. Want testen doe je natuurlijk vooral voor de bescherming van je omgeving. En dan zou privacybescherming geen onzekerheidsfactor moeten zijn.

Kernvraag

Hoe voorkom je dat, in uitzonderlijke situaties (logisch en noodzakelijk) verkregen informatie enkel gebruikt wordt voor het doel waarvoor het verzameld is?

De toenmalige minister Martin van Rijn (Medische Zorg) heeft midden april miljoenen patiëntendossiers voor de duur van de coronacrisis opengesteld, ook zonder toestemming (2). Hoe komt deze geest weer in de fles? In een Besluit van 27 augustus 2001, houdende nadere regels over het DNA-onderzoek in strafzaken (Besluit DNA-onderzoek in strafzaken) (3) en in het Wetboek van Strafvordering (bij grootschalige DNA-verwantschapsonderzoek door de politie (4) is het op papier geregeld. De burger vraagt naar de borging. De advocatuur is kritisch want het gaat te ver om mensen die niet verdacht zijn ook te verplichten hun DNA af te staan (5). De NOvA stelt o.a. dat principes als het recht op privacy en de onschuldpresumptie in het geding zijn.

Terecht dat privacybeschermers zoals Platform Bescherming Burgerrechten, Privacy First, het Humanistisch Verbond, Stichting KDVP en de Autoriteit Persoonsgegevens (AP) hier kritische vragen over stellen. Laatstgenoemde had op 1 april 2020 zelfs gesteld dat artsen geen inzicht in patiëntendossiers zouden mogen hebben, zonder akkoord van de patiënt (6).

Referenties

(1) https://ggdghor.nl/privacyverklaring-coronit/

(2) www.nrc.nl/nieuws/2020/04/15/miljoenen-medisch-dossiers-open-zonder-toestemming-a3996917

(3) https://zoek.officielebekendmakingen.nl/stb-2001-400.html

(4) www.politie.nl/themas/dna-verwantschapsonderzoek.html

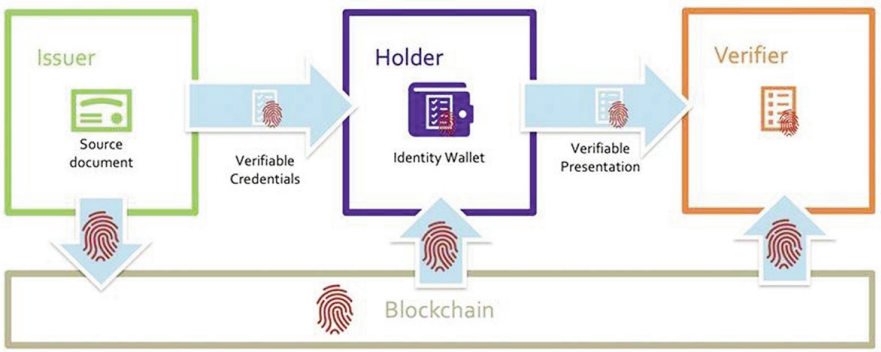
(5) www.security.nl/posting/593468/Minister+komt+met+reactie+op+verplichte+-dna-afname+na+oproep

(6) www.nu.nl/coronavirus/6041751/ap-artsen-mogen-medisch-dossier-coronapatient-niet-inzien-zonder-akkoord.html

Auteurs: Kim Schneider is Blockchain Specialist DT Strategy & Innovation en bereikbaar via kim.schneider@rabobank.nl, David Lamers is Blockchain Specialist – DT Strategy & Innovation en bereikbaar via david.lamers@rabobank.nl en Joris Lange is Innovation Lead Team IDA - Innovatie particulieren en bereikbaar via joris.lange@rabobank.nl.

Volledige controle over je persoonsgegevens met SSI

Iedereen deelt dagelijks data met verschillende partijen. Vaak accepteer je voorwaarden zonder te weten wat er daarna met jouw data gebeurt. Hoe mooi zou het zijn als je wel controle hebt en met één druk op de knop jouw persoonlijke brondata kunt versturen naar een instantie? Als het aan Rabobank ligt, is dit binnenkort geen toekomstmuziek meer. Als eigenaar van de data en gebruiker van producten bepaal je straks zelf met wie je jouw persoonlijke data deelt.



Afbeelding 1 - Technische werking SSI.

Het delen van data met één druk op de knop waarbij je zelf de controle hebt, is mogelijk met Self-Sovereign Identity (SSI). De SSI-methode maakt gebruik van blockchaintechnologie, waardoor jij door middel van een digitale wallet jouw gegevens veilig kunt opslaan en delen. Je kunt dit zien als een persoonlijk digitale kluis. Je kunt gegevens zoals identiteit, inkomen en adresgegevens ophalen bij de bron, die vervolgens de informatie ondertekent. In het geval van jouw inkomen, kun je dus bij het UWV de inkomensgegevens ophalen en in jouw wallet laden. Het UWV zet daar een digitale handtekening onder en jij kunt de gegevens delen met andere partijen die dit nodig hebben voor bijvoorbeeld een hypotheekaanvraag. Bedrijven die de data ontvangen, weten zo dat de data actueel en correct is. Dit vermindert de administratieve last voor beide partijen.

Digitale kluis en veiligheid

Momenteel is het al mogelijk om je te identificeren via bijvoorbeeld iDIN of DigiD, maar met SSI is het mogelijk om naast identificatie ook je gegevens uit te wisselen. Je laat dus geen kopie meer maken van je paspoort, maar deelt de benodigde gegevens via een digitaal dataverzoek.
Je weet welke organisatie je toestemming hebt gegeven tot jouw persoonlijke informatie, want dit wordt bijgehouden in jouw wallet. Deze bedien jezelf door biometrische beveiliging, bijvoorbeeld met een vingerafdruk of selfie. Deze methode is veilig omdat er digitale ondertekening plaatsvindt, er wordt gebruik gemaakt van blockchaintechnologie en je bent niet afhankelijk van een centrale partij. Aan de bedrijfszijde hoeft de data niet meer handmatig gevalideerd te worden, omdat er een automatische check wordt gedaan op de data.

Er zijn drie actoren:

- Issuer: deze partij geeft de brondata uit. In het voorbeeld van je inkomen is dit het UWV;
- Holder: de eigenaar van de data in een wallet. Dit ben jijzelf als eigenaar van jouw data;
- Verifier: de partij die de data wil checken. Dit is bijvoorbeeld de hypotheekverstrekker die controleert of jouw inkomen klopt.

Het platform waaraan wij werken, maakt het voor issuers en verifiers makkelijk om te koppelen met de oplossing. Zo hoeft een bedrijf geen kennis te hebben van SSI of blockchain, omdat de integratielaag van de oplossing deze logica bevat. Deze laag maakt gebruik van onder andere de nieuwe W3C-standaarden Decentralized Identifiers (DID's) en verifiable credentials. In de blockchain wordt slechts een vingerafdruk gezet die bij de credential hoort, de DID. Hiermee voldoet de oplossing volledig aan privacywetgeving (AVG) en wordt het voor bedrijven dus makkelijker om aan de AVG te voldoen. Iemands BSN wegkrassen uit een document is nu verleden tijd, je vraagt en verwerkt dus nooit meer informatie dan je nodig hebt.

Toepassingen SSI

Aan welke toepassingen van de SSI-methode en het gebruik van de wallet kun je dan zoal denken? Graag geven we een aantal voorbeelden van use cases waaraan we momenteel werken. Er zijn legio processen waarin je de identity wallet kunt gebruiken. Elke keer dat je documenten deelt, een pasje laat zien of inlogt, deel je data. In deze sectie gaan we dieper in op een selectie van toepassingen die wij onderzoeken.

Hypotheekdossier

Eén van de processen waar de identity wallet toe te passen is, is het hypotheekproces. Consumenten moeten allerlei documenten aanleveren. Dit gebeurt vaak in de vorm van een PDF of op papier. Het is voor hen moeilijk overzicht te hebben over wat nou precies nodig is en of het juiste is aangeleverd. Consumenten willen ook het liefst zo snel mogelijk duidelijkheid over of garantie voor hun hypotheek. Banken willen zeker weten dat de data juist is en nog actueel. Met de identity wallet is de benodigde data makkelijk te verzamelen en aan te leveren. Omdat er geen mid-office nodig is die de data handmatig verwerkt en valideert, weet je als consument sneller of je het droomhuis kunt kopen.

Autoverhuur

Je kent het vast wel. Je komt aan op het vliegveld en je kunt aansluiten in de rij bij je autoverhuurder om je paspoort en rijbewijs te overleggen. Deze worden gekopieerd en al je data, inclusief BSN, is gedeeld. Met de identity wallet lever je al tijdens het boekingsproces de minimaal benodigde informatie aan en kun je gelijk je auto ophalen.

Medische bewijzen voor corona

De identity wallet is ook toepasbaar in de medische sector. Zo werken we bijvoorbeeld aan medische bewijzen voor testresultaten van corona in het uNLock consortium (1), maar zou het ook kunnen worden ingezet om aan te tonen dat je in een latere fase het vaccin hebt gehad.

Inkomenstoets sociale huurwoningen

Een groot maatschappelijk probleem zijn de kosten van de inkomenstoets voor sociale huurwoningen. De toegestane foutmarge is zo klein dat ingerichte processen veel geld kosten. Met de identity wallet wordt de inkomenstoets uit handen van de woningcorporaties genomen. In plaats dat de huurder loonstroken moet delen, wordt in de identity wallet een zero knowledge proof gegenereerd op basis van je bij de Belastingdienst geregistreerde inkomen. Zo deel je alleen het cryptografische bewijs dat jouw inkomen onder een bepaalde grens ligt. Hetzelfde is toepasbaar op de markt van commercieel vastgoed waar jouw inkomen juist vaak boven een bepaalde grens moet liggen.

Klant blijft eigenaar persoonlijke data

Als bank willen we onze klanten helpen bij het maken van belangrijke financiële beslissingen. Om een goed inzicht te kunnen krijgen in de persoonlijke situatie van de klant, is inzicht in zijn persoonlijke data noodzakelijk. Dit geldt voor het verwelkomen van nieuwe klanten tot aan het verstrekken van bijvoorbeeld een nieuwe hypotheek of bedrijfsfinanciering. De persoonlijke data van de klant speelt in bijna alle processen een cruciale rol en is bepalend voor het uiteindelijke advies. Het is belangrijk dat de klant de eigenaar blijft van deze data en dat hij hier volledig de regie op moet kunnen voeren. Alleen de klant beslist met wie hij welke data deelt en wanneer.

Efficiëntieverbetering

In ons Tech Lab onderzoeken wij nieuwe technologieën en hoe deze ons businessmodel beïnvloeden. De technologieën die wij testen en ontwikkelen, proberen we praktisch toepasbaar te maken voor onze bedrijfsprocessen. Hierbij zoeken we naar oplossingen die bijdragen aan de ambities van de bank. Bij de SSI-oplossing komt dit heel mooi samen. We kunnen onze processen eenvoudiger, efficiënter, sneller en veiliger maken. Dit levert voordeel op voor de klant, maar ook voor onszelf.

Alle bedrijven - die persoonlijke data nodig hebben voor hun primaire processen - zouden graag gevalideerde data vanuit de oorspronkelijke bron gebruiken. Doordat klanten deze data niet meer kunnen aanpassen, kan deze data rechtstreeks in de processen gebruikt worden. Dit kan tot een enorme efficiëntieverbetering leiden bij veel bedrijven. De data hoeft immers niet meer te worden gecontroleerd. Bij veel bedrijven gebeurt dit in ieder proces nu meerdere keren per uitvoering en worden er alsnog fouten gemaakt. Dit komt deels door menselijk handelen, maar ook omdat het niet te controleren is. SSI zou hieraan kunnen bijdragen. Zeker wanneer dit een standaardoplossing in Nederland wordt waar bedrijven op een laagdrempelige manier op aan kunnen sluiten. Met een goede samenwerking tussen de publieke en private sector moeten we dit van de grond kunnen krijgen.

Referentie

(1) Meer informatie kun je vinden op www.unlockapp.nl

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
Jan van de Vis
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 2020 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

ALS HET GOED IS, IS HET GOED.

Maar verbetering zit in een klein hoekje.

Certificeren? Dan moet u voldoen aan de norm. DNV GL toetst u snel en goed. Maar iedereen houdt van opstekers, niet van standjes. Daarom kijken we bij certificering ook naar wat goed gaat en zelfs nog beter kan. Op die gebieden die voor uw bedrijf of organisatie belangrijk zijn. Aandachtspunten waarop u zélf beoordeeld wilt worden. Certificering die net even verder voert. Want verbetering zit in een klein hoekje.

U kunt ons bereiken via 010 2922 700 of www.dnvgl.nl/certificering

ONLINE BESCHIKBAAR

WAT IS EEN ISMS?

Wilt u meer weten over het opzetten van een information security management system?

Download de whitepaper via

www.dnvgl.nl/whitepaper