INFORMATIEBEVEILIGING MAGAZINE

- Learning by hacking
- Architectuur op basis van implied trust-zones
- Psychologen over het meten van gedrag in cybersecurity

JAARGANG 20 - 2020 - EDITIE 1

Mensenwerk

Nicole

De redactie is dit jaar vol enthousiasme begonnen en kijkt optimistisch naar de toekomst. De oplage van iB-Magazine is omhoog geschroefd, omdat nu ook studentleden het magazine ontvangen. Het PvIB is blij met jonge talenten onder de leden en we hopen dat de artikelen in het magazine laten zien hoe interessant het vakgebied is en hoeveel verschillende kanten een carrière in informatiebeveiliging op kan gaan.

Een van de thema's die bij veel studenten tot de verbeelding spreekt, is hacken. Het artikel 'Learning by hacking' vertelt over de nationale competitie 'Challenge the Cyber', waarbij het winnende team naar de European Cyber Security Challenge werd afgevaardigd. In dat artikel ook de oproep aan organisaties en professionals die bij de ondersteuning van de editie van 2020 betrokken willen worden. Het is voor organisaties en ervaren professionals een mooie kans om bij te dragen aan het ontwikkelen van talent voor de toekomst, want we hebben veel kennis en mensen nodig om die toekomst veilig te houden. Lees het boek van Huib Modderkolk er maar op na, zoals redactielid Chris gedaan heeft en ons daarover bijpraat in de boekreview.

Op weg naar die toekomst hebben we vandaag de dag eerst te maken met het implementeren van standaarden en richtlijnen. Dit magazine bevat daarover drie artikelen. Vanaf 1 januari 2020 is de BIO van kracht, het normenkader voor informatiebeveiliging voor de gehele overheid. Een tweede vernieuwde richtlijn is in ontwikkeling bij NIST en gaat over zero trust-architectuur. Later dit jaar wordt ook de herziene versie van de ISO 27031 'Information technology – cybersecurity – information and communication technology readiness for business continuity' verwacht. Overigens zal iB-Magazine nummer 5 helemaal in het thema van 'BCM' komen te staan.

Maar zonder mensenkennis kunnen we eigenlijk weinig voor elkaar krijgen met die standaarden. Daarom helpt Inge Wetzer ons deze keer weer om beter te worden in het meten en begrijpen van gedrag, want een veilige toekomst is mensenwerk.

Nicole van Deursen

IN DIT NUMMER

Auteur: Inge Wetzer is sociaal psycholoog cybersecurity & compliance bij Hoffmann en leidt het team van psychologen. Inge is bereikbaar via i.wetzer@hoffmannbv.nl.

Dit is het tweede artikel van de drieluik 'Het meten van gedrag in de cybersecurity'

Psychologen over het meten van gedrag in cybersecurity

En waarom vragenlijsten tekortschieten

Dat het niet eenvoudig is om de medewerkers van een organisatie weerbaar te maken tegen cyberdreigingen, zullen niet veel experts meer betwisten. In het eerste deel van dit drieluik werd toegelicht dat er een kloof zit tussen awareness en daadwerkelijk gedrag. Waar kennis nog relatief eenvoudig getoetst kan worden, is dat voor gedrag een stuk complexer. Door de verschuiving van awareness naar gedrag neemt de vraag naar gedragsmetingen toe. Standaard wordt ingezet op vragenlijsten waarin medewerkers moeten aangeven wat zij weten en hoe zij handelen.

Dit artikel beschrijft de tekortkomingen van vragenlijsten voor dit doel. Om te achterhalen waarom mensen bepaald gedrag nu niet vertonen zijn semi-gestructureerde interviews veel geschikter.

Van awareness naar gedrag

Dat de 'human-factor' een cruciale rol speelt in cybersecurity, behoeft gelukkig geen betoog meer. Een organisatie die cybersecurity serieus neemt, besteedt ook aandacht aan de menskant ervan. Recenter is het inzicht dat initiatieven op het gebied van de mens in cyber verder moeten reiken dan awareness (1). Daar waar het voorheen vooral een kwestie was van het zenden van kennis, is nu het beeld dat medewerkers zich vaak wel bewust zijn van de risico's van hun handelen. Ook weet men steeds beter wat er eigenlijk van hen verwacht wordt (een sterk wachtwoord hebben, pc locken, aparte wachtwoorden voor verschillende sites, etcetera.). Zoals deel 1 van dit drieluik illustreerde, zit er echter een grote kloof tussen de awareness en het daadwerkelijke gedrag van mensen (2). Met andere woorden: we wéten vaak wel wat we zouden moeten doen, maar handelen toch anders. We wéten wel dat we ons wachtwoord nooit moeten delen met een onbekende beller, toch doet 70% dit wel wanneer dit getest wordt …
Om effectiever te kunnen sturen op de cyberveilige medewerker, zullen initiatieven dus voorbij awareness moeten gaan. Het uiteindelijke doel van een campagne is namelijk cyberveilig gedrag. Het sturen op gedrag vraagt om een andere aanpak dan sturen op awareness. Inspanningen om awareness te verhogen zijn gericht op het zenden van kennis. Gedrag is echter complexer dan kennis alleen. De psychologie laat zien dat gedrag uit drie factoren bestaat (3): 'motivatie', 'capaciteit' en 'gelegenheid'. Met andere woorden: wil iemand het doen, is hij in staat om het te doen en krijgt hij de kans om het te doen? Deze gedragstheorie stelt dat motivatie, capaciteit en gelegenheid alle drie op een bepaalde drempelwaarde aanwezig moeten zijn, anders vindt gedrag niet plaats. Men dóet het pas echt, als men het wil, weet, kan én de kans krijgt om het te doen. Andersom betekent dit dus ook dat medewerkers die bepaald gewenst gedrag níet vertonen dat óf niet willen, niet weten, niet kunnen of niet de kans krijgen. Om gedrag te veranderen, zal dus eerst inzicht moeten ontstaan in deze factoren: ontbreekt het nou aan motivatie, aan capaciteit of aan gelegenheid? Wanneer dit bekend is, heeft men namelijk veel concretere handvatten voor maatregelen die genomen kunnen worden. Dat is daarmee een zeer belangrijke stap naar gedragsverandering. De belangrijkste vraag die hierbij speelt is: hoe kunnen de redenen voor de afwezigheid van gedrag zo goed mogelijk gemeten worden? Dit artikel zal inzoomen op deze vraag en uitleggen waarom vragenlijsten een minder geschikt middel zijn voor het meten van de menskant van cybersecurity. Tevens biedt het inzicht in een minder voor de hand liggende methodiek - die echter veel meer informatie ophaalt.

De traditie van vragenlijsten

Vragenlijsten, ze zijn nauwelijks weg te denken uit de huidige tijd van vele onderzoeken en behoefte aan metingen. De tendens voor het gebruik van dit meetinstrument is ook

zichtbaar op het gebied van cybersecurity. Zo wordt er onder andere door middel van vragenlijsten gemeten wat het kennisniveau is op het gebied van digitale veiligheid, van welke trends men al dan niet op de hoogte is, of in welke mate men weleens te maken heeft gehad met cybercrime. Zo wordt getracht een beeld te schetsen van verschillende aspecten van de menskant van cybersecurity. Vragenlijsten brengen echter een aantal nadelen met zich mee, waardoor de effectiviteit van deze methodiek in cybersecurity toch kritisch bekeken moet worden.

Wanneer vragenlijsten worden gebruikt als gedragsmeting, zijn er een aantal zaken waar heel bewust rekening mee gehouden moet worden. Ten eerste hebben mensen van nature de neiging tot sociaal wenselijk antwoorden (4). Zelfs al mogen we anoniem invullen hoe we in bepaalde situaties handelen, dan nog zijn we geneigd 'het goede antwoord' te geven. Deze bias leidt uiteraard tot een vertekend beeld van de werkelijkheid. Immers, als een groot deel van de respondenten nét een beetje positiever rapporteert over hun eigen handelen, kan een vragenlijst een beeld geven dat het allemaal best goed gaat. Niet het objectieve beeld dus (terwijl de vragenlijst daar juist wel voor bedoeld was).

Een tweede kanttekening bij het gebruik van vragenlijsten om gedrag te meten, is dat deze vragenlijsten feitelijk gedragsintentie meten in plaats van gedrag. Met andere woorden: mensen rapporteren wat ze van plan zijn te doen in een bepaalde situatie. De psychologie laat echter zien dat er een verschil is tussen intentie en daadwerkelijk

gedrag (5). De bekende 'theory of planned behavior' van Azjen (6) maakt een duidelijk onderscheid in gedragsintentie en gedrag. Hierin wordt gedragsintentie gezien als een indicatie van iemands bereidheid om bepaald gedrag te vertonen. Gedrag is iemands observeerbare respons in een bepaalde situatie. Dat een gedragsintentie niet altijd leidt tot daadwerkelijk gedrag komt door verschillende factoren. Zo speelt bijvoorbeeld 'perceived behavioral control' een rol: geloven mensen dat ze het gedrag ook daadwerkelijk goed kúnnen uitvoeren?

Terug naar het onderzoek uit artikel 1 van dit drieluik: Hieruit bleek dat 70% van de mensen zijn of haar wachtwoord weggeeft aan een onbekende beller. Hoeveel mensen zouden in een vragenlijst aangeven dat zij hun wachtwoord na een slim verhaal zouden weggeven aan een onbekende beller? Precies. Er is een verschil tussen gedragsintentie en gedrag en dat maakt vragenlijsten minder geschikt voor dergelijke metingen.

Vragenlijsten ongeschikt om redenen te achterhalen

Zoals in de inleiding van dit artikel werd beschreven, zouden inspanningen aan de menskant van cybersecurity zich moeten richten op het gedrag van mensen. Om het gedrag daadwerkelijk te veranderen, is het belangrijk om inzicht te hebben in de verschillende factoren van gedrag: motivatie, capaciteit en gelegenheid. Pas als duidelijk is aan welke factor het ontbreekt, kan concreet gestuurd worden op gedrag.

Het achterhalen van de redenen die mensen hebben om gedrag wel of niet te vertonen, is geen eenvoudige opgave. Tevens legt het een ander nadeel van (gesloten) vragenlijsten bloot: een vragenlijst kan alleen maar meten wat je als onderzoeker zelf al hebt bedacht als mogelijke antwoorden. Deze neiging tot het missen van dingen waar we onze aandacht niet op richten, gebeurt zelfs bij duidelijk zichtbare visuele prikkels. In de psychologie wordt dit fenomeen 'inattentional blindness' genoemd (7).

Een mooie illustratie hiervan is het beroemde onderzoek van Harvard, waarin onderzoekers Simon & Chabris (8) proefpersonen een potje basketbal lieten zien. De opdracht was te tellen hoe vaak het witte team de bal overgooide. Terwijl de bal werd overgespeeld, liep iemand in een gorillapak halverwege de video het beeld in. Deze 'gorilla' bleef in het midden stilstaan, sloeg opzichtig op zijn borst en liep vervolgens het beeld weer uit. Totaal onverwacht in deze context, maar niet te missen, zou je denken. De resultaten lieten zien dat de helft van de proefpersonen, die zeer aandachtig naar de video hadden gekeken, de gorilla hadden gemist. Dit onderzoek toont aan dat er een sterke menselijke neiging bestaat tot het focussen op één ding en dat daarmee andere zaken gemist worden. Wanneer je eigenlijk al denkt te weten waarom mensen bepaald gedrag niet vertonen en je op basis daarvan een vragenlijst opstelt, dan focus je jezelf op de oorzaken die je al verwacht had.

Wanneer medewerkers in een (gesloten) vragenlijst worden gevraagd of zij hun pas niet dragen om reden A, B, of C, zal je nooit reden D, E of F te weten komen. Terwijl de praktijk leert dat deze extra redenen er wel zijn. Ik voer met een team van psychologen inmiddels jarenlang onderzoek uit voor een grote variëteit aan organisaties. Opvallend vaak geven opdrachtgevers als CISO's vooraf aan dat zij wel weten waarom medewerkers bepaald gedrag (niet) vertonen, maar blijken deze aannames achteraf toch onvolledig of zelfs foutief te zijn. Het kan bijvoorbeeld lijken dat medewerkers hun computer niet locken, omdat ze gemakzuchtig zijn, maar feitelijk kan het zo zijn dat zij bijvoorbeeld vinden dat zij dit niet hoeven te doen zolang hun eigen manager het ook niet doet, of dat ze niet weten dat je snel kunt locken met de toetsencombinatie Windowstoets + 'L', of dat zij operationele redenen hebben waarom ze hun scherm niet kunnen locken. Allemaal redenen die niet vooraf bedacht zijn door de onderzoeker en die zouden worden gemist in een vragenlijstonderzoek. Dat maakt dat er gekeken moet worden naar een andere methodiek om redenen voor gedrag bloot te leggen: het semi-gestructureerde interview.

Het semi-gestructureerde interview

Om het gevaar van inattentional blindness te reduceren, bieden interviews een uitkomst. Door in alle openheid met medewerkers het gesprek aan te gaan, geeft dat een veel breder inzicht in hun gedrag dan dat vragenlijsten doen. We pleiten hierbij voor semi-gestructureerde interviews. Dit betekent dat de onderwerpen waarover gesproken zal worden in de interviews vooraf wel vast liggen, maar dat er geen concrete vragen zijn opgesteld die in het interview stapsgewijs worden nagelopen.

Het houden van semi-gestructureerde interviews over cyberveilig gedrag en de redenen daarvoor heeft verschillende voordelen. Door de open vragen krijgen respondenten meer ruimte om hun eigen mening te geven. Ze zijn immers niet beperkt tot vier mogelijke antwoorden, maar kunnen vrij spreken. Daarnaast kunnen openingen die mensen geven slim worden opgepakt en aangewend om verder door te vragen. Wanneer mensen voorzichtig zijn in hun antwoorden, kan een getrainde interviewer tevens technieken toepassen om uit te komen bij de relevante

Vijf tot zeven interviews leveren voldoende informatie op om concrete stappen mee te kunnen maken.

informatie. Een goede introductie en veilige sfeer zijn cruciaal voor het verkrijgen van eerlijke antwoorden. Door duidelijk te benoemen dat er geen goede en foute antwoorden zijn, maar dat het doel is om juist een beeld te verkrijgen, wordt getracht sociaal-wenselijke antwoorden te voorkomen. Het slim formuleren van vragen en het actief zoeken naar wat mensen op dit moment weerhoudt, is een groot voordeel van het semi-gestructureerde interview.

Het nadeel van interviews als onderzoeksmethode is dat niet de gehele doelgroep gemeten kan worden, maar slechts een steekproef. Daarbij is het houden van interviews tijdsintensief. De ervaring leert echter dat vijf tot zeven interviews voldoende informatie opleveren om vervolgens concrete stappen mee te kunnen maken. Belangrijk daarvoor is dat de steekproef van respondenten wel representatief is voor de doelgroep. Kies daarom mensen die een goede, eerlijke vertegenwoordiging zijn (en dus niet 'de beste jongetjes van de klas'). Tevens helpt het mensen te interviewen van wie verwacht wordt dat zij open en eerlijk zullen durven antwoorden. Wanneer de steekproef een goede vertegenwoordiging betreft, zal na vier tot vijf interviews de hoeveelheid nieuwe informatie snel afnemen. Dit is een goede check voor het bepalen van het aantal interviews om de benodigde informatie te verkrijgen.

Conclusie

Dit artikel ging in op het meten van cyberveilig gedrag. Specifieker ging het ook in op het meten van de redenen voor het ontbreken van cyberveilig gedrag, wat cruciale informatie is als men de stap naar daadwerkelijke gedragsverandering wil zetten. Het belichtte de traditie van het gebruik van vragenlijsten en gaf een beeld van de belangrijkste nadelen die dat met zich meebrengt. Vervolgens besprak het een alternatieve onderzoeksmethode die beter geschikt is voor het verzamelen van informatie over het huidige cyberveilig gedrag van mensen: het semi-gestructureerde interview. Belangrijker nog: om het gedrag van werknemers daadwerkelijk veiliger te maken, is het van belang eerst te weten welke barrières zij nu ervaren. De kans dat deze worden blootgelegd tijdens een semi-gestructureerd interview is groter dan dat zij uit een vragenlijst naar voren komen. Dit vraagt dus om een verandering van methodiek en dat is geen gemakkelijk proces. Toch toont de recente stap die het veld heeft gemaakt van awareness als einddoel naar gedrag als einddoel dat de inzichten uit de psychologie steeds meer worden omarmd.

Het laatste deel van dit drieluik gaat in op een specifiek voorbeeld van cybercriminaliteit waarin de mens een cruciale rol speelt: CEO-fraude. Wanneer men anderen vraagt of men geld zou overmaken naar een onbekende rekening, of geld zou overmaken zonder dat hierbij gebruik is gemaakt van het vereiste vier ogenprincipe, zal men dit met 'nee' beantwoorden. Toch is CEO-fraude aan de orde van de dag. CEO-fraude is op dit moment één van de meest voorkomende vormen van internetcriminaliteit. Het laatste artikel gaat in op de menskant van CEO-fraude, beantwoordt de vraag waarom awareness niet genoeg is en weergeeft hoe inzichten uit de psychologie kunnen bijdragen aan het vergroten van de weerbaarheid.

Referenties

(1) Wetzer, I.M. (2018). Cyberveilig gedrag: Waarom doen we het nou niet? Informatiebeveiliging, 18, 12-15.

(2) Wetzer, I. M., & Weijkamp, E. (2019). Een psychologische benadering van awareness in cybersecurity: Medewerkers geven hun wachtwoord niet weg via de telefoon, toch? InformatieBeveiliging (in druk).

(3) MacInnis, D. J., Moorman, C., & Jaworski, B. J. (1991). Enhancing and Measuring Consumers' Motivation, Opportunity, and Ability to Process Brand Information from Ads. Journal of Marketing, 55, 32-53.

(4) Edwards, A. (1957). The social desirability variable in personality assessment and research. New York: The Dryden Press.

(5) Norberg, P. A.; Horne, D. R.; Horne, D. A. (2007). "The privacy paradox: Personal information disclosure intentions versus behaviors". Journal of Consumer Affairs, 41, 100–126.

(6) Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50, 179-211.

(7) Mack, A., & Rock, I. (1998). Inattentional blindness. Cambridge, MA: MIT Press.

(8) Simon, D. J., & Chabris, C. F. (1999). Gorillas in our midst: Sustained inattentional blindness for dynamic events. Perception, 28, 1059-74.

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Voorwaarts leven

In een nieuw jaar worden prachtige voorspellende vooruitblikken gegeven. Afgelopen Kerst (nog slechts kort geleden) keken we achteruit en zagen we welke slagvelden we overleefden, triomfen we konden vieren en welke nederlagen we moesten ondergaan. Maar nu tijd voor nieuw optimisme in het komende jaar. Het leven wordt immers voorwaarts geleefd (edoch achterwaarts begrepen).

Toch nog een klein stukje terug naar een bewogen jaar - en dan zeker voor mijzelf. Ik raakte gedesillusioneerd, omdat mensen om mij heen privacy ineens niet erg belangrijk bleken te vinden. De periode na de hype moet vast vergelijkbaar in gevoel zijn als het gewaarworden van een junk die van een prachtige high afkomt, om zich heen kijkt en vaststelt dat de wereld toch iets minder intens geweldig eruitziet.

Ik ging op zoek naar mensen die er wél vol gepassioneerd over waren en op een privacypelgrimsroute kwam ik daar ergens op mijn weg een bijzonder man tegen. Wij deelden passie over het juiste doen met data, iets geweldigs willen neerzetten, maar wel altijd doordacht en doorwrocht van het feit dat je niet zomaar iets aan het doen bent en dat je erg goed moet nadenken over wat je doet. Wat doet het voor de mens? Wat doet het voor zijn privacy? Wie zijn wij eigenlijk en waar staan wij voor? Een half jaar later werd deze man mijn nieuwe baas.

Nu hoef ik niet meer achteruit te kijken en mag ik juist weer naar voren (daar waar het leven wordt geleefd). En in dat naar voren gaan, zie ik een hoop 'oude bekenden' weer opdoemen. Privacyonderwerpen die altijd blijven leven of weer opnieuw aandacht behoeven. In elke organisatie is standaard weinig kennis van privacy en werken heel veel mensen die je telkens weer mee moet blijven nemen in datgene wat het hart van onze passie inhoudt. Elk onderwerp dat je oppakt vergt niet alleen lef en doorzettingsvermogen, maar ook de finesse van de diplomaat die zorgt dat iedereen meegolft naar het zelfde einddoel.

Privacy bedrijven is en blijft een ingewikkeld vak, omdat het vele schakeringen kent en kennis van verschillende disciplines vereist. En dat maakt het toch elke keer weer heel bijzonder, zelfs als je weer al die oude bekende onderwerpen voorbij ziet komen. Maar het leukste nog steeds? De mensen. En dan al helemaal als ze (uiteindelijk) met je mee voorwaarts willen leven.

Ik hoop op een jaar vol nieuwe mooie mijlpalen en mensen met wie ik ze samen mag gaan bereiken. En als ik dan toch nog een tip mag geven om het jaar mee te openen: kijk om je heen en zie of je jezelf nog steeds met die gepassioneerde mensen omgeeft. Is dat niet het geval, werp je blik dan eens een stuk verder weg en ontmoet nieuwe mensen. Ik kan je in ieder geval met de hand op mijn hart zeggen dat het mijn 2019 weer goed heeft gemaakt en dan het mijn 2020 fantastisch gaat maken.

Rachel

Auteurs: Melanie Lemmen is manager hoger onderwijs bij dcypher. Melanie is te bereiken via m.lemmen@dcypher.nl. Michiel Oosterwijk is coördinator incident respons bij het Nationaal Cyber Security Centrum. Michiel is te bereiken via michiel.oosterwijk@ncsc.nl.

Learning by hacking

Door de toenemende digitalisering van de samenleving is ook de vraag naar cybersecurity-expertise drastisch gestegen. In de zoektocht naar nieuw cybersecuritytalent wordt dan ook geen middel onbeproefd gelaten. Capture the Flag-competities worden steeds vaker ingezet om jonge mensen op een speelse manier kennis te laten maken met het vakgebied. De challenges vormen daarbij een veilige brug naar de praktijk van de ethisch hacker en lenen zich bij uitstek om grote groepen mensen de benodigde competenties te laten ontwikkelen. Ook in Nederland bestaan diverse CTF-competities, waaronder het jaarlijkse Pentest-event van het PvIB.

Dit nieuwe evenement, georganiseerd door dcypher en het Nationaal Cyber Security Centrum (NCSC), vond op 7 september 2019 plaats. Aan 'Challenge the Cyber' deden meer dan honderd deelnemers mee, verdeeld over dertien teams. Wat maakte dat het NCSC en dcypher de handen ineensloegen om een nationale hackingcompetitie te organiseren, waarom is dit evenement anders dan andere CTF-events en wat is de visie op de toekomst?

De voorbereidingen voor Challenge the Cyber startten begin 2019 met het voornemen om een Nederlands team af te vaardigen naar de European Cyber Security Challenge (ECSC) in Boekarest. Deze ECSC richt zich specifiek op deelnemers van 14 tot en met 25 jaar en is een van de instrumenten die ENISA (het Europees agentschap voor netwerk- en informatiebeveiliging) inzet om de ontwikkeling van cybersecuritykennis en -vaardigheden te promoten en cybersecurity onder een breder publiek bekend te maken. Nederland schitterde al jaren door afwezigheid en het NCSC vond het tijd daar verandering in te brengen. Omdat deelnemende landen verplicht zijn een nationale voorronde te organiseren, riep het NCSC de hulp van dcypher in om deze 'noodzakelijke horde' te nemen.

Besloten werd de nationale voorronde, die de werknaam 'Challenge the Cyber (1) kreeg, pragmatisch te benaderen: een pilot die niet te veel tijd of geld zou kosten, met als doel een team samen te stellen voor de ECSC. Toen op 7 september de Dutch Innovation Factory in Zoetermeer volstroomde met jong cybersecuritytalent, werd echter duidelijk dat Challenge the Cyber meer is dan een noodzakelijke horde.

Dertien teams van zes universiteiten (Twente, Leiden, UvA, VU, Radboud en TU/e), drie hogescholen (Den Haag, Rotterdam, Fontys ICT), één ROC (Amsterdam), een bedrijfsopleiding (Motiv Academy) en een groepje jonge hackers gingen onder het toeziend oog van hun docenten de strijd aan op een gedeelde interesse: ethisch hacken. Drie grote organisaties (Cisco Nederland, KPN Security en Rabobank) verbonden hun naam aan het evenement. Met elkaar constateerden wij dat Challenge the Cyber in een breed gedeelde behoefte voorziet: het aanboren van nieuw en jong cybersecurity talent, het ontwikkelen en vergroten van de noodzakelijke competenties en het aanwakkeren van interesse in het vakgebied.

Ontwikkeling van competenties

CTF-challenges stimuleren op een laagdrempelige manier de ontwikkeling van cybersecuritycompetenties (een in gedrag waarneembare combinatie van kennis, vaardighe-

Foto 1 - Het Nederlands team tijdens de ECSC in Boekarest (foto: Edwin Schaap).

European Cyber Security Challenge (ECSC)
De European Cyber Security Challenge is een sinds 2014 bestaand, jaarlijks cybersecurity-evenement, dat afgelopen jaar van 9 tot en met 11 oktober 2019 plaatsvond in de Roemeense hoofdstad Boekarest. Hier kwamen tweehonderd jonge cybertalenten uit twintig landen samen om hun vaardigheden op het gebied van web- en mobiele beveiliging, cryptopuzzels, reverse engineering, forensisch onderzoek en hardware hacking te bewijzen. Ook moesten de deelnemers hun soft skills, zoals teamwerk en spreken in het openbaar, aantonen. Het Nederlands team, dat voor het eerst meedeed, werd zestiende.

Met de ECSC wil ENISA (het Europees agentschap voor netwerk- en informatiebeveiliging) het kwalitatieve en kwantitatieve tekort aan cybersecuritytalent adresseren en cybersecurity zichtbaar maken voor een groter publiek. De afgelopen jaren is de belangstelling voor de ECSC onder Europese en nationale cybersecurity stakeholders sterk toegenomen.

den, houding en/of persoonskenmerken waarmee in een arbeidssituatie doelen worden bereikt). Ze vormen, los van onderwijsniveaus, een brug van de theorie naar de praktijk. Het door ENISA (in samenwerking met internationale wetenschappers en industrie) ontwikkelde ECSC-curriculum (3) biedt een concreet en actueel raamwerk van cybersecuritykennis- en vaardigheden. De ECSC-challenges richten zich op een breed spectrum van aandachtsgebieden uit dit curriculum. Deelnemende teams moeten naast diepgaande kennis ten aanzien van de beveiliging van ICT-systemen en diverse typen aanvalsvectoren en kwetsbaarheden ook beschikken over voldoende technische vaardigheden. Oplossingen liggen vooral in het begrijpen van de conceptuele problemen die ten grondslag liggen aan kwetsbaarheden en niet zo zeer in kennis van het misbruiken van al bekende kwetsbaarheden. Ook Challenge the Cyber baseert zich op het ECSC-curriculum. Opleidingen kunnen ervoor kiezen onderdelen uit het curriculum in het onderwijs te integreren. Docenten Ron Mélotte van Fontys ICT en Daniel Meinsma van de Haagse Hogeschool, beide in 2019 mee als coach naar de ECSC, doen dat al. Zij stimuleren studenten bovendien om ook buiten school hacking skills zoals network & server hacking, crypto, reverse engineering en web security te trainen.

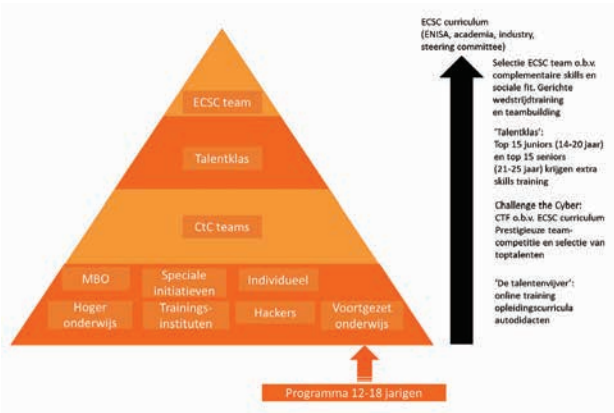
Een goed CTF-team beschikt echter over meer dan alleen technische skills en heeft ook een aantal belangrijke soft skills aan boord. Bij de ECSC kunnen de jonge talenten dit aantonen door het samenwerken, onderhandelen en verdelen van taken binnen het team, het documenteren van hun aanpak in write-ups, het presenteren van een complex beveiligingsrisico aan zowel technische als niet-technisch mensen, het onder tijdsdruk nemen van beslissingen en het tonen van leiderschap. Daarbij leren deelnemers communiceren met verschillende Europese culturen en ontwikkelen zij een eigen internationaal netwerk.

De toekomst

Challenge the Cyber boort nieuw en jong cybersecuritytalent aan, tilt de noodzakelijke cybersecurityskills (op basis van het ECSC-curriculum) naar een hoger niveau en inspireert jonge mensen een loopbaan in cybersecurity na te streven. Dat wordt onder andere gerealiseerd met:

- Een netwerk van Challenge the Cyber-ambassadeurs (te beginnen met de ECSC-alumni), dat de werving van nieuw talent bij opleidingen, studieverenigingen, hacking events, online CTF's, etcetera verzorgt.
- Een jaarlijkse talentklas voor de grootste Challenge the Cyber-talenten. Deze groep krijgt een meerdaagse training aangeboden, waarin gewerkt wordt aan harde en zachte vaardigheden, teambuilding en persoonlijk leiderschap. Een grotere groep talenten krijgt zo de kans extra training te volgen en een netwerk te ontwikkelen. Uit deze talentklas wordt op basis van complementaire skills en sociale fit het ECSC-team geselecteerd.
- Een hecht netwerk van ECSC- of talentenklasalumni dat betrokken is bij de organisatie van Challenge the Cyber en zich inzet bij de training en mentoring van jonge talenten.
- Een online opleidingsomgeving met trainingsmateriaal en

challenges, waar Challenge the Cyber deelnemers kunnen oefenen voor de competitie.
- Een programma voor de werving en opleiding van jong vrouwelijk cybersecuritytalent (3).
- Een programma voor 12- tot 18-jarigen om de volgende generatie kennis te laten maken met cybersecurity.
- Een netwerk van bedrijven en opleidingen dat nauw betrokken is bij Challenge the Cyber, onder andere in de vorm van financiële sponsoring, praktische en organisatorische hulp en het verzorgen van talentklas- en ECSC-trainingen.
- Europese samenwerking op het gebied van cybersecurityskillsontwikkeling en een internationaal netwerk van cybersecuritytalent.
- Jaarlijkse uitzending en begeleiding van tien toptalenten als Nederlandse vertegenwoordiging naar de ECSC-finale.



Figuur 1 - Visie op talentontwikkeling (bron: Melanie Lemmen).

Inmiddels is de organisatie van de tweede editie van Challenge the Cyber gestart. Het ECSC-team van 2019 is betrokken bij de organisatie en zet zich actief in om de grote ambities te realiseren.

De beoogde datum voor Challenge the Cyber is zaterdag 30 mei 2020. Aan een geschikte locatie op een centrale plek in Nederland wordt gewerkt. Bij deze tweede editie is ruimte voor ongeveer tweehonderd deelnemers, verdeeld over junior (14-20 jaar) en senior (21-25 jaar) teams. De maximale groepsgrootte is vijf personen, waardoor er meer van de individuele teamleden zal worden gevraagd. Uit de beste junior en senior teams zal een groep van dertig deelnemers worden uitgenodigd voor de eerste 'talentklas'. Na de zomer zal hieruit het team worden geselecteerd, dat Nederland in november mag vertegenwoordigen tijdens ECSC 2020 in Wenen.

Capture the Flag (CTF)

Een Capture the Flag-challenge is een wedstrijd waarbij deelnemers verschillende cybersecurityopdrachten moeten volbrengen om 'vlaggen' (vaak verborgen stukjes tekst) te veroveren. CTF-challenges raken meestal uiteenlopende cybersecurity-aspecten, zoals cryptografie, forensics, webbeveiliging, mobiele beveiliging en reverse engineering. Een goed team is zo samengesteld dat het alle expertises aan boord heeft.

Bij zowel de European Cyber Security Challenge als Challenge the Cyber werd een 'Jeopardy-style' CTF gebruikt. Hierbij worden opdrachten verdeeld over een aantal categorieën: het niveau van de vraagstukken binnen een categorie varieert van makkelijk tot zeer moeilijk. Teams verdienen punten per opgeloste opdracht, waarbij taken meer punten opleveren naarmate ze moeilijker zijn. Het team dat binnen de beschikbare tijd de meeste punten haalt, is de winnaar. De door Certified Secure ontwikkelde CTF voor Challenge the Cyber 2019 had vijf onderwerpen (web, crypto, server, netwerk en osint) met elk drie moeilijkheidsniveaus.

Oproep

Onze ambities voor de komende jaren zijn groot. Wij komen daarom graag in contact met professionals en organisaties die betrokken willen zijn bij ons programma. Dat kan in de vorm van een financiële sponsorbijdrage, het verzorgen van workshops of het beschikbaar stellen van trainingsruimte, maar ook door meedenken en -organiseren, het openstellen van netwerken, het coachen van talenten en docenten en het actief promoten van Challenge the Cyber. We horen graag van u via info@challengethecyber.nl en hopen dat wij op 30 mei - naast nieuw jong talent - ook veel betrokkenen uit het veld mogen begroeten!

Referenties

(1) www.challengethecyber.nl
(2) ECSC curriculum guide 2020, https://ecsc.eu/ecsccurricula.pdf/download
(3) Deloitte whitepaper Women in cyber in context of the European Cyber Security Challenge, https://europeancybersecuritychallenge.eu/about/women-in-cybersecurity.pdf

Governance assured

The Attributer has now written a number of progressive articles on the subject of good governance with reference to the failure of the Boeing 737 Max aircraft. You can refer to previous articles entitled Non-Conflicted (April 2019) and Governed (June 2019). In this follow up article we examine the latest developments in this tale of woe.

On Christmas Eve 2019 the BBC News website reported that Boeing had dismissed its Chief Executive, Dennis Muilenburg. The timing of the announcement is in itself interesting. The more cynical observer might comment that although this was a massive positive step to restore public confidence in the management of the Boeing Corporation, with most of the world focused on last minute Christmas shopping for presents and making sure that the turkey would fit in the oven, the possible negative impact was minimised. And the positive impact can be claimed whenever the matter is raised again in the future. Good call Boeing!

Cynical? Yes of course. After all, more than 340 people died in the two air crashes attributed to failure of the MCAS system on the 737 Max. This has led to allegations that Boeing put profit before safety. That is not something that an aircraft manufacturer or an operating airline would want to be associated with its products or services. Flight safety is such a sensitive issue that any disaster of this type affects the entire civil aviation industry, not just the manufacturer or the flight operator. The families of the victims welcomed Mr Muilenburg's resignation as being overdue. Public humiliation and consumption of humble pie has been demonstrated at the highest level.

This is intended to help to restore confidence in the Boeing product. However, the story still has many miles to run. Mr Muilenburg has been replaced by David Calhoun. Mr Calhoun has served on the board since 2009 and is its current chairman. He is also now chief executive and president. This raises several questions:

1. Is it wise to appoint someone who has been active in the board for the past ten years and can therefore be seen to represent the 'old guard'? Will this simply mean that the existing culture (perceived as profit over safety) will remain intact under a new captain? Is this a sign of Boeing's commitment to real change in the governance? Or is it cosmetic?
2. Corporate governance wisdom tells us that too much power in one pair of hands is a dangerous strategy. Now Mr Calhoun holds all three of the most senior roles in one appointment. Surely that is not the way to have strategic decisions questioned and challenged. Especially at a time when Boeing needs to assure its stakeholders that it will be governed properly in future.
3. The final humiliation that led to Mr Muilenburg's resignation came a week earlier, when Boeing announced it would have to suspend production of the 737 Max, because regulators had yet to clear the aircraft as safe to fly again. While the company had been hoping to have the best-selling jet back in the air by the end of this year, US regulators have made it clear that it would not be certified to return to the skies that quickly. For months, Mr Muilenburg had insisted the plane would be back in the air by the end of the year. He had lost credibility, and the board decided he had to go.
4. Whilst Boeing itself will almost certainly ride out the storm, its supply chain is deep and wide. Many small companies across the USA depend on the continued business from Boeing. With production of its most popular plane halted, the economic impact will be felt across the industry, with both jobs and companies being destroyed.

The title of this article is 'governance assured'. What should we do to provide such assurance? Governance itself is not sufficient – we must have some assurance of its quality and suitability. In this instance would it be best to appoint successors that have been around in the current governance structure and thus bring contextual experience? Or should Boeing start again with fresh blood brought in for outside the existing company? Only a structured analysis of the ecosystem will reveal the risk factors, positive and negative. That's the sort of analysis that SABSA can provide.

The Attributer

Auteur: Ard Ruiter werkt als privacy- en beveiligingsfunctionaris/senior inspecteur bij de ILT Inlichtingen- en Opsporingsdienst (ILT-IOD). Hij schreef dit artikel op persoonlijke titel. Ard is bereikbaar via ardlinkedin@hotmail.com

BIO: risicomanagement voor veilige communicatie tussen overheden, burgers en ondernemers in het digitale tijdperk

Alle overheidslagen gaan werken met een eenduidig gemeenschappelijk niveau voor informatiebeveiliging. De Baseline Informatiebeveiliging Overheid (BIO) is gebaseerd op de internationale norm ISO 27001/2. Interoperabiliteit, standaardisatie en de drie basisbeveiligingsniveaus zijn sleutelbegrippen bij de BIO. Evenzeer als risicomanagement: op basis van een risicoanalyse wordt het gewenste niveau van een van de drie informatiebeveiligingsniveaus bepaald.

Vooorgaande doet overigens niet af aan het privacyrecht. De bescherming van waardevolle en gevoelige bedrijfsinformatie is immers zowel een doel vanuit de informatiebeveiliging als de (personal/private) data protection. De BIO komt echter niet in de plaats van de DPIA. Is de BIO nu helemaal iets nieuws, of sluit het aan bij reeds bekende securitynormen? Een informerend en beschouwend artikel.

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle lagen van het openbaar bestuur: Rijksoverheid, 12 provincies, 355 gemeenten en 21 waterschappen. De invoering in het vorige en het huidige jaar van de BIO in de publieke sector kan om meerdere redenen ook voor het bedrijfsleven interessant zijn, zowel voor wat betreft het implementeren en organiseren van eisen van informatiebeveiliging, de toepassing van gegevensmanagement en risicomanagement én ten aanzien van de dienstverlening aan burgers/cliënten/consumenten.

De BIO is gestructureerd volgens de relevante NEN-ISO/IEC-normen. De online communicatie van overheden met burgers en ondernemers moet op een veilige manier verlopen, zodat iedereen kan blijven vertrouwen op de overheid, ook in het digitale tijdperk. Eén van de doelen van de BIO is ook de administratieve lasten te verlichten bij overheden en commerciële bedrijven op de markt, zowel voor afnemers als voor leveranciers. Tevens is het basisnormenkader van belang bij de Publiek-Private Samenwerking (PPS) en bij ondernemingen waarvan publiekrechtelijke instanties (mede)aandeelhouder zijn. Op de site (1) is een informerende film met illustraties geplaatst.

De samenleving digitaliseert steeds meer en is in hoge mate afhankelijk van overheidsdiensten die in die digitale samenleving opereren. Overheden verrichten veel cyberactiviteiten: alle activiteiten die via ICT mogelijk gemaakt worden. Zo kunnen aanvragen worden ingediend via 'Omgevingsloket online' en kan een 'vergunningencheck' worden gedaan. Door de overheid geregistreerde informatie over personenauto's en andere voortuigen kan worden geraadpleegd via internet en gemeenten communiceren met burgers via e-mail en allerlei social media.

Laboratoria voor internet en data-onderzoek

Overheden wisselen onderling steeds meer informatie uit via basisregistraties, delen gegevens in samenwerkingsverbanden en beschikken soms over eigen 'laboratoria' voor internet- en data-onderzoek, waarbij bijvoorbeeld big data wordt onderzocht in samenhang met eigen, 'unieke' gegevens. "De overheid heeft een grote verantwoordelijkheid ten aanzien van de beveiliging van gegevens die burgers en ondernemers aan haar toevertrouwen en de ICT-systemen waarmee zij werkt. Het op orde hebben en houden van het eigen informatieveiligheidsbeleid is dan ook randvoorwaardelijk voor de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens en systemen. Zodoende focust een aantal maatregelen zich op het op orde brengen en houden van de informatieveiligheid van overheidsorganisaties en het bevorderen van overheidsbrede samenwerking"(2). "Met name ten aanzien van de bescherming van gegevens van burgers en bedrijven mag van de Rijksoverheid juist een hoge mate van zorgvuldigheid worden verwacht. De plicht die zij oplegt aan burgers en bedrijven tot het verstrekken van gegevens onderstreept de hoge eisen die terecht aan haar worden gesteld"(3).

Uniformering van informatiebeveiligingsnormen

Informatiebeveiliging gaat over de maatregelen en procedures om beschikbaarheid, exclusiviteit en integriteit van informatievoorziening te garanderen. In het bijzonder om de continuïteit van de informatie en informatievoorziening te waarborgen en de gevolgen van incidenten tot een acceptabel niveau te beperken. Het is een uniforme basis, zodat de beveiliging van informatie(systemen) wordt bevorderd bij alle bedrijfsonderdelen van de overheid. Het doel is dat bedrijfsonderdelen erop kunnen vertrouwen dat gegevens die worden verstuurd naar of worden ontvangen van andere onderdelen van de overheid, in lijn met wet- en regelgeving, passend beveiligd zijn. Hierbij is 'compliance' typisch een thema van de governancelaag die de informatiebeveiliging zal beschouwen in het kader van wet- en regelgeving.

De BIO beschrijft de invulling – dus geen vervanging – aan de auteursrechtelijk beschermde NEN-ISO/IEC-normen:

1. 27000:2017 (information technology - security techniques - information security management systems - overview and vocabulary).
2. 27002:2017 nl (informatietechnologie - beveiligings technieken - praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging).
3. 31000:2009 nl (risicomanagement - principes en richtlijnen).
4. 31010:2009 (risicomanagement - risico-evaluatie technieken) voor alle bestuurslagen.

Deze standaardisatie van normen heeft namelijk een groot aantal voordelen. De gegevens- en berichtenstandaarden

richten zich op de uitwisseling van gegevens binnen overheden, bedrijven en burgers. De interoperabiliteit zorgt er in wezen voor dat de uitgewisselde gegevens juist zijn en op de juiste manier worden gebruikt, met andere woorden gezegd: de ICT-systemen gaan dezelfde 'ICT-taal' spreken. Aan de andere kant zal standaardisering misbruik moeten voorkomen zoals 'spoofing' - (dat is (digitale) identiteitsvervalsing), cache poisoning (als een computer of computernetwerk niet-authentieke gegevens ontvangt en in dit geheugen plaatst waardoor de computer kan worden 'overgenomen'), afluisteren en manipulatie.

Ruime definitie van informatiesystemen

In de theorie van het informatiemanagement wordt onderscheid gemaakt in feiten, gegevens, informatie, kennis en competenties (4).

(1) Feiten zijn gebeurtenissen of omstandigheden die zich in de werkelijkheid voordoen en objectief vastgesteld en controleerbar zijn.
(2) Als feiten op papier of in de computer worden vastgelegd, spreekt men van gegevens. Gebeurt dat door middel van geautomatiseerde systemen dan wordt het 'data' genoemd. Gegevensmanagement is dan ook omvangrijker dan datamanagement.
(3) Zodra een persoon daaraan waarde toekent, de objectieve gegevens/data (subjectief) interpreteert of een bepaalde betekenis daaraan toekent, dan is dat voor die persoon informatie.
(4) Kennis ontstaat uit informatie als die is aangevuld met vaardigheden en ervaring en op een bepaalde manier geordend is. Dit zit 'in de hoofden' van medewerkers, is vervat in handboeken en werkmethoden.
(5) Een competentie is de combinatie van kennis, vaardigheden, houding en gedrag die nodig is om in een bepaalde beroepssituatie goed te kunnen functioneren. Kennis en competentie leiden tot nieuwe gegevens die weer opnieuw geïnterpreteerd kunnen worden. Zo ontstaat de cyclus die we de 'informatiecyclus' noemen, waarbij het belang aanwezig is om deze voortdurend te spiegelen aan de feiten. Dit voorkomt dat data die in een onjuiste context is geïnterpreteerd een feitelijk onjuist, eigen leven gaat leiden.

Veel gegevensverzamelingen worden aangemerkt als informatiesysteem. Een informatiesysteem is in de BIO namelijk gedefinieerd als: "Een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie" (5).

Omdat erop mag worden vertrouwd dat de kwaliteit van de dienstverlening en de bedrijfsvoering van overheidsorganisaties of samenwerkingsverbanden waartoe zij behoren goed moet zijn, zal de BIO en het gegevensmanagement congruent zijn in de toepassing daarvan in die organisaties. Gegevensmanagement is immers het geheel van activiteiten om voor het primaire proces, ketens en samenwerkingsverbanden dat ertoe leidt dat een organisatievorm op het juiste moment over de juiste gegevens van de juiste kwaliteit te beschikken.

PDCA met risicomanagement

Informatiebeveiliging wordt niet gezien als een (tijdelijk) project dat je 'even' implementeert. Het is een proces volgens de cyclus van plan-do-check-act (PDCA). Door de toepassing van deze cyclus kunnen beveiligingsaspecten inzichten worden. Op basis van een expliciete risicoafweging kunnen de betrouwbaarheidseisen voor de informatiesystemen worden vastgesteld (risicomanagement) en vervolgens kunnen de maatregelen worden uitgedragen. Deze gecoördineerde activiteiten geven sturing aan het bewaken van risico's door middel van beoordeling, behandeling, acceptatie en communicatie. De ingeschatte risico's worden afgewogen tegen vastgestelde risicocriteria en bepalen in welke mate het risico significant is.

Concreet betekent dit dat de aanwezigheid van een beveiligingsorganisatie en een Information Security Management System (ISMS) op basis van risicomanagement de eventuele maatregelen bepalen. De PDCA-cyclus is de kern van ISMS. Daarbij zij overigens enigszins terzijde opgemerkt dat cybersecurity zich onderscheid van informatiebeveiliging (6).

Nieuwe regels en routines

In de managementliteratuur vinden we de relativering van de implementatie van controls. Daarbij worden expliciet ontwikkelingspaden van organisaties en de organische en evolutionaire aspecten van organisaties en veranderingsprocessen bekeken. Er wordt gekeken hoe het gedrag van mensen beïnvloed kan worden, hoe de doelcongruentie ondersteund kan worden en hoe het gedrag van mensen beïnvloed kan worden om uiteindelijk die doelcongruentie te bereiken.

Een managementcontrolsysteem is een opeenvolgende set van acties of activiteiten dat is beschreven om een gewenst

doel te bereiken (7). Een 'simpel' regulerende system wordt gezien als een oude, beperkte visie daarop (8). Burns and Scapens (9) hebben een raamwerk ontwikkeld dat geschikt is voor onderzoek naar veranderingen in managementcontrol die leiden tot gewenst gedrag van organisaties langs 'encoding', 'enacting', 'reproduction' en 'institutionalization'.

A. Encoding: het proces start met het vertalen van institutionele principes naar regels en routines, welke vervolgens leiden tot het vormen of hervormen van bestaande routines.
B. Enacting: het opvolgende proces van enactment bevindt zich in de actiezone en kan op basis van bewuste of onbewuste keuzes worden doorgevoerd, maar zal vaak het resultaat zijn van beschouwing en het toepassen van stilzwijgend aanwezige kennis over hoe dingen worden gedaan.
C. Reproduction: het derde proces bevindt zich eveneens in de actiezone en treedt op als repeterend gedrag van actoren invloed krijgt op routines. Verandering kan zich onbewust voordoen bij de afwezigheid van een systeem om de uitvoering van routines te monitoren of daar waar regels niet goed worden begrepen of worden verworpen door actoren.
D. Institutionalization: als laatste volgt het proces van institutionalisering waarbij regels en routines worden gereproduceerd door het gedrag van individuele actoren. De nieuwe regels en routines zijn dan de normale manieren van werken.

Basisbeveiligingsniveaus

"Om risicomanagement hanteerbaar en efficiënt te houden, kiest de BIO voor een diepgang van de uitwerking van het risicomanagement die proportioneel is aan de te beschermen belangen in combinatie met relevante dreigingen"(10). Voor de harmonisatie, de wens voor meer risicomanagement en de wens voor verschillende niveaus voor beveiligen onderscheidt de BIO drie basisbeveiligingsniveaus (BBN).

BBN's	B(C) (11)	I(I)	V(A)	Beschrijving niveau	Toepassingsbereik	Controls en overheidsmaatregelen
BBN1	laag	laag	laag	Nadruk op 'wat mag minimaal verwacht worden?'	Minimumeis voor alle overheidssystemen	- Wet- en regelgeving. - Algemeen geldende beveiligingsprincipes.
BBN2	midden	midden	midden	- Informatie is **maximaal** Departementaal Vertrouwelijk (DepV) (12). - Privacygevoelige informatie met een verhoogd vertrouwelijkheidsniveau. - Commercieel vertrouwelijke informatie -Informatie i.h.k.v. beleidsvorming	- Verwerking van vertrouwelijke informatie. -Mogelijke incidenten leiden tot bestuurlijke commotie. -Onzekerheid kan bestaan of ook alle informatie van derden open is. -De veiligheid van andere systemen is afhankelijk van de veiligheid van het eigen systeem.	- Wet- en regelgeving, in het bijzonder beveiligingseisen a.g.v. relevant privacyrecht. - Aansluitvoorwaarden van generieke/gemeen-schappelijke diensten. - Afhankelijkheden in ketens en netwerken. - Minimale eisen ten behoeve van een efficiënte beveiliging van BBN3.
BBN3	midden	midden	hoog	In geval van gerubriceerde informatie met minimaal DepV en vergelijkbaar vertrouwelijk bij andere overheidslagen; gerubriceerde informatie waarbij weerstand geboden moet worden tegen de dreiging die uitgaat van statelijke actoren en beroepscriminelen	- Verlies van informatie heeft een grote impact, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3. - Informatie met een rubricering (niet zijnde BBN2) wordt geleverd door derden. - Bij aansluiting op een infrastructuur BBN3 is vereist om informatie te kunnen verwerken op deze infrastructuur	Controls en overheids-maat-regelen uit BBN2 aangevuld met: - Eisen uit het VIRBI (13). - Bepalingen uit regelingen van andere overheidslagen en uit het NAVO-verdrag voor de beveiliging van informatie (14).

'De BIO zet de noodzaak voor een DPIA niet opzij'

Schematisch kan het als volgt worden weergegeven:
Risico's kunnen worden geaccepteerd. Preventieve, detectieve of repressieve maatregelen kunnen worden getroffen. Mogelijke dreigingen kunnen worden geneutraliseerd of een maatregelen kan worden genomen zodat de dreiging niet meer tot een incident leidt. Dit gebeurt aan de hand van het principe 'comply or explain'. De organisatie dient te beschikken over een registratie van overheidsmaatregelen waaraan niet of nog niet geheel kan worden voldaan: de 'pas toe of leg uit'- lijst met verplichte standaarden voor de publieke sector.

Connectie met DPIA: inzicht in risico's individu

De Data Protection Impact Assessment (DPIA) – of met een mooi Nederlands scrabblewoord de 'gegevensbeschermingseffectbeoordeling' (GEB) – blijft zeker van belang. De BIO zet de noodzaak voor een DPIA niet opzij. Kortweg kan gezegd worden dat de BIO meer een risicoschatting vereist voor de organisatie zelf – zoals het voorkomen van datalekken en de beschikking over een correct autorisatiesysteem. De DPIA kijkt meer naar de risico voor een individu wiens persoonsgegevens worden verstrekt. Een afgeronde DPIA is een analyse van de beoogde verwerkingen van persoonsgegevens voor persoonsgegevens en bevat de algemene context, informatie over de verwerkingen, beoordeling van de samenhangende risico's en concrete maatregelen die genomen worden om deze risico's te beheersen en ten slotte een uitspraak over de noodzaak van een voorafgaande raadpleging bij een DPIA.

Het privacyrecht richt zich op de belangen van natuurlijke personen. Het is theoretisch goed mogelijk dat een geautomatiseerd systeem helemaal state-of-the-art is op het gebied van security en daarmee de bedrijfsrisico's voor een organisatie nihil zijn, maar het voordoen van een enkel risico dat daaruit voortvloeit kan voor een enkel betrokken individu onacceptabel groot zijn, dat geconcludeerd moet worden om een geplande verwerking van persoonsgegevens geen doorgang te doen vinden. De Algemene Verordening Gegevensbescherming (AVG) versterkt immers de positie van individuele personen van wie gegevens worden verwerkt. De DPIA en een ISMS kunnen zeker wel overlappen en elkaar versterken; de bescherming van waardevolle en gevoelige bedrijfsinformatie is immers zowel een doel vanuit de informatiebeveiliging als de (personal/private) data protection.

Organisaties kunnen verplicht zijn een DPIA uit te voeren (art. 35 GDPR/AVG, art. 4c Wpg, art. 7b Wjsg). Bij gegevensverwerkingen met een hoog risico op een inbreuk op de persoonlijke levenssfeer zal een zogenoemd DPIA worden uitgevoerd waarin getoetst zal worden op rechtmatigheidsgrond en doelbinding. Ook gaat een DPIA over veel meer dan alleen de beveiliging van persoonsgegevens, zoals het vraagstuk van rechtmatigheid van verwerking: de rechten en vrijheden van natuurlijke personen om met name de oorsprong, de aard, het specifieke karakter en de ernst van dat risico te evalueren. Uiteindelijk gaat het om het vertrouwen dat burgers en bedrijven in het digitale overheidshandelen hebben. Voor het behoud van dat vertrouwen stelde de Nationale ombudsman op basis van onderzoeken vier uitgangspunten op: "Neem verantwoordelijkheid, wees toegankelijk, wees oplossingsgericht en wees gebruiksvriendelijk." Hij gaf daarbij aan dat de overheid digitalisering inzet in het belang van de gebruikers en niet alleen vanuit het gemak voor de overheid. "Laat goede dienstverlening daarbij het uitgangspunt zijn" (15).

Dat zou dus kunnen betekenen dat in bepaalde gevallen een 'papieren' procedure of een informerende gesprek wenselijker is voor burgers die niet volledig digitaalvaardig zijn. Voor organisaties kan het een aanbeveling zijn te zorgen voor een overzicht van alle processen en risicoanalyses (of DPIA's) om inzichtelijk te maken welke risico's aanwezig zijn rondom de verwerking van (persoons)gegevens.

Afsluitend: verschil tussen hard en zacht implementeren

Een citaat van Einstein met betrekking tot standaardisering is: "I believe in standardizing automobiles. I do not believe in standardizing human beings. Standardization is a great peril

which threatens American culture" (16). Het is eenvoudiger de standaardisatie van geautomatiseerde system te bewerkstelligen dan wanneer het gaat om eenduidig werken van gegevens en data waarbij zeker aspecten als cultuur, gedrag en competenties, maar ook zeker gevoel en ethiek van belang zijn. Standaardisatie is wel een basis voor een ambitie om steeds verder te verbeteren. Aan het welslagen draagt het welzijn van de burger (over wie informatie wordt verwerkt) wel bij. Privacy/security by design en/of by default is zeker niet minder belangrijk dan een 'safety by design'-cultuur. Een boeiende uitdaging voor iedereen die werkzaam is in dit vakgebied en dat ook enige inzet vraagt. "Niet omdat de dingen moeilijk zijn, durven wij niet, maar omdat wij niet durven zijn de dingen moeilijk" (17).

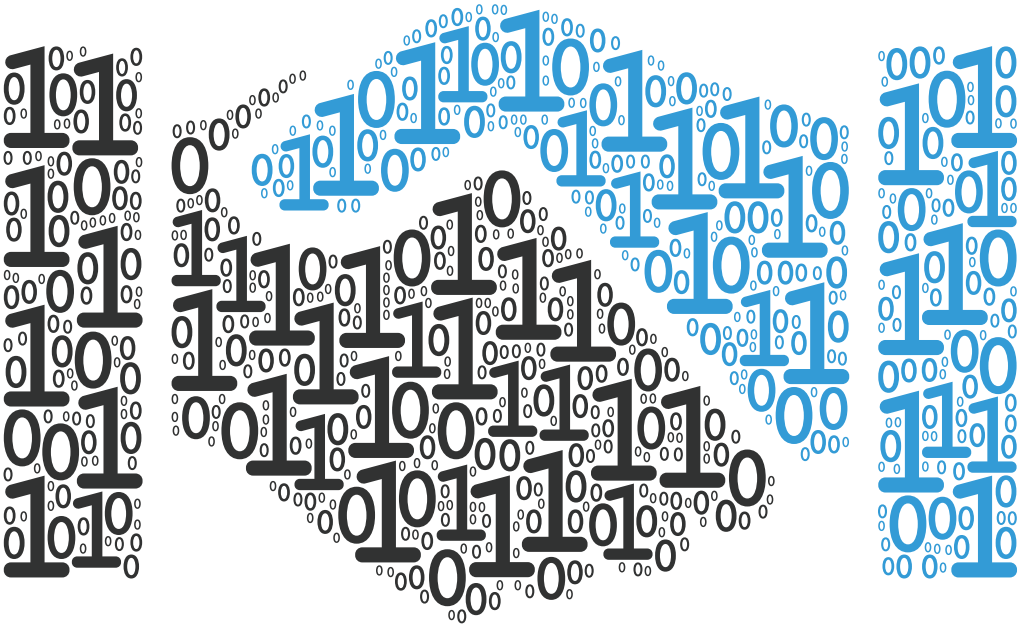
Referenties

(1) www.vimeo.com/user100586162
(2) Kamerstukken II, 2018/19, 26 643, nr. 574, p. 2.
(3) Kamerstukken II, 2018/19, 26 643, nr. 573, p. 1.
(4) Ook wel aangeduid als de informatieladder, zie: Bruins, R., B. Pinkster, Informatiemanagement, Amsterdam: Pearson Benelux, 2015; Grit, R., Informatiemanagement, Groningen: Noordhoff Uitgevers, 2016.
(5) Deze definitie komt overeen met die genoemd in artikel 1, sub b van het Voorschrift Informatiebeveiliging Rijksoverheid (VIR), Baseline Informatiebeveiliging Rijksoverheid (BIR), artikel 1, onder b van het Coördinatiebesluit organisatie en bedrijfsvoering rijksdienst 2011 en de begrippenlijst van de Informatiebeveiligingsdienst voor gemeenten (IBD).
(6) Van den Berg, J., 'Wat maakt cyber security anders dan informatiebeveiliging?, Magazine nationale veiligheid en crisisbeheersing 2015, nr. 2, p. 4-5.
(7) Anthony, R., V. Govindarajan, Management Control Systems, McGraw-Hill/Irwin, 12th ed., New York, 2007, p. 12 en 22-23.
(8) Merchant K.A., Van der Stede W.A., Management control systems; performance measurement, evaluation and incentives, 3th edition. Harlow: Pearson Education Limited, 2012, p. 42.
(9) Burns, J., Scapens, R.,, Conceptualizing management accounting change: an institutional framework, Management Accounting Research, 2000, vol. 11, no. 1, p. 3-35.
(10) Circulaire BIO, Staatscourant 2019, nr. 26526, p. 8.
(11) De eisen aan de informatiesystemen worden gebaseerd op de beveiligingskenmerken b(eschikbaarheid), i(ntegriteit) en v(ertrouwelijkheid); de BIV-driehoek naar het Engelstalige begrip 'the CIA triad': confidentiality, integrity and availability.
(12) Zoals gedefinieerd in het VIRBI 2013; dat staat voor het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013. Het VIRBI 2013 geeft de rubriceringsniveaus aan die zijn onderverdeeld in Staatsgeheim ZEER GEHEIM (afgekort Stg.ZG), Staatsgeheim GEHEIM (afgekort Stg.G), Staatsgeheim CONFIDENTIEEL (afgekort Stg.C) en Departementaal VERTROUWELIJK (afgekort Dep.V.).
(13) Zie onder 10.
(14) Verdrag tussen de Partijen bij het Noord-Atlantisch Verdrag inzake de beveiliging van gegevens, met bijlagen (Trb. 1998, 187 en 256).
(15) Ombudsvisie Digitalisering / Dossier Digitalisering van de Nationale ombudsman, https://www.nationaleombudsman.nl/dossier/dossier-digitalisering' geraadpleegd op 3 januari 2020
(16) "What Life Means to Einstein: An Interview by George Sylvester Viereck", The Saturday Evening Post, 26 oktober 1929, p. 17
(17) Non quia difficilia sunt non audemus, sed quia non audemus, difficilia sunt (Seneca, Epistuale Morales 104.26)

Meer informatie

- Circulaire toepassen Baseline Informatiebeveiliging Overheid in het digitale verkeer met het Rijk: https://zoek.officielebekendmakingen.nl/stcrt-2019-26526.html
- Website over BIO: https://www.bio-overheid.nl/
- Website Digitale Overheid: https://www.digitaleoverheid.nl/
- BIO bij provincies: https://ipo.nl/beleidsvelden/bestuur/e-dienstverlening
- BIO bij gemeenten: https://www.informatiebeveiligingsdienst.nl/
- BIO bij waterschappen: https://www.hetwaterschapshuis.nl/informatieveiligheid-en-privacy
- Video over BIO: https://vimeo.com/user100586162
- Ombudsvisie Digitalisering / Dossier Digitalisering van de Nationale ombudsman: https://www.nationaleombudsman.nl/dossier/dossier-digitalisering

Auteurs: Robert Seepers, Andre Smulders en Erik Meeuwissen zijn werkzaam bij TNO. Bob van der Kamp is werkzaam bij het NCSC. Robert is bereikbaar via robert.seepers@tno.nl.



Zero trust-architectuur op basis van implied trust-zones

'Zero trust' is een term die steeds meer draagvlak krijgt binnen de cybersecuritygemeenschap. Centraal achter het zero trust-gedachtegoed is dat er fundamenteel anders moet worden omgegaan met de beveiligingsarchitectuur van een organisatie en haar (IT) infrastructuur: van 'trust, but verify' naar 'don't trust, verify!' (1). In een zero trust-architectuur worden de resources van een infrastructuur – zoals systemen, data, applicaties of microservices – afzonderlijk beveiligd. Een zero trust-architectuur wordt hiervoor opgedeeld in kleinere, afzonderlijke beveiligde 'gebieden'. Wij noemen deze gebieden 'implied trust-zones', in navolging van een recent gepubliceerd NIST-document over zero trust-architecturen (2).

In vergelijking met gangbare beveiligingsarchitecturen bieden zero trust-architecturen – en daarbij implied trust-zones – de potentie om cyberaanvallen beter te voorkomen en detecteren. Het is echter nog niet duidelijk hoe een organisatie op de meest effectieve manier gebruik kan maken van dit concept. Hoe wordt een implied trust-zone bijvoorbeeld ingericht? En hoe kan ervoor gezorgd worden dat deze zones op een passende manier beveiligd zijn? In dit artikel verkennen we wat een implied trust-zone is en stellen we een aanpak voor die het mogelijk maakt om een zero trust-architectuur in te richten. Sleutelconcepten binnen deze aanpak zijn het toekennen van zone-eigenaarschap en een ontwerpmethode voor implied trust-zones.

In de volgende paragraaf bespreken we de belangrijkste publicaties achter het zero trust-gedachtegoed. Vervolgens bespreken we in paragraaf 3 hoe een zero trust-architectuur eruitziet op basis van implied trust-zones en wat de verschillende afwegingen zijn voor het ontwerp van een dergelijke architectuur. In paragraaf 4 introduceren we vervolgens het concept van de zone-eigenaar en de 'zoneringsaanpak', een methode voor het ontwerpen van een zero trust-architectuur op basis van implied trust-zones. Tenslotte bespreken we de conclusies van dit artikel en richtingen voor vervolgonderzoek in paragraaf 5.

State-of-the-art

In de periode 2003-2013 is er door het toenmalige Jericho Forum (nu onderdeel van The Open Group (3)) nagedacht over 'de-perimeterisatie': het verdwijnen van de klassieke perimeter van (interne) netwerksegmenten, met als resultaat: de 'Jericho Forum™ Commandments' en de 'Collaboration Oriented Architecture' (4). In 2010 werd, deels op basis van dit werk, een eerste opzet gemaakt voor een 'zero trust network architecture' door Forrester Research (1). NIST heeft recentelijk een nieuw document (SP 800-207) opgesteld (2), die gezien kan worden als een verdiepingsslag op de architectuurbeschrijving van Forrester Research. Kernonderwerp binnen SP 800-207 is het opsplitsen van een architectuur in afzonderlijke 'implied trust-zones', met strikte en fijnmazige access control-beslissingen bij elke toegang tot een zone. Er wordt echter niet besproken hoe een organisatie haar architectuur kan ontwerpen op basis van implied trust-zones.

In de praktijk wordt zero trust-architectuur slechts mondjesmaat toegepast: segmentatie vindt veelal plaats op fysiek netwerkniveau (vaak 'securityzones' genoemd). Een uitzondering op deze praktijk is Google's BeyondCorp: een vooruitstrevend voorbeeld van een opzet tot een zero trust-architectuur (5). In BeyondCorp krijgen gebruikers één van de vier 'trust tiers' toegewezen, op basis van bijvoorbeeld hun rol in de organisatie en de securitystatus van hun werkstation. Een bepaalde trust tier geeft toegang tot bepaalde functionaliteiten en data. Zowel security zones als BeyondCorp gaan uit van het splitsen en afzonderlijk beveiligen van functionaliteit, maar dit is veel grover van schaal dan binnen een zero trust-architectuur wordt nagestreefd (zoals verderop in dit artikel zal worden besproken).

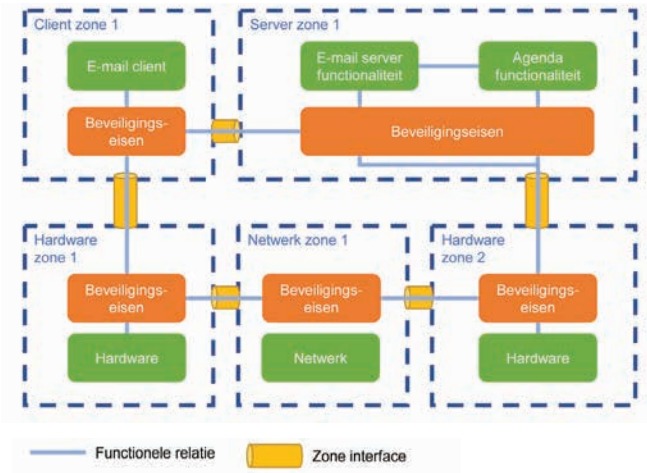
Op technologisch gebied zijn er een aantal ontwikkelingen die het al mogelijk maken om fijnmazigere zones aan te leggen – zoals virtuele machines en containerization (op basis van bijvoorbeeld Docker-containers en Kubernetes) of QubesOS (6). Deze worden echter nog niet volledig benut voor securitytoepassingen of het implementeren van een zero trust-architectuur. Deze state-of-the-art en het toenemende belang van het inrichten van een zero trust-architectuur is de aanleiding om een methode te ontwikkelen die het ontwerpen en inrichten van implied trust-zones ondersteunt.

Implied trust-zones

We definiëren een implied trust-zone als een afgebakend stuk functionaliteit dat individueel beveiligd is. Functionaliteit wordt hierbij in de breedste zin van het woord uitgelegd: zo kan het een bepaalde applicatie zijn (bijvoorbeeld een e-maildienst), een deelfunctionaliteit of microservice, een beveiligingsfunctionaliteit (zoals een firewall) of een stuk ondersteuningsfunctionaliteit (bijvoorbeeld hardware die rekenkracht en opslagcapaciteit levert). Het opzetten van een verbinding van en naar deze zone is alleen mogelijk als er aantoonbaar voldaan is aan de daarvoor geldende beveiligingseisen. De naam 'implied trust-zone' refereert naar het impliciete vertrouwen dat wordt toegekend als er aan deze beveiligingseisen is voldaan. Op basis van dit vertrouwen wordt het mogelijk om de verschillende functionaliteiten van de zone te gebruiken.

Een zero trust-architectuur bestaat uit meerdere, afzonderlijk afgeschermde implied trust-zones, zoals geïllustreerd in figuur 1. De verschillende functionaliteiten die een organisatie nodig heeft voor haar bedrijfsprocessen zullen zich bevinden in één of meerdere zones. Als deze functionaliteiten in dezelfde zone zitten dan kunnen deze direct met

elkaar communiceren (aangezien er implied trust is binnen een zone). Wanneer de functionaliteiten zich bevinden in meerdere zones, dan zal er eerst voldaan moeten worden aan de onderlinge beveiligingseisen voordat er communicatie plaats kan vinden. Dit wordt mogelijk gemaakt door een zone-interface (7).



Figuur 1 - Een voorbeeld zero trust-architectuur die is opgebouwd uit meerdere implied trust-zones.

Binnen het zero trust-gedachtegoed is het de voorkeur om implied trust-zones zo klein mogelijk te maken (lees: de geleverde functionaliteit per zone te beperken). Kleine zones brengen, in potentie, namelijk de volgende beveiligingsvoordelen:

- Beperking van de mogelijkheden tot lateral movement: door een architectuur op te delen in kleine zones, elk met beperkte functionaliteit, wordt het lastiger gemaakt voor een aanvaller om zich vrijuit te bewegen over de infrastructuur.
- Het wordt makkelijker om aanvallen te detecteren op basis van afwijkende communicatiepatronen omdat communicatie tussen zones op een meer gestructureerde en voorspelbare manier verloopt.
- Beperking van het aanvalsoppervlak omdat er slechts een (zeer) beperkte hoeveelheid functionaliteit wordt aangeboden 'van buitenaf'.
- Mogelijkheden om de beveiligingseisen zo nauw mogelijk af te stemmen op de geleverde functionaliteit en de door de organisatie gelopen risico's. Dit zou het mogelijk maken om een betere business-ICT-security alignment te realiseren.

Toch is het zo klein mogelijk maken van een zone niet in alle situaties even gewenst of mogelijk. Zo kan het zijn dat:

- De onderhoudbaarheid van de architectuur achteruitgaat doordat deze onoverzichtelijk is geworden. Bijvoorbeeld doordat het verkleinen van zones ervoor zorgt dat er meer communicatie en interacties tussen zones zijn, of doordat het fijnmazig beheersen van de beveiligingseisen meer tijd kost in vergelijking met grote zones.
- Het zoneren een te hoge impact heeft op functionele performance of communicatie, waardoor het niet meer mogelijk is om aan functionele eisen te voldoen.
- Het zo klein mogelijk maken niet past binnen (de principes van) een organisatie. Een voorbeeld hiervan is het 'buy don't build'-principe, waarbij een organisatie alleen gebruik maakt van commercieel verkrijgbare apparatuur en softwarepakketten. Dit zijn vaak pakketten die als geheel geleverd worden en daarbij niet fijnmazig kunnen worden opgesplitst in deelfunctionaliteiten.

De 'optimale' zonering is hierbij erg afhankelijk van de organisatie, haar capaciteiten en doelstellingen. Zo kan het zijn dat een organisatie de voorkeur heeft om haar architectuur op te delen in enkele grote zones (lees: meerdere grote blokken functionaliteit, die met één set beveiligingseisen worden afgedekt), omdat dit de onderhoudbaarheid ten goede komt; of om deze juist op te delen in veel kleine zones voor beveiligingsdoeleinden. Het inrichten van een zero trust-architectuur is hierbij een complexe puzzel waarbij er rekening gehouden moet worden met aspecten zoals de beheersbaarheid, functionele performance, de beveiliging van functionaliteiten en informatie, architectuurprincipes, wettelijke kaders en organisatiebeleid.

Decentraal architectureren en zoneringsaanpak

Zoals beschreven zijn er verschillende redenen om een architectuur te ontwerpen op basis van grote of kleine zones. Maar wanneer is een zone te klein, te groot, of precies goed? Wie bepaalt de beveiligingseisen van een zone? En wie bepaalt er of een architectuur goed is ingericht of dat er aanpassingen nodig zijn in de zonering om een betere afweging te maken tussen bijvoorbeeld de performance-, beveiligings- en onderhoudbaarheidseisen?

Eerst terug naar de basis: bedrijfsprocessen worden direct of indirect gefaciliteerd door verschillende functionaliteiten (ondergebracht in een of meerdere trust-zones). Elke zone

(en interacties tussen zones) kent hierbij een bepaald bedrijfs- of beveiligingsrisico: bijvoorbeeld dat de uitval of compromittatie van een zone een bedrijfsproces stillegt. De beveiligingseisen (en -maatregelen) voor een zone moeten ervoor zorgen dat dit risico voldoende is afgedekt, waarbij rekening moet worden gehouden met de bedrijfsvoering, wettelijke kaders, standaarden en (functionele) afhankelijkheden naar andere zones. Daarnaast moeten aspecten zoals onderhoudbaarheid en performance eisen ook voldoende geborgd zijn binnen een zone-inrichting.

In de meest gangbare architectuurraamwerken staat een enterprise- of beveiligingsarchitect centraal in het opstellen van de eisen en de daarvoor benodigde maatregelen. Ons beeld is dat met de opkomst van systems of systems een zero trust-architectuur niet meer ontworpen kan worden door een (centraal geplaatste) architect. Dit vanwege de hoge mate van detail en complexiteit die nodig is om een passende afweging te maken voor elk deelsysteem. Deze kennis is daarbij vaak decentraal belegd in een organisatie. Daarbij zal het hierbij nodig zijn om de verschillende relaties tussen zones nauwkeurig te modeleren en af te stemmen over de verschillende zone-interfaces. Om deze redenen stellen wij voor om het 'architectureren' op een decentrale manier te bedrijven, waarbij de uiteindelijke architectuur een composiet is van verschillende, op elkaar afgestemde, deelarchitecturen (de implied trust-zones). Om een architectuur gedecentraliseerd te kunnen ontwerpen is het in ieder geval nodig om:

- Een organisatorische entiteit te koppelen aan elke zone die er zorg voor draagt dat deze op de juiste manier wordt ingericht, geïmplementeerd en onderhouden.
- Een methodiek vast te stellen waarmee op overkoepelend niveau bepaald kan worden dat een architectuur de algehele risico's voor een organisatie dekt, ook wanneer deze uit meerdere deelarchitecturen bestaat.

De rest van dit artikel richt zich primair op de eerste bullet. We introduceren hierbij een nieuwe rol: de zone-eigenaar, de organisatorische entiteit die ervoor zorgt dat de zones waaraan hij/zij gekoppeld is op een juiste manier zijn ingericht en onderhouden. In wezen verricht de zone-eigenaar soortgelijke activiteiten als een (enterprise/-security) architect, maar dan op zoneniveau. De zone-eigenaar is hierbij als een spin in het web en het primaire aanspreekpunt voor de zone. Als onderdeel van deze rol zal de zone-eigenaar bijvoorbeeld moeten afstemmen met verschillende stakeholders die een directe relatie hebben met de zone, zoals beleidsmakers, technisch specialisten of andere zone-eigenaren (zie figuur 2), om de zonebeveiligingseisen voor een zone scherp te krijgen. Daarbij is de zone-eigenaar ook het primaire aanspreekpunt/escalatiekanaal indien er tijdens de bedrijfsvoering wijzigingen plaatsvinden die relevant zijn voor zijn zone (bijvoorbeeld uitval van een gerelateerde zone).

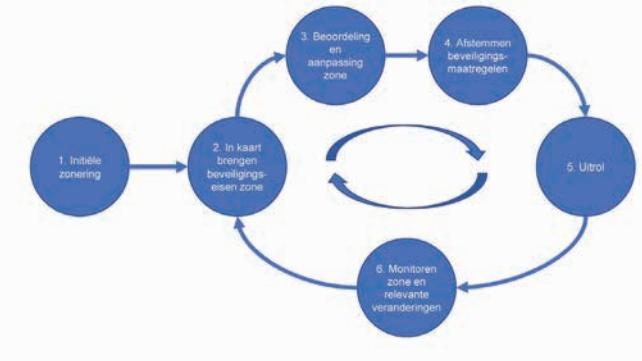
Figuur 2 - De zone-eigenaar is de spin in het zoneweb en het primaire aanspreek – en afstempunt - zowel tijdens de ontwerpfase als tijdens de operatie.

Onze verwachting is dat het decentraal beleggen bij individuele eigenaren zal leiden tot een betere afstemming tussen de verschillende (business)eisen en de inrichting van een implied trust-zone. Dit, omdat de zone-eigenaren een scherp beeld zullen hebben van de impact die een bepaalde functionaliteit heeft op de afhankelijkheden van en naar zijn zone, de securityrisico's die relevant zijn voor de zone en de beveiligingsmaatregelen die nodig zijn om deze risico's te voorkomen. Daarbij stelt dit totaalbeeld de zone-eigenaar in staat om snel keuzes te maken tijdens een incident, wat het herstelvermogen ten goede komt.

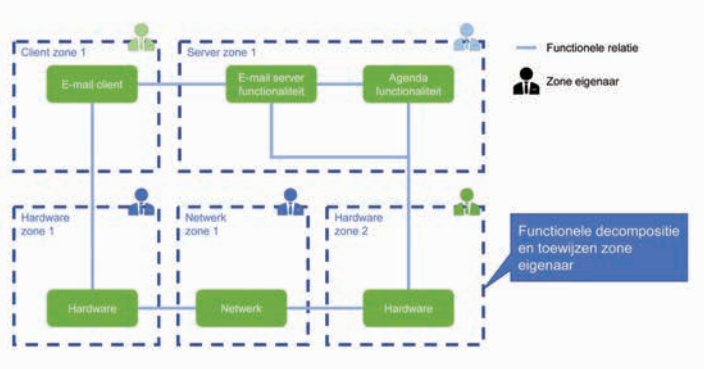
Zoneringsaanpak

In de vorige paragraaf lichtten we toe dat architectuur in onze optiek decentraal moet worden bedreven door meerdere zone-eigenaren. Maar hoe kan een zone-eigenaar de afweging maken tussen de inrichting van de hem toebedeelde zone? Hoe kan hij/zij rekening houden met bijvoorbeeld beveiligings- en onderhoudbaarheidsaspecten, en hoe zou hij/zij de zone-inrichting kunnen aanpassen als deze afweging niet conform zijn/haar eisen en wensen is?

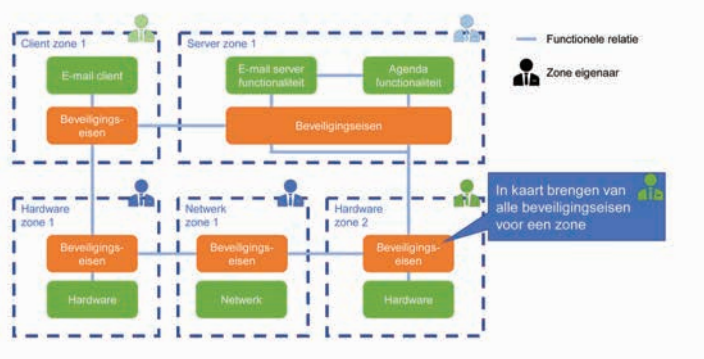
Als hulpmiddel hiervoor introduceren we de zoneringsaanpak: een iteratief proces dat door elke zone-eigenaar wordt doorlopen tijdens het inrichten (en beheren) van de zone. Het proces, geïllustreerd in figuur 3, toont de 6 stappen die gebruikt worden om: de functionaliteit en beveiligingseisen van een zone te definiëren, te toetsen of de zone-inrichting aansluit bij de wensen en doelstellingen van de zone-eigenaar en om (waar nodig) aanpassingen door te voeren. Let op dat dit een iteratief proces is waarbij niet alle stappen altijd in dezelfde mate van detail doorlopen hoeven te worden. We lichten deze stappen hieronder kort



Figuur 3 - Overzicht van de implied trust-zones ontwerpmethode 'zoneringsaanpak'.



Figuur 4 - Functionele decompositie en toewijzen zone-eigenaar (verschillende zone-eigenaars zijn weergegeven met aparte kleuren).



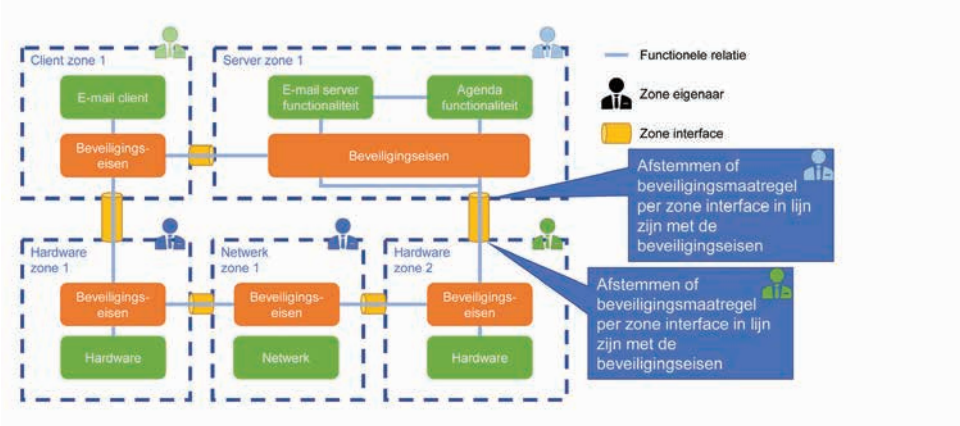
Figuur 5 - In kaart brengen van alle beveiligingseisen voor een zone.

Stap 1 – Initiële zonering: in deze stap wordt een functionele architectuur opgesteld voor de totale architectuur. Vervolgens worden er zone-eigenaren toegewezen aan functionaliteiten. Waar mogelijk wordt er hierbij gebruik gemaakt van reeds belegde verantwoordelijkheden (bijvoorbeeld proceseigenaren). Er ontstaat hierbij een eerste schets van de gezoneerde architectuur waarbij functionaliteiten zijn belegd in zones en elke zone een eigenaar toegewezen heeft gekregen (zie figuur 4). Beveiligingseisen worden nog niet meegenomen in stap 1.

Stap 2 – In kaart brengen beveiligingseisen: in deze stap leidt de zone-eigenaar beveiligingseisen af voor zijn zone (zie figuur 5). Als primaire input worden hierbij de verschillende afhankelijkheden van de zone gebruikt, waaronder die met andere zones, bedrijfsprocessen en organisatiebeleid. Waar mogelijk wordt hierbij gebruik gemaakt van reeds bekende beveiligingseisen, bijvoorbeeld afkomstig van eerder uitgevoerde risicoanalyses.

Stap 3 – Beoordeling en aanpassing zone: in deze stap bepaalt elke zone-eigenaar of zijn zone voldoet aan zijn wensen en eisen zoals: security en performance requirements, onderhoudbaarheid, kosten en compliance. Indien dit niet het geval is, dan wordt de zone – in afstemming met andere zone-eigenaars – opnieuw opgedeeld. Er worden nieuwe zone-eigenaars toegewezen aan deze nieuwe zone(s), waarna een nieuwe iteratie van de zoneringsaanpak wordt uitgevoerd (vanaf stap 2).

Stap 4 – Afstemmen beveiligingsmaatregelen: deze stap wordt bereikt als de zone-eigenaar(s) tevreden zijn met hun zone-opdeling en de daarvoor geldende beveiligingseisen. Op dit punt is er echter nog geen specifieke set maatregelen geïmplementeerd die nodig is om te voldoen aan de beveiligingseisen. In stap 4 wordt er afgestemd welke maatregelen er nodig zijn en door welke eigenaar ze worden ingericht (zie figuur 6).



Figuur 6 - Afstemmen van beveiligingsmaatregelen door de daarbij betrokken zone eigenaars.

Stap 5 – Uitrol: de ontwerpfase is afgerond en de zones worden geïmplementeerd. In deze fase heeft de zone-eigenaar de taak om te verifiëren dat het ontwerp op de juiste manier is geïmplementeerd en uitgerold.

Stap 6 – Monitoring: de zone-eigenaar vormt na uitrol het primaire aanspreekpunt en escalatiekanaal bij een (security) incident. Daarnaast houdt hij relevante veranderingen in de gaten in gerelateerde zones en binnen de organisatie om zijn zone up-to-date en beschermd te houden.

Conclusies en vervolgonderzoek

Implied trust-zones zijn afgebakende onderdelen van een infrastructuur die een stuk functionaliteit koppelen aan de daarvoor geldende beveiligingseisen en beveiligingsmaatregelen. In dit artikel hebben we verkend hoe een organisatie een zero trust-architectuur kan inrichten op basis van implied trust-zones. We introduceerden hierbij een nieuwe rol (de zone-eigenaar) die zorg draagt over de functionele- en de beveiligingsinrichting van zijn zone.

Ook introduceerden we de zoneringsaanpak, een methode die door individuele zone-eigenaren gebruikt kan worden om zones op een gestructureerde manier te ontwerpen, implementeren en beheren. Een enterprise-/beveiligingsarchitectuur is binnen dit gedachtegoed opgebouwd uit meerdere deelarchitecturen (de trust-zones). Door de koppeling tussen bedrijfsdoelen, functionaliteiten en beveiliging decentraal te beleggen onder één entiteit (de zone-eigenaar) verwachten we dat implied trust-zones gebruikt kunnen worden om een sterke business-IT-security alignment te realiseren.

Dit artikel is tot stand gekomen op basis van literatuuronderzoek, gesprekken met cybersecurityprofessionals (waaronder beveiligingsarchitecten), eigen ideeën en inzichten, en het toetsen van (delen van) de ontwerpmethode op een aantal bestaande ontwerpen. Als volgende stap zijn we van plan om de zoneringsaanpak verder te valideren in de praktijk. Daarnaast vragen wij ons af hoe een architectuur op centraal niveau kan worden beoordeeld als deze op decentrale manier is ontworpen. Ook deze vraag willen we beantwoorden in vervolgonderzoek.

Referenties

(1) J. Kindervag, „Build security into your network's dna: The zero trust network architecture.," Forrester Research Inc, 2010.
(2) S. Rose, B. Oliver, S. Mitchell en S. Connelly, „SP 800-207: Zero Trust Architecture (draft)," NIST, 2019.
(3) The Open Group, zie "https://www.opengroup.org/forum/security,".
(4) The Open Group, „Framework for secure collaboration-oriented architectures (O-SCOA)," The Open Group, 2012.
(5) R. Ward en B. Beyer, „Beyondcorp: A new approach to enterprise security.," usenix.org, 2014.
(6) J. Rutkowska en R. Wojtczuk, „Qubes OS architecture," Invisible Things Lab Tech Rep 54 , 2010.
(7) H. Hut, W. Langenkamp en M. S. R. Kea, „Advanced security architectures: Don't trust, verify!," in Innovating in cyber security, TNO shared research, 2019, 2019.

Auteur: Chris de Vries is redacteur van iB-Magazine. Chris is bereikbaar via impuls@euronet.nl.

Titel : Het is oorlog maar niemand die het ziet
Schrijver : Huib Modderkolk
Taal : Nederlands
Aantal pagina's : 272
ISBN-nummer : 978-90-5759-980-4

BOEKREVIEW

Het is oorlog maar niemand die het ziet

Het is oorlog maar niemand die het ziet leest als een thriller, maar een onthutsender en ontluisterend boek heb ik zelden gelezen. Iedereen die werkzaam is in de ICT-veiligheid weet dat er vele gevaren zijn voor de gebruiker van een computer, een slimme telefoon of een tablet. De moderne technologie biedt ons veel gemakken, maar doet ons ook de controle verliezen over onze persoonlijke informatie.

Amsterdam Internet Exchange [1]
De Amsterdam Internet Exchange is het belangrijkste internetknooppunt van Nederland en heeft na IX.br het grootste ledental. Een zeer groot deel van het internetverkeer met het buitenland en de gegevensstroom tussen Nederlandse internetproviders wordt afgehandeld via het netwerk van AMS-IX.

Mijn interesse voor computers ontstond in het midden van de zeventiger jaren, toen ik de intuïtie had dat de computer wel eens onze grootste vijand zou kunnen zijn. En uit het boek van Huib Modderkolk destilleer ik dat dan ook: de burger haakt vrijwel direct af wanneer hij de combinatie 'privacy', 'ICT', 'encryptie' en 'wachtwoord' hoort. Voor hem is het een ver-van-zijn-bed-show. Hij vertrouwt op zijn overheid en de aan haar dienstbare ambtenaren. In dit boek komen echter voorbeelden aan de orde waarbij sprake is van het inzamelen van alle data die men maar kan vinden. Om een voorbeeld te geven:

Gegevens	NSA (USA)	GHCQ (UK)
Datum	?	2011
Internetdata	312 miljard	50 miljard
Telefoondata	135 miljard	600 M
Aantal telefoongesprekken	19 miljard	100 M
Per periode	Maand	Dag
Omgerekend per dag	600 M	100 M

Tabel 1 - Gegevens ontleend aan het boek, pagina 95 en 112 (zie ook literatuurlijst pagina 258 & 259).

Iedereen doet er aan mee. De VS, Israël, Rusland, China, Noord-Korea, Engeland, Duitsland, Iran, India en niet te vergeten: Nederland (die overigens kwalitatief heel goed meekomt en ook wel het Zwitserland onder de geheime diensten wordt genoemd, aldus Huib Modderkolk). Al deze data leiden onder andere tot drone-aanvallen (6.786 bevestigde aanvallen met meer dan 10.000 doden, waarvan tussen de 800 en 1.700 burgerdoden en waaronder zeker 253 kinderen). Aanvallen die vaak gebaseerd zijn op het unieke IMEI-nummer van mobiele telefoons, mede verzameld door een Nederlands schip met Amerikaanse apparatuur, weet Huib Modderkolk ons mee te delen. Maar niet alleen mensen zijn aanvalsdoelen. De VS en Engeland hebben een digitale aanval gedaan op Belgacom (wellicht om marketingredenen hernoemd tot 'Proximus'), waarmee zij toegang kregen tot het enige buiten Amerika gelegen wereldwijde roamingnetwerk (BICS) met betrekking tot telefonie. Daarmee kregen zij toegang tot 1.100 bedrijven en instanties waaronder: de Europese Unie, het Europees Parlement en daarnaast 500 mobiele operators zoals KPN en T-Mobile. Men spreekt hier over de digitale roof van de eeuw (2010/2011). Van wereldwijde roamingnetwerken zijn er slechts 3 (ontleen ik aan het boek).
BICS is vergelijkbaar met het AMS-IX (Amsterdam Internet Exchange) en is voorzien van Amerikaanse apparatuur. Een ander aangehaald voorbeeld is de Yahoo-hack (de grootste dataroof van de 21e eeuw), waarbij van 500 miljoen gebruikers data gestolen werd door een 23-jarige man uit Kazachstan (wonende in Canada), maar waarvan vermoed wordt dat de Russische geheime dienst (FSB) erachter zat. En zo worden er vele voorbeelden aangehaald in dit boek waarbij de geheime diensten een oorlog met elkaar uitvechten, maar de allianties net zo snel wisselen als het weer in Nederland.

Wat in het boek ook naar voren komt, is dat menselijke nalatigheid of gemakzucht ook een belangrijke oorzaak van problemen kan zijn. Huib Modderkolk licht dat toe aan de hand van de KPN-hack door een 17-jarige hacker - die daarmee enorm veel schade had kunnen berokkenen, maar dat niet gedaan heeft. Het was een sociaal geïsoleerde (in pleegzorg) jongeling die als gevolg daarvan met justitie in aanraking kwam, het huis verliet en op 22-jarige leeftijd zelfmoord pleegde in Zuid-Korea. Zijn aanval baseerde zich op een HP Data Protector-exploit welke bij KPN niet afgedicht was. Een triest verhaal waarbij de vraag opkomt: lag er ook niet een verantwoordelijkheid bij de grote organisatie? Zo ook het fiasco bij DigiNotar: een aanval waarbij certificaten (uit naam van: Amazon, Microsoft, Google, de website van MI5, de CIA, allerlei Nederlandse organisaties, en de Israëlische geheimdienst Mossad; zie pagina 43) door een onbevoegde hacker werden uitgegeven, welke alles op de grondvesten deed daveren en onze Nederlandse overheid op slot had kunnen zetten. Het vermoeden bestaat dat dit een Iraans antwoord was op Nederlandse betrokkenheid bij de Stuxnet-aanval (de Iraanse nucleaire centrifuge sabotage via Siemens-apparatuur). Dit bleek allemaal mogelijk te zijn, omdat de gebruikers van het zwaar beveiligde & geïsoleerde DigiNotar-systeem het lastig vonden om tijd kwijt te raken aan het binnenkomen van die ruimte en dus even een netwerkkabeltje naar binnen hadden gelegd, natuurlijk bereikbaar via een onvoldoende beveiligde computer. Al deze verhalen en voorbeelden zijn terug te vinden in dit goed en vlot geschreven boek. Of het ons als burger meer vertrouwen in onze overheid en veiligheidsdiensten geeft, waag ik te betwijfelen. Daarvoor vallen er te veel onschuldige doden en gewonden, wordt er te makkelijk (en wellicht illegaal?) omgegaan met onze persoonlijke data en wordt er te makkelijk een doekje voor het bloeden over misstanden heen gedrapeerd. Alles met als motivatie: bestrijding van terrorisme en misdaad. Niets borgt macht beter dan het creëren van een wereld vol angst.

Referenties:

(1) www.wikipedia.org/wiki/Amsterdam_Internet_Exchange

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

IT en business continuity

Stel collega's eens de vraag: "Zou je zonder IT jouw werk kunnen doen?" In heel veel organisaties zal dan het antwoord iets in de richting zijn van: "Nee" of "Nou, daar vraag je me wat. Ik denk dat dat niet eenvoudig is." Naast de broodnodige applicaties zoals Outlook en Microsoft Office 365 zijn er veelal tientallen bedrijfsapplicaties die gebruikt worden in de bedrijfsprocessen. Maar wanneer er een probleem is, wijst iedereen waarschijnlijk naar de IT-afdeling, die het maar moet oplossen. Maar wat doet de proceseigenaar en eindverantwoordelijke zelf? Handjes in de lucht of over elkaar, achterover zakken en vertwijfeld rondkijken?

Het is duidelijk dat de afhankelijkheid van IT enorm is en dat het alleen nog maar verder gaat toenemen. Het is eigenlijk een onaanvaardbare afhankelijkheid waar we van wegkijken, het gemakshalve negeren of het zelfs glashard ontkennen. IT continuity of (indien er een 'probleem' is) disaster recovery (DR) is dan ook steeds belangrijker geworden. Er wordt veel tijd, geld en energie gestoken in redundancy. Bijvoorbeeld door middel van meerdere datacenters en allerlei andere mitigerende oplossingen om te voorkomen dat IT (waaronder informatiebeveiliging) uitvalt.

IT continuity

We kunnen vaststellen dat IT continuity - het zorgdragen voor continuïteit van de IT en een foutloze implementatie van het disaster recovery plan (DRP) - áls er toch iets gebeurt - iets anders is dan business continuity (BC). Dit is het zorgdragen dat we onze producten en diensten kunnen blijven leveren, wat er ook gebeurt en op een van tevoren bepaald niveau. Dat houdt dus niet in dat mensen op hun handen kunnen gaan zitten, naar de IT-afdeling kunnen wijzen en zeggen dat ze zonder IT niets kunnen doen.
Business continuity management (BCM) of bedrijfscontinuïteitsbeheer gaat over het zo optimaal mogelijk voorbereid zijn op het (on)verwachte, een bedreiging of (zoals u wilt) risico. Deze wordt werkelijkheid. De herziene versie van de ISO 22301-norm is kortgeleden gepubliceerd, echter er zijn geen schokkende wijzigingen ten opzichte van de eerste versie die in 2012 is gepubliceerd. Na zo'n zes jaar ervaring met de toepassing was dit nodig om de voortdurende veranderingen in de bedrijfscontinuïteitwereld weer te kunnen geven. De tekst is aangepast om meer duidelijkheid en consistentie te kunnen bieden, al gaat het voornamelijk om verduidelijking, vereenvoudiging van terminologie en definities. Daarnaast gaat het om het volledig in lijn brengen van de structuur met de high level structure (HLS), in overeenstemming met alle andere ISO-managementsysteemnormen (1).

Bedreigingen

Belangrijk is alleen om je te realiseren dat IT-uitval één van de grootste bedreigingen is voor organisaties. IT-uitval kan op zich ook weer vele oorzaken hebben. Het herstellen van bijvoorbeeld de toegang tot het netwerk, internet of een applicatie of het vervangen van falende hardware die de uitval veroorzaakt vallen dus onder IT continuity. De reactie van de gebruikers, het zorgen dat je je producten en diensten kunt blijven leveren aan je klanten dient te worden geregeld binnen het vakgebied BC. Verder zijn bijvoorbeeld brand, personeelstekorten (door een OV-staking), het stilvallen van een productielijn (door een storing) of problemen in de supply chain (als gevolg van extreem winterweer) ook serieuze bedreigingen voor de continuïteit van organisaties.
Eén van de belangrijkste elementen tijdens het implementeren van een business continuity managementsysteem (BCMS) is het uitvoeren van een risicobeoordeling. Krijgt de

afhankelijkheid van IT en de actuele bedreigingen rond dit thema, denk aan cybercrime, de juiste aandacht en het benodigde gewicht? Goed om in ieder geval in beeld te hebben welke geprioriteerde, kritische activiteiten of processen afhankelijk zijn van bepaalde applicaties of data. Bijvoorbeeld om zodoende te kunnen bewerkstelligen dat de juiste herstelstrategie ingericht is, als dit nodig is. Kunnen we tóch zonder toegang tot internet, applicaties of data tot op zekere hoogte producten en diensten blijven leveren? En het belangrijkste: wat kunnen we vóóraf regelen en in business continuity plannen (BCP's) opnemen als eventuele alternatieven? Wat is een acceptabele impact wanneer applicaties uitvallen of data niet beschikbaar is? IT, waaronder informatiebeveiliging (IB) en de herstelstrategie, hangt zeer nauw samen met BCM en de gekozen strategie in geval van een calamiteit. Niet wijzen of afwachten dus, maar samenwerken, informatie delen en je zoveel mogelijk voorbereiden. Al moet eerlijkheidshalve gesteld worden: voor zover mogelijk.

Beheersmaatregelen

Wanneer we specifiek kijken naar informatiebeveiliging is er een norm waarin ook de term 'continuity' voorkomt: ISO 27001, inmiddels bij iedereen een bekend fenomeen. Naast het managementsysteem is in deze norm tevens een annex A opgenomen met 114 beheersmaatregelen voor IB. Deze beheersmaatregelen dienen risico-gebaseerd geïmplementeerd te worden om tot een adequaat beveiligingsniveau te komen. Specialisten op dit gebied, zoals Johan Bakker van Unified Vision, spannen zich dagelijks in om dit goed onder de aandacht te brengen van gebruikers en dat is een uitdaging. In de genoemde annex A zit ook een hoofdstukje over BCM. Hierover ontstaat nogal eens verwarring wanneer men IB - conform ISO 27001 – implementeert met certificering als één van de doelstellingen.

Business impact analyse

In de praktijk wordt regelmatig op basis van de eisen in de annex A een volledig BCP opgesteld die gericht is op de belangrijkste bedrijfsprocessen. Hoewel dit vanuit een bedrijfscontinuïteitsperspectief bezien wellicht wenselijk is, is het voor ISO 27001-certificering echter niet noodzakelijk. Sinds de introductie van de 2013 versie van ISO 27001 komt deze verwarring al minder voor, omdat de eisen in annex A nu helderder geformuleerd zijn. In beheersmaatregel 17.1.1 staat dat de eisen voor IB gedurende calamiteiten vastgesteld moeten worden en dat tevens de continuïteit van het IB-beheerproces geborgd moet worden. Dit betekent dat de eisen in bij voorkeur DRP's dienen te worden toegevoegd die de vereiste mate van beschikbaarheid, integriteit en vertrouwelijkheid van bedrijfsinformatie gedurende calamiteiten definiëren. Daarnaast wordt er voor het IB-beheerproces een business impact analyse (BIA) uitgevoerd en worden er zo nodig preventieve en correctieve maatregelen voor de beschikbaarheid en tijdig herstel van (delen van) dit proces als onderdeel van de BCM ingeregeld.

ISO 27031

In dit kader is het jammer te noemen dat een norm waar beide onderwerpen tot op zekere hoogte bijeen worden gebracht redelijk onbekend en daardoor ook onbemind is. ISO 27031 'Information technology – cybersecurity – information and communication technology readiness for business continuity' slaat als het ware een brug tussen ICT (iets breder aldus dan IT) en BCM. Deze in 2011 gepubliceerde norm wordt momenteel herzien en verdient zeker extra aandacht nadat deze is gepubliceerd, waarschijnlijk in de loop van 2020. Het niet beschikbaar zijn van ICT-diensten, inclusief die veroorzaakt worden door het optreden van beveiligingsproblemen zoals hacking en malware-infecties, hebben nu enorm veel invloed op de continuïteit van de bedrijfsvoering zoals eerder gesteld. Het beheer van ICT en gerelateerde continuïteit en andere beveiligingsaspecten vormen aldus een belangrijk onderdeel van de vereisten voor BC. De binnen BCM vastgestelde geprioriteerde, kritische activiteiten die opgenomen dienen te worden in een BCP zijn nagenoeg altijd (volledig) afhankelijk van ICT. Deze afhankelijkheid betekent dat verstoringen van ICT strategische risico's kunnen vormen en uiterst kwalijk kunnen zijn voor de reputatie van de organisatie en haar vermogen om producten en diensten te leveren. In dit kader is ICT continuity een essentieel onderdeel voor veel organisaties bij de implementatie van BCM en IB. Als onderdeel van de implementatie en werking van een informatiebeveiligingsbeheersysteem (ISMS) zoals gespecificeerd in respectievelijk ISO 27001 en het BCMS in ISO 22301, is het van cruciaal belang om een plan voor de ICT-diensten te ontwikkelen en te implementeren om de continuïteit te verzekeren. De herziene versie van ISO 27031 zal zeker bijdragen aan het algehele continuïteitsbeheer, zowel van ICT als de bedrijfsvoering. Houd de ontwikkelingen dus in de gaten.

Referenties

(1) www.nen.nl

TECHNIEK EN MENS IN BEWEGING

Het nieuwe jaar is weer begonnen. Op 14 januari werd dit ingeluid tijdens een bijeenkomst over quantum computing. Een onderwerp waarbij in het nieuwe jaar automatisch de blik vooruit wordt geworpen. En dat doen wij als bestuur natuurlijk ook: even terugkijken, omarmen wat goed gaat, leren van wat beter kan en dan verder met de uitdagingen voor het volgende jaar. Binnen onze mooie vereniging, maar ook daarbuiten. Over dat laatste wil ik het even kort hebben. De digitale samenleving in Nederland verandert continue en in een rap tempo. Dat behoeft binnen onze beroepsgroep geen uitleg.

Bij die veranderingen staat de mens centraal. 'De mens is de maat van alle dingen', zei Protagoras. Dat was toen en is nu nog steeds zo. Dit is zichtbaar in maatschappelijke bewegingen en bedrijfseconomische belangen. Ook bij cybersecurity blijkt de mens vaak de kritische faal- en succesfactor te zijn als het gaat om bijvoorbeeld leiderschap of de gebruiker. Daarbij is de mens in onze kenniseconomie een cruciale factor. Mens en techniek zijn nauw verweven met elkaar en moeten als één geheel worden gezien. Innoveren, werken en leren is een driehoek die een belangrijke pilaar is in cyberweerbaarheid.

Cybersecurity in het onderwijs en het bedrijfsleven en de afschaffing van numeri fixi-systemen voor cybersecurity-opleidingen zijn reden tot zorg, net als de onvoldoende voorbereiding van de jeugd op de digitale toekomst en een groot tekort aan cyberspecialisten. Nieuwe technologische ontwikkelingen, zoals kunstmatige intelligentie, vragen om nieuwe kennis en vaardigheden. Deze specialisten hebben we nu en in de toekomst heel hard nodig.

Versplintering van initiatieven leidt ook bij het human cyber capital tot beperking van de slagkracht. Er is behoefte aan duidelijkheid in functies en kwalificaties. Op onderwijsvlak worden weliswaar initiatieven ondernomen, maar er is nog onvoldoende aansluiting op het vakgebied. Er zullen meer professionals gemobiliseerd moeten worden willen we voldoende kunnen versnellen in het bijblijven van alle cybersecurity-uitdagingen. Al deze bewegingen leiden tot de veel gestelde vragen: wie gaat dit allemaal organiseren en wie zorgt voor een uitvoerbare agenda voor ons human capital?

Terug naar de avond waarop we een toost uitbrachten op het nieuwe jaar. Het was afgeladen vol, maar voor mij hadden de gesloten gordijnen een symbolische waarde. Daar zaten we als gemotiveerde professionals bij elkaar, maar wie ziet ons? We hebben gezamenlijk heel veel kennis en ervaring, maar wie hoort ons? Wie herkent het enorme (human capital) potentieel dat wordt gevormd door ons als het PvIB?

Afgelopen jaar bleek dat organisaties om ons heen dit wel degelijk zien. De maatschappelijke relevantie van het PvIB werd gezien en leidde ook gelijk tot vragen. Vragen over betrokkenheid bij de veranderingen en uitdagingen die voor ons staan en de rol die wij daarin hebben.

Hoe bewegen we als PvIB mee met de veranderingen om ons heen en binnen de vereniging? Willen we van maatschappelijke herkenning naar erkenning? Willen wij een stem hebben in de toekomst van ons beroep? Belangrijke vragen waar we ons als bestuur over buigen. In 2020 zal er veelvuldig over gesproken worden, binnen en buiten het PvIB. Ik hoor graag van jullie als jullie daarover willen meepraten! Dit kan door te mailen naar evertvz@nnextsecure.com.

Evert van Zanten

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

Selecteren van adviseurs met de sinaasappelsaptest

Deze keer een meta-advies over het selecteren van geschikte adviseurs voor opdrachten op het gebied van IT, security en dergelijke. Adviseurs kunnen deze tips echter ook gebruiken. Ik behandel vier situaties.

1}. Er is geen probleem.

2}. Er is een probleem, maar je weet het nog niet (en dus is er geen opdrachtgever).

3}. Je weet dat er een probleem is en kent de oplossingsrichting.

4}. Je weet dat er een probleem is, maar kent zelfs de oplossingsrichting niet.

Situatie 1 is gemakkelijk: er is geen adviseur nodig. Dit komt alleen zelden voor. Het is belangrijk het verschil met situatie 2 te herkennen, dus je moet tijdig inzien wanneer er wel advies nodig is. In situatie 2 is het voor een adviseur - die het probleem beroepshalve wel ziet - verleidelijk om met 'ongevraagd advies' te komen. Zoals het vanuit de zaal corrigeren van de cijfers die de directeur toont tijdens de nieuwjaarstoespraak. Of je zegt: "Maar dat doe je ook helemaal verkeerd", als iemand vertelt over zijn bescheiden successen in werk of hobby (je kunt blijkbaar hardlopen op talloze foute manieren, zo heb ik gehoord). Vaak is dat onverstandig of slecht voor de relatie. Geef je tóch ongevraagd advies en doet men er niets mee, dan is dat vervelend voor jou als adviseur. Maar doet men er wel iets mee en is het zelfs succesvol, dan krijg je er niet voor betaald – en dat is óók vervelend. Denk eraan: als ze je niet (willen) inhuren als adviseur, los dan ook hun probleem niet op. Ook in situatie 2 is er geen adviseur.

In situatie 3 moet er een adviseur komen. Zelfs het benodigde specialisme van die adviseur voor de oplossing is al bekend. Een aantal voorbeelden:

- Je beste programmeur heeft zo'n tandpijn dat zij niet meer goed kan denken, waardoor ze steeds meer fouten in haar softwarecode maakt ('tandarts', of 'code peer review').
- Als een tester het toilet doortrekt, stroomt het over en staat iedere keer de hele testafdeling - met al die dure computers - blank (loodgieter of meer 'automated testing', dus minder testers).
- Je laat elke dag om middernacht de batchrun uitvoeren, maar op de laatste dag van een verslagperiode duurt dit te lang en is het niet op tijd klaar om daarna de systemen opnieuw te kunnen starten (batchspecialist als het elke maand is, of batch iets eerder starten als het alleen bij het jaarwerk is).

Stel de technisch adviseur in je intakegesprek de volgende vragen en scheid met de antwoorden het kaf van het koren.

Vraag 1: hoe krijg je een olifant in een kast?

Het doel is te kijken of iemand kan abstraheren en tenminste enig gevoel voor humor heeft - en daarmee kan relativeren. Ook wil je als opdrachtgever een adviseur die het probleem niet groter maakt dan het is, maar die planmatig in overzichtelijke stappen te werk gaat. Het juiste antwoord is: deurtje open, olifant erin, deurtje dicht. Maak het niet moeilijker dan nodig: Keep It Simple, Stupid.

Vraag 2: hoe krijg je een neushoorn in de kast?

Wie net heeft opgelet, weet het al: deurtje open, neushoorn erin, deurtje dicht. Want we zijn natuurlijk voor hergebruik van oplossingen zoals 'reusable code'. Maar de situatie moet zich er wel toe lenen. Het beste antwoord is hier: deurtje open, olifant eruit, neushoorn erin, deurtje dicht. Het gaat erom of de kandidaat-adviseur denkt aan de gewijzigde situatie (de kast is niet meer leeg) en belangrijke details (het deurtje moet ook weer dicht). In de vraag staat nu 'de kast'. Met andere woorden: leest de adviseur de opgestelde requirements nauwkeurig? Ook dient hij het 'wiel' van vraag 1 (helemaal zelf bedacht of net van jou gehoord als oplossing) ook zoveel als mogelijk toe te passen in een nieuw geval.
Ongetwijfeld is ook uw bedrijf of overheidsinstelling een 'lerende organisatie', dus alle medewerkers moeten blijven leren. Deze vragenset is een uitgelezen kans om het individuele leerproces te observeren bij een externe (of interne) adviseur. Lacht de kandidaat om eigen denkfouten en zie je hem/haar groeien en ervan leren en zich daarna meer ontspannen? Of gloeit iemand van schaamte (blozen) om die denkfout, wordt hij/zij steeds stiller en wordt zo het gesprek een gemiste kans? Dit zegt iets over de persoonlijke leerstijl. Je moet die leerstijlen van elkaar kennen om effectief te kunnen samenwerken. Neem enige tijd om hierover van gedachten te wisselen en stel daarna de laatste vraag.
(tk) Vraag 3: Koning Leeuw is jarig en hij heeft alle dieren formeel uitgenodigd voor het bijwonen van zijn verjaardagsfeest. Op één na zijn alle dieren aanwezig. Hoe verklaar je dit?
Het lied 'The Lion Sleeps Tonight' zit verkeerd met 'in the jungle, the mighty jungle …', want leeuwen leven niet in het bos. Tijgers wel, maar zijn geen koning. Zeg daarom niet 'alle dieren in het bos' als je de vraag stelt.
Het gaat erom dat de kandidaat de abstract geformuleerde vraag over verantwoordelijkheden, afspraken, governance en het wel of niet naleven van procedures vereenvoudigt tot: wie is er niet? Het antwoord is natuurlijk de neushoorn, want die zit nog opgesloten in de kast. Hier moet de adviseur laten zien dat hij de nieuwe vraag kan relateren aan het verleden. Hier nota bene een recente situatie waarin hij zelf advies gaf. Met andere woorden: de succesvolle oplossing van een eerder probleem heeft consequenties voor nieuwe situaties en opdrachten en daar moet een technisch adviseur rekening mee houden. Een kandidaat die antwoordt 'de olifant' is een adviseur die niet goed luistert en die heel langzaam (of niet) leert.

De sinaasappelsaptest

Als je wel het probleem maar niet de oplossingsrichting kent, nodig dan een algemene adviseur uit voor een kennismaking. Een mooie openingsvraag is of de adviseur weleens een seminar of symposium bezoekt. Meestal is dat zo: hoe moet een adviseur anders zijn/haar kennis op peil houden? Leg bij een onverwachte 'nooit' aan die kandidaat uit waarom hij/zij naar dergelijke studiebijeenkomsten zou moeten gaan. Je vindt immers actuele kennis heel belangrijk. Anekdote: symposium of symposion betekent 'samen drinken' en was in het oude Griekenland een feest waarbij gedineerd, gedronken, gebeden en vooral gediscussieerd werd. In kennisdeling is er dus, op het bidden na, niet heel veel veranderd in een paar millennia. Dit biedt een opstapje naar vraag 2: op die studiebijeenkomsten is het meestal goed verzorgd qua eten en drinken, vind je niet? Is het antwoord 'ja, altijd', dan weet je dat de adviseur vooral qua locatie, drank en spijs uitstekend verzorgde leverancierscongressen bezoekt. Bij 'vaak wel' zijn het meer de gratis seminars die worden bijgewoond. Beide antwoorden zijn goed. Ook is interessant om te zien of de adviseur de persoonlijke verzorging totaal onbelangrijk vindt (dat wordt geen gezellige collega), of dat zij juist overmatig geboeid is door de netwerkborrel aan het eind. Omdat je vraag eindigt met een suggestie, wordt vaak ook duidelijk of de kandidaat meebeweegt naar het gewenste antwoord of juist bijzonder eigenwijs (bij de afwijzing altijd 'authentiek' zeggen) is.

Dan komt vraag 3, de 'sinaasappelsaptest', bedacht door Jerry Weinberg. Je vertelt dat je zo'n seminar hebt georganiseerd voor 500 bezoekers en dat maandagochtend 9.00 uur op elke stoel een glas vers geperste jus d'orange moet staan. Kan de adviseur dat voor je regelen? Er zijn adviseurs die nadenken, mogelijke problemen overzien, de aanname doen dat zij het in hun eentje moeten uitvoeren, overwegen dat ze nooit op tijd op maandag in Amsterdam kunnen zijn en bezorgd zijn over wat te doen als er glazen omvallen en de stoelen helemaal nat zijn. Zij zeggen daarom 'nee' en vallen af.

Andere adviseurs ruiken omzet en zeggen meteen 'ja'. Dat is een beter antwoord, maar niet wat we zoeken. De ideale adviseur zegt namelijk: "Ja dat kan ik en dit is wat het gaat kosten." Met die toevoeging toont je aanstaande adviseur dat hij je probleem heeft begrepen, er serieus over heeft nagedacht en adequate oplossingen heeft gevonden. Hij zegt geen 'nee' vanuit de aanname dat je het 'te duur' zult vinden. Omdat het (objectief gezien) bijvoorbeeld duurder is dan de toegangsprijs voor het seminar of het gemiddelde honorarium voor een dagvoorzitter of meer is dan zijn 'echte' adviesopdrachten meestal opbrengen. Maar hij biedt, door de prijs te noemen, zijn opdrachtgever de keuze om het advies wel of niet aan te nemen.

Ook security-adviseurs doen er goed aan bij adviezen en go/no go's niet te zeggen 'nee', maar 'het kan en zoveel gaat het kosten'. Laat de opdrachtgever zelf besluiten of het te duur is.

Jaaroverzicht

Artikelen

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

Achter Het Nieuws

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.

Ransomware

'Verzekeraars moeten stoppen met losgeldbetalingen bij afperssoftware', zo luidt de kop van een artikel van Stijn van Gils op FD.nl op 27 december 2019 (1). Het artikel beschrijft dat verzekeringsmaatschappijen die verzekeren tegen 'cyberschade' soms ook een vergoeding uitkeren indien een bedrijf heeft betaald voor het afkopen van ransomware. De verzekeraars stellen dat dit beter is dan de bedrijven failliet te laten gaan, maar adviseurs stellen juist dat dit de criminaliteit in stand houdt.

Chris de Vries

Ransomware is in opmars. Hoe hoog de schade is, zal voor ons allen verborgen blijven. Wie betaalt uiteindelijk de nota? Jij en ik in de vorm van hogere belastingen, hogere premies en een hogere kostprijs van producten die wij bij onze leveranciers afnemen. Fouten worden namelijk altijd via de (fictieve) kostprijs afgewenteld op de consument.
In mijn optiek hoort er solide software ontwikkeld te worden met meer dan gemiddelde bescherming. Niet de gebruiker moet in zijn eentje maatregelen nemen om - in het geval van falen - de verantwoordelijkheid te dragen en dus de nota te betalen, maar de softwareproducent moet dezelfde minimale veiligheidsgaranties afgeven als producenten van automobielen, vliegtuigen, treinen, banken, assurantie- & pensioenmaatschappijen en voormalige nutsbedrijven - om maar enkele belangrijke (infrastructurele dan wel systeem) partijen te noemen.
Hier was vroeger het raakpunt tussen soliditeit, betrouwbaarheid en verantwoordelijkheid op basis van evenwichtige overheidsregulering het uitgangspunt. Dat is wat wij nu missen. Het uitgangspunt hoort te zijn dat de burger in zijn belangen beschermd wordt en niet enkel gezien wordt als hét middel tot inkomensverwerving en dus per definitie als consument die het te ondergaan heeft en in geval van falen de nota draagt.
Bij ransomware moet dus niet de ondeskundige - of niet voldoende professionele - gebruiker van software de tegenstander zijn, maar de professionele software-ontwikkelaar in samenspel met de securitydeskundigen en overheden. Security by design mag dan niet alleen een begrip zijn, maar een wettelijk verankerde eis. Het is nu al tijd voor een GDPR 2.0 gebaseerd op security by design 2.0

Fook Hwa Tan

Ransomware komt steeds meer voor. Vooral in het bedrijfsleven. Elke organisatie wordt geconfronteerd met

Fook Hwa Tan | Chris de Vries | Nicole van Deursen

de keuze of ze wel of niet het losgeld betalen. Veelal wordt deze keuze bepaald door het feit of ze voldoende mitigerende maatregelen hebben genomen om hun informatie veilig te stellen in dit soort situaties. Hierbij kun je denken aan onder andere het redundant bewaren van informatie of het beschikbaar hebben van back-ups om de informatie terug te zetten. Vaak is dit jammer genoeg niet zo. Dat betekent dat er moet worden gekozen om te betalen.
Het betalen van losgeld betekent het voortzetten van de dreiging, maar het betekent ook het voortzetten van de bedrijfsvoering. Het losgeld dat wordt gevraagd is niet heel veel en dat maakt het nog aantrekkelijker om te betalen. De keuze tussen het - zonder interruptie - door kunnen gaan met de operatie of de operatie moeten stoppen is dan snel gemaakt. Vanuit een commercieel perspectief voldoet het vaak ook aan de businesscase. Dit heeft echter wel tot gevolg dat na betaling het voor de crimineel duidelijk is dat een organisatie makkelijk tot betaling kan worden gedwongen. Dit maakt de getroffen organisatie aantrekkelijk voor de dader om opnieuw zijn slag te slaan. Desondanks is betalen dus nog steeds een logische optie. De laatste reden om te betalen is dat een verzekeraar de schade uitbetaald. Hierbij is er dus helemaal geen incentive meer om een andere keuze te maken dan het losgeld te betalen. Is dit het in stand houden van criminaliteit of in stand houden van de organisatie? Dit is blijkbaar een kwestie van perspectief. Als buitenstaander is dit mogelijk niet acceptabel, maar vanuit de organisatie of de verzekeraar is dit juist heel logisch. Al met al redenen genoeg om te betalen, maar het is ethisch gezien niet juist om zo criminaliteit in stand te houden. Organisaties dienen daarom het voorbeeld te geven en eerst te reflecteren waar hun informatiebeveiliging tekortschiet om vervolgens niet te betalen, maar de situatie op een andere wijze te herstellen.

Nicole van Deursen

Academici zoeken ook naar andere strategieën om met ransomware om te gaan. Speltheorie kan helpen om de optimale beslissing voor een collectief te berekenen. Toegepast op ransomware gaat het dan over de beslissing of de spelers aan de slachtoffer-zijde wel of niet het losgeld betalen en om de beslissing van de spelers aan de criminele-zijde om wel of niet de bestanden vrij te geven. Naar schatting krijgt ongeveer 50% van de slachtoffers die betalen ook daadwerkelijk hun bestanden terug, waarbij is berekend dat bij een markt waarin minder 'aanbieders' van ransomware actief zijn, de kans groter is dat ze de bestanden teruggeven dan wanneer er veel spelers aan de criminele-zijde actief zijn (2). Een van de afwegingen die invloed heeft op de keuze van een individuele organisatie om wel of niet het losgeld te betalen is de balans tussen de kosten voor de investering in backup technologie versus de mogelijke schade van een ransomware situatie (3). Wanneer meer spelers aan de slachtoffer-zijde investeren in goede backup strategieën, neemt de winst aan de criminele-zijde af omdat minder slachtoffers hoeven te betalen. Er is zelfs een optimum berekend: de winstgevendheid van ransomware voor de criminelen zal dalen wanneer 70% van de bedrijven die ze aanvallen een backup strategie heeft (4). Daarbij is een andere collectieve spelstrategie van de slachtoffers ook van invloed: het delen van de informatie over hun ervaringen. Veel organisaties communiceren niet openlijk dat ze hebben betaald en of ze hun bestanden hebben teruggekregen. Dit leidt tot situaties waarin meer bedrijven hun bestanden niet terugkrijgen terwijl ze wel betalen. Het delen van informatie kan echter ook leiden tot het vergroten van het vertrouwen in criminele organisaties wanneer blijkt dat zij netjes doen wat ze zeggen na betaling. Hiermee wordt dus de bereidheid tot betalen in stand gehouden (4). Het is dus helaas een keuze uit twee kwaden waarvan het niet delen van informatie wellicht grotere schade oplevert dan het wel delen van informatie. Het zou interessant zijn wanneer deze onderzoekers ook gaan kijken naar situaties met spelers in andere rollen. Beslissingen om te betalen kunnen anders uitpakken wanneer toezichthouders of verzekeringsmaatschappijen gaan meespelen, of wanneer er een spelleider wordt aangesteld die aan de kant van de slachtoffers zorgt voor een centrale regie.

Referenties

(1) https://fd.nl/ondernemen/1328543/verzekeraars-moeten-stoppen-met-losgeldbetalingen-bij-afperssoftware#
(2) Cartwright, A., E.Cartwright. Ransomware and reputation. Games, Juni 2019, 10(2).
(3) Lazka, A., S. Farhang, J. Grossklags. 2017. On the Economics of Ransomware. https://arxiv.org/pdf/1707.06247.pdf
(4) Tristan Caulfield, Christos Ioannidis, and David Pym. Dynamic Pricing for Ransomware. Working draft (2019): http://www0.cs.ucl.ac.uk/staff/D.Pym/ransomware-dynamic.pdf

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
José Broekhuizen
Lisa Petersen
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

COLUMN Berry

Een leven zonder euro's?

Ik ga het hebben over de ontwikkeling van het geld. Aan het begin van mijn carrière kreeg ik iedere vrijdag nog een loonzakje met daarin de inkomsten van die week. Dat was hartstikke leuk. De eerste tocht ging natuurlijk naar het dorpscafé. Het geld werd verdeeld over de verschillende potjes en moeder de vrouw kon weer een week voorruit.

Later ging John Cleese de girorekening actief promoten. Zijn slogan was: "Giroblauw past bij jou." Blauw is het al lang niet meer en ook de giro is ter ziele. Betalingen gaan nu vaak met de betaalpas, de overschrijvingen toetsen we vaak in op de telefoon, tablet, PC, laptop of wat je ook maar op internet kan aansluiten. De banken gaan een stapje verder en bieden ons de mogelijkheid om met de pas contactloos te betalen. Hiervoor is geen pincode nodig. Tot 25 euro kun je afrekenen door de pas gewoon boven de lezer te houden.

25 euro zonder pincode, is dat niet gevaarlijk? Stel dat iemand mijn pas steelt? Nee, dan kun je inderdaad beter je portemonnee verliezen. Dan heb je helemaal geen controle meer en dan weet je zeker dat je alles kwijt bent …

Maar ook het contactloos betalen met de pas is inmiddels een beetje achterhaald. ABN Amro begon er al mee en introduceerde de zogenaamde 'wearables', waarmee je betalingen kon verrichten. Een succes? Ik verwacht van niet, want een zeer sterk op plastic gelijkende ring waarmee je je benzine afrekent lijkt mij geen wannahave.

Inmiddels heeft Apple half juni in Nederland eindelijk Apple Pay geïntroduceerd. In eerste instantie bij ING, maar de grote banken hebben inmiddels hun weerstand in de kast gezet en hebben zich ook aangesloten bij Apple Pay. Het lijkt een must te zijn om je aan te sluiten bij Apple Pay. Contactloos betalen met de telefoon zonder dat de grens van 25 euro nog geldt.

Dat hoeft ook niet, want je moet jezelf eerst identificeren op je telefoon met behulp van een vingerafdruk of gezichtsscan. Uiterst veilig. Dat geldt ook voor de betaling met je horloge, omdat ook daar met een pincode moet worden ingelogd.

De marktkoopman in het kleine dorpje in Portugal keek voor de zekerheid wel even na of het bedrag daadwerkelijk werd bijgeschreven bij hem. Een geweldig eenvoudig en veilig betalingssysteem waarvan Apple van iedere betaling 0,15 % krijgt. Dat lijkt niet zoveel, maar ik denk dat ze erop binnenlopen. Het lijkt een kleine stap, maar ik ben er geweldig blij mee.

Nu moet ik nog een oplossing bedenken voor de kleinkinderen die trots hun rapport laten zien en wachten op hun beloning. Net als de collectant voor wie ik ook even in de voering van mijn jas kijk of er een munt inzit. Een leven zonder euro's? Nee, daar zijn we nog niet aan toe.

Berry

TSTC

ICT en Security Trainingen

Start 2020 goed met 20% PVIB korting op deze trainingen:

TSTC bestaat 20 jaar en geeft dit jaar PVIB leden
20% korting op geselecteerde trainingen op basis
van hun lidmaatschapsnummer.
Vermeld dit nummer bij uw inschrijving.

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