INFORMATIEBEVEILIGING MAGAZINE

- Uitslag lezersenquête
- De waarde van meldgedrag voor digitale weerbaarheid
- Column – De racist in de computer

JAARGANG 20 - 2020 - EDITIE 4

Slow motion

Nicole van Deursen

Het is een uitdaging om na het zeer goed gewaarde themanummer 'Privacy' (onder redactie van Rachel Marbus) weer een 'gewoon' iB-Magazine samen te stellen dat ook interessant is. Gewoon klinkt namelijk als 'doorsnee' of 'saai'. Gelukkig is er niets saais aan informatiebeveiliging en zitten wij als redactie ook niet stil. Aan het begin van dit jaar hebben wij een enquête onder onze lezers uitgezet en met bijna 200 reacties hebben we voorlopig genoeg acties om op te volgen. We gaan zeker met onze tijd mee, maar wel langzaam en met kleine stapjes. Gewoontes veranderen kost nu eenmaal tijd.

Enkele veranderingen zijn voor jullie al zichtbaar. De oplettende lezer was het in het vorige nummer al opgevallen: we hebben een nieuwe vaste columniste. Inge Wetzer publiceerde al vaker artikelen in iB-Magazine, maar nu schrijft zij een vaste column over informatiebeveiliging en gedrag. Daarnaast hebben we ook een nieuwe vaste rubriek: *De Scriptie*. Het PvIB verwelkomt al enige tijd een groeiend aantal studentleden en young professionals. Wij geven hen graag de kans om hun afstudeerscripties met het grote publiek te delen en wij kunnen ook weer iets nieuws leren van hun blik op het vak. Soms eisen opleidingen echter dat scripties in de Engelse taal worden opgeleverd en dan volgt ook automatisch een Engelstalige publicatie. Als redactie vinden wij dat prima, we zien ook de trend dat wij steeds vaker artikelen in het Engels ontvangen, zoals bijvoorbeeld een nieuwe reeks artikelen over security architectuur, die ook in dit magazine begint. Het geeft ons blad de kans om een breder publiek aan te spreken. Maar we veranderen niet alles tegelijk. Rustig aan, er spelen belangrijker zaken in de wereld.

Nicole

IN DIT NUMMER

Auteurs: Piet Kalverda werkt als Senior Security Officer bij PGGM. Piet is te bereiken via e-mail: piet.kalverda@pggm.nl. Renato Kuiper is principal consultant cybersecurity bij Capgemini. Renato is te bereiken via e-mail: renato.kuiper@capgemini.com

Een andere kijk op classificatie

Het doel (of nut) van informatiebeveiliging is het waarborgen van de betrouwbaarheid van bedrijfsinformatie en informatiesystemen. Betrouwbaarheid wordt onderverdeeld in beschikbaarheid, integriteit en vertrouwelijkheid, afgekort als BIV (1). Er zijn veel bedreigingen (2) die betrouwbaarheid van informatie kunnen aantasten, en daartegen zijn ook veel maatregelen te nemen. Welke maatregelen tegen welke bedreigingen bij welke data of systemen en bij welk gebruik nodig zijn, wordt vastgesteld door een risicoanalyse uit te voeren.

De risicobereidheid van de onderneming. Dit is behoorlijk complex omdat elke bedreiging meerdere maatregelen (elke maatregel bevat kwetsbaarheden) nodig heeft, en daarnaast één maatregel vaak voor meerdere bedreigingen werkt. Door één of meerdere basisbeveiligingsniveaus van maatregelen vast te stellen, bijvoorbeeld in een security architectuur, zijn risicoanalyses alleen nodig voor de belangrijke systemen. Of voor nieuwe bedreigingen waar het basisniveau onvoldoende bescherming biedt. Er moet dan eerst worden bepaald welke systemen belangrijk zijn qua beschikbaarheid, integriteit en vertrouwelijkheid.
Classificatie zorgt ervoor dat duidelijk is welke data en systemen belangrijk zijn, de zogenaamde kroonjuwelen, en welke minder belangrijk. De hiervoor meest gebruikte methode (BIV) is minder objectief dan het lijkt. Ook is het vaststellen van de juiste maatregelen niet gegarandeerd. Een andere methode, gebaseerd op kenmerken, is veel gebruiksvriendelijker omdat er geen vertaalslag nodig is.

Classificatie op basis van BIV

Net zoals een tuin minder belangrijk is dan een huis, verschillen informatiesystemen en data in belang, en worden ze geclassificeerd aan de hand van een impactscore op Beschikbaarheid, Integriteit en Vertrouwelijkheid. Bijvoorbeeld B0 betekent geen schade als het systeem niet beschikbaar is en V4 betekent zeer grote schade als de informatie op straat ligt. De 5x5x5 mogelijke BIV-combinaties worden vaak samengevoegd tot een paar profielen (bijvoorbeeld laag, midden, hoog).
Per systeem of dataset worden vragen gesteld over impact. Wat is de impact van niet-beschikbaar zijn en het niet-integer of niet-vertrouwelijk zijn van het systeem? En wat is de impact van informatie op managementbeslissingen, bedrijfsresultaten, reputatie, misbruik, herstel of juridische aansprakelijkheid? Is bij een van de vragen de impact hoog, dan is de classificatie ook hoog. Is het antwoord op alle vragen laag dan is de classificatie laag. Voor beschikbaarheid wordt de maximale uitvalsduur (hoeveel schade bij hoeveel uren uitval) en en maximaal gegevensverlies (uitgedrukt in uren herstelwerk); nog als een extra variabele gebruikt.

Waarom helpt de huidige BIV-classificatie methode niet?

De BIV-classificatie is subjectief. Bij het bepalen van de hoogte van de classificatie spelen meerdere belangen. Degene die moet betalen voor de implementatie van maatregelen is geneigd de classificatie wat lager in te schatten. Tenzij hij of zij net een awareness-training heeft gedaan en weet wat er allemaal mis kan gaan. Degene die erop wordt aangesproken wanneer het systeem niet beschikbaar is, is geneigd de classificatie wat hoger in te schatten zodat er meer maatregelen worden genomen. Dus de classificatie verschilt afhankelijk van wie het uitvoert. Aanbevolen wordt daarom om classificatie in een groep met minimaal tien mensen uit te voeren, maar in de praktijk is dan de budgethouder degene met de meeste invloed waar anderen zich naar schikken. Ook is het de vraag of iedereen precies weet wat met de vragen over Beschikbaarheid, Integriteit en Vertrouwelijkheid wordt bedoeld. Bijvoorbeeld voor wie of op welk moment het systeem niet beschikbaar is, of voor welke onbevoegden de informatie is te lezen en hoe ernstig de fout is in de data. Als een grote groep niet lukt, (classificeren is geen onderdeel van het primaire proces en krijgt mogelijk niet voldoende prioriteit) dan doet de informatie- of security architect het, eventueel samen met een security officer. En ook daar verschillen de belangen en interpretaties.

Het feit dat van de 125 verschillende BIV-combinaties meestal (tussen de drie en tien) profielen worden gemaakt, betekent al dat BIV-codering eigenlijk niet handig is. Het is dan beter om een aantal standaardprofielen met een betekenisvolle naam te gebruiken en de traditionele aanpak van de BIV-codering achterwege te laten. Maar ook dan blijven de interpretatieverschillen, overschatting en onderschatting bestaan. Daarom is er een betere methode.

Maatregelen op basis van kenmerken

Een gemiddelde eigenaar of manager weet het verschil niet tussen I2 en I3. Hij weet wél welke kenmerken het systeem of de informatie heeft, bijvoorbeeld of er persoonsgegevens of financiële gegevens verwerkt worden. Op deze kenmerken kan, naast basis beveiligingsmaatregelen, direct een beperkt aantal specifieke principes of verder uitgewerkte maatregelen toegepast worden. Classificatie gebeurt dan op kenmerkniveau en in context (waar en wanneer), objectief en zonder een codering te hoeven vertalen naar een profiel. Waar dan nog wel op gelet moet worden is dat het kenmerk niet de maatregel is, zoals bijvoorbeeld vaak gebeurt bij vertrouwelijkheid: een document is vertrouwelijk als niet iedereen er bij mag. Het beperken van toegang is juist de maatregel die je neemt als een document bijvoorbeeld persoonsgegevens bevat.

Kenmerken zijn (niet uitputtend):

- Strategische informatie of bijzondere persoonsgegevens;

- Gewone persoons-, financiële- of configuratie gegevens;
- Informatie met een bewaartermijn;
- Extern opgeslagen informatie;
- Extern draaiend systeem;
- Onderdeel (systeem en/of data) van primair bedrijfsproces;
- Webapplicatie (internet facing).

Ongeacht de classificatiemethode is er een voor alle systemen en informatie geldend basis beveiligingsniveau, bestaande uit een aantal altijd toe te passen basisprincipes of maatregelen. Basisprincipes zijn bijvoorbeeld:

- Accountability (elk account heeft een unieke identificeerbare en traceerbare eigenaar);
- Need to know (elke autorisatie is goedgekeurd door de systeemeigenaar o.b.v. de data dan wel de gedefineerde rol van de functionaris);
- Continuïteit (van alle data wordt dagelijks een back up gemaakt);
- Hardening van systemen (need to run, configuratie baseline monitoring, patch en kwetsbaarheden management, endpoint protection, password en sleutel management, mobile device management);
- Intrusion prevention (firewalls en fysieke toegangsbeveiliging);
- Security (en privacy) by design (bij ontwerpen en wijzigingen worden basisprincipes toegepast).

Basisprincipes worden voor een deel opgelegd door wetgeving of toezichthouders, een ander deel wordt bepaald door kosten van de maatregel en risicobereidheid van de onderneming.
Specifieke maatregelen zijn dan bijvoorbeeld voor de genoemde kenmerken naast de basisprincipes:

- Informatie met persoons-, financiële- of configuratiegegevens:
  - Multifactor authenticatie;
  - Minimale wachtwoordlengte;
  - Controle op autorisaties;
  - Logging van beheer activiteiten;
  - Alerting van ongewone activiteiten ;
  - Versleutelde datatransport;
  - Intrusion prevention: stepping stones, segmentering, monitoring, anomalie detective.
- Informatie met bijzondere persoonsgegevens, strategische bedrijfsinformatie:
  - Toegang is traceerbaar;
  - Encryptie;
  - Red team testen;
  - Locatiebeperking.
- Informatie met een bewaartermijn (alle informatie heeft een bewaartermijn):
  - Archiefformaat;
  - Verwijderen zodra termijn verstreken.
- Informatie staat extern of systeem draait extern:
  - Leveranciers (keten) check op hier vermelde principes en maatregelen.
- Webapplicatie:
  - Pentesten;
  - Source code review.
- Primaire bedrijfsproces systemen:
  - Synchrone replicatie/ hot standby;
  - Business Continuity Management.

BIV-codes overbodig

Door basisprincipes te hanteren en specifieke maatregelen toe te passen op basis van kenmerken wordt de classificatie aanpak met de BIV-codes overbodig. En daarmee ook subjectiviteit en kans op onderschatting en overschatting van maatregelen. Behalve voor uitzonderingen zijn ook risicoanalyses overbodig. Eigenaren van systemen en data kunnen daarmee hun verantwoordelijkheid waarmaken en de maatregelen (laten) implementeren die passen bij de risicobereidheid. Daarmee wordt informatiebeveiliging inclusief het al of niet accepteren van risico's een gezamenlijke verantwoordelijkheid van business en IT. In de bovengenoemde kenmerken, principes en maatregelen is nog wel bedrijfsspecifieke variatie mogelijk die verder uitgewerkt kan worden in een security architectuur. Specifieke maatregelen kunnen natuurlijk ook opgenomen worden in de basis-set. Een indicatie voor de verhouding tussen basis en specifieke maatregelen is dat ongeveer 80% van de data en systemen onder de basismaatregelen valt. Welke maatregelen al dan niet worden meegenomen in de basis-set is afhankelijk van bedrijfsdoel, risicobereidheid en wetgeving.

Weggooien

Misschien moeten we ook de kenmerken maar vergeten en er gewoon voor zorgen dat de belangrijkste basismaatregelen overal werken: encryptie van data, backups, testen, updates, 2FA, beperkte autorisaties, we gooien weg wat we niet meer nodig hebben en misschien nog meer. En dat doen we standaard voor alles. Dan hoeft niemand meer na te denken over dreigingen, kenmerken of BIV-codes en besparen we ons veel tijd en geld.

Referenties

(1) Informatiebeveiliging onder controle, Overbeek & Lindgren, 2000

(2) ENISA threat landscape report 2019

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

De racist in de computer

Het probleem is niet nieuw, maar het kwam dezer dagen terug in mijn geheugen. Er zit met enige regelmaat een hardnekkige racist in onze computer. Toen ik in de beginjaren van de 21e eeuw onderzoek deed naar gaming en de sociale en juridische aspecten daarvan, ontdekte ik racisme al in de vorm van de avatars. De beschikbare avatars waren eigenlijk praktisch alleen wit, met een enkele uitzondering daargelaten. Wie een zwarte huid wilde hebben, kon kiezen uit de optie 'Rastafarian'.

Computerprogrammeurs, witte heteroseksuele mannen van midden twintig, waren zich van geen kwaad bewust. Onderzoekers legden pijnlijk bloot dat er een onbewuste bias in de code was geslopen. Het beperkte wereldbeeld van de programmeurs vond zijn weerslag in het eindresultaat op het scherm. De gamewereld heeft gelukkig een mooie revolutie doorgemaakt en is sindsdien een stuk diverser geworden. Maar daarmee is het onderliggende probleem nog zeker niet de wereld uit.

Het pijnlijkste en ook gevaarlijkste voorbeeld dat momenteel aan de orde is, zijn de facial recognition systemen. Er zit een nare raciale bias in de algoritmes die worden ontworpen om gezichten van personen te herkennen. Vaak zetten handhavers deze systemen in om mensen op een 'hot-list' op te sporen. Het probleem is echter dat deze systemen niet goed zijn in het herkennen van zwarte gezichten. Er is te vaak sprake van een vals positief waardoor mensen ten onrechte als een crimineel worden aangemerkt, met alle gevolgen van dien.

Dat dit niet alleen een probleem is, in bijvoorbeeld de VS en het VK waar deze facial recognition technologie en dus ook de bias ten opzichte van niet-witte personen al veel gebruikt wordt, bewijst onze eigen Belastingdienst-affaire. Ook daar hadden wat witte mensen aan de knoppen zitten draaien om een racistisch algoritme in het leven te roepen wat mensen van een andere afkomst dan de Nederlandse bij voorbaat het stempeltje 'fraudeur' opplakte. De Belastingdienst haastte zich in het debat nog te zeggen dat echt iedereen met een dubbele nationaliteit het label opgeplakt had gekregen en dat daar heus ook een paar witte mensen tussen zaten. Dat het leeuwendeel bestond uit niet-witte mensen werd maar even terzijde gewapperd. We gaan vaker nat hoor in Nederland, lees er ook maar eens de informatie over de Verwijsindex Antillianen op na (gelukkig bestaat deze niet meer). De racist wordt in de computer gestopt door witte mensen. Soms zelfs nog wel met de beste bedoelingen, soms uit onwetendheid. En vaak door de eigen vooringenomenheid – de witte bias. Hoog tijd om de racist niet alleen uit onze maatschappij te weren, maar ook onze computers ervan te schonen.

BLACK LIVES MATTER!

Rachel

Wil je meer lezen over Racisme in Nederland? Kijk dan eens bij de Correspondent en lees het artikel 'Institutioneel racisme in Nederland: wat het is, waar het zit, en wat jij eraan kunt doen'. En als je dan toch bezig bent, kun je hier doneren aan de Stichting 'Nederland wordt beter': https://www.nederlandwordtbeter.nl/doneren/

Auteur: Chris de Vries, redacteur en zelfstandig professional met grote interesse voor ICT en leidt al meer dan 26 jaar zijn eigen onderneming De Vries Impuls Management. Chris is bereikbaar via: impuls@euronet.nl.

Digitalisering aan de grens, een Algemene Rekenkamer analyse

De Algemene Rekenkamer heeft tot taak onafhankelijk te controleren dat de Rijksoverheid publiek geld zinnig, zuinig en zorgvuldig uitgeeft. Dit hoge college maakt dus een balans op van de doelmatigheid van de ontvangsten en uitgaven. Risicoanalyse behoort daartoe. Zo heeft de Rekenkamer in 2019 de grenscontrole door de Koninklijke Marechaussee (KMar) aan een onderzoek onderworpen.

Op 20 april jl. is het rapport (Digitalisering aan de grens – cybersecurity van het grenstoezicht door de Koninklijke Marechaussee op Schiphol) (1) aan de Tweede Kamer aangeboden. Wij weten allen dat Schiphol belangrijk is en dat een groot aantal persoonsgegevens daar verwerkt wordt. Dus verwachten wij bij een dergelijk belangrijke toegangspoort tot Nederland, meer nog tot Europa (de EU) een gedegen controle. Het mag duidelijk zijn dat bij een slordige 80 miljoen reizigers per jaar reizigergegevens als nationaliteit, reisroute en -gezelschap en soms strafrechtelijke gegevens in de KMar IT-infrastructuur gedigitaliseerd wordt, maar dat dit tegelijkertijd ook een afhankelijkheid ervan creëert alsook nieuwe risico's. Het beleid van de EU, de Koninklijke Schiphol Groep N.V. e.a. is dan ook gericht op een nog grootschaliger inzet van deze technologie in de komende

Figuur 1 - Schiphol: de hub (bron: Algemene Rekenkamer).

jaren. Dat in een wereld waarbij cyberaanvallen van hackers en (vijandelijke en 'bevriende') staatsactoren tot het normale straatbeeld behoren en manipulatie van informatie immense risico's met zich meebrengen. Duidelijk dus waarom de Algemene Rekenkamer de status van de cybersecurity bij de KMar onderzoekt.

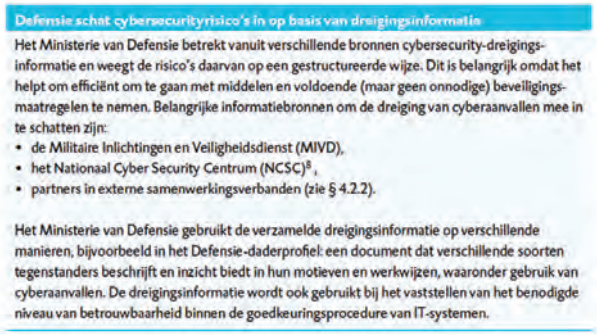
De drie kernthema's in dit onderzoek waren controle:

1. van aankomenden (tijdens de vlucht);
2. bij de KMar balies en
3. bij de 'self service passport control'.

Twee ministeries zijn voor de daar bijbehorende IT-systemen verantwoordelijk: het Ministerie van Defensie (1) en (2) en Ministerie van Justitie en Veiligheid (3). Dan zal het wel goed gaan; ministerieel toezicht van de twee voornaamste partijen op dit terrein. Niets is minder waar, want wat constateert de Rekenkamer: *'In het licht van alle komende technologische ontwikkelingen beoordelen we het huidige niveau van cybersecurity op het grenstoezicht als onvoldoende en niet toekomstbestendig' (2).*

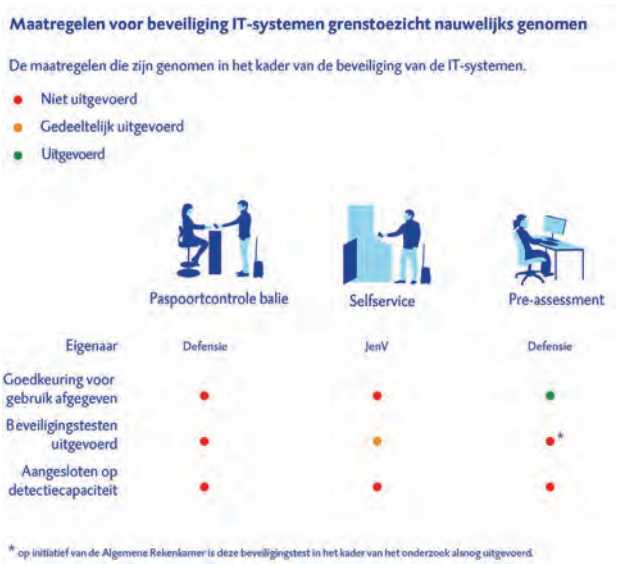
Figuur 2 - Goedkeuringsprocedure IT-systemen grenstoezicht (bron: Algemene Rekenkamer).

Deze conclusie baseert de Rekenkamer op het feit dat systemen operationeel zijn zonder de vereiste beveiligingsgoedkeuring van het Ministerie van Defensie. Daarnaast dat de niet-aansluiting op het Security Operations Center (SOC) het risico betekent dat de cyberaanvallen niet of te laat worden opgemerkt. Een gezamenlijke beveiligingstest op controlethema 3 lukte niet zoals men bedoeld had (moeizaam en minder breed), vanwege de samenwerking tussen de meerdere publieke en private partijen bij dit systeem. Ook het pre-assessment systeem, het balie IT-systeem en deels het 'selfservicesysteem' toonden elf kwetsbaarheden, zoals zwakke wachtwoorden en de optie om e-mails te verzenden uit naam van willekeurige defensiemedewerkers.



Figuur 3 - Cybersecurityrisico's en dreigingsinformatie (bron: Algemene Rekenkamer).

Tenslotte concludeert de Rekenkamer dat de procedures met betrekking tot verstoringen veroorzaakt door een cyberaanval door het ontbreken van concrete scenariovoorbereiding een probleem zouden kunnen blijken te zijn. Daarbij zijn er geen cyberoefeningen geweest voor het grenstoezicht, waardoor de vraag boven komt drijven of de reactie van het Ministerie van Defensie in de praktijk effectief zal zijn.



Figuur 4 - Genomen cybersecuritymaatregelen voor IT-systemen grenstoezicht (bron: Algemene Rekenkamer).

Scan en bekijk de animatie

De Algemene Rekenkamer benoemt in haar rapport dat inmiddels wel stappen zijn gezet om (delen van) deze problematiek uit te sluiten en daarnaast hebben zij in het rapport een aantal aanbevelingen gedaan:

Aan het Ministerie van Justitie en Veiligheid:

- goedkeuringsprocedure alsnog doorlopen;
- alle beveiligingseisen laten implementeren door Schiphol N.V.;
- is de cybersecurity voldoende voordat het selfservicesysteem overgedragen wordt aan Schiphol N.V. en sluit het selfservicesysteem z.s.m. aan op het SOC van Schiphol N.V.

Aan het Ministerie van Defensie:

onderwerp elk IT-systeem aan de jaarlijkse beveiligingstesten en borg opvolgingen/aanbevelingen en laat beide ministeries in samenwerking met alle ketenpartners het beheersen van crises als gevolg van cyberaanvallen oefenen.

Referenties

(1) https://www.rekenkamer.nl/binaries/rekenkamer-/documenten/rapporten/2020/04/20/digitalisering-aan-de-grens/Digitalisering+aan+de+grens+WR.pdf

(2) In het onder (1) vermelde rapport op pagina 7 en pagina 6 t/m 9 van Hoofdstuk 1 Samenvatting.

(3) https://www.emerce.nl/nieuws/ophef-stille-verhuizing-patint-gegevens-google-cloud of https://www.ad.nl/binnenland/honderdduizenden-patientgegevens-verhuisd-naar-google-kabinet-vraagt-om-onderzoek~afab53a7/

(4) https://nos.nl/artikel/2336709-minister-over-lek-corona-site-rivm-ongelukkig-maar-menselijke-fouten-blijven-voorkomen.html en over de `geruststellende'(?) informatie vanuit de Rijksoverheid: https://www.rijksoverheid.nl/onderwerpen/coronavirus-covid-19/openbaar-en-dagelijks-leven/apps

(5) https://www.rijksoverheid.nl/onderwerpen/coronavirus-app

(6) https://www.binnenlandsbestuur.nl/bestuur-en-organisatie/kennispartners/capra-advocaten/overheid-en-ambtenaren-strafrechtelijk.9217324.lynkx

(7) https://www.gemeente.nu/loopbaan/cao/stel-ambtenaar-aansprakelijk-voor-persoonsgegevens/

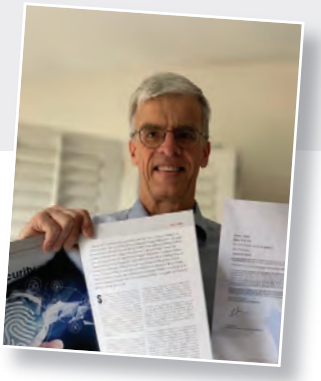
(8) https://www.wijnenstael.nl/nieuws/2019/onjuiste-informatieverstrekking-ambtenaar-gemeente-aansprakelijk

(9) Zie voor een video-animatie URL: https://www.youtube.com/watch?v=nEmNMExQq3k

Persoonlijke visie Chris de Vries

In het navolgende mijn persoonlijke visie. Dit rapport roept bij ons als burger vragen op. Dit was een rapportage uit 2019 onze aandacht nu volledig opgeslokt door het coronavirus de verlammende werking ervan op de wereldeconomie en ons dagelijks leven. Als burger vertrouwen wij op onze overheid, maar moet niet de vraag gesteld worden of dat terecht is? En als de vraag terecht is, wat betekent dat dan met betrekking tot de toezeggingen van politici en overheidsinstellingen dat zij zorgvuldig met de informatie (privacy) van burgers omgaan? Dat wij ons geen zorgen hoeven te maken over het in de Google-cloud plaatsen van honderdduizenden patiëntgegevens (3)? Het vrijgeven van patiëntendossiers aan het RIVM (ook van diegene die expliciet geen toestemming hebben gegeven de site infectieradar.nl van het RIVM!) (4) en de beoogde (en bij voorkeur verplichte) corona-app (5)? Te veel goedbedoelende mensen streven naar een maakbare (informatie)samenleving. Vertrouwen erop dat het wel goed gaat komen met menselijke fouten in ICT-oplossingen, dat tijdig ingegrepen wordt, dat de kans op misbruik klein is; en wanneer effectief benut door (staats)hackers van overzichtelijke omvang/grootte dus verwaarloosbaar. Daarnaast kan de overheid zich beroepen op het verschoningsrecht in geval van aanspraken en boetes. Dus hier is echt geen sprake van `gelijke monniken, gelijke kappen' (6). Interessant hoe Britse onderzoekers (namens Big Brother Watch) constateerden dat Britse overheden dagelijks vier keer over de schreef gaan als het gaat om persoonsgegevens. Vaak verwijst men daar dan naar IT-systemen en dat daar ook naar de oplossing wordt gezocht, terwijl het gaat om menselijke fouten en onvoorzichtigheden; zie artikel in www.gemeente.nu d.d. 17.08.2015; (7), alhoewel in een website artikel van WynStael advocaten d.d. 04.04.2019 als zeldzame uitzondering (?) een gemeente aan te spreken bleek (8).

Hebben wij dan geen zorg dat `perfecte' informatie (lees veelomvattend) - in handen van de verkeerden - misbruikt wordt ten kostte van velen? De historie leert ons dat, het heden toont ons dat, zodra wij realiseren hoeveel verkeerde (overheids/bedrijfs)machtshebbers aan hun imperia werken. Natuurlijk worden er fouten gemaakt (ook in de ICT-wereld). Wij sluiten niet alle risico's uit en moeten die illusie ook niet hebben, maar is de Algemene Rekenkamer-rapportage niet het zoveelste teken aan de wand? Moeten wij niet uitermate bezorgd zijn dat fundamentele IT-systemen zo kwetsbaar blijken te zijn en ambtenaren/politici enkel kunnen reageren met: "Sorry, zal niet meer gebeuren; risico was minimaal, is slechts kort een gevaar geweest en er is slechts beperkt misbruik van gemaakt." Of moeten wij wachten op het kind dat zegt: "Mama, waarom staan de waterkeringen bij deze storm nu open?" Het rapport van de Algemene Rekenkamer moet terug onder de aandacht komen om niet na het zoveelste parlementair onderzoek op de stapel van afgesloten, snel te archiveren stukken terecht te liggen; zonder dat daadwerkelijk aan de meest essentiële beveiliging is gewerkt. Het PvIB heeft enkele jaren terug veel tijd en moeite besteedt aan de `baseline ketenveiligheid' en nu werkt men in de markt aan de Baseline Informatiebeveiliging Overheid (BIO). Blijven dit papieren tijgers of leidt het daadwerkelijk tot iets?



Artikel van het Jaar 2019

Ook dit jaar is de jury weer bijeengekomen om de selectie van artikelen te beoordelen en tot een top drie te komen. De jury was snel uit de selectie van de shortlist, maar de keuze welk artikel op welke plek moest komen, leverde nog de nodige discussie op. Uiteindelijk is de jury tot de volgende top drie gekomen.

Ontwikkelingen rondom security in architectuur (Renato Kuiper)
Het artikel geeft veel informatie in de breedte, met veel standaarden, overzichtelijk aan elkaar gekoppeld. Goed is ook dat er zo veel aandacht is voor de invloed van 'andere partijen' (de 'business', wetgeving en dergelijke) op de architectuur-invulling. Ook de koppeling aan het Risk-domein is prettig verfrissend, die koppeling is in de praktijk nog te hard nodig... Gelukkig is er een dosis historische bespiegeling zónder treuren dat alles vroeger beter was. Het geheel is mede daardoor heel prettig leesbaar. Maar wat blijft, is de vraag: hoe dit nu te gebruiken? Het is eigenlijk een beetje schrikbarend dat er zo lang zo weinig met architectuur is gedaan. Kom op vakcollega's, dat moet beter! Waarom is er nog te veel onduidelijkheid over, om maar wat te noemen, de koppeling van cloud-architecturen aan security-architecturen? Dit artikel helpt hopelijk bij het op gang brengen van zulke verbeterslagen.

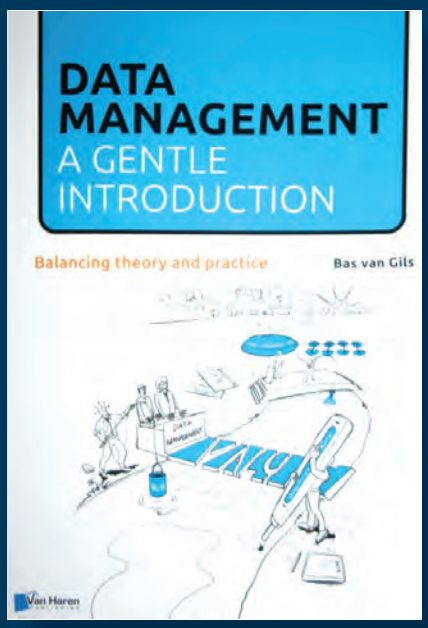
Secure by design: controle is goed, maar vertrouwen is beter (Sjoerd Peerlkamp)
Een zeer actueel en belangrijk onderwerp, nu steeds meer industrieën overstappen op meer of minder formele vormen van agile werken. Dit korte artikel doet de problematiek van een kritische infrastructuur uit de doeken en beargumenteert waarom zelfs deze industrie, uit de aard der zaak behoudend, overstapt op agile werken. Agile werken vergt een nieuwe benadering van informatiebeveiliging. Metaforen (duikboot en dolfijn) maken het verhaal visueel aantrekkelijk. De schrijfstijl is toegankelijk, ook voor de lezer die nog niet gepokt en gemazeld is in agile werken. Omdat het een kort artikel betreft zijn de handvatten om het zelf te gaan aanpakken wat onderbelicht.

Agile security (Lex Borger)
Een hyperactueel onderwerp dat ook speelt in de automotive industrie, waar steeds meer autofabrikanten worstelen met de overgang naar softwareontwikkelaar en de invoering van agile. Door het vele gebruik van agile-termen niet voor iedereen direct goed leesbaar. Duidelijk bedoeld voor de doelgroep die al agile werkt - maar is dat al een grote groep? De indeling van security features in de klasse niet-functionele requirements NFR kan beter, de ISO15408 standaard (Common Criteria for IT Security Evaluation) kent namelijk al meer dan 25 jaar Security Functional Requirements ... Dit artikel is een mooie aanvulling op het artikel Secure by design.

Na discussie kwam de jury op het standpunt uit dat het artikel Ontwikkelingen rondom security in architectuur op de derde plaats eindigt. Een goed geschreven artikel dat helaas niet direct van toepassing is. De artikelen Secure by design en Agile security eindigen op een gedeelde eerste plaats, mede omdat ze in combinatie met elkaar een toegankelijke inleiding en een praktische handleiding voor de gevorderde vormen. De jury feliciteert de winnaars van harte met dit mooie resultaat!

Namens de jury, Ellen Wesselingh, HAN University of Applied Sciences.

Auteur: Chris de Vries, is redacteur en zelfstandig professional onder de naam: De Vries Impuls Management, bereikbaar onder: impuls@euronet.nl.



Titel : Data Management: a gentle introduction
Schrijver : Bas van Gils
Taal : Engels
Aantal pagina's : 278
ISBN : 978 94 018 0550 6
ISBN eBook : 978 94 018 0552 0
ISBN ePub : 978 94 018 0555 1

BOEKREVIEW

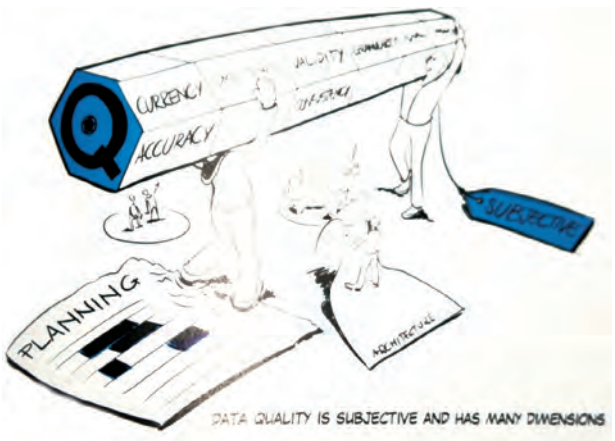
Data Management: a gentle introduction

Het was net vóór de lockdown dat ik de boeklancering bijwoonde in Tilburg. Een grote groep geïnteresseerde professionals had zich op de campus van de universiteit verzameld om kennis te nemen van het nieuwste boek over Data Management van Bas van Gils. Niet alleen dat was aan de orde, maar ook een leuk programma daar omheen. Het thema: 'Datamanagement, van data tot waarde', met daarnaast twee parallelsessies: 'De datamanagement-game' en de 'Datamanagement-opleiding'.

De meer ervaren lezer kan dan ook snel overzien of een bepaald hoofdstuk interessant is

Het was een verzorgde doop van een nieuw boek over datamanagement. Om met de auteur te spreken: "Datamanagement is geen nieuwe discipline, wel een discipline die de laatste jaren veel meer aandacht krijgt waarbij veel organisaties worstelen met de vraag hoe maak je het praktisch?" (Voor de goede orde: dit is geen letterlijk citaat, maar een samenstelling van zijn uitspraken).
Zowel de presentatie als Van Gils' boek betekenen een duik in het diepe; vandaar de analogie hierboven van een doop. En zoals ieder van ons die als klein kind zwemmen leerde: op een gegeven moment spring je het diepe in en voel je je hart in je keel kloppen; zo ervaren velen de duik in datamanagement. Het is dan ook prettig als iemand erbij is om je vertrouwen in te fluisteren.
Bas van Gils is onze vertrouwenspersoon bij de duik in datamanagement. Met recht heeft hij als subtitel gekozen voor 'A gentle introduction', want het is met zachtheid dat hij de lezer(es) meeneemt in de complexiteit van data. Hij cirkelt met ons om de kernbegrippen, laat deze regelmatig terugkeren en verdiept weer wat meer.
In zijn verzorgde en met grappige maar serieuze tekeningen verluchtigde boek (de tekeningen zijn visuele samenvattingen van elk hoofdstuk, goed uitgevoerd door illustrator Andy Lo Tam Loi) kan de beginnende professional, de geïnteresseerde ondernemer, de overheidsmedewerker, maar ook een leek het terrein van datamanagement verkennen en zijn kennis verdiepen. Terecht voegt Van Gils dan ook nog eens een sub-subtitel toe: 'Balancing theory and practice'. De doelgroep voor dit boek is dan ook uitbreidbaar met bachelors/master-studenten.

Wat het boek zo leesbaar maakt is dat de auteur de hoofdstukken niet ellenlang heeft laten uitdijen, maar getracht heeft kort te zijn en punten op de i te zetten. Ik denk dat hij daarin is geslaagd. Door de lay-out is ook een duidelijk onderscheid gemaakt tussen de tekst en de voorbeelden. De meer ervaren lezer kan dan ook snel overzien of een bepaald hoofdstuk interessant (verdiepend) is of kan worden overgeslagen. De gehele opbouw van het boek bevordert in ieder geval de leessnelheid.



Figuur 1 - Data quality is subjective and has many dimensions.

Her en der is de tekst verrijkt met interviews met dataspecialisten en managers uit de praktijk. Ook dat draagt bij aan de kennisoverdracht en het gevoel geaard te zijn met de praktijk van alledag.
Over de auteur zelf: Bas van Gils studeerde aan de Tilburgse universiteit en behaalde zijn MSc in informatiemanagement in 2002. Vervolgens studeerde hij aan de Nijmeegse universiteit waar hij werkte aan de 'information retrieval' op het web. Zijn dissertatie verdedigde hij succesvol in 2006 en dat verrijkte hem met de PhD in de computerwetenschap.
Sindsdien is Van Gils actief geweest in veel verschillende organisaties als consultant bij de politie en trainer en onderzoeker voor BiZZdesign bijvoorbeeld. Als logisch gevolg werd hij trainer en docent aan de universiteiten van Tilburg, Nijmegen, Utrecht en de Open Universiteit. Van Gils publiceert artikelen, schrijft boeken en treedt op als spreker. In 2016 startte hij zijn eigen onderneming Strategy Alliance (samen met Raymond Slot) en biedt diensten aan met betrekking tot de digitale transformatie.

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.

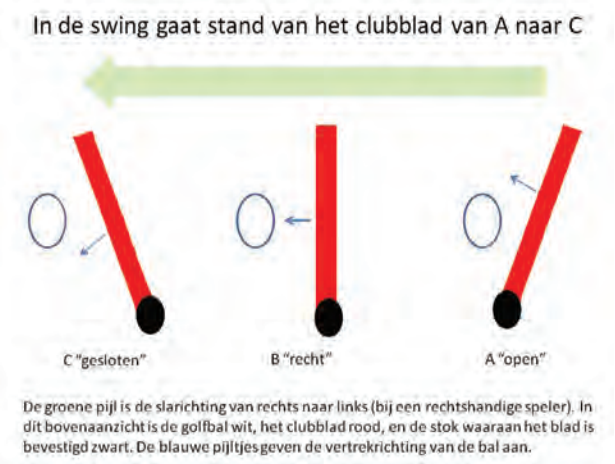
BLOG

Een betere golfswing voor security officers

Ook op de golfbaan kun je als security officer iets leren over het geven van doeltreffend (= effectief) security advies

Na hun succes als tv-actrice werden Annika Settergren en haar bekendere buurvrouw Pippilotta Viktualia Rullgardina Krusmynta Efraimsdotter Långstrump lid van onze golfvereniging. Wij mogen Pippi zeggen, al reageert ze – kribbig – ook op 'Rolgordijn'. Afgelopen vrijdag hadden zij bardienst. Ik zat met een alcoholvrij biertje aan de bar de ledenadministratie bij te werken en met Pippi te flirten. Rond 10 uur kwam ex-politiecommissaris Rob binnen. Besmet met het golfvirus en veel vrije tijd en 'niet onbemiddeld' is hij de vleesgeworden droom van alle lesgevende golfpro's.

Rob ging naast mij zitten en begon te huilen. Pippi, Annika en ik wisten meteen: hij had weer slecht gespeeld. Beide dames knikten zwijgend naar mij ten teken dat ik het deze keer moest vragen. Dat deed ik en Rob begon zijn relaas. "Voordat ik gisteren mijn rondje ging lopen, wilde ik inslaan op de driving-range. Ik tapte een emmertje oefenballen, legde een bal klaar en nam mijn favoriete driver." Ik fronste en Rob zag het. Hij wist drommels goed dat we op onze club bij het inslaan altijd begonnen met de kortere stokken met een schuiner geplaatst blad. Door telkens een langere stok te nemen, kom je via een serie steeds vlakker wordende boogballen, uiteindelijk bij de 'drivers': de lange jongens met een vrijwel vlak blad waar je wel 150 meter ver mee kunt slaan. Ik liet het gaan, want hij had verdriet. Rob dronk van zijn alcoholische versnapering en zei schuldbewust dat hij even die lekkere 'ping' moest horen, de droge knal als je de bal precies goed raakt. "Ik raakte hem goed en hij vertrok mooi, maakte een boog naar rechts en kwam terecht op het paadje waar net een motoragent passeerde. De bal raakte de achterkant van de helm van de agent. De agent schrok en viel. Achter hem reed met hoge snelheid een ambulance met daarin twee gewonde kinderen die de



De groene pijl is de slarichting van rechts naar links (bij een rechtshandige speler). In dit bovenaanzicht is de golfbal wit, het clubblad rood, en de stok waaraan het blad is bevestigd zwart. De blauwe pijltjes geven de vertrekrichting van de bal aan.

agent naar het ziekenhuis escorteerde. De chauffeur ontweek de agent, maar de ambulance kwam deels in de sloot terecht. In de andere richting was een brandweerauto op weg naar een brand in een boerderij. Die brandweerauto botste tegen de ambulance en kon niet verder rijden. Andere hulpdiensten konden met hun auto's de ravage niet bereiken, waardoor de kinderen met hun botbreuken in de brandweergreep weggedragen moesten worden. De boerderij is geheel afgebrand omdat de brandweer er te laat was. Ik ben ten einde raad. Wat moet ik in vredesnaam doen?" Ik vroeg zakelijk: "Op het ballenpad, is dat niet vreemd een ambulance daar? Vind je het ook niet toevallig dat er tegelijkertijd een brandweerauto rijdt? Was het de sloot van boer Harms en was die brand ook bij hem?" Ja, ja, ja, ja, ja knikte Rob. Hij nam een slok en snikte. Annika was al aan het schrijven op de blanco achterkant van een bestelblocnoteblaadje. Daarna las ze haar advies voor:

1. Alle motoragenten krijgen aanvullende rijvaardigheidstraining gericht op omgaan met schrikreacties;
2. Helmen worden aan de buitenkant voorzien van schuimrubber;
3. Aan het begin van het paadje komt een waarschuwingsbord m.b.t. golfballen. Voorafgaand aan de plaatsing, is er een nulmeting onder passanten of ze weten dat er bij een golfbaan soms ballen over het hek komen. Na plaatsing van het bord opnieuw meten en meetresultaten vergelijken;
4. Op het paadje is er voortaan eenrichtingsverkeer om tegemoetkomend verkeer, zoals nu de brandweerauto, te vermijden;
5. Bij motorescortes moet voortaan 30 meter afstand tot de motor(s) worden gehouden. Bij hoge snelheid meer, om tijdig te kunnen remmen;
6. Er komt een geautomatiseerd systeem dat voortdurend nauwkeurig de locatie bepaalt van alle hulpdienstvoertuigen en met licht- en geluidsignalen waarschuwt wanneer voertuigen elkaar (met grote snelheid) naderen. Liefst met een app.

Dat zou de risico's behoorlijk mitigeren, aldus Annika, die dit niet ter plekke verzon. Ze paste gewoon de maatregelen tegen 'Business Email Compromise' incidenten toe, die ze in haar werk als information risk manager al had bedacht. Opleiding, mailfiltering, waarschuwingen aan gebruiker bij mail uit externe bron, functiescheiding aanscherpen zodat social engineering via phishing minder kwaad kan, continue monitoring op incidenten inregelen. U kent het wel.
Rob keek opgelucht naar Annika en dronk zijn glas leeg. Pippi stopte met het politoeren van de wijnglazen en zei: "Je moet aan je grip werken Rob. Stop nou eens met zo hard in je stok te knijpen."

Advies

Wees als security officer in je adviezen Pippi en niet Annika. Geef dus een op 'root cause analysis' gebaseerde raad. Motiveer je cliënt tot effectieve gedragsverandering door de oorzaak aan te pakken, in plaats van alleen technische oplossingen of provisorische lapmiddelen te noemen.

De clou van Pippi's advies

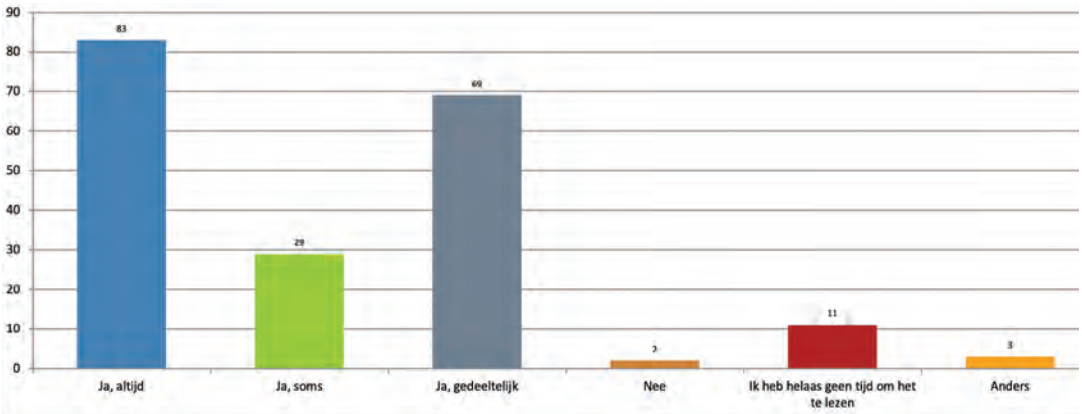
Bij het begin van de golfswing brengt een rechtshandige speler de club (de stok, niet de vereniging) naar achter boven de rechterschouder. Stand van het clubblad (niet het maandelijkse boekje met wedstrijden en jubilea) is 'open' (zie A in de figuur). Tijdens de swing naar de bal draait het blad naar 'recht' (zie B). Zo moet de bal geraakt worden om deze recht vooruit te slaan. Hou na het raken van de bal niet in, maar sla door, zodat de club doorswingt tot over je linkerschouder heen. Aan het eind van de swing is het blad 'gesloten' (zie C). Het gaat bij de golfswing niet om kracht, maar om opgebouwde snelheid en precisie bij het raken en de juiste souplesse in de draai van de stok. Knijp je te hard in de stok, dan beweeg je te stijf en is het blad (nog) te open wanneer je de bal raakt. De bal gaat naar rechts, soms met een curve. Knijp je te zacht, dan draait het blad teveel door en raak je de bal te 'gesloten' (zie C). Daardoor gaat de bal naar links. Je 'grip' bepaalt of je recht op je doel afgaat.

Uitslag lezersenquête iB-Magazine

Begin dit jaar hebben we PvIB-leden gevraagd een enquête in te vullen. Bijna 200 leden hebben de tijd en moeite genomen om dat te doen. Dat is een mooi resultaat en we willen via deze weg graag alle deelnemers hartelijk bedanken. De antwoorden op de vragen in de enquête zijn voor ons als redactie heel waardevol. De mening van onze lezers telt mee met redactionele beslissingen over de thema's van artikelen, maar het helpt ook bij onze langetermijnstrategie, zoals bijvoorbeeld de keuze of we het blad op papier blijven uitgeven of dat we de frequentie van verschijning moeten aanpassen.

Diverse groep lezers

We leerden van de enquête dat de meeste respondenten vooral PvIB-lid zijn om praktijkkennis op te halen. Artikelen met praktijkvoorbeelden worden dan ook goed gewaardeerd. De meeste respondenten (92%) lezen het magazine ook daadwerkelijk (al dan niet



Figuur 1 - Lees je iB-Magazine?

soms of gedeeltelijk). Uit de verschillende reacties van de lezers blijkt dat men soms de artikelen wat te diep vindt gaan, terwijl andere lezers juist weer vinden dat het wat dieper en technischer mag. Een enkeling vindt de artikelen te veel open deuren en bekende onderwerpen behandelen terwijl er ook lezers zijn die juist vragen om wat meer artikelen over de beginselen van informatiebeveiliging. We hebben dus te maken met een diverse groep lezers die zich op verschillende momenten van hun carrière bevinden: van student tot gepensioneerde CISO.

Verschijningsvorm en frequentie

Wij brengen het blad in gedrukte vorm uit en als pdf op de website. 41% van onze lezers leest liever de digitale versie omdat ze dat makkelijker vinden om mee te nemen en makkelijker vinden lezen. Iets minder dan een derde van onze lezers leest de papieren versie van het blad, om exact dezelfde redenen.

Figuur 2 - Hoe wil je het blad ontvangen?

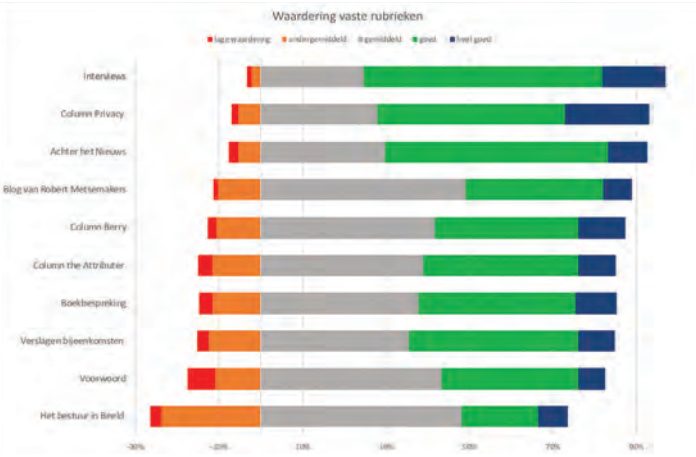
64% van de lezers vindt zes magazines per jaar een goede frequentie, 21% vindt vier keer per jaar wel genoeg. Er is weinig steun voor meer dan zes magazines per jaar. Het merendeel van de lezers ontvangt het blad graag ook digitaal. Uit de enquête blijkt ook dat de 'concurrentie' (andere media die onze leden lezen) van iB-Magazine zich vooral online bevindt. Daarom gaat de redactie met ons bladmanagement (MOS uit Nijkerk) en in overleg met het PvIB-bestuur verkennen of een digitale vorm meer functionaliteit biedt dan de huidige pdf-versie. Op dit moment zien we geen reden om de huidige vorm en frequentie al aan te passen.

Waardering onderwerpen

Er is een redelijke balans tussen de waardering voor het type artikelen: BCM/crisismanagement, awareness, management, privacy, techniek. Techniek wordt het vaakst gekozen (23%) en BCM het minst vaak (15%), maar het verschil is niet zo groot. De enquête was gehouden voor de covid-19 situatie, dus wie weet of BCM vandaag de dag hoger zou scoren… Slechts 9% van de lezers vindt de onderwerpen regelmatig of meestal niet interessant. De reacties zijn wisselend positief wat betreft de aansluiting bij het dagelijks werk. Van de vaste rubrieken worden de interviews het hoogst gewaardeerd, gevolgd door de Privacycolumn (die wel het beste scoort in de 'heel goed' categorie) en Achter het Nieuws.

Gevarieerd aanbod

De wisselende reacties op de artikelen die aansluiten bij het dagelijks werk en bij de kennisbehoefte zijn te verwachten, gezien de diversiteit van het vakgebied en de beroepen daarbinnen en de



Figuur 3 - Waardering per vaste rubriek.

verschillen tussen leeftijd en ervaring van onze lezers. Wij proberen als redactie dan ook een divers aanbod aan artikelen te bieden die gaan over praktijkervaringen maar soms publiceren we ook onderzoek of theorie. Voor de redactie is het zaak om de balans te vinden tussen praktijk, theorie, diepgang en innovatie. Daarnaast moeten we oog blijven houden voor verschillende thema's binnen het vakgebied. Dit kan ertoe leiden dat we themanummers uitbrengen over actuele onderwerpen, maar we moeten er tegelijkertijd voor zorgen dat de andere uitgaven een gevarieerd aanbod aan onderwerpen bieden. Tenslotte hebben we lezers die zich in verschillende fases van hun carrière bevinden. Bijvoorbeeld onze studentleden die we recent aan ons lezersbestand hebben mogen toevoegen. Voor en door hen hebben we nu een nieuwe vaste rubriek over afstudeerscripties. Wij hopen hiermee ook de lezers te bedienen die zoeken naar nieuwe ideeën of zienswijzen omdat studenten regelmatig een voor ervaren mensen bekend onderwerp met een verrassende blik benaderen.

Meeschrijven

We zijn enorm blij met de 49 mensen die hebben aangegeven een keer een artikel te willen schrijven. Een enkeling heeft echter geen contactgegevens achtergelaten, dus kunnen wij als redactie niet alle enthousiaste schrijvers persoonlijk benaderen. Maar voor iedereen die interesse heeft om ook een artikel of blog te publiceren: op de website van het PvIB staan de planning en de auteursinstructies. En bij vragen kun je ons altijd een bericht sturen. Goed om te weten is dat je per gepubliceerd artikel ook PE-punten ontvangt.
Denk je bij het lezen van dit alles: ik heb ook nog heel veel goede ideeën voor iB-Magazine en ik vind het ook leuk om auteurs te begeleiden? Naast nieuwe artikelen is een extra redactielid (liefst tweetalig Engels-Nederlands) ook van harte welkom, dus neem contact met ons op! (ibmagazine@pvib.nl)

Auteurs: Tom Bakker is redacteur van iB-Magazine. Tom is te bereiken via tombakker@pvib.nl Sandra Kagie is freelance tekstschrijver/-journalist. In het verleden is zij als eindredacteur nauw betrokken geweest bij iB-Magazine. Zij is te bereiken via info@sanscriptproducties.nl.

INTERVIEW

Advies 2020 Data Breach Investigations Report:

‘Deel je datalekken en incidenten’

Gabriel Bassett.

43% van het aantal datalekken wordt veroorzaakt door aanvallen op webapplicaties. Het is voor hoofd data-analist en co-auteur van het onlangs gepresenteerde 2020 Data Breach Investigations Report (DBIR), Gabriel Bassett, de meest opvallende uitkomst van het jaarlijkse onderzoek naar datalekken door Verizon. “Aanvallers follow suit”, concludeert hij.

“We doen met zijn allen steeds meer zaken online, bedrijfskritische werkprocessen worden naar de cloud verplaatst, het is dus logisch dat ook cybercriminelen steeds meer hun weg vinden naar de cloud”, legt Bassett uit. Wat volgens hem opvalt, is dat cybercriminelen voor dergelijke aanvallen geen kwetsbaarheden in webapplicaties nodig hebben. In meer dan 80% van de aanvallen werd namelijk gebruikgemaakt van gestolen of ‘brute forced’ inloggegevens. “Kwetsbaarheden zijn vaak al gepatcht,” geeft hij aan.

Belangrijke waarschuwing

De onderzoekers stellen in het rapport dat het niet zozeer cloudsecurity is die faalt. Nee, ze zien de toename van dit soort datalekken veel meer als een illustratie van het feit dat cybercriminelen steeds weer de snelste en gemakkelijkste route naar hun slachtoffers weten te vinden. Een belangrijke waarschuwing, zeker in het licht van de toename van het aantal thuiswerkers als gevolg van de coronacrisis. En let wel, dit rapport gaat nog over de periode vóór corona wereldwijd toesloeg. “Naarmate het werken op afstand toeneemt vanwege de wereldwijde pandemie, wordt end-to-end-beveiliging van de cloud naar de laptop van de werknemer van cruciaal belang”, zegt Tami Erwin, CEO van Verizon Business bij de presentatie van het 2020 DBIR eind mei jl. “We dringen er bij alle bedrijven op aan om niet alleen hun systemen tegen aanvallen te beschermen, maar ook hun werknemers te blijven voorlichten. Phishing-methoden worden namelijk steeds geavanceerder en schadelijker.”

Phishing blijft populair

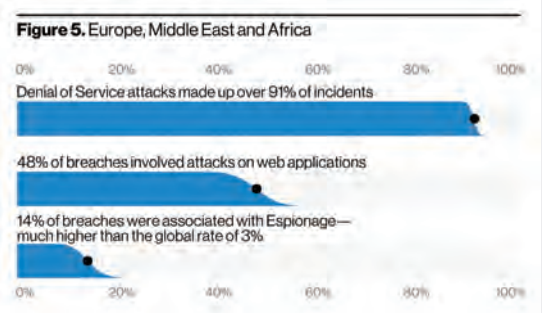
Phishing is en blijft volgens het onderzoek een vruchtbare aanvalsmethode voor cybercriminelen. De meest voorkomende oorzaken (meer dan 67%) van alle datalekken zijn diefstal van inloggegevens, fouten en social engineering-aanvallen, zoals phishing. Maar er is goed nieuws: de ‘click rates’ waren nog nooit zo laag! Uit phishingtesten blijkt

2020 DBIR: achtergrond

Om te komen tot het 2020 DBIR, alweer de 13e editie van het onderzoek, heeft een team van analisten, onder wie Gabriel Bassett, 157.525 aan security gelinkte incidenten bekeken. Hiervan bleek het in 32.002 gevallen te gaan om veiligheidsincidenten, waarvan 3.950 bevestigde datalekken. Bijna een verdubbeling ten opzichte van de 2.013 vorig jaar geanalyseerde datalekken.

Wie zijn de slachtoffers? Wie zit er achter de cyberaanvallen? Welke tactieken gebruiken cybercriminelen? Slechts een aantal van de vragen die de onderzoekers in het jaarlijkse rapport beantwoorden. Want, zo stellen zij: "The more you know about the threats you face, the better your chances of keeping your data secure and your name out of the headlines."

Dit keer is het DBIR gebaseerd op het onderzoek van incidenten afkomstig van 81 bijdragers uit evenzoveel landen. In het rapport wordt een uitsplitsing gemaakt in zestien sectoren, waaronder:



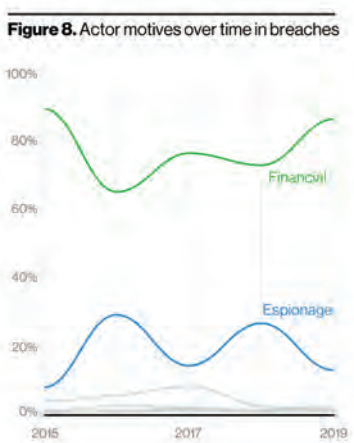
Afbeelding 2 - Europe, Middle East and Africa (Bron: 2020 DBIR Executive Summary).

de bouw, financiële sector, gezondheidszorg, onderwijs en de maakindustrie. Ook wordt een grove regionale analyse gemaakt. Hierbij worden Europa, het Midden-Oosten en Afrika als één regio beschouwd. Benieuwd wat de bevindingen zijn van de onderzoekers over bijvoorbeeld de sector waar jij in werkt? Het volledige 2020 Data Breach Investigations Report is beschikbaar via Verizon (1).

volgens Bassett namelijk dat nog maar 3,4% van de ontvangers klikt op een foute link. Wel is er wat hem betreft nog ruimte voor verbetering als het gaat om het melden van phishing: "Op dit vlak zien we in phishingtesten een stijgende lijn, maar niet zo'n snelle stijging als je zou wensen." Veruit de meest voorkomende phishingmethode is nepmail. Slachtoffers van phishing worden in 96% van de gevallen benaderd via een e-mail die afkomstig lijkt te zijn van een CEO of een andere leidinggevende. In de mails wordt volgens de onderzoekers steeds vaker direct gevraagd om een bedrag over te maken. De stap om bepaalde persoonsgegevens op te vragen wordt overgeslagen. "Why waste time with monetizing data?", lijkt het devies.

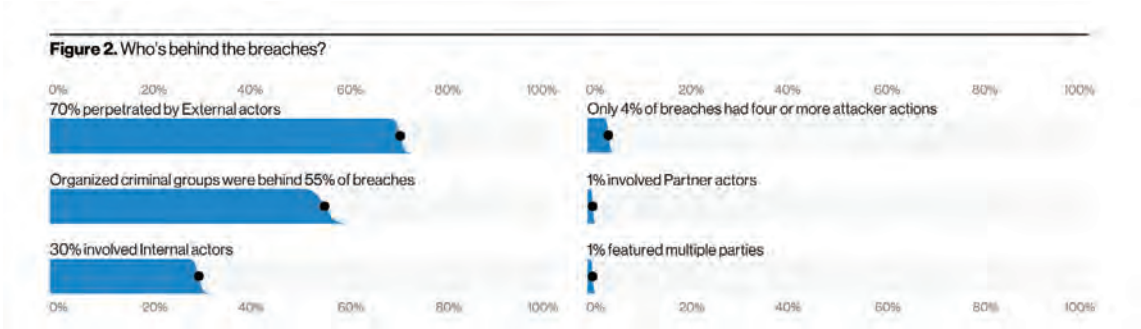
Geld, geld, geld

Money, money, money, is dé drijfveer van cybercriminelen. 86% van de datalekken was gericht op financieel gewin, zo blijkt uit het DBIR. In 2019 was dit nog 71%. Misschien wel de belangrijkste conclusie die je uit het rapport kunt trekken: de wereld van cybercrime draait nog altijd om geld. Bassett: "Ben je als organisatie dus bewust van wat je aan interessante 'waar' in huis hebt." De financiële drijfveer is sowieso



Afbeelding 3 - Actor motives over time in breaches (Bron: 2020 DBIR Results and analysis).

de belangrijkste trend die je volgens hem kunt afleiden uit de DBIR-rapporten van de laatste jaren. "Attackers try to make a buck", is de formulering die hij gebruikt. "En spionage komt dus veel minder voor dan je wellicht zou denken als je kranten, films en tv-series moet geloven."



Afbeelding 4 - Who's behind the breaches? (Bron: 2020 DBIR Executive Summary).

Dat veel aanvallers uit zijn op een 'easy buck' blijkt volgens Bassett bijvoorbeeld ook uit het feit dat het aantal gevallen van ransomware nog steeds toeneemt. Als er malware wordt aangetroffen gaat het in 27% van de gevallen om ransomware, tegenover 24% een jaar geleden. "Aanvallers hoeven als het om ransomware gaat niet eens over enige kennis op het gebied van IT of security te beschikken", geeft hij aan. "Ransomware-as-a-service is alom beschikbaar: superefficiënt, want directly moneytisable". Een groot probleem dat nog altijd groter wordt, zo waarschuwen de onderzoekers.

Be prepared to be imperfect

Een wijdverspreid misverstand dat door het onderzoek wordt ontkracht, is dat cyberaanvallen vaker van binnenuit dan van buitenaf plaatsvinden. Uit het onderzoek blijkt namelijk dat 70% van de datalekken wordt veroorzaakt door mensen van buitenaf. Grotendeels georganiseerde criminele groeperingen. Zij zitten achter 55% van alle datalekken.

Opvallend is wel dat de DBIR-onderzoekers een groot aantal datalekken hebben gevonden die terug te leiden zijn tot fouten van interne medewerkers. 881 tegenover 424 in het rapport van vorig jaar. "Errors definitely win the award for best supporting action this year", zo lezen we. Dit heeft volgens Bassett echter veel meer te maken met het feit dat fouten eerder en vaker worden gemeld, dan dat medewerkers méér fouten maken. Daarbij stelt hij 'is er bij het merendeel van de interne fouten géén kwade opzet in het spel'. Hij adviseert organisaties dan ook medewerkers zo goed mogelijk te faciliteren en hen te helpen hun werk te doen in een omgeving die het maken van fouten toestaat. "Be prepared to be imperfect", stelt hij. Dit door een omgeving te creëren waarin het toegeven van fouten de norm is en niet de uitzondering, omdat iemand ervoor wordt afgestraft. "Niemand is perfect. Bereid je dus voor op fouten, los ze vervolgens op, voorkom ze en ga samen verder. Don't overreact otherwise you get stuck in a blame game", waarschuwt hij.

Asset management

Een tweede belangrijke security tip die Bassett organisaties wil geven, heeft te maken met gedegen asset management. Hij noemt het 'the key issue to manage vulnerabilities'. Want, hoewel patching als het gaat om bekende kwetsbaarheden lijkt te werken - minder dan 5% van de datalekken wordt veroorzaakt door het misbruik van zo'n kwetsbaarheid, zo blijkt uit het onderzoek - kunnen grote problemen binnen organisaties door een gebrek aan gedegen asset management verborgen blijven. De crux zit volgens Bassett binnen veel organisaties in het ontbreken van een continu up-to-date inzicht in alle IT-assets. Wanneer een (klein) deel van de assets niet bekend is, de zogenoemde shadow IT, worden deze nooit gepatcht, en vormen ze dus de zwakke schakel. Niet alleen voor nieuwe kwetsbaarheden, maar juist ook voor oude. "Find the forgotten assets and provide the basics", benadrukt hij.

'Defender's advantage'

Gevraagd naar een overall advies voor organisaties kan Bassett kort zijn. "We hebben allemaal te maken met dezelfde issues. Dus focus op de basis, 'the obvious stuff': basic firewalls, basic antivirus en patching. En gebruik het gebrek aan verandering dat we zien in de wereld van cybercrime in je voordeel. Dit door te kijken naar het soort aanvallen en aanvalstactieken die het meest voorkomen. Zo kun je als potentieel slachtoffer een 'defender's advantage' creëren." Een laatste hartenkreet van Bassett is: "Collect your own breaches", oftewel: "Deel informatie over incidenten en lekken binnen een branche en/of regio met elkaar. Alleen zo kom je samen tot een steeds beter antwoord op cybercrime."

Referentie

(1) https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Valuable

The Attributer previously visited this attribute in 2013, following the 2007-8 global financial crash. People were asking "Where did all the money go?" "Who's got the money now?" There never was any money – only accounting entries in ledgers associated with real estate assets to underpin the valuations in a free market. You can find a more detailed description at https://sabsa.org/the-attributers-blog-valuable/.

In the original article we considered the possibility of the so-called 'carbon bubble' bursting, with the owners of fossil fuel reserves not yet extracted, being unable to materialize their book value because international governments might reach an accord on global warming that would ensure that those energy reserves would stay in the ground.

That event has not occurred, but who would have believed that on April 20th, 2020 the price of some crude oil would drop below zero when in January it had been in the region of $60 per barrel? Oil price had at one time been the marker of economic success; now it had become trash you would pay to have removed. How could that happen?

The underlying threat was the Covid-19 pandemic. Infection control measures curtailed all travel both locally and internationally and saw the civil aviation industry battered almost into non-existence. If no one is flying, then no one needs aviation fuel. The impacts of Covid-19 have also been intense in other industry sectors. The global economy will take a long time to recover from this interruption and at the time of writing no one is clear what the 'new normal' will look like, other than it will be very different from the 'old normal'. In true SABSA risk management style this 'threat' will offer huge opportunities for some parties.

Meanwhile the Attributer has been researching for a white paper on 'zero-trust architecture'. This turns out to be synonymous with 'data centric architecture'. The outcome of this line of enquiry is that there is an expectation that the 'new normal' will emerge with basic underlying asset values derived from new sources – not oil, not real estate, not staple foods and not clean water. The talk on the street is about the value of data and a future data-economy.

Every other type of asset is evaluated by the data that describes it. Its provenance, its quality, who owns and controls it are all attributes of data that contribute to its value. Data is emerging as the new meta-currency that describes the value of all other asset types. Whereas once the US dollar held that position, now you would question the value of a dollar by asking about the data that describes the US economy that underpins the dollar value.

All asset values are ultimately derived on a 'mark to market' basis, meaning how much will a buyer pay for this asset when it is offered for sale in an open market. Those who trade such assets are increasingly sophisticated in the ways that they can capture and analyze the data that forms the meta-currency behind all asset values. Why did the price of oil plummet on April 20th, 2020? Because all the market data relating to the demand for oil showed that the suppliers needed to shift it onto the market where it could be sold, and their stockpiles reduced.

Business analysts have been telling us for a long time that the value of data is such that it needs to be protected from threats such as theft, loss, destruction, fraudulent representation and many more such outcomes. The Attributer believes that these warnings have not been taken entirely seriously. They have been seen only as an illustrative comparison of real asset value. Now we begin to perceive that the analysts were not being loose with their language – they understood that data really is the new meta-currency, replacing the likes of oil and real estate.

Perhaps investors thought that if this type of global crisis materialized, they would have time to get out as the market peaked. But, as we pointed out in 2013, not everyone can get through the exit at the same time because sellers need buyers, and most will fail because the collapse will be very quick. In the three months between mid-January 2020 and mid-April 2020 some oil prices fell more than 120%. Maybe the world with its emerging data-economy needs a bit more SABSA thinking injected into it.

The Attributer

Auteur: Sander Ebbers is docent-onderzoeker aan de Onderzoeksgroep Cybersafety van NHL Stenden Hogeschool en promotieonderzoeker aan de Open Universiteit. Sander is te bereiken via sander.ebbers@nhlstenden.com of 06-11231807.

De waarde van meldgedrag voor digitale weerbaarheid

Inzicht in kwetsbaarheden voorkomt potentiële incidenten. Daarvoor is een organisatie voor een groot deel afhankelijk van het meldgedrag van medewerkers. Meldgedrag draagt bewezen bij aan een weerbare organisatie als het gaat om fysieke veiligheid (1). Maar kan meldgedrag ook waardevol zijn als het gaat om digitale veiligheid? Kan het potentiële security-incidenten en datalekken voorkomen?

Als we spreken over meldgedrag kunnen we grofweg twee categorieën onderscheiden. Categorie één bevat preventief meldgedrag van kwetsbaarheden (2). Kwetsbaarheden kunnen o.a. veroorzaakt zijn door de melder zelf, de werkgever, een kwetsbaarheid in een systeem of een samenspel van deze factoren. Denk hierbij aan een medewerker die per ongeluk bestanden onveilig deelt, opmerkt dat bestanden niet conform beleid geclassificeerd worden, of opmerkt dat een groot deel van de collega's het scherm niet vergrendelt bij het verlaten van de werkplek. Dit gedrag hoeft niet per definitie te leiden tot een incident, maar het melden leidt wel tot extra bescherming van de organisatie en kan dus worden aangemerkt als preventief gedrag.

Categorie twee omvat al het gedrag dat we kunnen definiëren als reactief meldgedrag, oftewel naar aanleiding van confrontatie met een dreiging, met een incident tot gevolg (3). Het bekendste voorbeeld is wanneer een medewerker slachtoffer is geworden van phishing en dit meldt. Een ander voorbeeld is een medewerker die vaststelt dat hij heeft meegewerkt aan een dubieus telefonisch verzoek door een onbekende beller.

Het kan voorkomen dat vermeend preventief meldgedrag, reactief gedrag blijkt te zijn. Preventief meldgedrag kan in sommige gevallen bijvoorbeeld een 'gemist' datalek aan het licht brengen en is daarmee in feite reactief meldgedrag. Daarnaast zorgt reactief meldgedrag regelmatig voor preventief gedrag. Denk bijvoorbeeld aan een medewerker die een phishingaanval meldt en er daarmee voor zorgt dat andere collega's preventief maatregelen kunnen nemen, door de phishingmail te verwijderen.

Meldgedrag interessant voor digitale weerbaarheid

Allereerst geeft meldgedrag van medewerkers inzicht in de kwetsbaarheden op de werkvloer. Niet alle risico's kunnen goed in beeld worden gebracht door systemen of procedures (4). Meldgedrag brengt dus risico's in kaart die waarschijnlijk anders minder snel (of te laat) aan het licht waren gekomen. Ten tweede versterkt meldgedrag het lerend vermogen van een organisatie, met name wanneer er een focus is op preventief meldgedrag (2). Meldingen van medewerkers zijn namelijk goede indicatoren van kwetsbare processen, procedures of applicaties waar potentieel incidenten kunnen plaatsvinden. Een derde argument dat meldgedrag interessant maakt, is dat het de medewerker maakt tot sterke schakel in het beveiligingsproces. Dit in tegenstelling tot het monitoren van medewerkersgedrag door technische monitoringsystemen. Monitoring gaat vaak uit van de medewerker als zwakste schakel. Meldgedrag doet het tegenovergestelde; het zorgt dus voor een werkgever-werknemer-relatie die meer in balans en volwassen is. Medewerkers appreciëren het dat ze als waardevolle actor worden gezien in een vitaal bedrijfsproces.

Voorwaarden meldgedrag

Zo'n rol voor medewerkers klinkt ideaal, maar meldgedrag veronderstelt een aantal essentiële voorwaarden. Ten eerste hebben alle betrokken medewerkers bepaalde basiskennis en basisvaardigheden nodig om cyberrisico's te kunnen herkennen (5). De samenleving wordt steeds meer 'techsavvy' en veel mensen zijn zich daarmee ook meer bewust van cyberrisico's op de werkvloer. Het verschilt nog wel sterk per sector hoe 'volwassen' het kennisniveau is (6). De tweede voorwaarde is dat de werknemer gemotiveerd moet zijn om kwetsbaarheden te melden bij de werkgever. De werknemer moet het idee hebben dat melden bijdraagt aan het weerbaar maken van de organisatie en moet bereid zijn hier, buiten de functieomschrijving om, extra moeite in te steken, en daarmee een stap extra te zetten voor de werkgever. Het lijkt hierbij dus belangrijk te zijn in hoeverre een werknemer zich verbonden voelt, zich gewaardeerd voelt en tevreden is met de werkgever (7). Daarnaast, en dat is voorwaarde drie, moet de werkomgeving van de werknemer meldgedrag stimuleren. Dit betekent enerzijds dat het een medewerker eenvoudig moet worden gemaakt om kwetsbaarheden en dreigingen te melden. Anderzijds is er ook een faciliterende meldcultuur nodig. Geeft de directe leidinggevende bijvoorbeeld blijk dankbaar te zijn voor gemelde kwetsbaarheden? Durven collega's elkaar aan te spreken op risicovol gedrag? En wordt meldgedrag beloond (8)?

Promotieonderzoek naar meldgedrag

Meldgedrag kan bijdragen aan een digitaal weerbare organisatie en er zijn potentiële voorwaarden die meldgedrag bevorderen. De genoemde voordelen en voorwaarden zijn in de context van informatiebeveiliging (nog) niet wetenschappelijk onderzocht. Allereerst is meer inzicht nodig in welke kenmerken van een organisatie, een team of een individu preventief en reactief meldgedrag bevorderen en belemmeren. Vervolgens moet onderzocht worden of, hoe en wanneer deze kenmerken te beïnvloeden zijn met als doel om de digitale weerbaarheid van organisaties te versterken. Met mijn promotieonderzoek zal ik een bijdrage gaan leveren aan het beantwoorden van deze vragen.

Geïnteresseerd om verder te praten over meldgedrag en kennis uit te wisselen? Neem dan contact met mij op!

Referenties

(1) Hofmann, Burke & Zohar (2017)
(2) Bair, Bellovin, Manley, Reid & Shostack (2018)
(3) Heartfield, Loukas & Gan (2017)
(4) Oltramari, Henshel, Cains & Hoffman (2015)
(5) Cain, Edwards & Still (2018)
(6) Nederlandse Cybersecurity Agenda (2018)
(7) Culiberg en Mihelič (2017) en Pfeiffer, Manser en Wehner (2010)
(8) Cox, Jones en Collinson (2006)

Auteur: Evert van Zanten is bestuurslid en te bereiken via evertvanzanten@pvib.nl.

Mede mogelijk gemaakt door het PvIB

Een veilige digitale samenleving, mede mogelijk gemaakt door het PvIB. Dat klinkt niet alleen stoer maar is het ook. Want als er iets is waar we allen individueel dagelijks mee bezig zijn, is het wel het verhogen van de veiligheid van onze organisaties en daarmee ook onze samenleving. Dit heeft geleid tot meer zichtbaarheid en erkenning van onze rol als kennisorganisatie en daardoor tot betrokkenheid bij een aantal landelijke samenwerkingsverbanden.

Dit is niet alleen van belang vanuit onze maatschappelijke ambitie maar ook relevant in de belangenbehartiging van onze beroepsgroep, het werkveld en de toekomst daarvan. Inmiddels zijn we actief bij de Cyber Security Alliantie (CSA) en de Online Trust Coalitie (OTC), hebben we een bijdrage geleverd aan de Nationale Cyber Security Educatie (NCSE) Agenda van dcypher en worden er op individuele basis gastcolleges gegeven op diverse onderwijsinstellingen. De laatste spreken voor zich maar de CSA en OTC behoeven wat nadere uitleg waaruit ook blijkt dat we inmiddels met de meeste relevante partijen in ons vakgebied verbonden zijn.

Cyber Security Alliantie

De CSA biedt partijen een netwerk om samen te werken aan een digitaal weerbaar Nederland. Zij ondersteunt de projecten met kennis en kunde van de aangesloten organisaties en verbindt partijen in de publiek private samenwerking. In de CSA vertegenwoordigen wij een rol als kernadviseur en nemen wij deel aan de coördinatiegroep. Tevens zijn wij in drie werkgroepen vertegenwoordigd. Naast het PvIB zijn onder meer VNO-NCW, Bol.com, NCTV, NCSC, ECP, Booking.com, PostNL, OM, Rabobank, Siemens, CIO-Platform, DTC, Cyberveilig Nederland, Deloitte, Philips en Microsoft aangesloten.
Als kernadviseur hebben wij mede een stem in de keuze voor projecten die door de CSA worden uitgevoerd of ondersteund. Draagt het project concreet bij aan de cyberweerbaarheid van Nederland en is het haalbaar? Heeft het voldoende urgentie? Zijn er al vergelijkbare initiatieven of vult het project deze juist aan? Die rol geeft ons de mogelijkheid projecten in te brengen en mee te doen aan projecten die wij belangrijk vinden vanuit onze vereniging.
Op dit moment zijn er drie werkgroepen gestart waaraan wij deelnemen:

1. Cybersecurity Landschap
De thematische werkgroep 'Het Nederlandse Cybersecurity Landschap' heeft tot doel om tegemoet te komen aan de grote wens van het netwerk om een overzicht van en inzicht te bieden in de diverse landelijke initiatieven. Het doel is primair om een goed overzicht te hebben dat gebruikt kan worden om vanuit de aanbodzijde 'blank spots' te definiëren, vergelijkbare initiatieven aan elkaar te verbinden en te beoordelen of een nieuw initiatief een gewenste ruimte invult. Daarnaast is er ook een behoefte om vanuit de vraagzijde inzichtelijk te hebben waar welke kennis en kunde beschikbaar is en welke mogelijke oplossingen al in de maak zijn.

2. Cybercompas
In deze snel veranderende maatschappij is het belangrijk om digitaal weerbaar te blijven. Ontwikkelingen in het

digitale domein gaan razendsnel en de complexiteit neemt toe. Het is daarom cruciaal zicht te hebben op de uitdagingen die op ons afkomen. De basis voor dit kompas zal worden gevormd door de landelijke meerjarige vergezichten zoals o.a. het NCSE Compas. Deze worden vertaald naar een praktische handreiking voor acties op de kortere termijn.

3. Cyber Oefenen

Eén van de voornaamste redenen om te oefenen is dat de weerbaarheid van een organisatie tegen een digitale dreiging groter wordt. Een oefening helpt organisaties om beter voorbereid te zijn bij potentiële ontwrichting naar aanleiding van een incident in het digitale domein. Deze constatering is onlangs ook door de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) gedaan. Ook uit onder andere het Cyber Security Beeld Nederland (CSBN) 2019 blijkt dat er sprake is van een toenemende digitale dreiging. Door te oefenen verbetert zowel de interne als de externe samenwerking. Hierdoor wordt men in staat gesteld om snel en effectief te handelen bij een daadwerkelijk incident.

Online Trust Coalitie

Het doel van de OTC is het beschikbaar maken van een eenduidige, efficiënte methode waarmee leveranciers van clouddiensten kunnen aantonen dat hun diensten betrouwbaar en veilig zijn. En die methode helpt bij het invulling geven aan de relevante wet- en regelgeving.

Veiligheid, beschikbaarheid en privacy zijn daarbij belangrijke aandachtspunten, maar niet de enige. Ook zaken als het snel weer kunnen opstarten van een dienst na een incident en transparante toedeling van verantwoordelijkheden wanneer meerdere aanbieders betrokken zijn bij een dienst, spelen een rol.

De OTC is een samenwerkingsverband van leidende nationale en internationale partijen, zowel aanbieders als afnemers van clouddiensten, betrokken overheden en experts, die zich actief bezighouden met cybersecurity, compliance, conformiteit en assurance. Het PvIB is actief onderdeel van de klankbordgroep die verder bestaat uit o.m. het Ministerie van Economische Zaken en Klimaat, directie digitale Economie, Wolters-Kluwer, TAA NL, NLdigital, Erasmus Universiteit, ISPConnect, Cyberveilig Nederland, VNO-NCW, Agentschap Telecom, NEN, FME, Autoriteit Persoonsgegevens, ECP | Platform voor de InformatieSamenleving, Zeker-OnLine, CIO Platform Nederland, NOREA, Microsoft, Nationaal Cyber Security Centrum en EY.

Op dit moment zijn er twee werkgroepen binnen de OTC gestart. Hierin leveren wij op dit moment nog geen inhoudelijke bijdrage maar dat zou wel kunnen.

1. Werkgroep Whitepaper

Vanuit de eerste OTC Klankbordgroep bijeenkomst van 11 februari jl. komt het voorstel om een whitepaper op te stellen dat oplossingen en oplossingsrichtingen schetst voor de beschreven situaties vanuit het manifest van de OTC. Het whitepaper beoogt, in de vorm van een statement, een advies te geven vanuit de coalitie naar de Nederlandse en Europese overheid, naar het bedrijfsleven en toezichthouders. Het manifest van de OTC zal op de PvIB website geplaatst worden zodra dit beschikbaar is.

2. Adviesgroep Europa

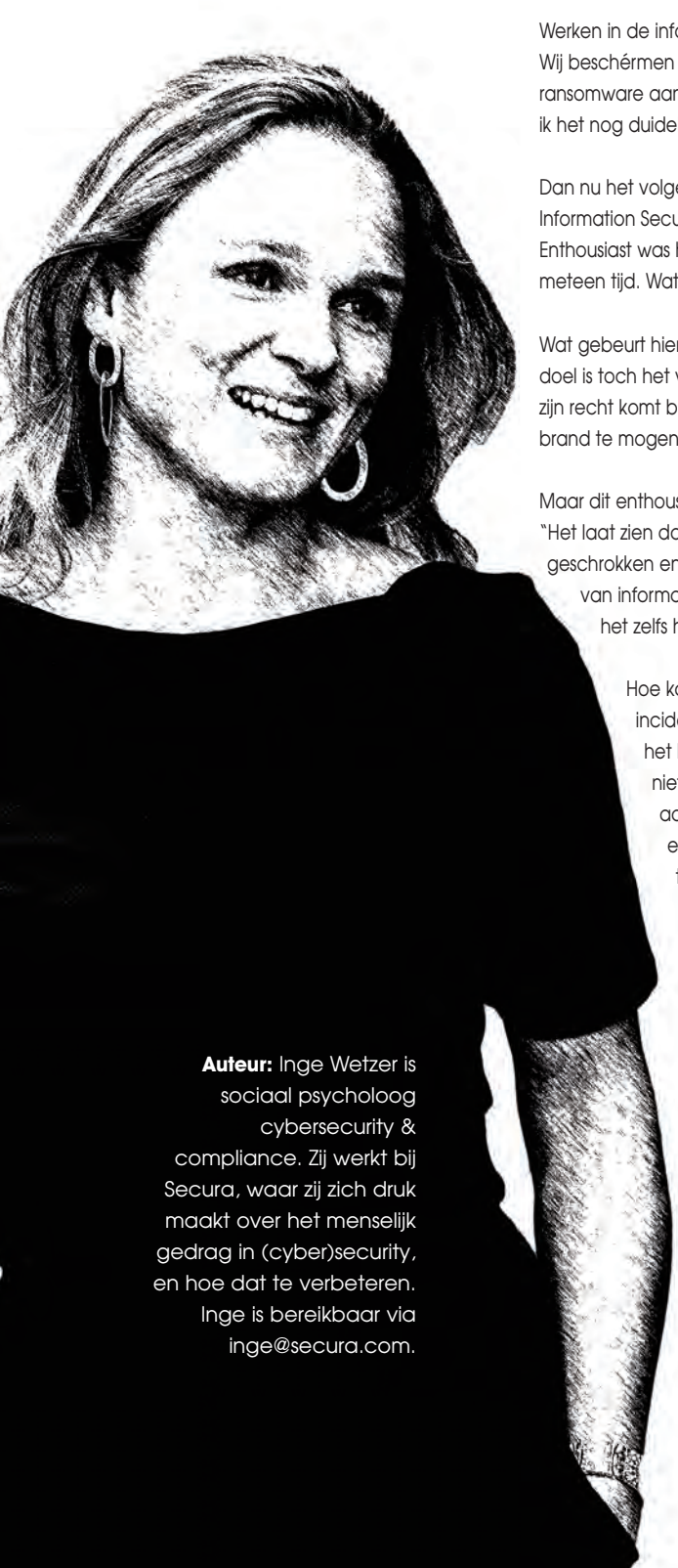
In de periode voorafgaand aan de oprichting van de OTC zijn er in het kader van het overbrengen van de Partnering Trust-gedachte binnen Europa, werkzaamheden verricht door een kerngroep. Tijdens de eerste Klankbordgroep bijeenkomst van de OTC op 11 februari jl. is voorgesteld om een advies werkgroep in te stellen. De aanname is dat er door de breedte van de OTC, de gezamenlijke inhoudelijke kennis, het brede bestuurlijk draagvlak en de voorsprong van Nederlandse stakeholders met betrekking tot thema's als certificering en assurance, een 'OTC EUROPA ADVIESGROEP' voor afstemming en harmonisering kan zorgen over de te communiceren boodschap binnen Europa voor toezichthouders, ministeries en andere gremia in Nederland. En hiermee binnen de EU-gremia (denk aan de Europese Commissie en ENISA e.a.) kan helpen richting te geven aan een eenduidige boodschap/ beleid vanuit Nederland aan het te vormen EU-beleid.

In de loop van het jaar zal er nog een inhoudelijke publicatie rond de OTC komen.

Draag inhoudelijk bij

Al deze initiatieven, onze maatschappelijke bijdrage en erkenning van het PvIB en haar leden, geven ruimte voor de leden om zichzelf te ontwikkelen en hieraan bij te dragen. Wil je graag een inhoudelijke bijdrage (kennis en tijd) leveren of meewerken aan inventarisaties in het werkveld voor één of meerdere werkgroepen bij de CSA of de OTC dan ben je van harte welkom om contact op te nemen. Daarnaast is het goed om te weten welke leden op individuele basis al maatschappelijk actief zijn vanuit ons vakgebied. Graag horen we je verhaal.

Yes! Een incident!



Werken in de informatiebeveiliging betekent dat je je bezighoudt met het voorkómen van incidenten. Wij beschérmen organisaties. Wij zorgen ervoor dat organisaties niet het slachtoffer worden van een ransomware aanval. Wij zijn ervoor verantwoordelijk dat er géén datalek komt. Oké? Ik weet niet hoe ik het nog duidelijker kan omschrijven. Wij willen géén incidenten! Eens? Ja toch?!

Dan nu het volgende: vorige week ontving ik een zeer enthousiast berichtje van de CISO (Chief Information Security Officer) van een organisatie die ik ondersteun bij hun informatiebeveiliging. Enthousiast was hij, goed nieuws had hij, of ik snel even kon bellen. Nieuwsgierig geworden maakte ik meteen tijd. Wat bleek het goede nieuws? Er was een incident! Euh...

Wat gebeurt hier nou, dacht ik (ja, met het stemmetje van juf Ank: "Ik vind dit héél bijzonder"). Ons doel is toch het voorkómen van incidenten? Is het misschien dat onze passie voor dit vak het best tot zijn recht komt bij een incident? Brandweerlieden vinden het immers toch ook mooi om naar een brand te mogen om daar te kunnen helpen?

Maar dit enthousiasme was toch van een andere soort. Dat bleek uit het vervolg van het telefoontje: "Het laat zien dat het dus écht kan gebeuren! Het is niet uit de hand gelopen, maar we zijn wel geschrokken en nemen het serieus. Hopelijk kan ik nu eindelijk...." Het incident maakte het belang van informatieveiligheid duidelijk. Het onderstreepte de reason to be van de CISO. Misschíen zou het zelfs helpen om eindelijk eens een `1' op zijn rekest te krijgen.

Hoe kan het toch dat wij – voorkómers van incidenten – regelmatig toch blij zijn met een incident? Omdat we het nodig hebben! Voor draagvlak, budget en ondersteuning van het bestuur. Helaas is het risico van slechte informatiebeveiliging voor veel bestuurders niet tastbaar, helder of reëel genoeg om er prioriteit aan te geven. Er is iemand voor aangewezen in de organisatie en daarmee is het onderwerp afgedekt. En eerlijk is eerlijk, het is een stuk lastiger uitleggen aan de board dat je investeert om dingen níet te laten gebeuren. Zeker als die dingen de afgelopen periode ook niet zijn gebeurd, dan denkt men al gauw dat het zo toch prima gaat. Risico is kans × impact. De kans wordt graag onderschat en de impact gebagatelliseerd. Dan valt het risico best mee.

Met enige regelmaat heb ik CISO's horen verzuchten dat ze eigenlijk een incident nodig hebben. Let wel, dit incident moet natuurlijk wel aan onze voorwaarden voldoen: het mag niet té groot zijn, want dan zijn de consequenties te omvangrijk. En niet te klein, want dan maakt het nog geen indruk. We willen dus graag een precies goed incident. En dan niet gesimuleerd, want dan krijgen we weer te horen dat het toch nep was en in het echt nooit zou gebeuren. En niet bij een ander, want dan wordt gezegd dat wij een heel ander type organisatie zijn en dat risico niet lopen. En met impact, zodat men even schrikt van de mogelijke gevolgen. Vandaag hadden wij geluk. Wat een geluk! Wij hadden precies het goede incident. Yes!

Inge

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

Auteur: Kimberly Hengst is werkzaam in de informatiebeveiliging en bereikbaar via hengst.kimberly@gmail.com

Best practices in cloud incident handling

Stel je voor: je werkt op de financiële administratie en je krijgt een telefoontje van een leverancier over een niet betaalde factuur. Je kijkt het na en volgens jouw administratie is deze factuur wel betaald. Je hebt namelijk een maand geleden de betaling verstuurd naar het nieuwe rekeningnummer van de leverancier. Wat blijkt, de leverancier heeft nooit nieuwe bankgegevens gestuurd. Dat was een crimineel die de mailbox van jouw leverancier heeft gehackt.

Dit lijkt misschien een onwaarschijnlijk scenario, maar helaas gebeurt het vaak en zorgt het voor grote financiële schade. Denk aan Pathé (1), een Toyota-leverancier (2) of Rijksmuseum Twenthe (3). In de afgelopen jaren werden zij voor miljoenen opgelicht. Dit zijn voorbeelden van BEC-fraude, een type incident waarbij aanvallers mailverkeer van organisaties manipuleren om geld of informatie te stelen. Omdat e-mail tegenwoordig veel als clouddienst wordt afgenomen, is dit een voorbeeld van een cloud incident. Niemand wil in deze situatie terechtkomen, daarom heb ik mij voor mijn afstudeeronderzoek gericht op het bepalen van best practices in cloud incident handling.

Het verschil tussen on-premise en cloud-omgeving

Hoe komt het dat cloud incident handling een andere aanpak vereist? IT-infrastructuur bevindt zich traditioneel gezien op het terrein van jouw bedrijf, oftewel een 'on-premise omgeving'. Je hebt totale controle over jouw infrastructuur. In cloud-omgeving neem je vaak een dienst af, waarbij de infrastructuur beheerd wordt door de cloud service provider. Over het algemeen kunnen clouddiensten ingedeeld worden in drie categorieën: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) en Software-as-a-Service (SaaS). Elk servicemodel onderscheidt zich door de mate van controle. Waar je in een on-premise omgeving alles kunt installeren wat je wilt, ben je bijvoorbeeld met SaaS (zoals Google Drive) compleet afhankelijk van wat de cloud service provider je biedt. Daarnaast staat data in cloud-omgeving verspreid over meerdere systemen, waarbij meerdere cloud servicegebruikers dezelfde resources delen.

Incident handling

Niemand wil een incident in de eigen omgeving. Daarom worden er verschillende methodieken gebruikt om goed te reageren op incidenten. Deze incident handling frameworks

bieden concrete handvatten om incidenten te voorkomen en adequaat te handelen om schade tot een minimum te beperken. Het bekendste incident handling framework is de NIST Incident Response Lifecycle (4). Dit framework beschrijft alle aspecten van het afhandelen van een incident en bestaat uit vier fases: 1. Preparation, 2. Detection & Analysis, 3. Containment, Eradication, and Recovery en 4. Post-Incident Activity.

Het incident handling proces is helder en uitvoerig beschreven voor on-premise omgevingen. Vanwege de eigenschappen van cloud-omgeving zijn deze processen niet toereikend voor cloud incidenten. Er is echter weinig geschreven over cloud incident handling. Dit zorgt bij veel organisaties voor uitdagingen. De oplossingen voor deze uitdagingen heb ik onderzocht in mijn afstudeeronderzoek.

Onderzoeksvraag

Het onderzoek naar best practices in cloud incident handling voerde ik uit bij het Nationaal Cyber Security Centrum (NCSC) gedurende een periode van een half jaar. Er waren twee hoofdvragen: wat is de huidige best practice in cloud incident handling en in hoeverre is deze best practice toereikend in het huidige cloud incident handling landschap? Ik heb deze vragen beantwoord door middel van een literatuur- en een praktijkonderzoek. In het praktijkonderzoek heb ik twaalf interviews afgenomen bij CSIRTs bij meerdere Nederlandse organisaties. Onder deze organisaties bevonden zich cybersecurity dienstverleners en multinationals. De resultaten uit het praktijkonderzoek vergeleek ik vervolgens met de literatuur om tot een huidige best practice te komen.

De vijf belangrijkste aanbevelingen

Mijn onderzoek resulteerde in ruim negentig aanbevelingen. Deze aanbevelingen zijn opgedeeld in de vier fases van de NIST Incident Handling Lifecycle en beschrijven alle onderwerpen die raakvlak hebben met cloud incident handling waaronder: cloud security, risicomanagement en wettelijke regelgeving. Er zijn vijf belangrijke aanbevelingen:

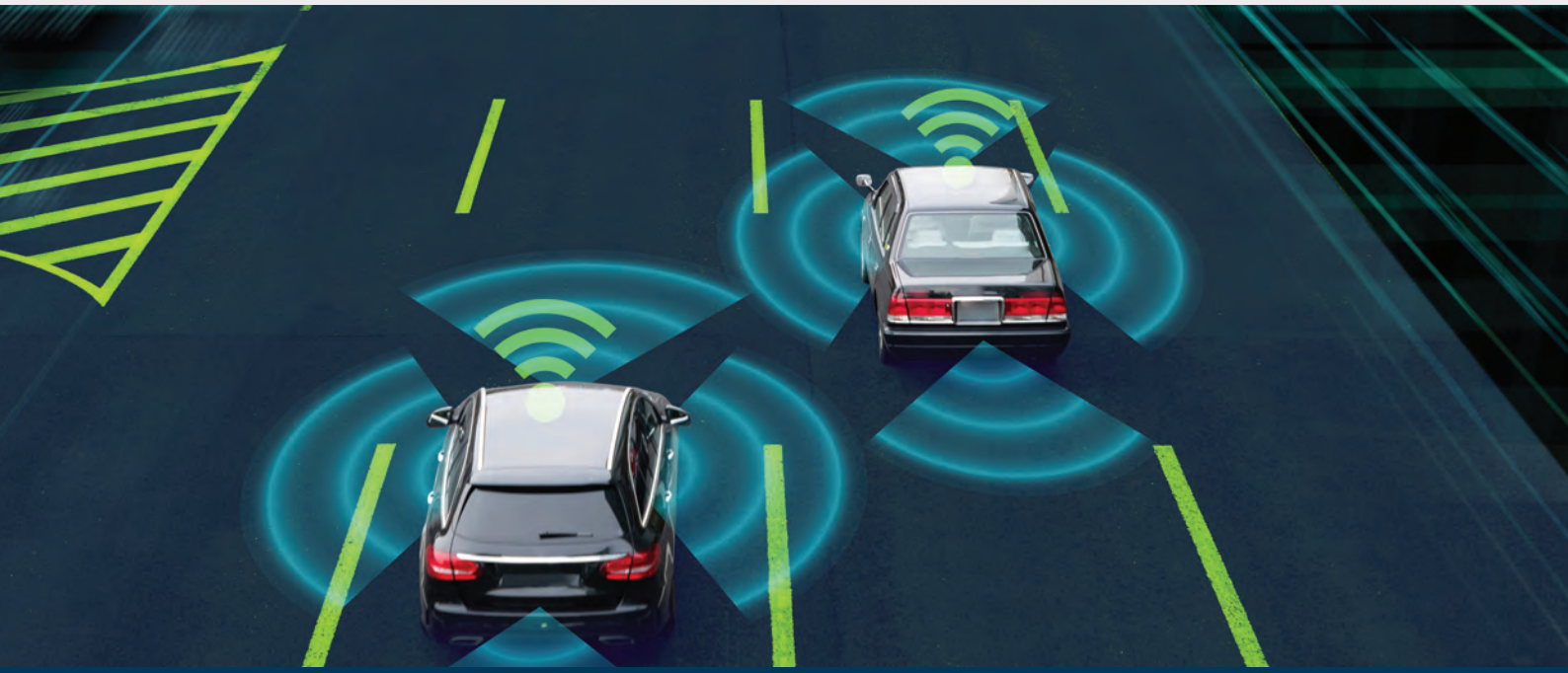
1. Cloudgebruikers moeten zichzelf op de hoogte brengen van de eigenschappen en mogelijkheden van een cloud-omgeving;
2. Cloudgebruikers moeten zichtbaarheid verkrijgen in hun omgeving door cloudmanagement te implementeren. Denk hierbij aan het gebruik van een cloud access security broker of het bijhouden van een interne wiki. Niet alleen helpt dit inzicht krijgen in het cloudgebruik binnen de organisatie, maar helpt dit ook met het contacteren van relevante partijen;
3. Cloudgebruikers moeten ervoor zorgen dat hun cloud-omgeving veilig is. Daarbij hoort zowel het beveiligen van de omgeving op een technisch level, als het implementeren en handhaven van security policies (zoals het gebruik van multi-factor authentication);
4. Alle afspraken, eisen en verantwoordelijkheden moeten vastgelegd worden in de service level agreement;
5. Informatie over incidenten moet gedeeld worden. Dit zorgt ervoor dat cloud service providers verantwoordelijk gehouden kunnen worden. Daarnaast weten andere partijen hierdoor waar ze op moeten letten en worden zo verdere incidenten voorkomen.

Voor het volledige overzicht en de diepgaande toelichting op alle aanbevelingen verwijs ik naar mijn thesis, die publiek beschikbaar is (5).

En verder...

Nu dit onderzoek de basis heeft gelegd voor cloud incident handling, zijn er de nodige vervolgstappen. Ten eerste is het belangrijk dat organisaties de aanbevelingen implementeren waar dat nodig wordt geacht. Ten tweede moet er kwantitatief onderzoek verricht worden om de aanbevelingen uit dit onderzoek te valideren en evalueren. Ten derde moet er gekeken worden naar de rol van cloud service providers in cloud incident handling. Hierbij kan worden gedacht aan het implementeren van een keurmerk voor cloud security voor cloud service providers. Tenslotte moet het veilig delen en uitwisselen van cloud incident-informatie onderzocht worden. Dit zou zich kunnen richten op een gestandaardiseerd uitwisselingsprotocol, maar ook op het opbouwen van vertrouwensrelaties tussen partijen om de informatie-uitwisseling te faciliteren. Met deze vervolgstappen wordt Nederland veiliger en zullen criminelen minder impact hebben op onze economie.

Auteurs: Matthias Rebergen, Mischa de Haan, Nathalie Lokken, Gijs Schimmel, Roy Brüggemann en Thomas Gerrits zijn tweedejaars studenten Automotive aan de HAN. De auteurs zijn te bereiken op PM.Rebergen@student.han.nl, MN.deHaan@student.han.nl, AN.Lokken@student.han.nl, HT.Schimmel@student.han.nl, R.Bruggemann@student.han.nl en TBH.Gerrits@student.han.nl.



Vehicle-to-Vehicle-communicatie, weg van de privacy?

Vehicle-to-Vehicle-communicatie (V2V-communicatie) is het principe waarbij voertuigen op de weg draadloos met elkaar communiceren. Het systeem zendt tien keer per seconde gegevens uit over locatie, snelheid en rijrichting naar auto's in de buurt. Die gegevens zijn mogelijk te herleiden naar de bestuurder. V2V-communicatie neemt snel toe en nu er in veel landen getest wordt met dit systeem, groeit de vraag hoe het zit met privacy en hoe je die waarborgt.

De gegevens die met V2V-communicatie worden verzonden worden ook wel basic safety messages (BSM) of in Europa Cooperative Awareness Messages (CAM) genoemd. Beide typen worden in dit artikel aangeduid als veiligheidsberichten. De veiligheidsberichten hebben een certificaat waardoor de integriteit is gewaarborgd. Ze zijn echter niet versleuteld om vertraging in de communicatie te voorkomen. De beschikbaarheid van V2V-communicatie is erg belangrijk als het op de weg toegepast gaat worden. Er zal een manier gevonden moeten worden om ook V2V-communicatie mogelijk te maken voor auto's die dat momenteel niet hebben. Ook heeft het signaal van de V2V-communicatie een beperkt bereik van ongeveer 300 meter. De vertraging tussen het verzenden en het ontvangen van het bericht zal geen beperking opleveren. Want als drie auto's tien meter tussenruimte met elkaar hebben, levert een vertraging tot 0,5 seconde bij 130 km/h en een vertraging tot 0,7 seconde bij 100 km/h geen problemen op met de tussenruimte en de vertraagde inzet van de remmen. Dit valt binnen de technische mogelijkheden van het systeem.

Het feit dat de communicatie niet versleuteld is kan leiden tot een inbreuk op de privacy.
Het traceren van de bestuurder: de bestuurder zou geïdentificeerd kunnen worden op basis van kennis over thuis- en werkomgeving. Door de V2V-certificaten te volgen, zou deze informatie verzameld kunnen worden en kunnen worden gebruikt voor bijvoorbeeld ongewenste advertenties;
Function creep: function creep is een proces waarbij dingen zoals informatie, programma's of maatregelen op een andere manier worden toegepast dan waarvoor ze oorspronkelijk bedoeld zijn. Dit proces vindt geleidelijk en over langere tijd plaats. In de context van V2V-communicatie gaat dit over de verzamelde gegevens. Deze gegevens kunnen bijvoorbeeld gebruikt worden om automatisch bekeuringen te geven.
Op dit moment is er voor V2V-communicatie nog geen specifieke regelgeving. Wel zijn de E-Privacyrichtlijn en de Algemene Verordening Gegevensbescherming (AVG) van kracht. De AVG gaat over alle vormen van verwerking van persoonsgegevens, terwijl de E-Privacyrichtlijn zich specifiek op de verwerking van persoonsgegevens voor elektronische communicatiediensten richt. De Europese Commissie heeft een voorstel gedaan voor verdere uitwerking van elektronische communicatiediensten in een E-Privacyverordening, een verscherping van de regels in de huidige E-Privacyrichtlijn. Dit voorstel ligt nu bij de Europese Raad en het zal nog wel even duren voordat de verordening in werking treedt. Aangezien de AVG van recenter datum is dan de E-Privacyrichtlijn, zal de AVG in veel gevallen voorrang genieten in de toepassing. Wanneer de E-Privacyverordening in werking treedt, zal deze meer van toepassing worden dan de AVG, doordat het specifiek op de verwerking van persoonsgegevens voor elektronische communicatiediensten richt en dus specifieker en recenter is. Omdat de E-Privacyverordening een verordening is, zorgt het in tegenstelling tot de E-Privacyrichtlijn voor een wetgeving die voor alle lidstaten in de Europese Unie gelijk is.

Het voorstel zoals het er nu ligt, is van toepassing op locatiegerichte gegevens en dat is het geval bij V2V-communicatie. De belangrijkste regel van dat voorstel is dat data gebruikt mag worden als de consument om toestemming is gevraagd. Dit introduceert een nieuw potentieel probleem wanneer je je auto tweedehands wil verkopen. Als de V2V-data wordt opgeslagen in het systeem van de auto, kan de nieuwe eigenaar de gegevens van de oude eigenaar inzien en kan er een datalek ontstaan. Een mogelijke oplossing hiervoor is dat er met een account moeten worden ingelogd op een centraal V2V-systeem. Als er met een nieuw account wordt ingelogd, wordt opnieuw toestemming gevraagd omtrent de verwerking van persoonsgegevens en wordt de historie automatisch gewist. Waar de Europese Unie vooral inzet op generieke regelgeving, wordt in de Verenigde Staten gewerkt aan sectorspecifieke regels. De National Highway Traffic Safety Administration (NHTSA) heeft een aantal reglementen gepubliceerd die ons kunnen inspireren.

Het NHTSA heeft een aantal technische regels voorgesteld om persoonsgegevens beter te beschermen.
Bescherming van gevoelige persoonsgegevens: voertuigen verzenden geen gevoelige persoonsgegevens in de veiligheidsberichten die herleidbaar zou kunnen zijn naar het voertuig, de bestuurder of de eigenaar (bijv. namen, licentienummers, Voertuig Identificatie Nummer (VIN), kenteken-informatie en dergelijke);
Certificaten: voertuigen ontvangen twintig roterende certificaten per week. Deze valideren de veiligheidsberichten voor vijf minuten terwijl ze zeven dagen lang roteren. Om een persoon of voertuig te volgen zijn alle twintig certificaten nodig, die om de vijf minuten worden geroteerd.

Daarna worden de certificaten verwijderd en wordt een nieuwe set in gebruik genomen;

Anonimiteit rond de certificaten: er zijn afzonderlijke beleidsregels rond het ontvangen, maken en uitgeven van de certificaten, zodat geen enkele autoriteit de complete informatie van een certificaat in bezit heeft. Omdat geen enkele autoriteit toegang heeft tot alle informatie die een certificaat bevat, voorkomt dit ook aanvallen van insiders.

Daarnaast heeft NHTSA beleidsregels gepubliceerd over het gebruik van een V2V-systeem, onder andere dat een V2V-systeem:

- geen gegevens over individuen of individuele voertuigen verzamelt of opslaat, noch het de overheid toestaat dit te doen;
- geen gegevens bevat die door wetshandhavingsinstanties of particuliere entiteiten kunnen worden gebruikt om snelheidsovertreders of onrechtmatige bestuurders persoonlijk te identificeren. Dit geldt zowel voor veiligheidsberichten die worden uitgewisseld tussen voertuigen als gegevens die worden verzameld door het V2V-beveiligingssysteem;
- het niet toestaat om door ruimte of tijd voertuigen te volgen die zijn gekoppeld aan specifieke eigenaren, bestuurders of personen;
- geen financiële informatie, persoonlijke communicatie of andere informatie met betrekking tot individuen verzamelt en geen toegang biedt tot het voertuig voor het extraheren van deze gegevens.

Momenteel heeft de NTHSA dus sectorspecifieke beleidsregels rond V2V-systemen en de veiligheidsberichten die de nodige informatie bevatten. De Europese Unie maakt voor de regelgeving omtrent V2V momenteel gebruik van de AVG, die in de toekomst aangevuld wordt met de E-Privacyverordening. Er zijn overeenkomsten maar ook verschillen. In de VS heten de veiligheidsberichten zoals eerder genoemd BSM's, in de EU worden ze aangeduid als CAM. CAM-berichten bevatten alles wat BSM-berichten bevatten, maar ook informatie als: positie, beweging, voertuiggrootte, voorgaande route en de StationID (voertuig pseudo ID). De informatie over de positie, voorgaande route en StationID, behoren tot gevoelige informatie doordat ze gebruikt kunnen voor de identificatie van de bestuurder.

Onder de AVG dient deze gevoelige informatie beschermd te worden door pseudonomisatie, die bovendien zo dicht mogelijk bij de bron moet plaatsvinden. Pseudonomiseren is een proces waarbij gevoelige informatie niet te herleiden is zonder dat het algoritme ervan bekend is. De regelgeving in de VS schrijft voor dat er geen gevoelige informatie in de veiligheidsberichten mag staan zoals kentekenplaat of informatie die naar de bestuurder te herleiden is.

Voor de automobilist die in de nabije toekomst een V2V-systeem in de auto heeft, is de bescherming van de persoonsgegevens te regelen. Onder de AVG zijn de rechten op dataprotectie en privacy voor alle individuen van de Europese Unie sterk toegenomen. Daarbij verdienen persoonsdata of persoonlijk identificeerbare informatie speciale berscherming. In de VS zorgen de regels van de NHTSA ervoor dat de privacy van consumenten zo goed mogelijk worden gewaarborgd.

De regels zijn echter niet erg bruikbaar voor V2V-systemen, met name zaken als data-minimalisatie en pseudonimisering, maar ook toestemming voor het gebruiken van de data en dergelijke, zijn dingen die lastig te implementeren zijn. Feit is dat veiligheidsberichten niet versleuteld worden en dat ten koste gaat van de prestaties en kan leiden tot datalekken, hoewel dat bij het huidige bereik van ongeveer 300 meter geen heel groot probleem lijkt te zijn. Het is echter niet uit te sluiten dat er misbruik van kan worden gemaakt.

Referenties

(1) http://blog.onboardsecurity.com/blog/ V2V-communications-what-about-my-privacy

(2) https://www.embedded-computing.com/embedded-computing-design/privacy-in- V2V-communications-is-somebody-watching-you

(3) https://www.frank.news/nl/article/marketing/maakt-eprivacy-wet-als-die-er-ooit-komt-eind-aan-de-cookie.html

(4) https://www.privacy-web.nl/themadossier/e-privacy

(5) https://www.researchgate.net/publication/327529242_An_Integrated_-Communication_Message_Framework_of_Inter-Vehicles_for_Connected_-Vehicles_using_Mobile_Virtual_FenceMVF

https://www.cargroup.org/wp-content/uploads/2017/03/nhtsa_V2V_nprm_review_car_20dec20161.pdf

(6) https://ec.europa.eu/transport/sites/transport/files/legislation/c20191789.pdf

(7) http://data.europa.eu/eli/reg/2016/679/oj

(8) http://data.europa.eu/eli/dir/2002/58/2009-12-19

(9) https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

(10) https://www.eerstekamer.nl/eu/edossier/e170003_voorstel_voor_een

WAPEN JE TEGEN ONLINEMOEHEID

Het zijn bizarre en onwerkelijke tijden. Wanneer je deze editie van iB-Magazine leest, hoop ik dat er weer meer versoepeling mogelijk is. Alleen vrees ik dat het advies 'blijf thuis en werk vanuit huis' nog lang van kracht zal zijn. Daarom wil ik het graag in deze editie met je hebben over hoe wij mentaal sterk blijven in deze moeilijke periode. Met tips van de stoïcijnen.

Deze lockdownperiode besef ik des te meer wat een mooie verenging wij hebben. Hoe waardevol de persoonlijke contacten met en tussen de leden tijdens onze PvIB-bijeenkomsten zijn. Daarom ben ik ook verheugd dat onze activiteitencommissie een alternatief biedt voor onze fysieke bijeenkomsten. De PvIB-activiteiten worden je middels webinars aangeboden. Een eerste evaluatie geeft aan dat jullie de webinars als zeer positief hebben ontvangen, waarvoor onze dank. Ik ben blij dat wij naast onze iB-Magazines ook via webinars in contact met elkaar kunnen zijn. We vergaderen, videobellen en trainen meer online, we drinken vaker virtueel koffie en we volgen vaker webinars online. Door deze explosie aan onlinecommunicatie merk ik bij mijzelf dat er een soort van 'onlinemoeheid' optreedt. Nu de kans reëel is dat wij nog lang massaal blijven skypen, teamen, zoomen of Google hangouten, is het zaak om niet alleen fysiek maar ook mentaal sterk te blijven. Mijn collega Nino Mulder heeft mij een paar waardevolle tips gegeven hoe wij mentaal deze lastige periode kunnen doorkomen. Hierbij gebruikt Nino de wijsheden van de stoïcijnen en andere Griekse filosofen. Graag wil ik zijn tips met je delen.

De stoïcijnen geloofden dat 'een goed leven' betekende dat de mens leeft volgens zijn sociale en rationele aard. Dit resulteerde in vier praktische richtlijnen, ook wel de vier hoofddeugden: wijsheid, matigheid, rechtvaardigheid en moed. Hieronder lees je beknopt hoe de stoïcijnen daar terecht zijn gekomen.

- **Wijsheid:** neem het leven zoals het komt. Proberen te beheersen wat u niet kunt, is dus een absolute verspilling van tijd en energie. Zoals Epictetus het uitdrukte: "Probeer niet alles te laten gebeuren zoals je zou willen, maar wens liever dat alles gebeurt zoals het werkelijk zal gebeuren - dan zal je leven goed stromen."
- **Matigheid:** zelfbeheersing. Voor de stoïcijnen is matiging gelijk aan zelfdiscipline. Stoïcijnen hielden zich verre van overdaad. Vraag jezelf de volgende keer wanneer je boodschappen gaat doen of kleren wilt kopen: heb ik dit nu echt nodig? Waarschijnlijk niet. Met zelfdiscipline kun je dit overwinnen. Kortom, word niet afhankelijk van externe dingen om gelukkig te zijn.
- **Rechtvaardigheid:** Het gaat niet om jou. Volgens de stoïcijnen zijn mensen niet alleen rationeel, maar ook sociaal van aard. Net als andere dieren hebben we een natuurlijke genegenheid voor onze familie. Wat betekent dat in onze huidige situatie? Welnu, als je de hele wereld als je familie beschouwt, wiens interesses je even belangrijk vindt als die van jezelf, wordt het vrij eenvoudig. Je vecht niet met je zus over een rol wc-papier, je koopt niet al het eten voordat je moeder een aandeel krijgt en je gaat zeker niet naar buiten als je weet dat het je oma kan schaden. Een goed leven leiden gaat niet alleen over jou.
- **Moed:** Wees niet bang, wees voorbereid op het ergste. Stoïcijnen wapenden zich tegen tegenspoed door zich voor te bereiden op de slechtst mogelijke resultaten. Zoals we nu ervaren, is gisteren geen garantie voor vandaag. De stoïcijnen wisten dat er op elk moment iets vreselijks kon gebeuren. Dat is de reden waarom ze hun angsten frontaal onder ogen zagen met de zogenaamde 'premeditation of adversity'. Ze visualiseerden bijvoorbeeld dat ze hun huis kwijtraakten, in ballingschap werden gestuurd en zelfs hun eigen dood. Kortom, bereid je in tijden van vrede voor op oorlog.

Ik hoop dat de wijsheden van de stoïcijnen net als mij jou ook mentale kracht geven in deze lastige periode. Hou vol, blijf gezond of word snel weer beter.

Henk Brandon

Auteurs: Lisa de Kok (onderzoeker) en Marcel Spruit (lector) zijn werkzaam bij het lectoraat Cyber Security & Safety aan de Haagse Hogeschool. Lisa de Kok is te bereiken via l.c.dekok@hhs.nl, Marcel Spruit via m.e.m.spruit@hhs.nl.

Analyse volwassenheids-modellen voor informatiebeveiliging

Organisaties die belang hechten aan hun informatie moeten ervoor zorgen dat de informatiebeveiliging goed is geregeld. Als de informatiebeveiligingsprocessen niet voldoende zijn ingericht en er geen duidelijke afspraken en verantwoordelijkheden worden vastgelegd, is de kans aanwezig dat een incident (te) laat wordt gesignaleerd. Via een volwassenheidsmeting wordt inzicht verkregen op welk niveau de informatiebeveiliging is georganiseerd.

Een volwassen persoon is een volgroeid persoon. Volwassen worden gebeurt in meerdere fases en niet van de een op de andere dag wanneer iemand 18 wordt. Een organisatie kan ook in meerdere of mindere mate volwassen zijn met betrekking tot informatiebeveiliging. Hoe volwassener, des te beter de organisatie in staat is de ontwikkeling en handhaving van informatiebeveiliging in goede banen te leiden. Dit betekent echter niet, dat elke organisatie moet streven naar het hoogste niveau van volwassenheid. Er moet altijd een gedegen afweging te worden gemaakt welk niveau passend is bij de wensen van de organisatie.

Naarmate een organisatie volwassener wordt in de informatiebeveiliging, betekent dit dat de informatiebeveiliging op een meer integrale manier is georganiseerd (8). Praktisch betekent een hogere mate van volwassenheid een hogere mate van institutionalisering van het desbetreffende proces via beleid, standaarden en organisatorische structuren (12). Bij een minder volwassen organisatie wordt meer ad hoc of minder doordacht ingespeeld op de problematiek.

Wat is een volwassenheidsmodel?

Om te weten in hoeverre een organisatie volwassen is, zijn volwassenheidsmodellen ontwikkeld. Een model is een vereenvoudigde weergave aan de hand waarvan een meting kan worden uitgevoerd. Een volwassenheidsmodel is een set van kenmerken, indicatoren of patronen die gekoppeld zijn aan volwassenheidsniveaus in een bepaald domein of discipline (2). Daarmee geven volwassenheidsmodellen een indicatie van de capaciteiten van een organisatie. In elk van de gebruikelijke vijf volwassenheidsniveaus ligt vast welke kenmerken erbij horen. Deze niveaus, van initieel (1) naar geoptimaliseerd (5), vullen elkaar cumulatief aan (14).

Volwassenheidsmodellen zijn wijdverspreid in het domein van computerwetenschappen en informatiesystemen, maar ook in andere domeinen zoals biologie, sociologie en psychologie (7). De huidige volwassenheidsmodellen binnen de IT-sector zijn veelal gebaseerd op het Capability Maturity Model (CMM). Deze werd ontwikkeld door het Software Engineering Institute in het midden van de jaren ’80 (12). Bij dit model wordt gekeken naar procesvolwassenheid bij software engineering. Dit betekent dat volwassenheid zich uit in de mate waarin een (software engineering) proces effectief, gedefinieerd, beheerd, gemeten en gecontroleerd is (12).

Een meting aan de hand van een volwassenheidsmodel kan voor beschrijvende of voorschrijvende doeleinden worden gebruikt. Een volwassenheidsmeting heeft een beschrijvend doel als het wordt toegepast voor een beoordeling van de huidige capaciteiten van de organisatie op het desbetreffende domein (14). Met deze omschrijving kan een vergelijking worden gemaakt met een eerdere meting, een ander organisatieonderdeel of een vergelijkbare organisatie. Aanvullend kan het een voorschrijvend doel dienen, als richtlijnen worden gegeven met concrete maatregelen om een ander niveau van volwassenheid te bereiken (14).

Soorten volwassenheidsmodellen

Er worden verschillende soorten volwassenheidsmodellen onderscheiden in de literatuur, zoals capability modellen, progress modellen en hybride volwassenheidsmodellen. De kenmerken van deze verschillende modellen worden hieronder omschreven.

Een capability model kijkt naar de mogelijkheid in hoeverre een organisatie in staat is om specifieke taken uit te voeren in een bepaald domein of discipline (2). Aan de hand van een capability model is een organisatie in staat op verschillende onderdelen van bijvoorbeeld informatiebeveiliging zijn huidige capaciteiten (capabilities) zichtbaar te maken. De gemeten niveaus geven een indicatie van de organisatievolwassenheid; wordt iets ad hoc uitgevoerd of systematisch en kwantitatief gemonitord. Een progress model meet volwassenheid aan de voortgang (progress) van een bepaald kenmerk in een model (2). In tegenstelling tot een capability model meer dan alleen de aanwezigheid van bepaalde kenmerken, maar ook de organisatorische vaardigheid om dat kenmerk uit te voeren en het institutionaliseren ervan. Een hybride model is een combinatie van een progress en een capability model.

De vraag is in hoeverre deze soorten modellen in de praktijk daadwerkelijk te onderscheiden zijn. Uiteindelijk gaat het allemaal om een maat van de volwassenheid, ofwel in de aanwezigheid van kenmerken (progress model) dan wel in welke mate de activiteiten zijn geïnstitutionaliseerd (capability model). Belangrijker is om te weten wat een volwassenheidsmodel een goed volwassenheidsmodel maakt in de informatiebeveiliging. In dit artikel wordt daarom geen onderscheid gemaakt tussen verschillende soorten modellen, maar wel bekeken of de benodigde elementen aanwezig zijn in het volwassenheidsmodel. Daarvoor is het nodig om te weten welke elementen in een volwassenheidsmodel zouden moeten zitten en aan de hand van welke criteria volwassenheidsmodellen kunnen worden geëvalueerd.

Eerdere reviewstudies hebben in totaal negentien volwassenheidsmodellen voor informatiebeveiliging naast elkaar gelegd en met elkaar vergeleken (1, 6, 8, 9, 10, 13, 15). Er zijn een paar beperkingen aan deze eerdere studies. Zo wordt bij deze onderzoeken slechts een deel van de relevante modellen meegenomen (15), wordt geen consistente en inzichtelijke review gegeven van de modellen (6, 10, 13), is de documentatie van de modellen niet vrijelijk beschikbaar waardoor geen beoordeling kan worden gemaakt (4, 6, 9), zijn criteria aan de hand waarvan de volwassenheidsmodellen worden geëvalueerd niet duidelijk beschreven (8, 9), worden modellen meegenomen die in feite geen volwassenheidsmodellen zijn (1, 8, 10), of waarin slechts een onderdeel van informatiebeveiliging wordt gemeten (1, 3, 6, 8, 9, 10, 15). In Tabel 1 is het overzicht gegeven van de informatiebeveiligingsvolwassenheidsmodellen die niet zijn meegenomen in de nadere analyse vanwege een van bovenstaande beperkingen. Vier modellen worden wel meegenomen, namelijk NBA-LIO, C2M2, ISM3 en het 3-Pijlermodel (5, 11, 18, 20). De toegevoegde waarde van dit artikel is de combinatie van het opstellen van de elementen van een volwassenheidsmodel, het opstellen van criteria waaraan de volwassenheidsmodellen kunnen worden geëvalueerd en een overzicht van volwassenheidsmodellen waarin informatiebeveiliging met al zijn elementen wordt meegenomen. De criteria die zijn opgesteld, kunnen als checklist gebruikt worden om uiteindelijk een volwassenheidsmodel te kiezen. De vraag die hier centraal staat is: welk informatiebeveiligingsvolwassenheidsmodel is pragmatisch voor een meting in een organisatie? Daarom wordt ingegaan op welke verschillende volwassenheidsmodellen voor informatiebeveiliging er zijn en welke elementen deze bevatten. Verder worden criteria opgesteld aan de hand waarvan de volwassenheidsmodellen kunnen worden geëvalueerd.

Elementen volwassenheidsmodel

Ondanks hun verscheidenheid hebben volwassenheidsmodellen in principe eenzelfde structurele basis waar ze uit bestaan. De elementen staan hieronder benoemd. Eerdere studies waarin volwassenheidsmodellen met elkaar worden vergeleken grijpen meestal niet terug op deze structurele basis (1, 6, 9, 13). Omdat er niet wordt uitgegaan van deze structurele basis, worden modellen in de evaluatie meegenomen die eigenlijk geen volwassenheidsmodellen zijn. Caralli et al (2) hebben een overzicht gemaakt van de elementen van een volwassenheidsmodel. Dit overzicht komt overeen met een van de eerste volwassenheidsmodellen (CMM) (12).

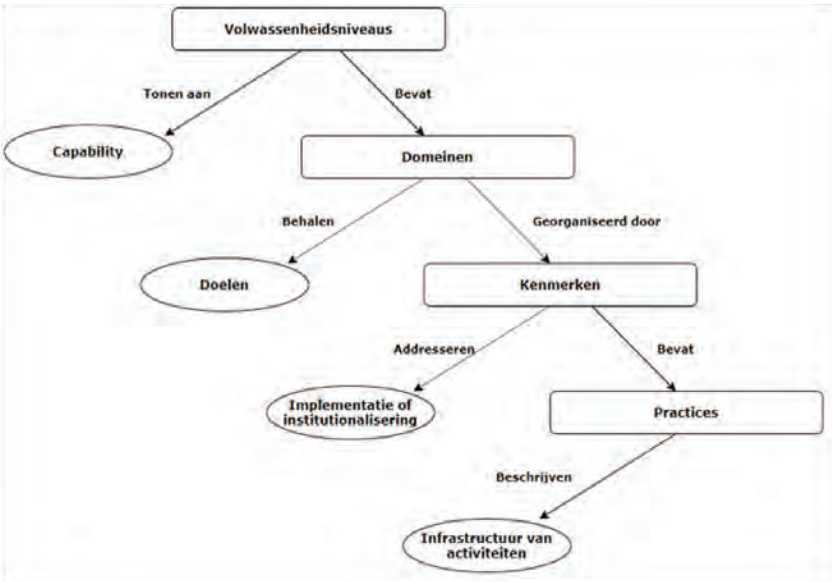
		Exclusie-criteria	Referentie
1.	CITI-ISEM	- Geen volledige documentatie beschikbaar - Omvat een te beperkt deel van informatiebeveiliging (security awareness)	[6, 8]
2.	ISM2	- Geen volledige documentatie beschikbaar	[6, 8, 9]
3.	GISMM	- Geen volledige documentatie beschikbaar	[8]
4.	Praktisch VM	- Geen volledige documentatie beschikbaar	[4]
5.	ISFM IBM	- Onvolledig uitgewerkt in beschikbare documentatie	[6, 8]
6.	ISMS (Im)-Maturity Model	- Onvoldoende uitgewerkt - Niet makkelijk en praktisch uit te voeren	[6]
7.	ISMS	- Geen volwassenheidsmodel maar een managementsysteem	[8, 10]
8.	COBIT 5	- Geen volwassenheidsmodel maar een management framework	[1]
9.	SSE CMM	- Omvat een te beperkt deel van informatiebeveiliging (security engineering)	[1, 8, 9, 15]
10.	CSF NIST	- Omvat een te beperkt deel van informatiebeveiliging (cybersecurity risk management)	[6, 8, 10, 13]
11.	CIP Privacy-model	- Omvat een te klein deel van informatiebeveiliging (privacy)	[3]
12.	CERT RMM	- Omvat niet specifiek informatiebeveiliging (operational resilience)	[8, 10, 13]
13.	NICE CSMM	- Omvat een te beperkt deel van informatiebeveiliging (workforce management)	[8, 10, 15]
14.	COBIT Process Assessment Model	- Omvat een te beperkt deel van informatiebeveiliging (IT-processen)	[1,9]
15.	CCSMM	- Omvat een te beperkt deel van informatiebeveiliging (community cyber security)	[8, 15]

Tabel 1 - Overzicht niet-geselecteerde informatiebeveiligingsvolwassenheidsmodellen.

De structurele basis bestaat uit de volgende elementen:

Niveaus:
Geven de schaal aan van de volwassenheid van (proces)capaciteit. De niveaus gaan van initieel (1) naar geoptimaliseerd (5). De niveaus zijn cumulatief, dit betekent dat de eigenschappen van de vorige niveaus behouden blijven bij een volgend niveau en er nieuwe eigenschappen aan toegevoegd worden. Van elk niveau dient een gedegen beschrijving te zijn. Elk niveau bevat een set van doelen dat een belangrijke eigenschap van het proces bevat. Elk volwassenheidsniveau bestaat uit sleutelprocesdomeinen, welke bestaan uit gemeenschappelijke kenmerken waaruit belangrijke werkwijzen worden gespecificeerd (12).

Domeinen:
Onderdelen van het gehele onderwerp, in dit geval informatiebeveiliging, in logische categorieën en/of praktijken verdeeld.



Figuur 1 - Visualisatie van de structuur van een volwassenheidsmodel (12).

Doelen:
Elk volwassenheidsniveau bevat een aantal procesdoelen. Deze vatten de belangrijke good practices samen en worden gebruikt om te bepalen of een organisatie effectief de domeinen heeft geïmplementeerd.

Kenmerken:
Ook wel attributen, karakterkenmerken, indicatoren, praktijken of processen genoemd. De kenmerken geven een indicatie in hoeverre de implementatie en institutionalisering van een domein effectief, herhaalbaar en blijvend is. Daarnaast is voor de uitvoering van de methode nodig:

Scoringsmethode
Zodat op een uniforme manier de meting wordt uitgevoerd.

Stappenplan ter verbetering
Op basis van de uitkomst van de scoringsmethode, concrete acties om het volwassenheidsniveau te verhogen.

Criteria volwassenheidsmodel

De criteria op basis waarvan de volwassenheidsmodellen worden geëvalueerd, staan hieronder beschreven en onderstreept. Aan de hand van gestelde criteria kunnen de volwassenheidsmodellen tegen een maatstaf worden aangelegd.
Uitgangspunt is dat een volwassenheidsmodel pragmatisch is. Wat zijn criteria voor een pragmatisch volwassenheidsmodel? Synoniemen van pragmatisch zijn: praktisch, toepasbaar, doelmatig en waardevol. Een pragmatisch volwassenheidsmodel is geschikt om gebruikt te worden door een bepaalde doelgroep. De doelgroep voor deze volwassenheidsmodellen zijn medewerkers die de meting niet op dagelijkse basis uitvoeren, maar wel gedegen kennis hebben over informatiebeveiliging en hier een beoordeling van kunnen maken.
Primair is het belangrijk dat een model de hiervoor genoemde structurele elementen bevat van een volwassenheidsmodel om zich ook zo te noemen. Een volwassenheidsmodel is bruikbaar indien het ingezet kan worden in verschillende omgevingen. Het is daarom belangrijk dat een volwassenheidsmodel algemeen van aard is en niet alleen gebruikt kan worden binnen een bepaalde organisatie of industrie. Daarvoor dient het model flexibel te zijn, zodat het aangepast kan worden aan de wensen en eisen van de organisatie waar de meting wordt uitgevoerd.
Verder is de gebruiksvriendelijkheid van belang. Een evenwicht moet worden gevonden tussen het hebben van te veel maatregelen, eigenschappen en vragen, versus te weinig eigenschappen om te komen tot een consistente en juiste beoordeling." (2). Gebruiksvriendelijkheid is essentieel; in een eerder verschenen evaluatie-template van volwassenheidsmodellen door experts krijgt het een prominente status (16). Gebruiksvriendelijkheid is onderverdeeld in de volgende kenmerken: begrijpelijkheid, gebruiksgemak en uitvoerbaarheid (16). Onder uitvoerbaarheid valt ook de hoeveelheid tijd en moeite die het kost om een meting uit te voeren. Het is niet wenselijk dat dit langer dan enkele dagen duurt of alleen door een hiervoor opgeleide specialist kan worden uitgevoerd. Onder gebruiksgemak valt ook de

toegankelijkheid van gedetailleerde documentatie (13).
Belangrijk bij een meting is dat deze valide en betrouwbaar is. De validiteit van een meting geeft aan in hoeverre het meetinstrument meet wat het zou moeten meten. Een indicatie hiervoor is hoe het begrip informatiebeveiliging in een volwassenheidsmodel wordt beschreven en gemeten. Omdat een (capability) volwassenheidsmodel de capaciteiten van een organisatie meet om informatiebeveiliging uit te voeren, ligt de nadruk op de goede manier organiseren van de informatiebeveiliging. Een startpunt daarin is het opstellen van informatiebeveiligingsbeleid. Beleid heeft een preventieve, signalerende en correctieve functie (17). Inhoudelijke input voor het beleid kan gehaald worden uit een norm, zoals bijvoorbeeld de ISO 27001. Beleid alleen is niet voldoende, controle of het beleid wordt nageleefd door systematische monitoring (17) en het toekennen van verantwoordelijkheid van informatiebeveiliging aan medewerkers is ook onderdeel van het organiseren van informatiebeveiliging (19). Verder is erkenning van het model door andere academici en/of vakgenoten van belang voor de validiteit. Tot slot is een betrouwbare meting vrij van willekeurige meetfouten. Om een betrouwbare meting te bewerkstelligen is een heldere diagnostische methode nodig.
Uit de voorgaande tekst zijn de volgende criteria af te leiden voor een pragmatisch volwassenheidsmodel:

- Bevat de benodigde elementen van een volwassenheidsmodel;
- Is flexibel;
- Is gebruiksvriendelijk (begrijpelijkheid, gebruiksgemak en uitvoerbaarheid, toegang tot gedetailleerde documentatie);
- Is valide: goede organisatie van informatiebeveiliging, informatiebeveiligingsbeleid, naleving, koppeling norm, verantwoordelijkheid, erkenning model door academici/practici;
- Is betrouwbaar (diagnostische methode).

Vier volwassenheidsmodellen

Hieronder worden de vier overgebleven volwassenheidsmodellen, NBA-LIO, C2M2, ISM3 en het 3-Pijlermodel, geëvalueerd. In een voorafgaande deskresearch die door ons is uitgevoerd zijn negentien volwassenheidsmodellen voor informatiebeveiliging naar boven gekomen. De andere vijftien zijn niet meegenomen in de analyse omdat deze niet voldoen aan de meest basale criteria, genoemd in tabel 1. De analyse is gedaan op basis van de beschikbare documentatie, tools, reviews en literatuur en aan de hand van de gestelde criteria. Ieder van de vier modellen wordt omschreven en de belangrijkste voor- en nadelen worden genoemd. De resultaten zijn samengevat in tabel 2.

	Validiteit									
	Elementen	Flexibel	Gebruiksvriendelijk	Koppeling norm	Beleid	Naleving	Verantwoordelijkheid	Erkenning	Betrouwbaarheid	Totaal
NBA-LIO	++	±	++	++	±	+	±	+	+	9
C2M2	++	±	+	+	±	+	±	+	+	7
ISM3	-	++	--	±	+	++	++	±	±	4
3PijlersIB	+	±	+	±	±	++	++	±	++	8
Meting	-- (-2) / - (-1) / ± (0) / + (1) / + + (2)									Schaal: (-18 / + 18)

Tabel 2 - Analyse volwassenheidsmodellen a.d.h.v. gestelde criteria.

NBA-LIO

De Nederlandse Beroepsorganisatie van Accountants (NBA-LIO) heeft een volwassenheidsmodel van vijf niveaus voor informatiebeveiliging gemaakt (11). In deze versie is de samenhang verwerkt met de Inherente Cyber Risicoanalyse (ICR) en het Cyber Security Assessment (CSA) van de NOREA (beroepsorganisatie van IT-Auditors). Het model vindt aansluiting met andere raamwerken en standaarden zoals het NIST-raamwerk, COBIT, ISO27002 en de Baseline Informatiebeveiliging Overheid (BIO).
Het model van NBA-LIO is gebruiksvriendelijk. In de Excel-matrix staat op een volledige en korte manier omschreven wat kenmerkend is op elk van de 15 aandachtsgebieden en deelgebieden voor dat volwassenheidsniveau. Door de matrix in te vullen kan het volwassenheidsniveau worden bepaald. Beleid heeft een plek in het gebied governance onder 'policy'. Dit heeft maar een beperkt gewicht ten opzichte van het geheel. In het tweede domein 'organisatie', wordt gefocust op het belang van verantwoordelijkheid. Naleving wordt geborgd in het domein human resources, het domein incident/problem management en Business Continuity Management. Het aangereikte volwassenheidsmodel biedt expliciete richtlijnen om organisatiebreed, organisatieoverstijgend en/of sectorbreed volwassenheidsniveaus van informatiebeveiliging vast te stellen en een handreiking om de meting uit te voeren.
Het model is nog niet erkend of beschreven in de academische wereld. Door de samenwerking met NOREA, de beroepsvereniging voor IT-auditors, kan gezegd worden dat de erkenning rond vakgenoten wel aanwezig is. De diagnostische methode is duidelijk en eenduidig, wat een positieve uitwerking heeft voor de betrouwbaarheid.

Verantwoordelijkheid zit in het domein workforce management en in de richtlijnen bij de managementdoelen

Doordat automatisch grafieken worden gegenereerd, worden vergelijkingen tussen bedrijfsonderdelen of 'industry peers' eenvoudig gemaakt. Het model heeft een overzichtelijke matrix met gewichten en eisen. Of de meting wordt uitgevoerd op basis van een automatische matrixrapportage of door interviews, komt niet duidelijk naar voren.

C2M2

Het beschrijvende Cybersecurity Capability Maturity Model (C2M2) is ontwikkeld door 'the United States Department of Energy' (20). Dit model hanteert vier niveaus in plaats van de gebruikelijke vijf, genoemd Maturity Indicator Levels (MILs). Hierdoor is minder spreiding en moeten meer activiteiten uitgevoerd worden om een volgend niveau te halen. Binnen het model zijn tien domeinen die zich onderscheiden in verschillende soorten processen van de organisatie. Elk domein heeft een logische groepering van cybersecuritypraktijken (15). De inhoud van het model komt voort uit standaarden van NIST en ISO.

De gebruiksvriendelijkheid van C2M2 is vrij goed. De Excel vult makkelijk in, maar het aanvullende document van meer dan tachtig bladzijdes is niet erg prettig. Met betrekking tot de validiteit laat de focus op beleid te wensen over. In elk domein staan een of enkele punten voor het streven naar documentatie en/of beleid. Hierin is echter geen duidelijke lijn en bovendien is documentatie niet hetzelfde als beleid. Verantwoordelijkheid zit in het domein workforce management en in de richtlijnen bij de managementdoelen voor ieder domein. Deze richtlijnen zijn slechts 10 van de in totaal meer dan 300 richtlijnen, waardoor uiteindelijk weinig gewicht hangt aan het zorgen voor verantwoordelijkheid met betrekking tot informatiebeveiliging. Naleving is ook een van de managementdoelen. Daarnaast wordt op verschillende domeinen gecheckt op logging en monitoring, waardoor de naleving van de cybersecurity wordt gecontroleerd.

Erkenning van dit model kan gevonden worden in de wetenschappelijke kringen; veel artikelen namen C2M2 mee en het is een geregistreerd trademark van de Carnegie Mellon University. Een evaluatie met de C2M2 is uit te voeren met een zelfevaluatie toolkit in één dag. De omschrijvingen zijn abstract waardoor het model breed toepasbaar is voor organisaties van verschillende groottes en contexten. Er zijn geen 'good practices' aan gekoppeld en bij het invullen van het format wordt niet gerefereerd aan welk(e) (deel van) de norm dit is gekoppeld. Of de meting wordt uitgevoerd door interviews of dat medewerkers het zelf invullen, komt niet naar voren in de handleiding.

ISM3

Information Security Management Maturity Model, ISM3, is een informatiebeveiliging volwassenheidsstandaardgepubliceerd door de Open Group (standaardisatieorganisatie), voor het laatst herzien in 2017 (5). Volwassenheid uit zich in de uitvoering van de belangrijkste processen die gekoppeld zijn aan de doelen van een organisatie. In plaats van te kijken naar maatregelen, ligt de focus op processen die in bepaalde mate voor elke organisatie van toepassing zijn. Beveiligingsdoelen zijn gekoppeld aan de doelen van de organisatie. ISM3 is toepasselijk voor allerlei soorten organisaties en gekoppeld aan verschillende standaarden, waaronder ISO 27001.

Het procesmodel van ISM3 wordt als uitgangspunt genomen en bestaat uit vier punten: good practices en strategisch, tactisch en operationeel management. Als basis wordt het belang van goede documentatie genoemd in de algemene good practices; hier valt beleid ook onder. Naleving wordt geborgd middels operationeel management door rapportages, controles, testen, monitoring en het omgaan met incidenten.

Verantwoordelijkheid is overal in verweven omdat het als onderdeel wordt gezien van procesmanagement.
ISM3 heeft niet het standaard format van volwassenheidsmodellen; het bestaat niet uit domeinen maar heeft wel volwassenheidsniveaus. Meetwijzen zijn zelf te kiezen en gekoppeld aan de doelen van de organisatie. Grootste nadeel is dat het geen self-assessment tool is die vrijelijk beschikbaar is. Desondanks is dit volwassenheidsmodel wel meegenomen in de analyse omdat uit de beschikbare documentatie naar eigen invulling en wens wel een check kan worden gedaan op de mate van volwassenheid. Een uiteindelijke beoordeling is gemaakt op basis van referenties vanuit ISM3 zelf, eerder uitgevoerde cases, en de wetenschappelijke literatuur (6, 8). Hierdoor is ook geen beoordeling te maken over de gebruiksvriendelijkheid.

3 Pijlermodel, volwassenheid informatiebeveiliging

Het volwassenheidsmodel ontwikkeld door Spruit, 3-Pijlermodel, gaat uit van drie pijlers: 1 - het uitvoeren van de goede activiteiten, 2 - het goed uitvoeren van de activiteiten en 3 - het goed beleggen van de uitvoering en aansturing (18). De norm ISO 27001 is als uitgangspunt genomen voor de eerste pijler. Een omschrijving van elk van deze pijlers is gekoppeld aan vijf volwassenheidsniveaus. De meting wordt uitgevoerd met een vragen-format voor semigestructureerd interviews.
Onder de eerste pijler wordt beleid als slechts een van de acht belangrijke onderdelen gezien, wat duidt op een beperkte nadruk op beleid. De tweede pijler checkt de kwaliteit van de werkwijze. De focus in dit model ligt op de uitvoering en naleving; de meeste interviewvragen worden gesteld over testen, risicoanalyses, monitoring en rapporteren van incidenten. Bij de derde pijler ligt het accent op verantwoordelijkheid en dit uit zich ook in een veelvoud aan vragen in het interviewformat met betrekking tot verantwoordelijkheid.
Het onderscheidend kenmerk van dit model is dat de meting wordt uitgevoerd door middel van semigestructureerde interviews en dat de vragen hiervoor al zijn uitgeschreven. Het uiteindelijke volwassenheidsniveau kan worden vastgesteld aan de hand van een analyseschema. Het voordeel en gelijk het nadeel van deze methode is dat het vrijheid geeft aan de interpretatie van de afnemer van de meting. Daarnaast is slechts één eerdere meting uitgevoerd onder 23 waterschappen en is er nog niet (wetenschappelijk) over gepubliceerd, waardoor de erkenning beperkt is. Verder is het model alleen beschikbaar in het Nederlands.

Welke volwassenheidsmeting is de beste?

In dit artikel zijn de vier meest relevante informatiebeveiligingsvolwassenheidsmodellen omschreven en geanalyseerd aan de hand van gestelde criteria, zodat elke organisatie kan bepalen welk volwassenheidsmodel het meest relevant is. Drie van de vier geselecteerde volwassenheidsmodellen hadden een vergelijkbare score, waar het model van NBA-LIO uiteindelijk de hoogste score had.
Samengevat hebben de modellen de volgende sterke en

minder sterke punten. **NBA-LIO** springt er positief uit op het gebied van de aanwezigheid van de elementen van een volwassenheidsmodel, gebruiksvriendelijk, koppeling met de verschillende normen. Minder sterk ontwikkeld is de flexibiliteit, de nadruk op het belang van beleid en verantwoordelijkheid. **C2M2** scoort over zijn geheel voldoende maar niet uitzonderlijk en heeft een goede structurele basis die alle elementen van een volwassenheidsmodel bevat. **ISM3** is flexibel en benadrukt het belang van de naleving en verantwoordelijkheid. De gebruiksvriendelijkheid laat echter te wensen over doordat de documentatie niet in zijn geheel beschikbaar is. Het **3-Pijlermodel** legt de nadruk op uitvoering, naleving en verantwoordelijkheid en heeft een betrouwbaar meetinstrument, over zijn geheel scoort het ook voldoende maar niet uitzonderlijk positief of negatief.
De korte omschrijvingen in dit stuk zijn waarschijnlijk te beperkt voor een uiteindelijke keuze, maar geeft een mooie opstap voor een gesprek over welk model in een organisatie toepasselijk is. Als in de toekomst een volwassenheidsmeting op de planning staat, kan deze analyse als input dienen.

Referenties

(1) Almuhammadi, S., & Alsaleh, M. (2017). Information Security Maturity Model for Nist Cyber Security Framework. Computer Science & Information Technology (CS&IT), 7(3), 51-62.

(2) Caralli, R., Knight, M., & Montgomery, A. (2012). Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability Mark Knight, CGI Group and GridWise Architecture Council (GWAC) Member.

(3) CIP. (2017). Grip op Privacy: Privacy Volwassenheidsmodel - Model voor organisaties om te groeien in de omgang met privacy. www.cip-overheid.nl/media/1141/20171102-privacy-volwassenheidsmodel-v3_0_9.pdf

(4) De Bruine, H., Lucero Garau, F., & Spruit, M.E.M. (2019, 6) Een praktisch volwassenheidsmodel voor informatiebeveiliging. iB-Magazine, 4-9 www.pvib.nl/actueel/ib-magazines/ib-magazine-2019-6/downloaden

(5) ISM3 Consortium. (2007). ISM 3 Information Security Management Maturity Model

(6) Karokola, G., Kowalski, S., & Yngström, L. (2011). Towards An Information Security Maturity Model for Secure e-Government Services : A Stakeholders View. In Proceedings of the 5th International Symposium on Human Aspects of Information Security & Assurance, Haisa (pp. 58-73).

(7) Kohlegger, M., Maier, R., & Thalmann, S. (2009). Understanding maturity models results of a structured content analysis. Proceedings of I-KNOW 2009 - 9th International Conference on Knowledge Management and Knowledge Technologies and Proceedings of I-SEMANTICS 2009 - 5th International Conference on Semantic Systems, (December 2016), 51-61

(8) Le, N.T., & Hoang, D. B. (2016). Can maturity models support cyber security? In Proceedings of the 35th IEE International Performance Computing and Communications Conference. Las Vegas.

(9) Luma, A., Abazi, B., Selimi, B., & Hamiti, M. (2018). Comparison of Maturity Model Frameworks in Information Security and Their Implementation. In International Conference on Engineering Technologies (ICENTE'18) (pp. 102–104)

(10) Miron, W., & Muita, K. (2018). Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure. In Technology Innovation Management Review (Vol. 4).

(11) NBA-LIO. (2019). Handreiking bij Volwasssenheidsmodel Informatiebeveiliging. www.nba.nl/globalassets/over-de-nba/ledengroepen/lio/lio-new/nba-lio-norea-handreiking-bij-volwassenheidsmodel-informatiebeveiliging-januari-2019.pdf

(12) Paulk, C., Curtis, B., & Chrissis, M. B. (1993). Capability Maturity Model , Version 1.1. Software Engineering Institute, 18–27. https://doi.org/10.1109/52.219617

(13) Payette, J., Anegbe, E., Caceres, E., & Muegge, S. (2015). Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects. Technology Innovation Management Review, 5(6), 26-34.

(14) Poppelbuss, J., & Roglinger, M. (2011). What Makes A Useful Maturity Model? A Framework of General Design Principles for Maturity Models and Its Demonstration In Business Process Management. In European Conference on Information Systems (ECIS)

(15) Rea-Guaman, A., San Feliu, T., Calvo-Manzano, J. A., & Sanchez-Garcia, I. D. (2017). Comparative Study of Cybersecurity Capability Maturity Models. In Mas, A., Mesquida, A., O'Connor, R.V., Rout, T., Dorling, A. (eds.) SPICE 2017. CCIS, vol. 770 (pp. 100-113)

(16) Salah, D., Paige, R., & Cairns, P. (2014). An Evaluation Template for Expert Review of Maturity Models. In Product-Focused Software Process Improvement (pp. 318-321).

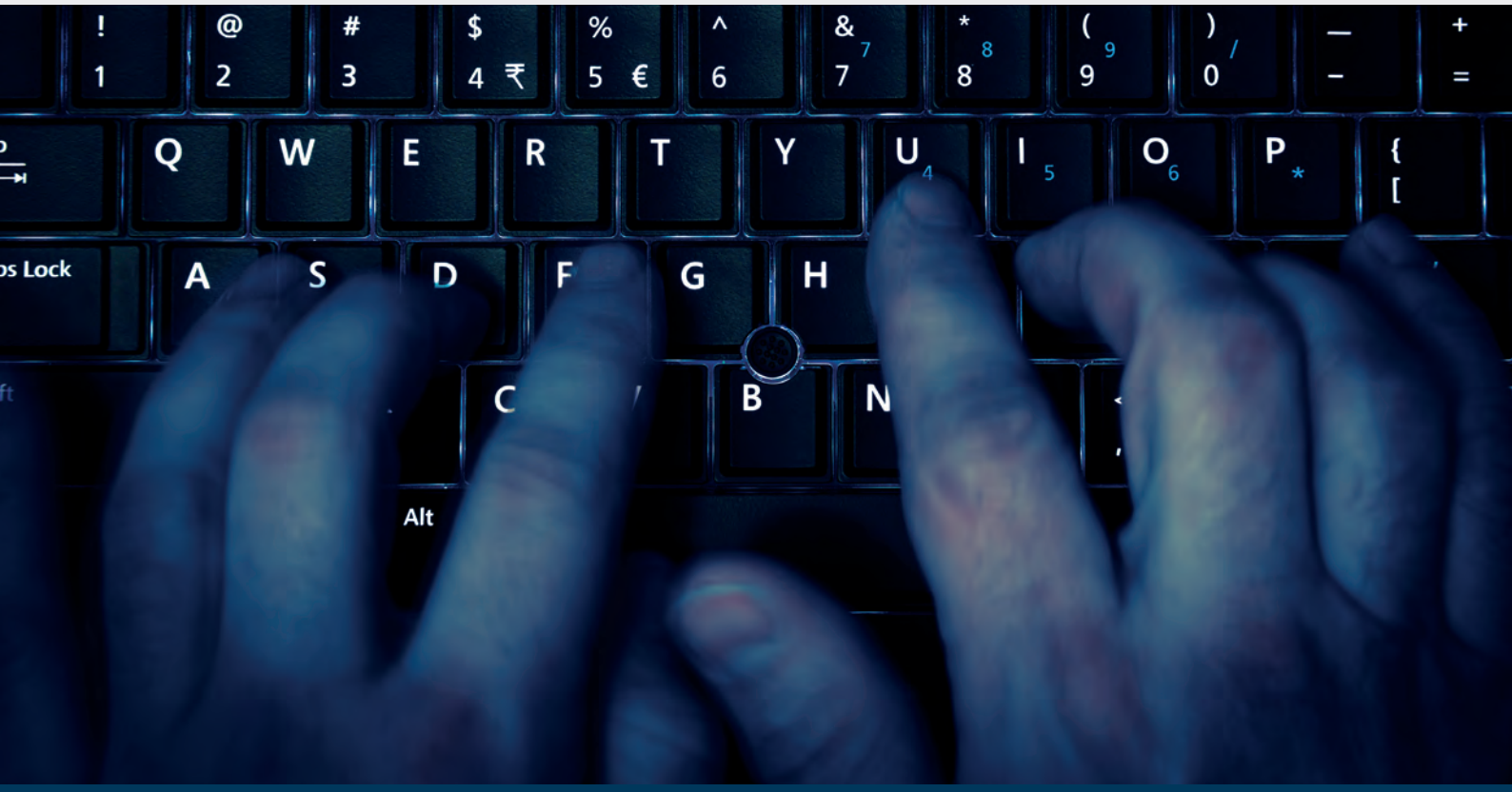
(17) Saleh, M.F. (2011). Information Security Models. International Journal of Computer Science and Security, 5(3), 316-337.

(18) Spruit, M. (2017). Volwassenheid Informatiebeveiliging; 3-Pijlermodel. RAAK-project Veilig Water.

(19) Thomson, K., & Von Solms, R. (2006). Towards an Information Security Competence Maturity Model. Computer Fraud & Security, (May), 11-15.

(20) US Department Homeland Security. (2014). Oil and Natural Gas Subsector Cyber Security Capability Maturity Model (ONG-C2M2) Version 1.1.

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 1: Cybercriminelen gijzelen Stock Foundation

Het ene moment lijkt er geen vuiltje aan de lucht, het volgende ogenblik komt de ontdekking. Alle bestanden zijn versleuteld, bedrijfsgeheimen en persoonsgegevens liggen op straat. Elke dag opnieuw lukt het cybercriminelen om bedrijven stil te leggen, af te persen en grote sommen geld afhandig te maken.

Totdat je zoiets zelf meemaakt blijft dit feit vooral een abstract gegeven uit de krant. Getroffen ondernemers en bestuurders ondervinden echter aan den lijve dat deze vorm van cybercrime een buitenproportionele impact heeft. Niet elk bedrijf of elke instelling komt zo'n slag financieel te boven. Maar ook de persoonlijke ervaring is zeer impactvol voor slachtoffers. Verplaats je eens in de derde generatie ondernemer van een groot familiebedrijf die zich realiseert dat hij wellicht degene is die het bedrijf verliest. Het bedrijf dat opa oprichtte en vader groot maakte.

Waargebeurd verhaal

Northwave helpt dagelijks organisaties die in zo'n situatie terechtkomen. Op basis van vijftien jaar ervaring met emergency response onderzoeken gaan we in een reeks van drie artikelen in op hoe een organisatie haar Cyber Resilience kan vergroten. We nemen in elk artikel steeds een waargebeurd verhaal als uitgangspunt. Namen en sommige details zijn veranderd om de slachtoffers te beschermen. We geven vanuit de evaluatie van elk van die incidenten realistische handvatten voor uw besluitvorming. We hopen daarmee een bescheiden bijdrage te leveren aan het aanscherpen van uw veerkracht. We nemen daarbij bewust het perspectief van de portefeuillehouder van het management van informatiebeveiliging. Die rol noemen we voor het gemak hierna de Information Security Officer.

De unified kill chain

Binnen het Northwave Computer Emergency Response Team (NW-CERT) spreken we vaak over `de grote drie': ransomware, business e-mail compromise en insider threats. Dat zijn de inbreuken waar we het meest frequent bij assisteren. De Unified Kill Chain is een model om aanvallen inzichtelijk te maken. De Unified Kill Chain is in 2017 voorgesteld door Paul Pols, als afgeleide van de Cyber Kill Chain® van Lockheed Martin, het MITRE ATT&CK framework en enkele andere modellen. Het deelt cyberaanvallen op in achttien unieke stappen binnen drie fasen (IN, THROUGH en OUT) - waarbij overigens niet elke stap in elke aanval wordt doorlopen.

We ontleden elke aanval in deze reeks artikelen aan de hand van dit model. Elk stadium in dit model biedt aanknopingspunten voor defensieve maatregelen ten aanzien van specifieke dreigingen. Zo'n model voor dreigings- en aanvalsanalyse is dus zeer bruikbaar om een risicobehandelplan actueel te houden.

IN	THROUGH	OUT
INITIAL FOOTHOLD Compromised System	NETWORK PROPAGATION Internal Network	ACTION ON OBJECTIVES Critical Asset Access
De acties die de aanvaller onderneemt om het netwerk binnen te dringen tot aan het punt dat dit gelukt is.	De acties die de aanvaller onderneemt om zich binnen het netwerk te bewegen.	De acties die de aanvaller onderneemt om zijn uiteindelijke doel te bereiken.
- Reconnaissance - Weaponization - Delivery - Social Engineering - Exploitation - Persistence - Defensive Evasion - Command & Control	- Discovery - Privilege Escalation - Execution - Credential Access - Lateral Movement	- Collection - Exfiltration - Target Manipulation - Objectives

Tabel 1 - Killchain.

Meeste slachtoffers door ransomware

We beginnen met een praktijkgeval van een aanvalsvorm die verreweg de meeste slachtoffers maakt. Ransomware of gijzelsoftware is kwaadaardige software die de systemen of bestanden van een slachtoffer versleutelt, waarna de sleutel tegen betaling wordt aangeboden. Ransomware kan leiden tot significante impact op de continuïteit van een bedrijfsvoering. Vaak komen de primaire processen van organisaties voor meerdere dagen, soms langer, volledig tot stilstand. De financiële gevolgen gaan daarmee vaak veel verder dan de betaling van het losgeld. Afgezet in het model van IN, THROUGH en OUT ziet een dergelijke aanval er in algemene zin zo uit:

IN	THROUGH	OUT
Uitbuiten van een kwetsbaarheid van een server die aan het internet hangt. Voor bekende kwetsbaarheden zijn vaak kant-en-klare hulpmiddelen beschikbaar.	Laterale beweging: ver-spreiden door het netwerk (via kwetsbare systemen of onvoldoende toegangscontrole). De aanvaller hopt hier van computer naar computer.	Versleutelen van bestanden en losgeld vragen. De aanvaller laat een cryptografische functie los op de bestanden – de sleutel die nodig is om deze versleuteling ongedaan te maken moet van de aanvaller worden gekocht.
Phishing e-mail. Een e-mail met malafide attachment of link. Deze e-mails kunnen op maat gemaakt zijn en zijn dan vrijwel niet van legitieme e-mail te onderscheiden.	Privilege escalation: Admin worden door wachtwoord raden, onveilig ingestelde gebruikersrechten of kwetsbaarheden. De aanvaller probeert op een computer meer rechten en daarmee meer mogelijkheden te krijgen.	Downloaden van gevoelige gegevens - dreigen met publiceren. Bedrijfsgevoelige gegevens of persoonsgegevens worden van de server gestolen. Het slachtoffer moet betalen om publicatie te vermijden.
Remote access software – kwetsbaar wachtwoord. Als vanaf het internet ingelogd kan worden kunnen de aanvallers proberen het wachtwoord te raden.	Laterale beweging en privilege escalation kunnen om en om worden ingezet. Wissen van de backup-bestanden.	Laat zich goed combineren met versleutelen.

Tabel 2 - Killchain.

Tabel 3 - Killchain.

We zien opties om binnen te komen (IN), het raakvlak uit te breiden (THROUGH) en ook verschillende routes naar het creëren van impact (OUT). Uiteindelijk wil een aanvaller een positie van waaruit voldoende grip en kennis wordt verkregen om eisen te stellen en die ingewilligd te krijgen. Tamelijk abstract nog, maar wel degelijk al functioneel in de beoordeling van eventuele maatregelen. Laten we nu eens kijken hoe dat verloopt in een noodgeval dat zich daadwerkelijk heeft voorgedaan.

Krantenkop: 'Ransomware treft Stock Foundation'

Het is maandagochtend. Zoals altijd is Jan-Jaap de eerste op kantoor. Hij start Word op, maar krijgt een melding dat het laatst geopende bestand, waar hij vrijdagmiddag nog aan werkte, niet meer bestaat. Hoe kan dat? Hij bekijkt zijn persoonlijke map op de fileserver en ziet dat alle bestanden een voor hem onbekende extensie hebben. Hij vindt ook een ransom.txt bestandje. Daarin staat dat alle bestanden van Stock Foundation zijn gegijzeld en dat losgeld wordt gevraagd. De boodschap verwijst naar een website voor verdere instructies. Stock Foundation maakte in het verleden gebruik van de applicatie Confluence. Deze software was bereikbaar via internet. Het programma werd niet meer actief gebruikt maar was ook niet verwijderd. Confluence had een recente security-bug die het aanvallers mogelijk maakte om via de applicatie commando's op het onderliggende systeem te draaien. De kwetsbaarheid was onlangs gepatcht, maar Stock Foundation draaide een oude versie van het programma. Iets meer dan een maand na het bekendmaken van de kwetsbaarheid, werd Stock Foundation via Confluence aangevallen. Omdat Confluence draaide met domain administrator-rechten kon de aanvaller vanuit de Confluence server eenvoudig het merendeel van de servers in het netwerk bereiken. Hij kopieerde de database en installeerde een bekende ransomwaretool op de servers. Dit werd door het antivirusprogramma herkend en geblokkeerd. Hierop probeerde de aanvaller een nieuw type ransomware. Deze variant werd niet gedetecteerd. De aanvaller besmette vanuit de Confluence-server andere systemen in het netwerk, vernietigde de back-ups, schakelde de antivirussoftware uit en versleutelde de bestanden. Systeeminformatie werd naar een door de aanvaller beheerde computer gestuurd om later de ontsleuteling mogelijk te maken. Tenslotte liet de aanvaller een ransomnote achter - een bericht met betaalinstructies voor het slachtoffer. Stock Foundation werd niet als enige getroffen door deze aanval. De aanvallers hadden internet gescand op kwetsbare systemen en de aanval vrijwel geheel geautomatiseerd. Uiteindelijk betaalde Stock Foundation ruim 1,2 miljoen euro losgeld aan de aanvallers. Er kan met enig succes worden onderhandeld over de hoogte van dat losgeld, maar de aanvallers zijn zeer goed op de hoogte van de financiële mogelijkheden van het slachtoffer en de positie waarin men zich bevindt. In een drukke periode hebben de systemen twee weken stilgelegen.

De schade is dus een veelvoud van dit bedrag. Als we deze aanval plaatsten in het model, ziet deze aanval er zoals bovenstaande tabel uit:

Incident evaluatie

Zet je de gebeurtenissen bij Stock Foundation af tegen dat model in vereenvoudigde vorm, dan zie je waar het beter had gekund. Het voorgaande voorbeeld betreft slechts één van de mogelijke scenario's. In de praktijk is elke aanval anders. Het is dus van belang voor de Information Security Officer om ook de varianten in ogenschouw te nemen.

Risicobewustzijn

Onder de lezersgroep van iB-Magazine hoeven we waarschijnlijk geen lans te breken voor het belang van een gestructureerde aanpak van Information Security Management. In de analyse van het incident bleek dat een dergelijke structuur ook grotendeels ontbrak bij Stock Foundation. Er was niemand aangesteld die zich specifiek met deze risico's bezighield. IB was een aangelegenheid die werd verondersteld te worden geregeld door de IT-afdeling. Die liet dat over aan een tweetal Service Providers. Veel organisaties worden nog steeds verrast door een aanval. Dat is verbazingwekkend. Immers, als je de actualiteit volgt en weet dat je afhankelijk bent van digitale informatievoorziening, lijkt het een eenvoudige optelsom dat een dergelijk scenario voor jouw bedrijf ook tot de mogelijkheden behoort. Toch zien we met name het senior management (als reflectie van positie, soms ook van leeftijd) nog behoorlijk onvolwassen acteren. Het is tragisch dat incidenten

nodig zijn om de organisatie te motiveren om haar continuïteit adequaat te beschermen. Voor bestuurders schuilt daarin ook steeds nadrukkelijker een persoonlijk aansprakelijkheidsrisico. Verzekeraars reageren hierop met aanvullende uitsluitingsclausules en nieuwe producten. Het is de verantwoordelijkheid van de Information Security Officer om ook op dit risico te wijzen.

Detecteren en reageren

Door goed te monitoren welke componenten zich in de omgeving bevinden en wat hun actuele status is ten aanzien van bekende kwetsbaarheden (vulnerability & asset management), kan daarop worden ingegrepen in geval van een incident. Uit onze praktijk blijkt dat het voor eigen IT-teams, maar zelfs ook voor IT-Service Providers vaak lastiger is dan je mag verwachten, om zelfs maar de basis-hygiëne op orde te houden. Dat is doorlopend dus een punt van zorg voor de Information Security Officer.
Ook op end points (EDR), in het netwerk (NIDS) en op applicatie-niveau kunnen allerlei gedragingen worden gedetecteerd die aanwijzingen zijn voor IN-, THROUGH- en OUT-gerelateerde events. Er zijn allerlei tools en technologieën om die monitoring en detectie te doen. Voor veel organisaties blijkt het echter vrijwel onmogelijk om zelfstandig de response op alarmering uit die tools te operationaliseren. Eigen IT-teams zijn te krap bezet, de kennis om analyse van alarmering te doen is beperkt. Om die reden wordt (vaak) voor outsourcing gekozen, door een MDR-dienst (ook wel SOC/SIEM service) in te kopen.
De Information Security Officer kan zichzelf daarbij een groot plezier doen door hiermee haar of zijn onafhankelijke informatiepositie te waarborgen. Juist omdat dergelijke monitoring veel inzicht geeft in de kwaliteit van de intrinsieke veiligheid (beheer en maatregelen) binnen de IT-omgeving, is deze functie een waardevol instrument om doorlopend de kwaliteit te meten en interne en externe IT-leveranciers scherp te houden. Bovendien kan dergelijke monitoring ook veel informatie verschaffen over de kwaliteit van niet-technische maatregelen, door use cases te bouwen die gericht zijn op het meten van het effect van beleidsmatige, procedurele en gedragsgerichte maatregelen. De rapportage van zo'n dienst wordt dan een belangrijke (near-real time) input voor de 'check' fase van het kwaliteitsmanagementsysteem.

3-2-1-strategie

Het incident heeft ook laten zien dat de bestaande back-upmechanismen onvoldoende bescherming bieden tegen ransomware. Om te beschermen tegen ransomware, moet het back-upmechanisme bestand zijn tegen een zogeheten 'insider threat', iemand met volledige interne netwerktoegang en de daarbij behorende inloggegevens. Idealiter volgen back-ups de 3-2-1-strategie:
3 actuele (procesafhankelijk) kopieën van de data in totaal;
waarvan 2 lokaal maar op verschillende media of apparaten; en
minstens 1 exemplaar off-site.
Dit resulteert niet direct in bescherming tegen aanvallen van binnenuit, maar er zijn verschillende strategieën om dit in de praktijk te brengen:

1. Gebruik één medium waaraan alleen data toegevoegd kan worden, zoals een tapedrive of een set harde schijven met een proces voor offline opslag. Dit zorgt ervoor dat de back-ups niet kunnen worden overschreven of verwijderd;
2. Gebruik een pull-strategie om de back-upgegevens naar een apart apparaat toe te trekken, een apparaat dat niet op een domein is aangesloten en correct is beveiligd. Deze machine kan inloggen op de machines die een back-up nodig hebben (deze haalt dus de gegevens op), zodat de machines niet direct de inloggegevens van de back-upmachine hebben;
3. Gebruik een cloudservice voor de off-site back-up op locatie. Cloudservices bieden verschillende methoden om het verwijderen van een back-up niet toe te staan. Daarnaast bieden deze services vaak uitgebreide controle over de dataretentie.

De Information Security Officer kan hier waarde toevoegen door, zoals dat hoort, naast opzet en bestaan, vooral ook de werking te testen. Uit vrijwel alle zaken die we doen blijkt steeds weer dat men dacht een werkende back-upstrategie te hebben. Alleen was dat nooit getest of beoefend. Oefenen is een zeer kosteneffectief middel om de kwaliteit te bepalen. Je krijgt er behalve een vaststelling van werking van je aanpak immers ook ervaring, kennis en kunde voor terug. Oefeningen, zeker als ze gebaseerd zijn op een goed scenario, spreken daarnaast tot de verbeelding van alle collega's in de organisatie. Breed delen dus die resultaten!

Never waste a good incident

Met dat veelgehoorde adagium sluiten we dit artikel af. We dringen er bij al onze klanten op aan ervaringen te delen met hun stakeholders. Intern richting al het personeel en extern in elk geval in de ketens waarin je actief bent. Niet in de laatste plaats omdat je nooit kunt uitsluiten dat bij de aanval op jouw organisatie niet ook een aanvalsroute is open komen te liggen naar je leveranciers of afnemers. Sommige dappere ondernemers kiezen zelfs voor de route naar de pers. Een mooi voorbeeld daarvan is Richard van der Helm, directeur en eigenaar van het gelijknamige transportbedrijf. Hij gaat na een fiks ransomware-incident in gesprek met Volkskrant-journalist en cyber-auteur Huub Modderkolk (1) en (2).
Hoe dan ook, het delen van kennis is, in deze toch ongelijke strijd, een wapen dat we altijd kunnen inzetten. Dus laten we dat ook doen. Organisatie, de techniek én de mens.

Referenties

(1) Het is oorlog maar niemand die het ziet, 2019. Uitgeverij Podium, 11de druk
(2) https://www.volkskrant.nl/nieuws-achtergrond/niet-betalen-aan-computergijzelaars-klinkt-goed-tot-je-wordt-gehackt~bf580bf6/

Auteur: Tim Janssen is werkzaam bij Visma Software B.V. en is bereikbaar via tim.janssen@visma.com.

Met een SSI behoudt de gebruiker regie over zijn eigen data

Met de introductie van de General Data Protection Regulation (GDPR) is er bij het grote publiek en in het bedrijfsleven meer aandacht voor privacy, gegevensbescherming en het correct gebruik van persoonlijke data. Een belangrijke eis van GDPR is toezicht en toestemming bij het verwerken van gevoelige data. Tegelijkertijd zien we dat grote internetbedrijven steeds rijker en machtiger worden door het verzamelen en verkopen van gebruikersdata aan derden. Een SSI (Self Sovereign Identity) kan uitkomst bieden.

Met PSD2 moeten banken API's beschikbaar maken voor derde partijen. Derden mogen met toestemming van de gebruiker betalingen verrichten en data gebruiken voor analyses. PSD2 gaat het weliswaar om partijen met een vergunning die onder toezicht staan van centrale banken, maar het idee dat bankgegevens of betaalinformatie buiten je eigen bank terecht kan komen maakt veel mensen toch wantrouwig. Het feit dat ook bedrijven als Facebook en Google in bepaalde landen al een licentie hebben gekregen sterkt dit wantrouwen. Met PSD2 worden grote databedrijven nog rijker en machtiger. Daarnaast gebruikt een groot aantal internetdiensten Facebook- en Google-identiteiten om gebruikers te authentiseren waardoor er nog meer data verzameld wordt. Inloggen met je Facebook- en Google-profiel levert niet alleen gemak op, maar ook data voor deze bedrijven net als de veelgebruikte Facebook-pixel die ook data van niet Facebook-gebruikers vastlegt. De roep om data-soevereiniteit terug te geven aan de gebruiker wordt steeds luider. Een belangrijke voorwaarde voor data-soevereiniteit is een betrouwbare en veilige digitale identiteit. Visma Software B.V gelooft dat de Self Sovereign Identity (SSI) de beste kanshebber is. Daarom is Visma Connect Sovrin steward ontwikkeld en werken wij value added services om de adoptie van SSI te bevorderen.

Regie over je eigen data

Met een SSI behoudt de gebruiker regie over zijn eigen data. Het SSI-concept is verder uitgewerkt door Christopher Allen in `The path to Self-Sovereign Identity' waarin hij de tien guiding principles beschrijft (1). De belangrijkste eigenschap van SSI is dat de gebruiker bepaalt of data wel of niet gedeeld wordt en ook met wie. Dit sluit perfect aan met privacywetgeving zoals GDPR, waarin steeds meer nadruk ligt op toestemming van de gebruiker bij het verwerken en gebruiken van data. Nog een ander belangrijk aspect dat SSI gemeen heeft met GDPR is dataminimalisatie. Met SSI geef je alleen de minimaal benodigde data om jezelf te authentiseren. Stel bijvoorbeeld dat je in de kroeg een biertje bestelt. Dan kan het zijn dat een gebruiker zich moet identificeren. Momenteel gebeurt dit met een ID-kaart. Een ID-kaart bevat veel meer informatie dan nodig is om te bepalen of iemand een biertje mag drinken. Zo staat er op welk geslacht je hebt, wat het land van herkomst is en zelfs je BSN.

Voorbeeldauthenticatie met SSI

Met SSI zou deze situatie er heel anders uitzien. SSI werkt met attributen zoals een verjaardag, maar ook `gebruiker is Nederlander', of `gebruiker is 18+'. Deze attributen moeten eerst bij een vertrouwde instantie opgevraagd worden zoals de overheid, de bank of het CBR; instanties die al veel persoonlijke informatie bezitten. Via de SSI-app kan de gebruiker vervolgens op DigiD of iDIN inloggen om de persoonlijke informatie om te zetten in digitaal ondertekende attributen op je telefoon. Aan de digitale ondertekening kan een andere partij zien waar de attributen vandaan komen, zodat ze hier op kunnen vertrouwen. Om terug te komen op het voorbeeld van het bestellen van een biertje, de SSI-gebruiker laat een QR-code zien en de barbediende scant deze. De SSI-gebruiker krijgt vervolgens een pop-up dat het attribuut `18+' opgevraagd wordt. De SSI-gebruiker kan dan akkoord gaan om dit attribuut te delen. Als de SSI-gebruiker akkoord gaat en inderdaad het `18+'-attribuut heeft staan in zijn telefoon, dan krijgt de barbediende een groen licht te zien. Op deze manier krijgt de barbediende alleen informatie die relevant is en dus niet een BSN of een geboorteplaats. Sterker nog: zelfs je leeftijd komt de barbediende op deze manier niet te weten. Dit sluit dus naadloos aan op het dataminimalisatie-aspect van GDPR. Er zijn ondertussen veel verschillende SSI-oplossingen waar we iets dieper op in zullen gaan.

Verschillende SSI-implementaties

De verschillende SSI-oplossingen kennen elk hun voor- en nadelen. Veel van deze oplossingen gebruiken een blockchain op de achtergrond. Een blockchain is in feite een speciale database die gedistribueerd is over verschillende computers waarbij elke computer een identieke kopie bevat. Elke toevoeging aan de blockchain, moeten alle deelnemers in het blockchain-netwerk als transactie accepteren. Dit gebeurt met zogenaamde consensus algoritmes. Hierdoor weet je zeker dat iedereen in het netwerk naar dezelfde waarheid kijkt. De eerste toepassing van blockchain is bitcoin waarbij de blockchain gebruikt wordt om waarde-transacties uit te voeren zonder bank. In plaats van een bank die controleert of transacties aan alle spelregels voldoen, zijn deze vastgelegd in de blockchain en wordt dit decentraal gecontroleerd door alle deelnemers in het blockchain-netwerk. Een blockchain is eigenlijk niets anders dan een alternatief vertrouwensmodel waarbij er niet op een centrale partij vertrouwd hoeft te worden, maar dit collectief door een netwerk gedaan wordt.

Blockchain heeft kenmerken die interessant zijn voor bepaalde aspecten van SSI, al moet je hier wel mee oppassen. Door onder andere het gedistribueerde karakter van blockchain is het zeer lastig om informatie aan te passen of te verwijderen. Dit is deels de kracht van blockchain, maar het is daardoor ongeschikt voor het opslaan van persoonlijke

informatie. We hebben namelijk ook te maken met het recht om vergeten te worden. Daarnaast is een blockchain doorgaans publiek goed en is het dus niet bepaald slim om daar überhaupt gevoelige data in op te slaan. Dit is dan ook niet waar blockchain voor wordt ingezet; ook niet bij SSI.

Voordelen blockchain in SSI

Blockchain in SSI wordt hoofdzakelijk gebruikt voor zogenaamde decentralized identifiers (DIDs). Een DID is te vergelijken met een URL die naar een persoon verwijst, maar kan ook ingezet worden om naar organisaties, datamodellen en andere zaken te verwijzen. Het vernuftige van DIDs is dat deze uniek is voor elke relatie. Met andere woorden: mijn DID voor de Rabobank is anders dan voor de ING en ook weer anders voor de overheid. Hierdoor wordt correlatie voorkomen bij interactie met verschillende diensten. Een DID is ondertussen ook als standaard opgenomen door World Wide Web (W3) (2) en wordt steeds meer gezien als de toekomst voor een betrouwbaarder internet. Momenteel wordt er gebruik gemaakt van certificate authorities (CA's) om de veiligheid van een website te kunnen garanderen. Hiervan bestaan ondertussen veel valse certificaten. Met DIDs is het mogelijk om deze valse certificaten eenvoudig te verwijderen, hierover staat meer in het artikel Decentralized Public Key Infrastructure (3). Een ander voordeel van blockchain bij het gebruik van SSI is het gebruik van zogenaamde revocation hashes. Dit concept is bedacht door Sovrin waarbij elk attribuut standaard gelabeld is als ongeldig. Een gebruiker moet dan eerst met een hash op de blockchain bewijzen dat zijn attribuut geldig is. Door middel van een smartcontract op de blockchain kan een rechter bij een verkeersovertreding het rijbewijs-attribuut intrekken door de revocation hash op de blockchain te updaten. Het kunnen intrekken van attributen is een belangrijk aspect waarmee Sovrin momenteel voorop loopt ten aanzien van andere SSI-oplossingen. Op dit moment bestaan er nog geen goede alternatieven voor het intrekken van attributen op niet-blockchain varianten. Er zijn wel concepten om dit met een revocation server te doen, maar het gevaar daarbij is dat identiteiten eenvoudig te censureren zijn door een centrale partij en dat is juist iets wat we met SSI niet willen. Visma Software B.V. is te spreken over de oplossing van Sovrin en is Sovrin Steward om deze ontwikkeling te bevorderen en te participeren in het consensusprotocol van het Sovrin-blockchain-netwerk. We moedigen echter ook de ontwikkeling van andere SSI oplossingen aan en staan open voor alternatieven, eventueel zonder blockchain. Naast het Sovrin stewardship bevorderen wij de adoptie van SSI door het bouwen van nieuwe modules.

Autorisatie-register

Wij zijn in de logistieke sector als beheerder van iSHARE (4) betrokken bij de ontwikkeling van het autorisatie-register. iSHARE is een afsprakenstelsel voor het delen van data in de logistiek sector. Eén aspect van data delen is het vastleggen welke partij je machtigt om jouw data in te zien en te gebruiken. Tot nu toe resulteren implementaties van dit stelsel in (één of meerdere) centrale machtiging-registers. Ons onderzoek richt zich op een decentrale verwerking met een SSI oplossing, zoals Sovrin, waarbij gebruikers deze zelf kunnen beheren en niet afhankelijk zijn van een centraal register. De oplossing is zodanig dat het niet uitmaakt welke SSI oplossing de gebruiker benut en de hij/zij dit zelf kan beslissen. Het doel van dit autorisatie-register is om machtigingen makkelijker te maken. Het gebeurt nog regelmatig dat gebruikers het regelen van machtigingen te omslachtig vinden en in plaats daarvan wachtwoorden delen met familieleden of collega's. Dit is natuurlijk niet veilig en daarom moet het makkelijker gaan, zodat dit niet meer als een drempel ervaren wordt. Tevens maakt het autorisatie-register het mogelijk dat er minder data in een centraal register staat, waaronder de machtigingen die een gebruiker afgegeven heeft. Door dit bovendien overzichtelijk in een register te zetten hoeft een gebruiker ook niet meer meerdere omgevingen te beheren waarin al diens data staat.

Meer regie over data

Met de huidige wijze van data delen via internet lopen persoonsgegevens veel risico's en hebben mensen geen zicht op wat er met hun data gebeurt. Eén van factoren, die daarbij meespeelt, is een gebrek aan een vertrouwde, digitale identiteit. Een SSI is een type identiteit dat anders met persoonsgegevens omgaat en waarbij de gebruiker de regie weer terugkrijgt over zijn eigen data. SSI biedt de mogelijkheid om de echtheid van bepaalde gegevens te bewijzen (bijvoorbeeld leeftijd of kredietwaardigheid) en die op een minimale manier te delen met derden, waarbij voor die derden de noodzaak verdwijnt om details over de persoon op te slaan (geboortedatum, bankgegevens, etc.). Vanuit dit oogpunt zetten wij ook in op modules om gebruikers meer regie te geven en bereiken we minimalisatie van de data die door onze systemen verwerkt wordt.

Referenties

(1) http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

(2) https://www.w3.org/TR/did-core/

(3) https://www.weboftrust.info/downloads/dpki.pdf

(4) https://www.ishareworks.org/

COLUMN Berry

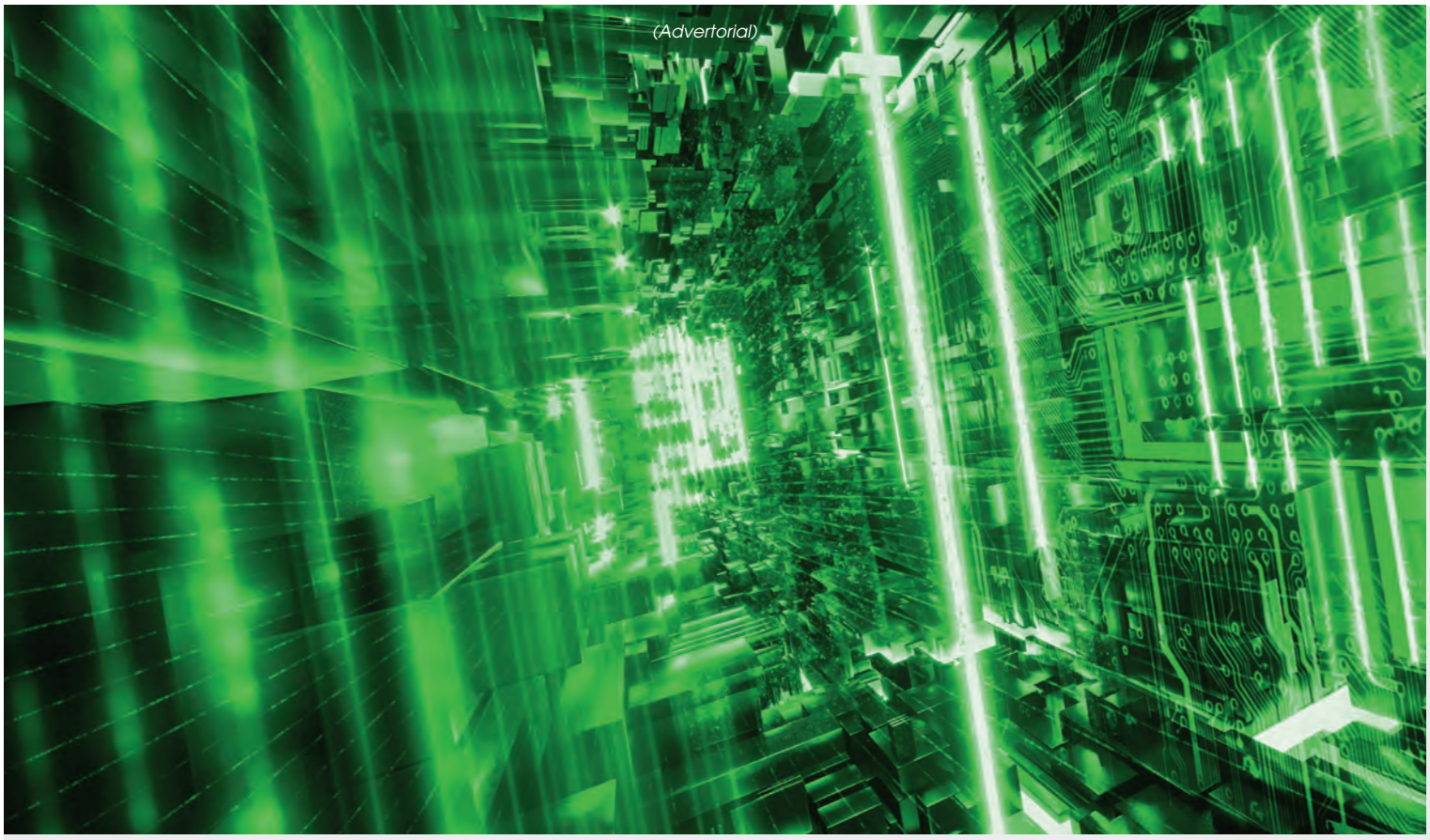
De hond is weer de dupe

Ik ben van de oude stempel; dat zal bij de trouwe lezers van mijn column geen verassing zijn. Ja, ik heb de opkomst van de PC meegemaakt. Ik was de trotse eigenaar van een echte IBM die onder IBM-DOS draaide. Deed het goed, maar was niet spectaculair. Nieuwe besturingssystemen kreeg je nooit en had je ook niet nodig, want het meeste werk deed je zonder dat je aangesloten was op een netwerk. De floppy bracht gewillig bestanden over naar een andere computer.

We zijn nu een paar jaar – zeg maar 40 jaar – verder en het leven is veranderd. Ik heb al heel lang geen floppy meer en de IBM is vervangen door een Apple. Een standalone PC bestaat niet meer want alles moet over het netwerk. Ik werk in een groot bedrijf met een netwerk van duizenden devices, laptops, kassaregisters, printers, telefoons, netwerkapparatuur en ik weet niet wat nog meer. Bij elke software update checkt een groot team van medewerkers of applicaties nog goed werken. Het kan gaan om hele kleine aanpassingen die heel veel werk met zich meebrengen. Als iedereen zijn groene bordje heeft opgestoken, kunnen we de aanpassingen uitrollen over alle werkplekken en beginnen we met de nieuwe update enzovoort enzovoort.

Totdat er donkere wolken verschijnen en de leverancier van ons besturingssysteem aangeeft te stoppen met de versie waar wij toevallig op draaien en die binnen 48 maanden niet meer gesupport wordt. Alarmfase 1, rode hoofden en wilde blikken in de ogen. Onze primaire applicatie draait niet op het nieuwe besturingssysteem en er wordt ook geen nieuwe versie meer gebouwd. We hebben nog vier jaar de tijd om een oplossing te bedenken en ik word niet goed. Ik ken onze gebruikersgroep een beetje.
Ik sla even drie jaar over. We zijn geen steek verder gekomen en de leverancier van het besturingssysteem blijft bij het standpunt, nog één jaar en ze stoppen met support. De paniek slaat helemaal toe, er wordt contact opgenomen of ze echt niet even willen doorgaan met support zodat we de systemen ook veilig kunnen houden. Jawel hoor dat willen ze wel, kost natuurlijk wel wat want er moet een heel team achterblijven om dit te doen. Jullie denken dat ik een beetje doorsla; was het maar zo. Grote gemeentes zoals Amsterdam, Tilburg, Nijmegen zijn nog niet toe aan een upgrade en betalen fors aan Micro$oft. Gemeente Amsterdam bijvoorbeeld, betaalt er 375.000 euro voor. Misschien moeten we toch de hondenbelasting of de onroerend zaakbelasting iets verhogen?

Berry



LEVEN IN EEN QUANTUMSAFE WERELD

Met Quantum Computers in het verschiet volgen wij een driepijlerbenadering om organisaties te ondersteunen die quantumsafety willen opbouwen.

Overzicht

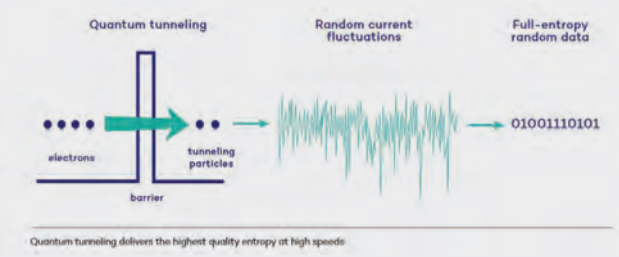
De computertechnologie gaat snel vooruit, met het volledige potentieel van quantumcomputing in het verschiet. Door gebruik te maken van de kracht van de quantumfysica zullen quantumcomputers in staat zijn om zeer complexe berekeningen uit te voeren in een fractie van de tijd die de beste supercomputers van vandaag nodig hebben.

Hoewel spannend, heeft deze toekomst ook zijn duistere kant. Gezien de snelheid en de kracht van quantumcomputers hebben ze het vermogen om mathematisch complexe problemen op te lossen waarop sommige van onze veiligheidssystemen zijn gebaseerd. Daarom hebben de cybersecurity-deskundigen het alarm geslagen dat quantumcomputers makkelijk de linies kunnen verslaan die worden gebruikt om onze gegevens te beveiligen. De implicaties zijn enorm en de race is om cybersecuritymaatregelen te bedenken en te implementeren die een quantumaanval tegen kunnen houden. De vraag is dan: hoe kunnen de bedrijven van vandaag hun beveiligingsinfrastructuren veilig maken voor de 'postquantum' wereld?

1. Gebruik echte, willekeurige getallen

Cybersecurity begint met sterke encryptiesleutels. Quantumsafe zijn, betekent dat gegevens worden beschermd met zo sterk mogelijke sleutels. Maar traditionele deterministische RNG's (Random Number

Generators) hebben mogelijk onvoldoende entropie om veilig te blijven bij een quantumaanval. Het integreren van volledige entropiesleutels in uw beveiligingsarchitectuur is een belangrijke eerste stap bij het bouwen van quantumveiligheid.
Gelukkig is deze technologie direct beschikbaar en kan deze gemakkelijk worden geïntegreerd. Door het meten van quantumtunneling-'ruis' genereer je willekeurige gegevens. Dit is een fenomeen waarbij een deeltje over een potentiaalbarrière reist dat het volgens de klassieke (Newtoniaanse) mechanica niet zou moeten kunnen oversteken.
In een RNG (Random Number Generator) wordt spanning gezet op een voorwaartse diodeverbinding. De diode bevat een barrière waardoor ladingsdragers kunnen 'quantumtunnelen'; zelfs als ze de energie missen om de barrière te kunnen doorbreken. Het aantal deeltjes dat in een bepaald moment in de tijd zal tunnelen is niet te voorspellen, waardoor het proces een ideale bron is voor willekeurige gegevens.



Dit type capaciteit zal nodig zijn ongeacht het gebruikte coderingstype - of het nu gaat om symmetrische codering met langere sleutels, die waarschijnlijk bestand zal blijven tegen quantumaanvallen -, of om het gebruik van nieuwe quantumbestendige algoritmen, die op dit moment worden onderzocht.

2. Integreer nieuwe coderingsalgoritmen in een crypto-agile omgeving
Cybersecurity is gebaseerd op verschillende industriestandaard-encryptie-algoritmen zoals RSA, AES en ECC, die elk bewezen hebben tot op een bepaald niveau van bescherming te presteren en met verschillende gebruiksdoeleinden. Symmetrische encryptie-algoritmen die worden gebruikt om opgeslagen gegevens te beschermen, zoals AES, zullen naar verwachting veilig blijven in een quantumwereld zolang er langere, 'full entropy'-sleutels worden gebruikt.
Asymmetrische algoritmen die worden gebruikt voor sleuteluitwisseling, zoals integer factorisatie (RSA), discrete logaritme (DH en DSA) en elliptische curve (ECC), zullen echter niet langer veilig zijn. Dit omdat quantumcomputers het type wiskunde dat wordt gebruikt om ze te beveiligen, kunnen doorbreken. Een van de reacties hierop is de implementatie van postquantum algoritmen, waarbij gebruik wordt gemaakt van wiskundige structuren zoals 'Latice-type' algoritmen die bestand zijn tegen quantumaanvallen.

3. Beschermen van de sleuteluitwisseling
Veilig sleutelbeheer vereist replicatieknooppunten - extra servers met de mogelijkheid om kopieën van sleutels te repliceren als een deel van het systeem om welke reden dan ook uitvalt. De overdracht van gegevens tussen replicerende knooppunten gebeurt doorgaans via een wederzijds geauthentiseerde TLS-verbinding, waarbij gebruik wordt gemaakt van RSA- of ECC-asymmetrische versleuteling voor de initiële sleuteluitwisseling. Dit deel van de TLS-verbinding zal kwetsbaar zijn voor quantumaanvallen. Symmetrische sleutelverpakking kan dit beschermen: een willekeurig getal kan worden gebruikt om een symmetrische sleutel te maken die een lading 'omwikkelt' (de RSA/AES-sleutel of een ander object), wat resulteert in een extra beveiligde TLS-overdracht.
Op een bredere schaal kan de QKD-technologie (Quantum Key Distribution) worden geïntegreerd in de beveiligingsarchitectuur om de veilige uitwisseling van sleutels mogelijk te maken zonder te vertrouwen op quantumresistente algoritmen. In plaats daarvan worden de wetten van de natuurkunde gebruikt om de belangrijkste uitwisseling te beschermen, wat de beste toekomstbestendige beveiliging voor de meest gevoelige communicatieverbindingen oplevert. Dit type technologie kan zelfs 'one-time pad' (OTP) encryptie ondersteunen, met behulp van echte willekeurige cijfers uit een quantumbron.

De bedreiging van quantumcomputers is zeer reëel en er moet snel maatregelen genomen worden om gevoelige gegevens te beschermen tegen toekomstige aanvallen. Het goede nieuws is dat meerdere facetten van quantumresistente cybersecurity al beschikbaar zijn. Een doordachte, systematische implementatie van onze drie pijlers kan een organisatie effectief sterk en operationeel houden voor de lange termijn

SRC
Secure Solutions

Contact
SRC Secure Solutions B.V. is de Nederlandse partner van QuintessenceLabs. Op srcsecuresolutions.eu vindt u meer informatie over quantum number generation en key management.

Auteur: Rens van Dongen is responsible for security & privacy risk and compliance for Consumer Identity & Access Management (CIAM). You can reach him at rens.van.dongen@iwelcome.com or @mosymuis on Twitter.

Fighting security risks beyond the bug

Data leaks have become an all-too-common societal problem. Still, 99% of the problems do not involve scary zero-day bugs. So why is security still hard? We need to accept that technology isn't going to save us. Rather, thinking it can, got us in this situation in the first place. We need a new way of teaching and implementing security across our organizations. I am introducing the AVA=Risk Security Model to help us get there.

Credential-stealing and abuse is the most common attack vector. That means there is no use for burglars to break the lock if they can just turn the key they copied and walk in. So, securing the door alone is not enough: how we handle our keys requires our attention as well, assuming we even locked the door in the first place. An emerging trend of explosive cyber leaks involves unprotected databases that are out there in the open. As we speak, organizations are unknowingly spitting out billions of sensitive records to anyone curious enough to look.

What use is having strong technology, if we forget about the people using it or neglect the information we entrust to it? Sure, those databases need to be better protected by technology. They require strong authentication or shouldn't be exposed to the public web. However, we already understand those solutions and still, we see that these mistakes in setup and maintenance are too easily made. That is a vulnerability in the technology itself, which is slowly addressed by vendors. They may improve default configurations and add scanning abilities, but next time it will be yet another type of vulnerable technology. And how will we cope in the meantime?

Broken communication

Let's consider phishing scams. While challenging, email security protocols can (and should indeed) be implemented to secure against domain spoofing. But an email mimicking a trusted domain or person will still pass the test. As a result, people will continue to be tricked and have their privileged credentials stolen. Not to mention the extraordinary success of CEO scams, raking in damages over $12,5B in 2018 according to FBI's Internet Complaint Center. Technology is part of the problem rather than the solution to abuse. Email, as well as the phone, are fundamentally vulnerable. This will not be fixed in the foreseeable future, if ever. That means we need to fight the problem from other angles.

We can use an analogy here. Fighting fire is possible in three ways, and we can pick which one is most effective and practical given the circumstances. Water is often convenient to combat heat, but if you want less oxygen in the case of a grease fire, a fire blanket is safest. Lastly, isolating the fuel can sometimes be most pragmatic: just wait for the fire to extinguish itself. Borrowing from this fire triangle, we can regard security risks as having three sides to attack as well. Spoiler alert: fixing vulnerabilities, let alone software bugs, plays only a part in one of those approaches.

Introducing the AVA=RISK Security Model

It's time to widen our scope of how to teach security and treat risk. First, we should clearly separate information security risks from technology. Unfortunately, security is regarded as an IT or engineering responsibility in most organizations. The AVA=RISK Security Model exposes the illusion of total security through technology. It provides us with a lens to treat risk, by shining light on Actors, Vulnerabilities and Assets. Explain each side for any risk, and mitigation measures can be selected. Usually, addressing only one angle will not suffice. Let's take the phishing problem as our example. The ease by which hackers can impersonate others through email is the vulnerability. And as we have seen, we do not have enough tools to adequately protect us against this. But water against heat isn't our only option. Luckily, we can also fight the fire by taking away actors or assets.

Actor

There are two active parties of actors in the phishing game: hackers and victims. We can't magically block or cure hackers from playing, so let's work with our colleagues. Security awareness is a fast-growing practice, yet it remains largely ineffective. Gamification, repetition and simulations should improve education programs. But how can we really engage our colleagues? At the core of the problem is the accountability perception that spam filters should do the job. And if it's the security team who believes this, how can we expect the controller or sales rep to take responsibility? We need to train anyone with an email address to build security hygiene habits. Reducing mistakes through better judgement skills results in fewer victims. And with victims reduced from the equation, there are fewer actors to participate in the phishing game. That will lower our risk of a data breach.

Vulnerability

Securing things by resolving vulnerabilities sounds easier than it is. If email is a fundamentally flawed system, what can one do? To some extent, organizations can decide on alternative means of communication. Slack is essential to millions of businesses, as are collaborative platforms like Microsoft Teams. Their closed and centralized nature is a strength for security. It will drastically lower chances of responding to an impersonated colleague asking for that payment or permission. For external reach though, email still has merit. When it is combined with encrypted file sharing, like the brand new Firefox Send, this vulnerability can be managed.

Asset

The third side requires us to consider what information assets are available and accessible. The 'principle of least privilege' should be the golden rule. Its application tends to fade over time as convenience takes over, so data governance is important. The GDPR also provides great advice in this regard. Both data minimization and data retention are guiding principles to decide on what to process, and for how long. If any one person has access to only a few data sources, a hacker will be limited in the same way, even if a phishing scam succeeds in stealing credentials. The famous criminal Willie Sutton was once asked why he robbed banks. He supposedly stated: "Because that's where the money is." Data is the new gold, so providing access to it must be thought of in the same way.

Technology is a tool

I'm inspired by how technology, society and policy interact. My professional career started with a decade in web development and a fascination for application security. Later roles in product and management allowed me to reassess our dependence on technology. Now, digital transformation allows us to transform our economy. We can scale our services and optimize our workforce. But technology can also take us hostage if it is not bounded. Security is like the brakes on our car. It may slow us down, but it also enables us to go faster. We should regard technology as just one of the tools in the security toolbox. If security is subject to technology, we are blind to many risks. And worse, we would miss out on great opportunities to combat risk. With AVA=Risk in mind, we can find better solutions and further raise security awareness.

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

Website security

'Het nieuwe normaal' op basis van RIVM-richtlijnen is inmiddels een bekende term in het nieuws, net als het RIVM als instituut waar de overheid haar gezondheidsbeleid op afstemt. Des te pijnlijker dat beveiligingsonderzoeker Tom Wolters in samenwerking met de NOS op 6 juni jl. onthulde dat de website infectieradar.nl een lek bevatte (1).

Op infectieradar.nl kunnen Nederlanders doorgeven of ze de afgelopen week coronaklachten hebben gehad. Iedereen met enige technische vaardigheid kon de antwoorden op persoonlijke en medische vragen van de deelnemers inzien. Direct volgden de verklaringen van het RIVM en de websitebouwer: de kwetsbaarheid zou al bekend zijn en niet doorgevoerd door de websitebouwer (1), maar die websitebouwer weet van niets (2). Hoe het ook zij, het lek wordt gedicht maar infectieradar.nl is op moment van schrijven (17 juni jl.) nog niet beschikbaar (3). Dat geeft te denken over website security. Hoe veilig zijn alle miljarden websites op het internet eigenlijk? Hoe zorg je als organisatie voor een veilige website? In hoeverre vertrouw je op je leverancier? Is de aandacht die het lek in de RIVM-website gekregen heeft terecht?

Fook Hwa Tan | Chris de Vries | Maarten Hartsuijker

Vertrouwen, vertrouwen en vertrouwen

Een websitegebruiker vertrouwt op de deugdelijkheid van een site zonder onderzoek te doen naar de kwaliteit van de websitemakers. En meer nog wanneer het gaat om een overheidswebsite, want wie staat meer op de bres voor onze burger dan de overheid? Waar begint vertrouwen ook alweer? De lezer van ons magazine grijpt even terug op het artikel van Erik Schoppen 'Keynote tijdens de security bootcamp 2019' (4). Daarin stelt deze neurowetenschapper dat vertrouwen begint in onze hersenen. Hij beschrijft dat vertrouwen zich ontwikkelt 'from brain trust to trust systems'. In zijn artikel: 'Vertrouwen gaat niet over veiligheid maar over vrijheid' (5) diept hij dat uit en licht toe dat in dit digitale tijdperk organisaties en samenwerkingsverbanden steeds complexer worden. De essentie is dat systeemvertrouwen (juist bij overheidsorganisaties) gebaseerd is op de kredietwaardigheid en reputatie van hun digitale netwerken. En dat vertrouwen heeft nu een forse deuk opgelopen.

Combineer dat met de beoogde verplichte corona-app en de vrijwillige overgave van patiëntendossiers (ook van degenen die uitdrukkelijk 'neen' hebben gezegd) door het ministerie. Waarom zouden wij onze overheid nog vertrouwen op hun vaak als loos ervaren toezeggingen en beloften?

Zorgplicht van een leverancier?

Onlangs is de discussie weer begonnen over de plichten van een IT-dienstverlener met betrekking tot beveiliging. Een uitspraak van de rechter van november 2018 werd onlangs openbaar (6). De zaak was aangespannen door een klant van een IT-bedrijf. Het IT-bedrijf had bij een opdracht onvoldoende beveiliging toegepast waardoor de klant slachtoffer werd van een ransomware-aanval. De rechter stelt dat het IT-bedrijf deze opdracht niet naar behoren heeft uitgevoerd. Dat de klant de voorgestelde beveiligingsmaatregelen van de hand zou hebben gewezen, maakt hier geen verschil. Het IT-bedrijf heeft een zorgplicht.
Dit komt nog meer tot uiting, omdat de klant vaak niet bewust is van de risico's die hij loopt bij het digitaliseren. Dus ondanks dat de verantwoordelijkheid daar ligt, kunnen we niet verwachten dat de klant duidelijke beveiligingseisen stelt. De klant is vaak ook niet bekwaam en mist kennis om duidelijke eisen te kunnen stellen. Als hij dat wel had, dan had hij het ook zelf kunnen doen. Door gebrek aan bewustzijn en kunde op het gebied van informatiebeveiliging zijn afnemers vaak ook niet in staat de oplevering te toetsen of het voldoende beveiligd is. Dit alles betekent, dat een leverancier de zorgplicht heeft om haar klanten goed beveiligde producten op te leveren. Bij deze plicht hoort ook het verder bewustmaken van de klant over de gelopen risico's. Beveiliging doen we samen!

Controle, controle, controle

Vertrouwen is goed, maar controleren is beter. Het is een bekend gezegde dat ook bij websitebeveiliging op gaat. Nu ben ik hier enigszins van wc-eend, want ik verdien mijn brood grotendeels met het uitvoeren van website penetratietesten. Maar daardoor kan ik ook uit ervaring zeggen dat ik tijdens pentests meer websites tegen kom met een ernstige fout zoals bij het RIVM, dan dat ik sites tegenkom waarin alles perfect op orde is. Als organisatie doe je er goed aan om altijd zelf de regie te voeren op de veiligheid van je sites. Ook als je ze extern afneemt. Dat begint bij het maken van goede (inhoudelijke) afspraken met de leverancier die de site bouwt en eindigt met een controle. Controleert de leverancier zelf aantoonbaar zijn product? Dan volstaat vaak een beknopte eigen controle die de kwaliteit ervan bevestigt (of eigenlijk: niet tegenspreekt). Controleert de leverancier niets (of alleen geautomatiseerd), dan doe je er verstandig aan zelf een volwaardige pentest uit te voeren.

Referenties

(1) https://nos.nl/artikel/2336416-lek-in-rivm-coronasite-gegevens-van-gebruikers-makkelijk-in-te-zien.html
(2) https://beveiligingnieuws.nl/nieuws/websitebouwer-spreekt-minister-tegen-over-rivm-lek
(3) https://www.rivm.nl/nieuws/infectieradar-tijdelijk-niet-beschikbaar
(4) informatiebeveiliging magazine nr. 4 pagina 34 t/m 36
(5) informatiebeveiliging magazine nr. 5 pagina 4 t/m 7
(6) https://www.security.nl/posting/660081/IT-bedrijf+moet+schade+door+ransomware+bij+klant+grotendeels+vergoeden

Auteur: John Sherwood Chief Architect of The SABSA Institute C.I.C. john.sherwood@sabsainstitute.org

The Open Security Architect: Concepts, Principles and Models

Here we launch a new regular column for the magazine. This is the first one of the series, penned under the nom de plume of The Open Security Architect. In every issue of IB there will be a new topic described over 2 to 3 pages by this mythical persona. Over time this will accumulate into a small encyclopaedia of security architecture. The guest author is John Sherwood, Chief Architect of The SABSA Institute C.I.C., although the use of a persona allows for other guests to be invited should that be appropriate. John is one of the world's leading thinkers in security architecture and the lead author of the book: Enterprise Security Architecture (1), in which SABSA is described.

To begin this series, we shall first look at some of the basic language used in describing security architecture. One of the key purposes of architecture is to have a common language in which to express design patterns for systems. In this short paper we define the common terms and the concepts that they represent. Terms in bold italics are the key terms being established here. SABSA is a security architecture framework that uses all these terms in the context described here from the relevant ISO standards. They are generic terms used not only within SABSA, but of course SABSA uses this common lexicon.

Systems

ISO/IEC 15288 (1) describes systems as: 'being man-made and may be configured with one or more of the following: hardware, software, data, humans, processes (e.g. processes for providing service to users), procedures (e.g. operator instructions), facilities, materials and naturally occurring entities'. The term architecture is traditionally the description of the built environment, such as villages, towns and cities in which humans reside, work and pursue leisure. It has also traditionally been applied to the building of ships (naval architecture). Now with this ISO definition we can see that these traditional examples are merely special cases of systems architecture. In the 21st century what is also implied is the presence of information technology (IT), along with every other kind of engineering discipline, depending on the purpose and function of the system of interest.

All the parties with an interest in the system are known as stakeholders. The stakeholders' interests are expressed as concerns about the system (see ISO/IEEE/IEC 42010 (2)). One of the concerns of a stakeholder is the purpose that the stakeholder ascribes to the system – the desired outcome from operating the system. Some internal stakeholders are themselves part of the system (such as system operators and users) and some are external stakeholders, being part of the system environment. Such external stakeholders may be affected by system function and malfunction, whilst they are not actively involved in the working of the system. Living next door to an oil refinery would be one example. Figure 1 shows a diagram of the key elements of a system of interest and its environment.

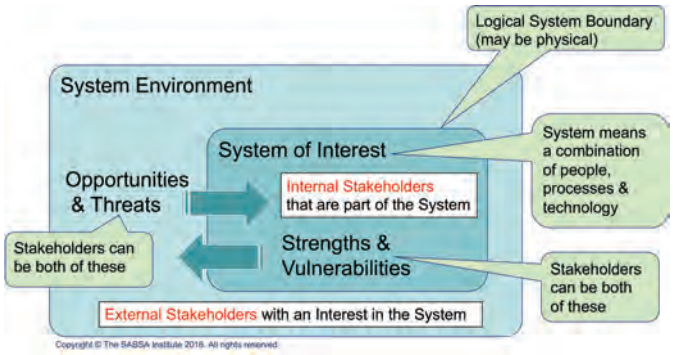


Figure 1: System of Interest.

The interests (concerns) of the various stakeholders define the boundary of the system of interest. At the extreme level the entire universe can be viewed as a system, although very little of that is man-made, and then only limited to what humans have built on planet earth. What we really expect is that the boundaries of the system of interest will be clearly expressed by the stakeholders, and that everything else in the universe is the system environment. This environment may also be truncated to a fairly local version of the universe, depending on the purpose of the system and how far out the system environment is relevant to that purpose.

Security and Risk

Any system has a purpose to fulfil, perhaps many purposes, each of interest to different stakeholders. Each purpose will be to create value for one or more of the stakeholders. There will be expected outcomes from operating the system, that are part of a value chain in which opportunity for gain is identified and exploited by some stakeholders. The nature of the universe and its laws dictates there will always be some level of uncertainty of outcome and that nothing can be predicted with total certainty. This quality of system operation is known as risk. In designing and constructing systems, we humans wish to minimise the level of uncertainty of outcome to an acceptable level. We call this level risk appetite and the process of limiting risk with our appetite is known as risk management (3). Different stakeholders may have different risk appetites. They will take the risk of losing value, in order to create value. The definition of value depends upon what the stakeholder(s) considers to be valuable to them. These valuables, whatever they are, are known as assets. They may be material objects of value, or

bookkeeping entries in a ledger, or capabilities to achieve certain goals.
In order to protect assets from loss or damage, and to ensure that operating the system increases asset value, we deploy security. Security within and around the system is the set measures taken to prevent threats from causing damage to the desired valuable outcomes. A threat is something that exists beyond the control of the system itself. The system environment is simply full of threats, some of which we know about and some of which we do not know. There are known knowns – things we know we know; known unknowns – things we know that we don't know, and unknown unknowns – things we don't know that we don't know. Threats come in all these three categories.
In figure 1 we see that threats are to be found in the system environment – external to the system. However, the diagram can be misleading unless we recognise that the system of interest is a sub-domain (sub-set) of its environment, which means that the environment is just as much inside the system of interest as outside it. The system boundary does not exclude the environment, but merely defines which part of the entire environment is occupied by the system itself. Hence the use of the term insider threat with regard to many business systems, referring to corrupt or malicious internal stakeholders.

Some stakeholders will be more concerned with the opportunities that the system strengths provide for increasing value and protecting accrued assets. Others will be more concerned with protecting against the perceived threats to the system. Both types of stakeholder require security to fulfil their ambitions. Security is a combination of measures to improve system strength and reduce system vulnerability (weakness). Security is most efficiently and effectively achieved by referring to the goals of the system for creating value and the threat landscape within which it is positioned.
Threats can exploit vulnerabilities to cause negative impacts on system goals. Opportunities can exploit system strengths to create positive impacts. We deploy security to meet both these types of stakeholder concern.

Coming Next Issue

Systems Architecture. Layering. Stakeholder Viewpoints and Views. ISO 42010. Security Architecture. Network Architecture. ISO 7498-1 and ISO 7498-2.

The Open Security Architect
June 2020

References

(1) ISO/IEC/IEEE 15288: 2015. Systems and software engineering — System life cycle processes
(2) ISO/IEC/IEEE 42010: 2011. Systems and software engineering — Architecture description
(3) ISO 31000: 2018: RISK MANAGEMENT

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

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