iB
INFORMATIEBEVEILIGING
jaargang 17 - 2017
#1

IB IN NEDERLAND

Interview Ludo Baauw: “Wij geven 100% kaaskoppengarantie!”

Crisisoefening OZON: bruggen bouwen

Kwalificatiestelsel Q&A

TSTC

ICT en Security Trainingen

TSTC is een gerenommeerd IT opleidings-instituut en erkend specialist in informatie-beveiliging- en cybersecurity trainingen.

Security professionals kunnen bij TSTC terecht voor bijna vijftig security trainingen op zowel technisch als tactisch- strategisch gebied. Naast alle bekende internationaal erkende titels is het ook mogelijk diepgang te zoeken in actuele security thema's.

www.tstc.nl/security

Overzicht trainingen:

- Certified Ethical Hacker (CEH)
- CyberSec First Responder (CFR)
- Certified Chief Information Security Officer (C|CISO)

- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)

- Certified Information Systems Security Professional (CISSP)
- Certified Cloud Security Professional (CCSP)
- Certified Cyber Forensics Professional (CCFP)

- ISO 27001 Lead Implementer
- ISO 27001 Lead Auditor

Want security start bij mensen!!

NIEUWE WEBSITE

Het PvIB is 2017 begonnen met een nieuwe website. Deze website heeft meer interactiemogelijkheden dan de oude website en daar willen we met IB-magazine ook gebruik van gaan maken.
Eén van de dingen die bezoekers van de ledenvergaderingen mij zullen hebben horen roepen, is dat we met het blad meer elektronische mogelijkheden moeten benutten. En dit jaar is het jaar dat we daar als redactie gebruik van zullen gaan maken:
- Artikelen zullen ook online verschijnen, als de auteurs daar toestemming voor geven. In dit geval is het voor leden mogelijk om commentaar toe te voegen en interactie te hebben over het artikel met de auteur en andere leden.
- Uitgaven van IB-magazine zullen online en offline goed leesbaar beschikbaar komen voor verschillende vormfactoren, zoals smartphone, tablet en PC.

Het komende jaar zullen we hiervoor ook aan de achterkant de redactie- en publicatieprocessen aan moeten passen. Het zal dus niet vlekkeloos verlopen vanaf het begin. Wat we hierbij ook nodig hebben, is jullie feedback. Graag horen we van de leden wat jullie vinden. Wat gaat er goed? Wat kan er beter?
Ik verwacht dat 2017 een jaar wordt met meer, meer, meer: meer grote security-incidenten, meer DDoS-aanvallen, meer ontdekte kwetsbaarheden en meer gehackte accounts. Het is aan ons, security professionals, om er ook een jaar van te maken met meer veilige oplossingen, die security laagdrempelig naar de gewone gebruiker brengt. En de redactie gaat dit allemaal in de gaten houden om er over te kunnen schrijven en laten schrijven.

Lex Borger, hoofdredacteur

In dit nummer

Interview Ludo Baauw, Intermax

"WIJ GEVEN 100% KAASKOPPENGARANTIE"

In een artikelreeks kijkt IB-Magazine mee bij vernieuwende bedrijven in de branche. In deze editie: Intermax Cloudsourcing. Het Rotterdamse bedrijf is ook de bedenker van de innovatieve Nederlandse internetwasstraat, de NaWas, die DDoS-aanvallen afwendt. Een interview met oprichter en algemeen directeur Ludo Baauw.

Baauw is algemeen directeur van de Rotterdamse cloudaanbieder en internetprovider Intermax. Hij nam kortgeleden dat stokje over van medeoprichter John Knieriem die na ruim 22 jaar Intermax toe was aan iets anders. Baauw is initiatiefnemer van de Nationale Anti-DDoS Wasstraat, ook wel de NaWas, die de strijd aangaat tegen DDoS-aanvallen. Met vier datacenters in Nederland en cloudcapaciteit bij Azure, Amazon en IBM Bluemix heeft Intermax websites en bedrijfskritische applicaties onder haar hoede van ziekenhuizen en grote wereldwijde spelers, maar ook van kleinere bedrijven: zo'n 26.000 in totaal. Naast Intermax richtte Baauw ook het beveiligingsbedrijf Guardian360 op, dat in hetzelfde onlangs geopende kantoor in hartje Rotterdam zit. Distributed Denial of Service-aanvallen (DDoS-aanvallen) zijn een steeds groter probleem. "Als hostingbedrijf hebben wij daar zelf ook last van, want als één van onze klanten 'ge-DDoSt' wordt, liggen mogelijk al onze andere klanten ook plat. Tegenwoordig is het zo makkelijk, je kunt voor zeven dollar een DDoS-aanval kopen om een bedrijf het leven zuur te maken. We weten bijvoorbeeld precies wanneer het weer tentamenweek is bij de hogescholen waar we de website van hosten. Dan wordt die vier keer per dag ge-DDoSt", vertelt Baauw. Het schetst het probleem. Een DDoS-aanval is makkelijk te regelen en komt ook steeds vaker voor. Bedrijven in de software- en technologiesector zijn vaak het haasje, evenals gaming-bedrijven. Wat kun je daar tegen doen? Baauw: "Er zijn genoeg anti-DDoS-bedrijven, maar ze zijn vrijwel allemaal Amerikaans en ze zijn heel erg duur. Of je betaalt per website per maand. En met de aantallen sites en applicaties die Intermax onder zijn hoede heeft, is dat niet echt een optie."

Wat is een Denial-of-Service (DoS)-aanval?
Bij een DoS-aanval probeert een aanvaller te voorkomen dat gewone gebruikers toegang krijgen tot online informatie of diensten.

De meest voorkomende vorm van DoS-aanval is als een aanvaller een netwerk 'overstroomt' met informatie. Een server kan slechts een bepaald aantal verzoeken tegelijk verwerken, dus als een aanvaller de server overbelast met aanvragen, kan de server jouw verzoek niet verwerken. Dit is een 'denial of service' omdat jij geen toegang meer hebt tot die site.

Een aanvaller kan ook je e-mailaccount vullen met spamberichten. Elk e-mailaccount heeft een bepaald quotum die de hoeveelheid gegevens in je inbox op een bepaald moment beperkt. Door het versturen van vele, of grote, e-mailberichten naar je account verbruikt een aanvaller die quota en kun je geen legitieme berichten meer ontvangen.

Ook kan een aanvaller zich voordoen als een ander; spoofing. Dan doet één computer zich voor als meerdere, wat een aanval vergroot en moeilijker detecteerbaar maakt. De aanvaller kan zich ook voordoen als de server van de website zelf en elders op het internet grote hoeveelheden informatie opvragen, bijvoorbeeld bij DNS-servers of tijdservers (met NNTP). Niet de aanvaller, maar de website ontvangt de vele antwoorden, wat resulteert in denial of service van de website. Dit zijn reflectie- en amplificatieaanvallen. Ze reflecteren het verkeer van een aanvaller via een andere site naar het doelwit en de gereflecteerde berichten zijn veel groter dan het origineel, tot wel een factor honderd.

Wat is een Distributed Denial-of-Service (DDoS)-aanval?
Bij een DDoS-aanval gebruikt een aanvaller andermans computers om een website of dienst aan te vallen. Door beveiligingslekken of zwakke plekken te gebruiken, neemt een aanvaller andermans computers over. Deze computers worden dan een 'botnet'. De aanvaller dwingt die botnet grote hoeveelheden data te versturen naar een website of spam te versturen naar bepaalde e-mailadressen. De aanval is 'gedistribueerd', omdat de aanvaller zijn botnet gebruikt.
Een redelijk nieuw verschijnsel is dat een 'botnet' niet bestaat uit servers en PC's, maar uit simpele apparaten met een internetaansluiting: het Internet of Things (IoT). Er zijn tegenwoordig meer things op het internet aangesloten dan computers en ze hebben vaak ook kwetsbaarheden die de leverancier niet patcht. Ook al zijn deze apparaten niet krachtig, door hun aantal zijn ze een flinke bedreiging.

Hoe groot is een (D)DoS-aanval?
Om succesvol te zijn, moet een aanvaller meer data pompen naar een website dan de internetverbinding van de provider aankan. Je moet een brandslang hebben die meer water spuit dan de afvoerleiding aankan. Providers hebben vaak verbindingen van 10 tot 100 gigabit per seconde. Wat anti-DDoS-diensten doen, is tijdelijk de brandslang omleiden naar een grotere afvoer. Hun verwerkingscapaciteit is vele malen groter dan die van providers. Ze hebben grotere aanvallen dan 1.000 gigabit per seconde te verwerken gekregen, ook al zijn die nog een zeldzaamheid.

DDoS-aanvallen liggen dan ook tussen de 10 en 1.000 gigabit per seconde in grootte. Op de website 'Digital Attack Map' [4] vind je DDoS-aanvallen internet-breed.

Ter referentie: het grote internetknooppunt van Nederland, de AMS-IX, heeft in november bekendgemaakt een nieuw topgebruik gehad te hebben van 5.000 gigabit per seconde op de zondagavond.
We hebben het hier over DoS-aanvallen op het netwerkniveau. DoS-aanvallen kunnen ook gericht zijn op de applicatielaag. Dan gaat het niet om de omvang van het netwerkverkeer, maar om met speciaal gerichte berichten de webapplicatie te laten vastlopen. Hier zijn andere strategieën voor nodig.

Chantal Craandijk is via Craandijk Communicatie onder andere werkzaam als interviewer en is bereikbaar via www.craandijk.com.

Het begin van de NaWas

Ze moesten dus wat anders verzinnen. Nu is Baauw ook bestuurslid bij de Nationale Beheersorganisatie Internet Providers, de NBIP [1]. "Vergelijk dat maar met een SSC voor de Nederlandse internet- en telecomproviders." Een groep van zes internetproviders heeft de NBIP in 2002 opgericht, vanwege de Telecomwet die toen in werking ging. "Internetproviders moesten toen hun netwerk laten aftappen. Dat doen zij nu vanuit een gezamenlijke organisatie: de NBIP." Er zijn inmiddels 150 NBIP-deelnemers; een mooie basis voor de oplossing van het DDoS-probleem. "Ik ging concurrenten bellen om te kijken of zij ook last hadden van DDoS-aanvallen. In de eerste instantie natuurlijk niet, er klonk: 'ons netwerk is veel beter', maar uiteindelijk was men toch geïnteresseerd. Het grote voordeel van de NBIP is dat het een stichting is, zonder winstoogmerk. Dat maakt samenwerken met concurrenten een stuk minder gevoelig." Toen de eerste zes bedrijven mee wilden doen, kochten ze gezamenlijk voor meer dan een half miljoen euro aan specialistische apparatuur van verschillende leveranciers in een neutraal datacenter. En daarmee werd de Nationale Anti-DDoS Wasstraat geboren.

Binnen twee maanden bouwden ze de NaWas op. Eind 2014 begonnen ze met de bouw en begin 2015 kon de 'wasstraat' van start. "Het werkt supergoed", vertelt Baauw enthousiast. "Binnen no-time groeiden we naar twaalf deelnemers." Inmiddels zijn het er 55. En door het stijgende aantal deelnemers stijgt ook het aantal aanvallen. "Vorig jaar hebben we achthonderd DDoS-aanvallen opgevangen en succesvol afgeslagen. In 2016 gaan we richting de duizend."

Hoe werkt het?

"Als jij naar een bepaalde website gaat, weet je router op welk IP-adres hij moet zijn voor die website", legt Baauw uit. "Maar als een IP-adres onder vuur ligt door een DDoS-aanval, dan is er opeens heel erg veel verkeer voor dat adres. Als gevolg is die website onbereikbaar. Een sensor in het netwerk van de hostingprovider merkt de verkeerslast en 'vertelt' dan de internetrouters dat verkeer naar het geDDoSte IP-adres niet langer naar de aansluiting van de hostingprovider gestuurd moet worden, maar naar de aansluiting van de NaWas. Binnen twee minuten doet elke router ter wereld dat, waarmee al het verkeer naar de website, inclusief de DDoS-aanval op die site, wordt weggeleid naar de wasstraat. En daarmee rust geeft op jouw netwerk." De NaWas checkt dan wat normaal verkeer is en wat niet: een DDoS-aanval bestaat uit nepverkeer, wat de wasstraat kan herkennen. Het niet-normale verkeer wordt weggespoeld door het putje, de 'bittenbak', en het normale verkeer wordt weer teruggeleid naar het internet. "Dus echte bezoekers merken helemaal niet wat er achter de schermen gebeurt."

Volgens de wet is een DDoS-aanval een criminele actie. "Dat klopt, het is ook strafbaar. Vergis je niet, je kunt er zelfs twee jaar voor de gevangenis in verdwijnen. Er komt gewoon een digitale vrachtwagen met een enorme bom binnenrijden en met de NaWas zetten wij er heel snel een betonnen iglo omheen. Dus je weet dat hij afgaat, maar je probeert het binnen de perken te houden. Eigenlijk zijn we al blij als het internet het gewoon blijft doen bij een heel grote DDoS-aanval."

Het aantal aanvallen stijgt elk kwartaal met tientallen procenten. Maar wat lastig is: "de enige beschikbare DDoS-cijfers zijn gemaakt door de anti-DDoSbedrijven", vertelt Ludo. "Zo is het lastig een onafhankelijk beeld te krijgen. Zij hebben natuurlijk ook baat bij een bepaalde angstreactie. Er wordt bijvoorbeeld verteld dat er DDoS-aanvallen zijn van 600 gigabit per seconde maar onafhankelijke informatie is er niet. Daarom is het voor ons heel belangrijk dat onze wasstraat geen winstoogmerk heeft. We delen kennis en informatie met elkaar." Een ander groot voordeel van de NaWas, volgens Baauw "vooral voor de Nederlandse overheid" is dat het internetverkeer in Nederland blijft. "Wij geven 100% 'kaaskoppengarantie' en dat vinden heel veel mensen prettig."

Digitale Deltawerken

"Ideaal zou zijn dat hackers op een gegeven moment afzien van aanvallen als ze zien dat de websites in Nederland draaien", zegt Baauw". Lachend: "De Digitale Deltawerken. Met de Amsterdam Internet Exchange en de Neutral Internet Exchange samen hebben we al het grootste internetknooppunt ter wereld, het zou toch heel gaaf zijn als we dat dan ook kunnen waarmaken. Het is voor het gedeelde goed en dan moet je gewoon samenwerken, bijvoorbeeld via de NBIP. Met een beetje creativiteit kun je heel veel samen doen, ook al ben je concurrenten van elkaar. Eigenlijk is de NBIP met de NaWas de Melkunie van het internet. Je kunt het gebruiken als je het nodig hebt. Heb je 't niet nodig dan is dat ook prima."

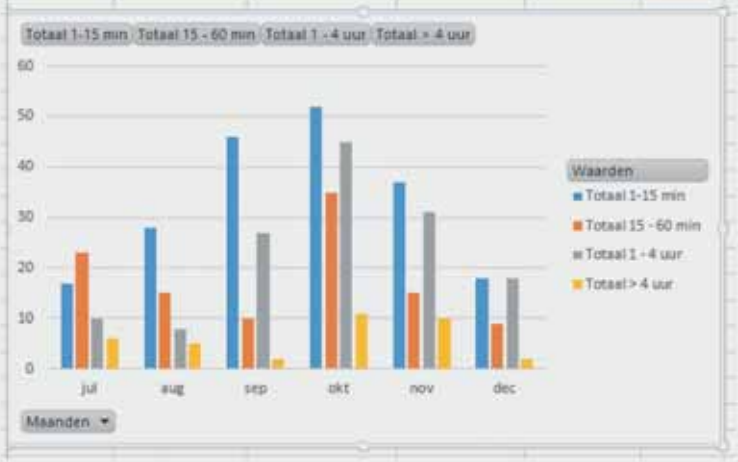
De ambities zijn hoog: "We willen eigenlijk dat de DDoS-aanvallen stoppen, maar dat is lastig, want je weet niet wie de aanvallers zijn." En ondanks dat een DDoS-aanval strafbaar is, zijn bedrijven zijn er ook niet heel happig op om aangifte te doen. "Net alsof je fiets gestolen is. Doe jij daar nog aangifte van? Er wordt niets mee gedaan." Daarom kijkt de NBIP nu zelf wat voor verkeerspatronen ze kunnen ontdekken. "We proberen daarna de overheid, politie en justitie te interesseren om mee te denken in de bestrijding."

Wat als de NaWas niet groot genoeg is? "We denken sinds 2015 over een soort digitale ophaalbrug, het trusted network initiative. Helaas is dat toen afgekapt, omdat twee grote Nederlandse telecomproviders eruit stapten, maar we willen het toch weer nieuw leven inblazen. We moeten namelijk voorbereid zijn op een heel grote aanval en er in geval van nood het buitenlandse internetverkeer kunnen afkappen zodat Nederland een digitaal eiland wordt. Op die manier kan het noodzakelijke internetverkeer voor betalingen en bijvoorbeeld verkeer en vervoer nog steeds door gaan. We hebben een soort noodnet

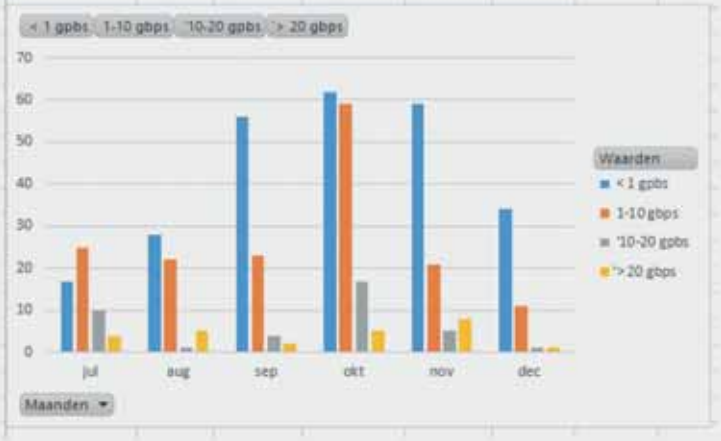
Cijfers NBIP DDoS-aanvallen
Het aantal en de duur van DDoS-aanvallen die de NBIP in 2016 heeft afgeslagen. De NBIP heeft deze cijfers naar eer en geweten opgesteld. Er kunnen hieraan echter geen rechten worden ontleend, noch is NBIP aansprakelijk voor eventuele onjuistheden.

Periode 1 juli t/m 14 december 2016

Maanden	Totaal 1-15 min	Totaal 15 - 60 min	Totaal 1 - 4 uur	Totaal > 4 uur	
jul	17	23	10	6	56
aug	28	15	8	5	56
sep	46	10	27	2	85
okt	52	35	45	11	143
nov	37	15	31	10	93
dec	18	9	18	2	47
Eindtotaal	**198**	**107**	**139**	**36**	**480**



Maanden	< 1 gpbs	1-10 gbps	'10-20 gpbs	'> 20 gbps	
jul	17	25	10	4	56
aug	28	22	1	5	56
sep	56	23	4	2	85
okt	62	59	17	5	143
nov	59	21	5	8	93
dec	34	11	1	1	47
Eindtotaal	**256**	**161**	**38**	**25**	**480**



nodig." Ondanks dat de NaWas een winstloze stichting is, hebben Intermax -en de andere 54 deelnemers- er toch commercieel voordeel van. "Onze klanten krijgen de anti-DDoS-wasstraat er gratis bij. Klanten vinden het innovatief. We hebben die kennis in huis en we delen het. Het boek 'Je hebt wél iets te verbergen – over het levensbelang van privacy voor iedereen' [2] sturen we onze klanten daarom als kerstcadeautje. Met dat boek proberen we mensen bewust te maken. Want als je niet weet wat je bedreigt, kun je er ook niets tegen doen. Ik wil mensen niet bang maken, je gaat immers niet dood aan een DDoS-aanval. Je kunt je er tegen weren. Ik wil ze informeren over de risico's zodat ze dan bewust kunnen kiezen voor het wel of niet accepteren ervan."

Internet of shit

"We moeten een leertje gaan kopen om de lekkende kraan te maken, in plaats van een steeds grotere dweil neer te leggen. En proberen die DDoS-kanonnen van het internet af te laten halen. Ik vind het Internet of Things ook erg risicovol: ik noem 't dan ook wel 'internet of shit'. Al die met internet verbonden apparaten zijn allemaal nieuwe manieren die gebruikt kunnen worden om DDoS-aanvallen mee uit te voeren. Ik wil niet dat mijn waterkoker kan praten met internet. Ik wil gewoon een kopje thee. In plaats van de hostingprovider te waarschuwen dat een IP-adres fout verkeer genereert, kan er beter een importverbod komen op camera's waarvan je weet dat die zo lek zijn als een mandje. Ik bedoel, Intermax heeft tienduizenden IP-adressen. Daar kan ik paar man fulltime mee bezighouden. En wie gaat dat betalen? Zo'n importverbod kan zelfs op Europees niveau. Het schiet dus nog niet echt op. Beveiligingsexpert Bruce Schneier zegt al 'Someone is learning to take down the internet' [3]. Dan denk ik: 'Mooi. Laat ze maar eens voelen hoe dat is. Dan gebeurt er tenminste wat. Maar niet te lang alsjeblieft.'"

Links

[1] Het NBIP: www.nbip.nl
[2] Het boek 'Je hebt wél iets te verbergen – over het levensbelang van privacy voor iedereen': https://decorrespondent.nl/nietsteverbergen
[3] Blog 'Schneier on Security': https://www.schneier.com/blog/archives/2016/09/someone_is_lear.html
[4] Digital Attack Map: http://www.digitalattackmap.com/understanding-ddos/

Mr. Rachel Marbus
@rachelmarbus op Twitter

OP EEN VERBAZING-WEKKEND JAAR!

Dit jaar, 2017, is het jaar dat mij meteen aan de start wist te verbazen. Ik hou daar normaal gesproken erg van, zo u weet. Deze verbazing voelde wat wrang, maar ik zie vooral mooie kansen om het anders te doen. Omdenken, weet u, super hip en lekker in lijn met de start van een nieuw en fris jaar.

Op 1 januari wilde Jamie afreizen naar de U.S.A. voor een studiereis. Terwijl ze door de bagagecontrole ging, werd haar paspoort gestolen uit het bakje waar ze het in had moeten leggen om door de scanners te gaan. De marechaussee reageerde op zijn zachtst gezegd laks. Ze moest het zelf maar zien op te lossen en de camerabeelden bekijken was geen optie. Als het nu nog om een duur horloge had gegaan, dan hadden ze wel willen kijken. Aldus Jamie in haar verhaal aan Metro.

Dit verhaal heeft mij om heel veel redenen verbaasd. Botte en lakse mensen verbazen mij niet, die heb je overal. Maar dit is nu juist een doelgroep waarvan je als burger mag verwachten dat ze niet laks zijn (bot, ach ja, het zij zo) en dan zeker niet als het gaat om een paspoort. Van de marechaussee mag je verwachten dat zij niet alleen die paspoorten streng controleren, maar dat ze ook alert zijn als er een – onder hun eigen ogen nota bene – gestolen wordt. Er is, voor zover ik weet, geen onderzoek gedaan naar de vraag welke doelgroep er met gestolen paspoorten reist, maar een 'educated guess' is de groep criminelen/terroristen/illegalen. Het is een levendige handel trouwens, cijfers uit 2014: 40 miljoen gestolen en vermiste paspoorten wereldwijd. Die komen netjes in een database die raadpleegbaar is voor autoriteiten. Probleem is alleen dat die database slechts steekproefsgewijs wordt aangeroepen. Dat verbaasde me dan weer.

Het verbaasde me ook dat dit verhaal niet verder werd opgepakt door andere media, al was het maar om weer eens het onderwerp 'veiligheid, paspoorten, grenscontroles en terrorisme' te tackelen. Toch hot topics in deze tijden. Nu is een verloren paspoort nog niet echt heel spannend, maar als je de reacties op Facebook mag geloven is het geen alleenstaand incident. Op zijn minst het onderzoek waard. Mijn journalisten-buikgevoel slaat in ieder geval helemaal aan. Wellicht moet het nog even broeden en zien we binnenkort mooie kritische verhalen over nut, noodzaak en effectiviteit van al die veiligheidsmaatregelen.

Daarnaast verbaasde het me dat de politiek dit niet opgepakt heeft. Ik zie namelijk een win-win situatie voor zowel liefhebbers van privacy als liefhebbers van security. Een gestolen identiteitsbewijs staat tegenwoordig bijna gelijk aan een gestolen identiteit (naast het feit dat het gewoon echt super vervelend is als het je overkomt). Hoeveel identiteitsfraude er in Nederland gepleegd wordt, is niet helemaal duidelijk, maar in augustus 2016 werd daarbij het cijfer 500 keer per dag geopperd. Deskundigen die door NRC daarover aan de tand gevoeld werden, gaven allen weliswaar aan dat er geen concrete cijfers zijn, maar dat het een heel aardig eind in de richting lijkt te komen. Ik geloof niet dat ik nog hoef te vertellen dat gestolen paspoorten een 'security-dingetje' zijn toch? Ofwel; prachtig voer voor de politiek.

Dus, ik hoop gewoon binnenkort weer verbaasd te zijn. En ditmaal omdat iedereen wakker is geworden en fris aan de slag gaat om 2017 nog privacyvriendelijker en securityvriendelijker te maken.

OZON: BRUGGEN BOUWEN

Een cybercrisisoefening

In oktober 2016 heeft SURF de eerste landelijke cybercrisisoefening gehouden voor de onderwijssector. Aan deze tweedaagse oefening deden 28 instellingen mee op zowel operationeel, tactisch als strategisch niveau. Aan de hand van een uitdagend scenario werd een meerlaagse aanval van een hackerscollectief gesimuleerd met technische uitdaging en met dilemma's voor het bestuurlijke niveau. Meer dan 200 specialisten speelden twee dagen mee in een realistische oefening, ICT-specialisten, juristen, communicatiedeskundigen, bestuurders, security en privacy officers. De oefening was een initiatief van SURFcert, het emergency response team van het Hoger Onderwijs.

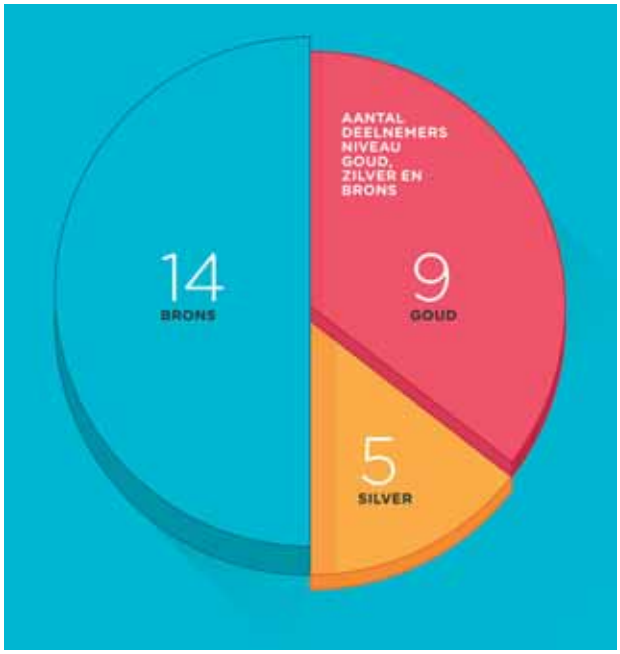
Ken je dat? Kom je 's ochtends als SO op kantoor en dan staan ze al klaar. "Heb je dat artikel op Nu.nl gelezen?", vraagt de een, "Twitter slaat op hol", zegt de ander, "Moeten we het crisisteam bij elkaar roepen?", vraagt een derde. Chaos en paniek, het begin van iedere crisis. Precies dit stond SURFcert voor ogen toen zij in februari 2016 het idee voor een landelijke oefening lanceerde. SURFcert had zelf in 2015 meegedaan aan ISIDOOR, een landelijke oefening van het NCSC voor CERT-teams.

Organisatie van de oefening

Geïnspireerd door ISIDOOR wilde SURFcert een oefening organiseren voor zowel het operationeel als voor het strategisch niveau. Wat aanvankelijk begon met een goed idee, mondde uit in een grootschalige sectorbrede cybercrisisoefening gehouden op 4 en 5 oktober 2016. De animo was overweldigend. Er was gehoopt op minstens vijf deelnemers, het werden er maar liefst 28: universiteiten, hogescholen, mbo's, ziekenhuizen en onderzoeksinstellingen. De inschrijving moest vervroegd worden gesloten.

Instellingen speelden op goud-, zilver- of bronsniveau mee. Op goudniveau werd tot het hoogste strategisch niveau meegespeeld, bij zilver oefende vooral het operationeel/tactisch niveau en bij brons observeerden de instellingen de ontwikkeling van de oefening en speelden een 'capture the flag'-oefening.

Met een kern van SURFcert is een projectteam opgebouwd dat in een half jaar tijd de oefening heeft voorbereid. Technische elementen zijn ontwikkeld, scenario's geschreven, 'fictieve' mediaberichten voorbereid (Facebookberichten, krantenberichten, tweets, blogs, enzovoorts.), de instellingen geholpen bij het schrijven van eigen scenario's en zowel de

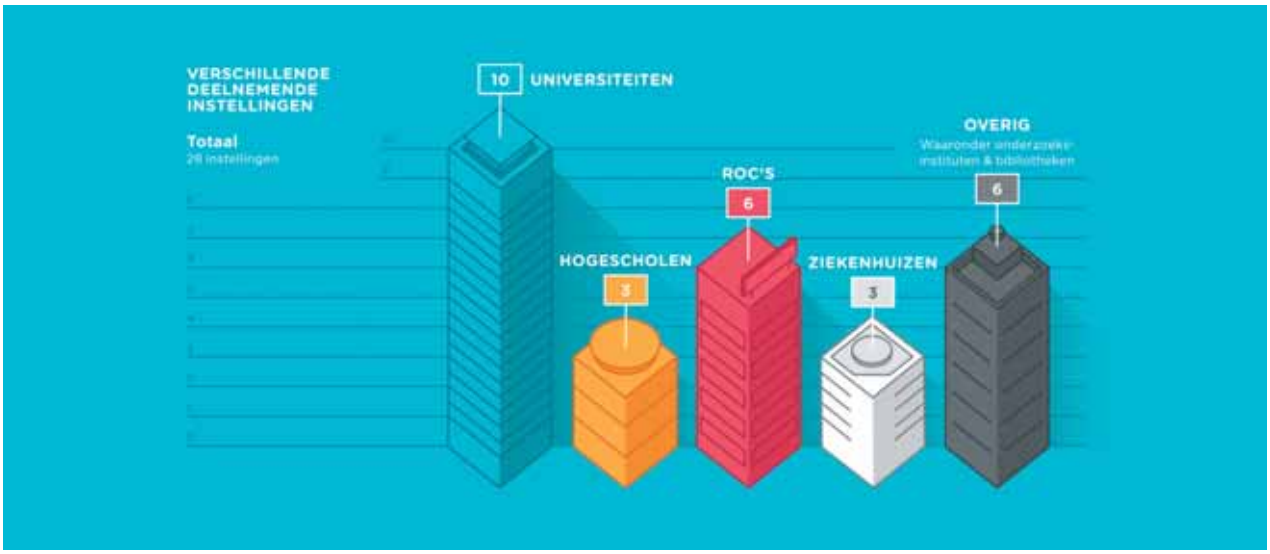


interne als de externe communicatie voorbereid. Naast het projectteam was er een programmagroep waarin de oefenvoorbereiders van de instellingen deelnamen. Ook was er een stuurgroep ingesteld waarin strategische beslissingen werden genomen. De stuurgroep heeft van begin af aan blind gevaren; dat wil zeggen dat ze niet van de inhoud van de oefening op de hoogte waren, omdat ze zelf wilden meespelen.

Voorbereiding scenario

Het overkoepelende scenario is gebaseerd op het hoofddoel voor de oefening 'de weerbaarheid en het bewustzijn van

Alf Moens en Sandy Janssen werken voor SURFnet. SURFnet is onderdeel van de coöperatie SURF, de ICT-samenwerkingsorganisatie van het onderwijs en onderzoek in Nederland. Binnen SURF werken universiteiten, hogescholen, mbo-scholen, onderzoeksinstellingen en de universitaire medische centra (UMC's) samen aan ICT-voorzieningen én -vernieuwingen. Alf Moens is naast Security Officer voor SURFnet ook Corporate Security Officer bij SURFnet en nauw betrokken bij het onder controle brengen van informatiebeveiliging bij de aangesloten instellingen. Sandy Janssen is deelnemer aan het Jong Talenten-programma van SURFnet en heeft het opzetten van de oefening en de uitwerking van de scenario's voor OZON begeleid.



instellingen in een cybercrisissituatie vergroten' en de subdoelen 'het testen van de keten', 'de effectiviteit van de crisiscommunicatie toetsen' en 'de samenwerking binnen instellingen en tussen de instellingen vergroten'. De instellingen kregen te maken met twee simultane dreigingen: een aanval van een idealistisch hackerscollectief en een dreiging met een criminele component. Een ethisch dilemma maakte dat instellingen ook onderling de samenwerking zouden moeten opzoeken.
Het scenario kende zowel strategische als technische elementen. Instellingen hebben eigen instellingsscenario's gebaseerd op het overkoepelende scenario en konden het scenario zo inkleuren dat het voor hen voldoende herkenbare en realistische elementen bevatte. Zowel het overkoepelende scenario als de instellingsscenario's zijn vastgelegd in een draaiboek waarin interventies en acties zijn opgenomen. Dit draaiboek is de basis voor het gepland en geïmproviseerd doen van sturing en bijsturing.

Het scenario

Een hackerscollectief vindt dat teveel informatie om economische redenen niet publiek gemaakt wordt. Dit hindert de ontwikkeling van de menselijke beschaving. Alle data moet daarom voor iedereen beschikbaar zijn, en intellectueel eigendom druist daar tegenin. Ze doen alles om zoveel mogelijk gegevens integraal openbaar te maken en houden geen rekening met privacygevoelige data. Medische dossiers, persoonsgegevens, onderzoeksdata, bedrijfsgegevens en organisatiegegevens komen op straat te liggen.

De ene instelling wordt hard geraakt doordat onderzoeken over dierproeven openbaar worden gemaakt, of controversiële onderzoeken naar de effecten van suiker bij kinderen. Anderen krijgen bijvoorbeeld te maken het openbaren van psychologische dossiers van studenten. Bij ziekenhuizen kwamen onder meer patiëntengegevens en medicijngebruiksgegevens op straat te liggen. Ook werd declaratiegedrag van bestuurders aan de kaak gesteld.

Dit is een enorme bedreiging voor het imago, persoonlijke reputaties, reputatie van de organisatie of kan zelfs leiden tot bestuurlijke aansprakelijkheid of financiële (schade)claims. Door dergelijke stevige technische en strategische dilemma's die niet zonder een beslissing op bestuurlijk niveau op te lossen zijn, werd zowel de interne communicatie als de escalatie naar het hoogste managementniveau geoefend.

En alsof dat nog niet voldoende was, blijkt halverwege de dag dat niet alleen data openbaar gemaakt is, maar dat het ook mogelijk blijkt te zijn om cijfers, tentamengegevens, diplomagegevens en zelfs medicatiegegevens tegen betaling te manipuleren. Niet duidelijk wordt of hetzelfde hackerscollectief hiervoor verantwoordelijk is.

Techniek

OZON was geen papieren oefening. Om de oefening zo realistisch mogelijk te maken en ook de technici voldoende te doen te geven waren verschillende technische componenten in de oefening geschreven en gerealiseerd. De website van het hackerscollectief was gebouwd bij een buitenlandse cloudprovider en werd gedurende het verloop van de oefening geactualiseerd. Op deze website verschenen voorbeelden van datasets die bij de deelnemende instellingen zouden zijn buitgemaakt. Ook waren hier logfiles terug te vinden van hacking activiteiten. De website werd gemirrord op verschillende plekken onder meer op Raspberry PI's die bij een

tiental instellingen verborgen waren. Sommige deelnemers hadden voor hun eigen scenario kopieën gemaakt van productieomgevingen waar de technici als 'in het echt' op zoek moesten naar aanwijzingen. Ten slotte was er ook nog 'malware' ontwikkeld die communiceerde naar een command-and-control center (maar verder niets deed). Voor het verspreiden van deze malware waren studenten van de security management opleiding van de Haagsche Hogeschool gecharterd om met een 'besmette' laptop deelnemende 'brons-instellingen' te bezoeken voor een 'capture-the-flag'-component in het scenario. Hier schoot het realisme enigszins door: de besmette laptops werden wel gesignaleerd en op papier onschadelijk gemaakt, het was voor sommige deelnemers niet duidelijk dat er daadwerkelijk een indringer in hun gebouw zat!

Een belangrijke component in de oefening was het simuleren van mediaberichten. Met een interactieve simulator werden krantenberichten verspreid en werd Twitter en Facebook gesimuleerd waarbij de spelers ook konden reageren. Met de mediasimulator kon, net als in real-life, een veelheid aan informatie en desinformatie over de spelers uitgestort worden, waardoor de druk op de teams opgevoerd werd. Het volgen van alle mediaberichten was een dagtaak op zich, duidelijk een uitdaging voor de taakverdeling binnen een crisisteam.

Uitvoering

Om zo dicht mogelijk bij het dagelijkse proces te blijven, is gekozen voor een simulatieoefening waarbij spelers in hun eigen werkomgeving met het oefenscenario geconfronteerd werden. Ten einde de oefening in de hand te kunnen houden, was deze gesloten opgezet en speelden alleen tevoren geselecteerde personen mee. De rest werd gesimuleerd door de responscellen. Ook enkele externe partijen zoals het NCSC en de Nationale Politie speelden mee, het NCSC in hun eigen rol en de politie had een portal voor aangiften ingericht. De Autoriteit Persoonsgegevens leverde informatie voor het oefenen van het melden van datalekken.

Voor alle deelnemers was een briefing opgesteld met de regels van het spel en op grote lijnen het verloop van de oefening. Een van de deelnemende instellingen had op eigen initiatief als teaser een journaalitem gemaakt en de avond voorafgaand aan de oefening verspreid.

Het SURFnet kantoor is omgedoopt tot zenuwcentrum van de oefening. Met de publicatie van een 'krantenartikel' waarin het hackerscollectief haar dreigingen uit, wordt de oefening afgetrapt. Daarbij blijft open of je wel of niet een target bent. Spelers op de werkvloer kijken elkaar nog aan met de vraag; 'zou dit ons ook raken?'. Gaandeweg komen er dreigmails binnen waarbij gesteld wordt; "jullie maken je data openbaar of wij doen het". Bedenktijd geeft de indruk dat je de situatie nog in de hand hebt. Maar dan blijkt dat op een hiervoor in het leven geroepen website de ene na de andere set met gevoelige data openbaar gemaakt wordt. De dreigingen worden werkelijkheid en het scenario ontwikkelt zich van een dreiging tot een volwaardige crisis. Twitter stroomt vol met berichten van medewerkers die de actie van het hackerscollectief steunen en ongeruste studenten die zich afvragen of al hun gegevens nu op straat liggen. Studenten melden dat ze nu eindelijk een voldoende staan.

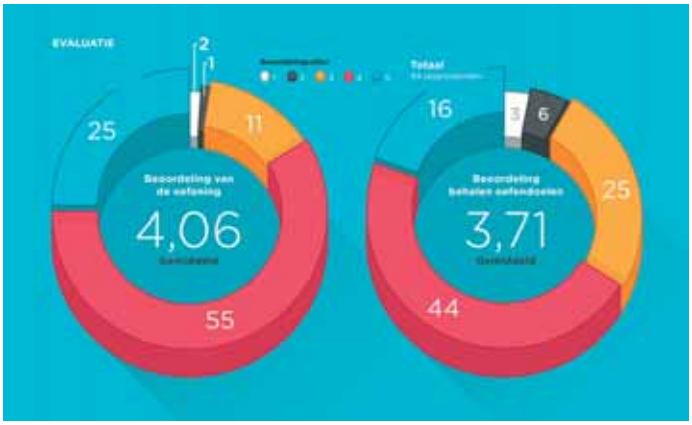
Ook de politiek en media krijgen lucht van de ontwikkelingen en duiken er bovenop. De telefoons van de oefenleiders, die zowel de interventies uitvoeren als ook de responscel bemannen, staan roodgloeiend. Afdelingsmanagers, juristen, communicatiemedewerkers, ICT-managers, ICT-medewerkers, directieleden, studenten, docenten, patiënten, journalisten, burgemeesters, leden van de raden van toezicht, de politie; iedereen raakt betrokken.

De druk werd zo opgevoerd en als realistisch ervaren, dat instellingen zelfs na het sluitsignaal nog in crisisoverleg zijn en er geen onderscheid meer is tussen fictie en werkelijkheid. Er werd alleen tijdens kantoortijden gespeeld. Zo kon iedereen even tussen de eerste en tweede speeldag op adem komen, dat bleek ook wel nodig.

In de anderhalve dag van de oefening zijn uiteindelijk meer dan 650 tweets verstuurd (waarvan 500 voorbereid), 40 Facebookberichten gemaakt en 11 krantenartikelen gepubliceerd. Er werden 7 aangiften bij de politie gedaan, en 8 meldingen datalekken bij de Autoriteit Persoonsgegevens. Ook werden drie medewerkers (fictief) op non-actief gezet. Meer dan 200 spelers hebben fanatiek meegespeeld.

Conclusie

Cybercrisisoefening OZON was een succesvolle eerste cybercrisisoefening voor de onderwijs- en onderzoekssector. De oefening werd als zeer realistisch en leerzaam ervaren, zowel voor de techniek als voor het strategisch niveau. Het enthousiasme was groot; ruim na het eindsignaal werd nog fanatiek doorgespeeld en verschillende bestuurders hebben hun agenda leeggeruimd en verzocht of ze langer mochten meespelen.



Lessons learned en aanbevelingen: crisisorganisatie

Het functioneren van de keten is getest en de effectiviteit van de crisiscommunicatie getoetst. Tijdens de oefening blijkt taakverdeling, onderlinge communicatie (zowel intern als extern) en het duiden van informatie een uitdaging. Meer coördinatie en regie, binnen de instelling en tussen de instellingen, kunnen bijdragen aan een snellere en efficiëntere informatiedeling. Ze kunnen er ook toe leiden dat instellingen gezamenlijk zoeken naar oplossingen, zowel op tactisch/operationeel niveau als op strategisch niveau. Informatie moet zowel intern als tussen instellingen eerder in het crisisproces gedeeld worden. Dit maakt het voor betrokkenen eenvoudiger om informatie te duiden, het proces te coördineren en gezamenlijk problemen aan te pakken.

Aanbevolen wordt om te onderzoeken of en in welke mate er landelijke coördinatie nodig is bij een sectoroverstijgende cyberdreiging. Hierbij moet het mandaat voor landelijke coördinatie en de autonomie van organisaties in acht genomen worden.

De oefening benadrukt dat cybersecurity een integraal onderdeel van crisismanagement moet zijn en heldere afspraken over proces, rollen

Projectonderdeel	Bestede dagen
Organisatie en advies:	50 dagen
Begeleiding instellingen:	40 dagen
Projectleider:	16 dagen
Techniek:	24 dagen
Projectsecretaris:	20 dagen
Oefenvoorbereiders van de instellingen	80 dagen (20 maal 4 dagen)
Totaal voorbereiding	**230 dagen**
Uitvoering van de oefening (28 instellingen)	400 dagen (200 maal 2 dagen)
Totaal uitvoering	**400 dagen**

Tabel 1 – Totale tijdsbesteding

en taken in een crisisplan vastgelegd dienen te worden. Het vastleggen van draaiboeken meer gericht op cybersecurityrisico's kan hierbij helpen.

Cybercrisisoefening OZON is een 'gap bridging exercise' geweest waarbij bruggen zijn geslagen tussen bestuurders, communicatie en de ICT-afdelingen, zowel binnen als tussen de instellingen. Het belang van oefenen voor het vergroten van de bewustzijn en weerbaarheid is gevoeld. Voor deelnemende instellingen is OZON een directe aanleiding om meer aandacht aan cybersecurity te besteden. Vaker oefenen, zowel groot- als kleinschalig, gericht op sector, doelgroep en/of onderwerp, draagt bij aan het vergroten van weerbaarheid, bewustzijn en draagvlak.

Lessons learned en aanbevelingen: organisatie van een crisisoefening

De voorbereiding is intensief geweest en heeft de oefenvoorbereiders veel tijd gekost. Ook voor de spelers bleek de oefening zwaarder dan verwacht. Het moeilijkst was in te schatten hoe de escalatie en communicatie tussen operationeel, ICT- en strategisch niveau zou verlopen. Bij cybercrisisoefening OZON is veel moeite gedaan om dit onderdeel goed vorm te geven. Ook waren een aantal sleutelpersonen van de instellingen onderdeel van het voorbereidingsteam, waardoor ze in de operatie gemist werden. Dat was tijdens de oefening merkbaar.

Gedetailleerde oefenscenario's per instelling zorgen voor een realistische oefening, maar kosten veel tijd. Hier is gericht begeleiding bij het opstellen van het scenario noodzakelijk. In het voorbereidingsteam dient zowel voldoende operationele als strategische kennis aanwezig te zijn. Een oefening voorbereiden en uitvoeren kost veel tijd en inspanning, daarom is het aan te raden om dit gezamenlijk aan te pakken.

Wat kost dat nou?

In het voorgaande hebben we gezien dat het opzetten en uitvoeren van een cybercrisisoefening nogal wat voeten in aarde heeft. Centrale en decentrale voorbereiding, uitvoering, ondersteuning, techniek, afronding, noem maar op. Aan de oefenvoorbereiding van OZON hebben circa dertig personen meegewerkt, tien voor de algemene opzet, het centrale scenario en de techniek, twintig als oefenvoorbereider en scenarioschrijver voor de deelnemende instellingen. Aan de oefening namen in totaal circa tweehonderd personen deel. De totale tijdsbesteding staat in tabel 1 uitgewerkt.

Naast tijdsbesteding waren er ook out-of-pocket kosten voor onder meer externe projectbegeleiding, techniek, bedankjes en goodies en reis- en verblijfskosten voor ongeveer 40.000 euro. OZON is gefinancierd uit het SURF Innovatie Programma Betrouwbare en Veilige Omgeving, de deelnemende instellingen hebben de inzet van hun eigen medewerkers voor hun rekening genomen.

Whitepaper en promotiefilm

De lessen uit cybercrisisoefening OZON hebben Sandy Janssen en Alf Moens beschreven in een whitepaper. Hierin wordt uitgebreid ingegaan op de achtergronden van crisisoefeningen en op de verschillende vormen van oefeningen. Het whitepaper is zowel in het Nederlands als in het Engels beschikbaar op de website van SURF [1]: Daar is ook een korte filmimpressie te vinden over de oefening van oktober 2016.

Links[1] www.surf.nl/kennisbank/2016/whitepaper-cybercrisisoefening-ozon.html.

VRAGEN EN ANTWOORDEN OVER QIS

Het programma QIS (Qualification of Information Security) is in september 2013 gestart als publiek-private samenwerking die streeft naar een overzichtelijke en transparante situatie op het gebied van kwalificatie en certificatie van informatiebeveiligers. Het doel van QIS is het realiseren van een uniform stelsel dat breed wordt gedragen en aansluit op de actuele dagelijkse beroepspraktijk, bestaande kwalificatiestelsels en het Europese e-Competence Framework (e-CF). Om tot gedragen en kwalitatief goede producten te komen, is de beroepsgroep via PvIB betrokken bij de ontwikkeling.
Zie voor de deelnemende organisaties de informatie aan het eind van dit artikel.

Dit artikel geeft antwoorden op veel gestelde vragen over het certificatiestelsel voor informatiebeveiligers in Nederland.

1. Waarom dit initiatief ?

Vanwege de groeiende economische en maatschappelijke belangen en de toenemende afhankelijkheid van informatie, wordt het steeds belangrijker dat informatiebeveiligers een erkend en herkenbaar niveau van vakbekwaamheid hebben dat toepasbaar is in alle sectoren van de samenleving. Gebleken is dat er behoefte is aan een uniform en transparant certificatiestelsel met heldere beroepsprofielen en eenduidige competenties. Op dit moment kunnen organisaties die informatiebeveiligers willen aanstellen door de verscheidenheid aan opleidingen, certificaten en titels nog moeilijk bepalen of informatiebeveiligers voldoende deskundigheid in huis hebben, dan wel met welke opleiding(en) kennis en vaardigheden dat aangevuld kan worden.

2. Voor wie is dit initiatief interessant en wat is de toegevoegde waarde?

Het initiatief is interessant voor werkgevers, opleidingsinstituten en voor zowel bestaande als nieuwe professionals. Bij werkgevers wordt werving en selectie van informatiebeveiligers beter ondersteund omdat er beter zicht is op de eisen die er gesteld worden aan – in de markt – vergelijkbare informatiebeveiligingsfuncties en vergelijkbare informatiebeveiligings-functies en opleidingen. Zij kunnen hun functieprofielen aan de hand daarvan bijstellen en bij vacatures goede selecties maken. Daarnaast kunnen zij kennis en kunde van sollicitanten verifiëren middels het raadplegen van het openbare register. Professionals kunnen controleerbaar aantonen over welke competenties (kennis en vaardigheden) en ervaring zij beschikken en kunnen door inschrijving in het register hun marktwaarde vergroten. Aanbieders van opleidingen kunnen gerichter informatiebeveiligingsopleidingen ontwikkelen die aansluiten bij de praktijk en aan studenten duidelijk maken voor welke functies en beroepen de betreffende opleiding geschikt is.

3. Wordt het initiatief ondersteund door de Nederlandse overheid en het bedrijfsleven?

Absoluut. De CIO-Rijk van BZK was betrokken in de opstartfase. Het Ministerie van Veiligheid & Justitie – onderdeel NCTV – ondersteunt het initiatief, evenals de Cyber Security Raad. Ook hebben de afgelopen jaren diverse organisaties hun ondersteuning uitgesproken middels het ondertekenen van een convenant en deelname in de stuurgroep QIS. Het betreft onder meer: AkzoNobel, ABN Amro, Alliander, Eneco, Equens, EY, ING, KPN, Rabobank en UWV. Verder hebben ECP, CIO Platform Nederland en de beroepsvereniging voor informatiebeveiligers (PvIB) zich achter het initiatief geschaard.

4. Wat houdt het certificatiestelsel in?

Met het certificatiestelsel voor informatiebeveiligers is het mogelijk de kwaliteit van het beroep van informatiebeveiliger te realiseren, te bevorderen en in stand te houden. Hierdoor is het mogelijk dat de informatiebeveiliging zich op een maatschappelijk en vakinhoudelijk verantwoorde wijze ontwikkelt ter bescherming van de belangen van organisaties en beroepsbeoefenaren in alle sectoren van het bedrijfsleven en de overheid. Aan professionals worden eisen gesteld voor het up-to-date houden van hun kennis en vaardigheden. De volgende beroepsprofielen zijn gedefinieerd:

- **Chief Information Security Officer** (CISO)
- **Information Security Officer** (ISO)
- **ICT Security Manager**
- **ICT Security Specialist** (doorlopende leerlijn op de niveaus mbo-4, hbo en wo)

Het certificatiestelsel wordt op nationaal niveau uitgewerkt en ingevoerd. Het stelsel wordt beheerd door een stichting zonder winstoogmerk en onder toezicht van private en publieke partijen. Het is gebaseerd op internationale standaarden voor competenties en certificatie. Daarmee kan het nationale certificatiestelsel in een later stadium een internationale status krijgen door internationale erkenning, of door dit stelsel aan te laten sluiten op een buitenlands kwalificatiestelsel. Het certificatiestelsel is opgezet overeenkomstig tal van bestaande en gerespecteerde beroepen, zoals IT-auditors, ingenieurs, financieel planners, medische beroepen, tandartsen, advocaten, enzovoorts.

5. Wordt de vakbekwaamheid bijgehouden in deze dynamische wereld van digitaal en cyber?

Om de voor het beroep benodigde kennis en vaardigheden te onderhouden, dienen over een bepaalde meetperiode (maximaal twee jaar) de kennis en vaardigheden aantoonbaar en controleerbaar te worden verbeterd door middel van opleiding, training en andere voor het beroep relevante activiteiten. Dit dient betrekking te hebben op de voor de beroepspraktijk relevante onderwerpen, waarvan een deel specifiek is gericht op de gespecificeerde hoofdthema's voor het betreffende informatiebeveiligingsberoep.

6. Stimuleert dit initiatief het vergroten van het aanbod van jong en goed opgeleid talent?

Nederland heeft te weinig opleidingsmogelijkheden in cybersecurity. Zowel in het beroepsonderwijs (mbo en hbo) als het wetenschappelijke onderwijs (wo) is slechts een handvol opleidingen beschikbaar. Vanaf 2018 komen van de ROC's de eerste jonge mensen op de arbeidsmarkt die gekwalificeerd zijn overeenkomstig het beroepsprofiel ICT Security Specialist (mbo-4). Aan het realiseren van opleidingen op hbo- en wo-niveau die aansluiten bij het mbo-4 niveau en op de overige beroepsprofielen, wordt nog gewerkt.

7. Voldoen bestaande certificaten, opleidingen en cursussen dan niet (meer)?

In binnen- en buitenland geven opleiders, maar ook andere organisaties zoals beroepsverenigingen, certificaten en titels uit die soms op opleidingen zijn gestoeld, soms op beroepservaring en soms op beide. Instellingen voor middelbaar, hoger en wetenschappelijk onderwijs en commerciële opleiders stemmen hun opleidingen op het gebied van informatiebeveiliging niet of nauwelijks af waardoor ze niet gestandaardiseerd en geharmoniseerd zijn. Daardoor is onduidelijk in hoeverre verschillende opleidingen met elkaar te vergelijken zijn en welke in het kader van doorstroming goed op elkaar aansluiten. Het ontwikkelen en aanbieden van een coherente verzameling cybersecurity-opleidingen is niet alleen goed voor het vergroten van het aantal cybersecurity-professionals en het verbeteren van hun kennisniveau, maar het is ook goed voor het versterken van een kennisdomein dat belangrijk is voor de Nederlandse economie. Opleidingen en cybersecurity-kennis zijn mogelijke exportproducten.

8. Hoe ziet de internationale aansluiting eruit?

Om het certificatiestelsel optimaal aan te laten sluiten bij de competenties uit de dagelijkse beroepspraktijk zijn de beroepsprofielen gedefinieerd op basis van het European e-Competence Framework (e-CF, EN 16234-1:2016). Het e-CF is ontwikkeld door het CEN, het Europese Standaardisatie Comité (www.cen.eu). Europese Standaarden worden geaccepteerd en erkend in 33 Europese landen: alle lidstaten van de Europese Unie plus IJsland, Noorwegen, Zwitserland, Kroatië, Turkije en Macedonië. Samen met het Ministerie van Veiligheid & Justitie wordt het initiatief de komende periode onder de aandacht gebracht van de Europese Commissie om een verdere uitrol in Europa mogelijk te maken.

9. Hoe zit het met de onafhankelijkheid?

Het publiek-private programma QIS heeft sinds mei 2013 een certificatiestelsel ontwikkeld dat geschikt is voor publieke en private organisaties en implementeert dit in Nederland. Binnen het stelsel worden eisen gesteld aan de opleidingsinstituten en worden gecertificeerde professionals opgenomen in een openbaar register



Wim Hafkamp is Chief Information Security Officer bij de Rabobank en voorzitter van de stuurgroep QIS. Wim is bereikbaar via qis@pvib.nl.
Fred van Noord is kwartiermaker van de stichting die het certificatiestelsel gaat beheren. Fred is bereikbaar via qis@pvib.nl.
Marcel Spruit is lector Cyber Security & Safety aan de Haagse Hogeschool en adviseur bij PBLQ. Marcel is bereikbaar via m.e.m.spruit@hhs.nl.

van een stichting zonder winstoogmerk. De stichting is gerelateerd aan de beroepsgroep middels de beroepsvereniging PvIB.
Geaccrediteerde onafhankelijke certificerende instanties beoordelen de vakbekwaamheid overeenkomstig de internationale standaard voor persoonscertificatie ISO/IEC 17024 en de ISO/IEC 27000-serie voor informatiebeveiliging.

10. Wat zijn de voordelen ten opzichte van bestaande (wereldwijde) certificatieprogramma's?

De verscheidenheid aan binnenlandse en buitenlandse certificeringen is zeer groot. Vaak wordt aan een certificatie ook een titel gekoppeld die op een business card achter de naam geplaatst wordt. Bekende voorbeelden hiervan zijn CISSP, CISM en CISA. Het geharmoniseerde en geüniformeerde certificatiestelsel van QIS heeft als kenmerken:

1. geschikt voor het beoordelen van vakbekwaamheid in de praktijk
2. geschikt voor het ontwikkelen van opleidingen voor zowel jong talent als huidige experts
3. van elk beroepsprofiel is de inhoud en het niveau van kennis en vaardigheden eenduidig vastgesteld overeenkomstig de Europese e-CF standaard EN16234 en het internationaal geaccepteerde onderwijskundig model van de taxonomie van Bloom
4. kennis en vaardigheden van de beroepsprofielen zijn transparant, waardoor de inhoud van bestaande certificaten goed is te vergelijken
5. een deel van de eisen voor permanente educatie worden controleerbaar getoetst.

QIS en PvIB werken aan een eenduidige procedure om bestaande certificaathouders vrijstelling te verlenen voor competenties die zij hebben verkregen via andere certificatieprogramma's.

11. Wat is de huidige status en de planning van QIS?

In 2017 wordt het certificatieschema verder uitgewerkt, getest en gevalideerd. De organisaties van QIS en de beroepsvereniging PvIB zijn voornemens om eind 2017 het certificatieschema voor informatie-beveiligers te implementeren in Nederland. Een onafhankelijke stichting gaat het certificatiestelsel beheren inclusief het inrichten van een openbaar register met gecertificeerde professionals. In de transitiefase worden de producten die door het project QIS zijn ontwikkeld, ondergebracht in het beheerproces van de stichting.

12. Wat zijn de kosten voor een formele en geregistreerde certificatie?

De kosten voor de professional van certificatie zijn momenteel nog niet bekend. De ervaringen bij andere beroepsgroepen zijn hiervoor een belangrijke indicator. In veel gevallen zijn dat kosten voor:
- het uitvoeren van een assessment door een certificatie-instantie
- opname in het register
- jaarlijkse contributie

Heeft u nog andere vragen over dit initiatief, stuur dan een e-mail naar: qis@pvib.nl.

Betrokken organisaties

PvIB (Platform voor Informatiebeveiliging) is met ruim 1300 leden hèt kennisplatform op het gebied van informatiebeveiliging in Nederland. Het platform is een open, breed samengestelde vereniging van professionals die actief inhoud geven aan informatiebeveiliging, door het uitwisselen van kennis en ervaring. Daarnaast bevordert PvIB het 'netwerken' van personen die in het vakgebied werkzaam zijn. PvIB streeft naar maatschappelijke profilering van het vakgebied informatiebeveiliging en het professionaliseren van de beroepsgroep van informatiebeveiligers, onder meer door zich in te zetten voor de ontwikkeling van een erkende kwalificatiestructuur. Er wordt gestreefd naar afstemming op Europees niveau.
PvIB, Platform voor InformatieBeveiliging
Postbus 1058, 3860 BB NIJKERK, www.pvib.nl

Het programma QIS (Qualification of Information Security) is een publiek-private samenwerking, die streeft naar een overzichtelijke en transparante situatie op het gebied van kwalificatie. Het doel van QIS is het realiseren van een uniform kwalificatiestelsel voor informatiebeveiligers dat breed wordt gedragen en aansluit op:

- de dagelijkse beroepspraktijk;
- bestaande kwalificatiestelsels op het gebied van informatiebeveiliging;
- het Europees e-Competence Framework (e-CF 3.0).

Het programma QIS is in september 2013 gestart. De volgende organisaties hebben er deelgenomen: Rabobank, ABN Amro, Ministerie van Veiligheid & Justitie (NCTV), Rijksoverheid (BZK), ECP (Digivaardig & Digiveilig), ING, EY (Ernst & Young), AkzoNobel, KPN, Cyber Security Raad, PvIB.

QIS-klankbordgroep

Voor de ontwikkeling van de producten van QIS is dankbaar gebruikgemaakt van de inzet van de professionals van de onderstaande organisaties.
Werkgevers - CIO Platform Nederland, CIP, VNO-NCW, MKB
Opleiders - HBO-i, ECABO (SBB), VOI (ICT Leerplatform), SPIH, CSA
Beroepsverenigingen - NOREA, Ngi-NGN.

Convenant

Op 30 mei 2013 is door de CIO's en CISO's van ABN Amro, AkzoNobel, Alliander, Eneco, Equens, ING, Rabobank en UWV met het ondertekenen van een convenant het volgende commitment afgegeven:
"Wij, de ondertekenaars van dit convenant, geven aan dat we het initiatief steunen om te komen tot een uniform kwalificatiestelsel voor professionals informatiebeveiliging. We geven aan dat we de intentie hebben om het kwalificatiestelsel binnen onze eigen organisatie, respectievelijk branche, in te zetten voor werving en selectie van professionals informatiebeveiliging. Tevens zetten we ons in om te zorgen dat organisaties waaraan wij gelieerd zijn, zoals ketenpartners, leveranciers en afnemers, het kwalificatiestelsel ook toe gaan passen en zo bijdragen aan een brede acceptatie ervan."

INFO-WARFARE READY

It is January 2017, and as Donald Trump prepares to take over as the new President of the USA, the debate rumbles on about the possible hacking, leaking and disinformation associated with Hilary Clinton's election campaign. So what should we make of these allegations? Let's look at what we know.

In March 2016 Hilary Clinton's campaign manager, John Podesta, received an email warning him that his Internet mail account password had been compromised and that he should immediately change it. Unfortunately, Mr. Podesta was naïve regarding Internet mail security and was unaware that he was the victim of a spear-phishing attack. He responded to the warning and his mail account was hacked with the greatest of ease. What was the impact?

Many people have speculated about the source of this and other associated attacks, citing foreign state sponsored interference in the US election process, but for our purposes here it hardly matters who were the perpetrators – the fact is that someone with malicious intent wanted to discredit the Clinton campaign and was using information warfare as a means to achieve that aim. We can let the politicians rant and rave about who and why, but it provides a very useful case study in how information warfare can be used against a potential target – you for example.

Once the integrity of your systems is brought into question you become vulnerable to all sorts of accusations, which may or may not be true. One outcome is that some embarrassing truths are leaked and revealed – dirty washing exposed in public. However, it's not clear whether this information is indeed the truth. If your opponents can demonstrate that your system is compromised, then they can spread both truth and lies without anyone being able to tell the difference, and without you being able to defend yourself. What would you do? Admit that some is true in order to deny the untruths? Will you be believed? Probably not, because once the opponents can demonstrate that the integrity of your system has been breached they can quickly turn that into a breach of your own personal and corporate integrity. There will always be doubt about counter-claims and denials that you make.

Let's skip into another business domain to see this effect more clearly. You are a large pharmaceutical company and have invested huge amounts of money developing and testing a new drug. You have five years of clinical trial data stored on a system, data that is essential for gaining public confidence and receiving a license to release the drug for general use on humans. Someone hacks into your database and claims to have altered the data, rendering it unusable. Your investments are under threat. What do you do next?

You can try to deny that the data is corrupted, that you have back-ups in safe places, that you have integrity checks on the data, and so on. Claims and denials are one thing, but what matters is the ability to demonstrate integrity – to support your claims and denials with hard evidence. The opponent needs no such rigour, because just by claiming to have penetrated your system they have brought the integrity of your data into question. They may not even have made a successful attack – this is all about confidence and proof, the onus of which is always on you. Legal principles do not apply – you are guilty until you can prove otherwise (ask Hillary Clinton). There's no smoke without fire. Confidence is based on belief, and the only way to change belief is by presenting evidence that is believable.

So, assume that one day you will be subject to an information warfare attack. Do some scenario planning and understand the possible consequences. Then decide on measures you need to be able to refute untrue allegations. Oh – and make sure your staff are not so naïve and stupid as Mr. Podesta. Education and culture development are very important. SABSA thinking can help by identifying the attributes that characterise your business requirements and provide measurable hard evidence that can be shown in public to support any claims or denials you will need to make when this happens to you.

The Attributer

VERSLAG TIENDE CIP-CONGRES

KROKETTEN EN LOEMPIA'S

Het lustrum CIP-congres wordt door de dagvoorzitter Jelle Kuiper geopend. Uit door het publiek ingevulde enquêtes blijkt dat de kroketten en loempia's zeer gewaardeerd worden, deze zullen blijven. Natuurlijk leidt dat tot enige hilariteit in de zaal. Jelle zorgt voor het aan elkaar praten van de dag op een luchtige manier. Deze rol zit hem als gegoten, evenals zijn nieuwe jasje.

Hierna vertelt de voorzitter van het CIP, Ad Reuijl, over de ontwikkelingen en producten van het CIP in 2016. Zo is bijvoorbeeld de norm SSD (Secure Software Development) in het Engels vertaald. Vanwege het jubileum wordt aan een viertal mensen in de zaal, die bij alle congressen aanwezig waren, een cadeautje gegeven. Hieronder bevinden zich onder andere Fred van Noord en Carl Adams, beiden bekend binnen het PvIB.

De slide met de belangrijkste resultaten van 2016 voor het CIP neemt minstens tien minuten spreektijd in beslag. Voor 2017 staan veel nieuwe producten en werkgroepen op het programma. Door de werkgroep testen wordt het laatste product dat gereed is, het testframework voor SSD, aangeboden aan Ad.

Brenno de Winter krijgt de ruimte om mensen uit het publiek opnamen te laten maken van een ingestudeerd stukje. Deze opnamen op camera's/telefoons van mensen uit het publiek wenst hij te ontvangen op zijn e-mailadres. De zaal is hierin gewild of ongewild figurant. De opnamen zullen worden gebruikt voor de openingsscène van de ketengame-in-ontwikkeling.

IT-risico's

Aart van de Vlist, trendwatcher, CTO en CIO van UWV neemt de eerste keynote voor zijn rekening. Hij presenteert een drieluik en stelt dat ieder bedrijf op zijn kop gaat door IT-ontwikkelingen, die zich exponentieel voordoen. Voorbeelden hierbij zijn zelfrijdende auto's en het inchecken in een Japans hotel door robots. De aan deze ontwikkelingen gelieerde IT-risico's groeien net zo hard, dus eveneens exponentieel. Voor deze risico's zijn nieuwe security designs noodzakelijk en zal privacy heruitgevonden moeten worden. Vanwege de omvang zal hiervoor moeten worden samengewerkt, stelt Aart. Als voorbeeld geldt bijvoorbeeld de recente aanval op de website van Krebs (on security). Bij deze aanval is een DDoS ingekocht door één persoon en hierbij is een botnetwerk bestaande uit 'huishoudapparaten' (IoT) ingezet. De hoeveelheid verkeer dat deelnam aan de aanval was ongeëvenaard groot. Zelfs grote organisaties als het UWV moeten samenwerken. UWV kiest daarom onder meer voor aansluiting op het Nationaal Detectie Netwerk. Uit de zaal komt de vraag of architectuur nog nodig is. Aart schat de waarde van architectuur hoog. Maar de tijd dat ontwerpen voor lange tijd vastgezet werden, is wel voorbij. Architectuur moet vooral gaan over 'loosely coupled' elementen.

Het vervolg zijn vier parallelsessies die elk twee keer gegeven worden. Sebastian Dinjens vertelt over het Nationaal Detectie Netwerk en Ivo Luijendijk over Blockchain en Bitcoin. Gerben Klein Baltink, Han Zuidweg en Bart Knubben geven handvatten ter voorkoming van e-mailfraude. Kees van der Maarel, Douwe Leguit en Bert Boerrigter lichten het veranderkrachtmodel toe met als praktijkvoorbeeld het invoeren van de Baseline Informatiebeveiliging Rijks (BIR) vanuit BZK. De toelichting van het veranderkrachtmodel is zeer aansprekend en biedt veel stof tot overdenking en toepassing. Aan de hand van een filmpje van

een versperd kruispunt in India worden de verschillende leiderschapsrollen (of zo gewenst, benodigdheden) toegelicht. De participatiegraad vanuit de zaal is hoog.

Na de lunch met kroketten en loempia's mogen zes ondernemers toelichten waarvoor ze een SBIR (cybersecurity subsidie) vanuit Rijksdienst voor Ondernemend Nederland hebben ontvangen. Stuk voor stuk interessante en vernieuwende ontwikkelingen. Mariska Warnars van RVO geeft aan dat er tot 31 januari 2017 voor overheidsorganisaties en commerciële partijen nog gelegenheid is om in het kader van een nieuwe SBIR-ronde voorstellen in te dienen voor subsidie [1].

De Rolls Royce onder de authenticatiemiddelen

De laatste keynote geeft Steven Luitjens. In sneltreinvaart komen er veel onderwerpen voorbij die eigenlijk allemaal op zich een keynote waardig zouden zijn. Dit maakt het interessant, maar voor goede reflectie is meer tijd nodig. Als voormalig directeur van Logius en inmiddels beleidsdirecteur bij BZK schetst hij onder andere de ontstaansgeschiedenis van DigiD en de start van de beoogde opvolger e-ID. Niet iedereen weet dat DigiD gestart is als laagdrempelig authenticatiemiddel voor niet meer dan het digitaal inzien of uitwisselen van gegevens. Het is niet opgezet om de Rolls Royce onder authenticatiemiddelen te zijn. De start van e-ID was de vertrouwenscrisis naar aanleiding van DigiNotar. Deze creëerde het bewustzijn dat het leunen op één authenticatiemiddel (DigiD) wel heel dun ijs is. Als dat omvalt, staat de dienstverlening stil. De continuïteit van de dienstverlening is erbij gebaat als meerdere oplossingen van meerdere leveranciers beschikbaar zijn. Een en ander wel onder een afdoende ingericht toezicht vanuit BZK. Steven schetst het belang van wetgeving om het e-ID-stelsel te conditioneren.
Te midden van de authenticatieoplossingen die op de markt komen, zal DigiD ook blijven bestaan. De merknaam DigiD is ook sterk; de technologie wordt verbeterd zodat er meer zekerheid is dat wie inlogt ook de persoon is die hij/zij claimt te zijn. Als laatste de opmerking dat er tot op heden geen beperking is opgeworpen op de toelating van middelen.

Na deze keynote is het tijd voor het Sinterklaasgedicht van Jelle. Hij schetst het huidige succes van het CIP onder de bezielende leiding van Ad Reuijl en hierin komt onder andere voorbij: "als Ad gaat praten dan wordt het stil".

Als laatste een link naar de vrij beschikbare producten ontwikkeld onder de leiding van het CIP [2]. Doe er je voordeel mee in informatiebeveiliging en privacy-land.

Links

[1] Nieuwe ronde SBIR subsidie: http://www.rvo.nl/subsidies-regelingen/sbir/3e-tender-sbir-cyber-security
[2] CIP-producten: https://www.cip-overheid.nl/wp-content/uploads/2016/11/PDC%20CIP%2015%20nov%202016.pdf

Brenda Langedijk is security consultant van de Software Improvement Group (SIG). Brenda is te bereiken via b.langedijk@sig.eu.

VERSLAG

Alert Online Cyber Security Awareness Symposium

HOE ORGANISEER JE EEN GOED SECURITY AWARENESS PROGRAMMA?

Op 13 oktober waren zo'n 75 deelnemers afgekomen op het Alert Online Cyber Security Awareness Symposium op de HSD Campus in Den Haag. Dit symposium, georganiseerd door Insite Security, TNO en HSD, was bedoeld om security managers en security officers een praktische aanpak te geven om in hun bedrijf of organisatie een goed security awareness programma op te zetten.

De dag werd geopend door Wilbert Pijnenburg, commercieel directeur bij Insite Security. Na een korte introductie nam Robin de Haas, community manager HSD, het stokje over en vertelde hij de aanwezigen over de opzet en doelstellingen van The Hague Security Delta, het grootste security cluster in Europa. Naast het genereren van maatschappelijk (meer veiligheid) en economisch rendement (meer banen) biedt HSD toegang tot kennis, innovatie, kapitaalmarkt en talent. Als voorbeeld noemde Robin het onderzoek naar een 'National Testbed', waar bedrijven en instellingen uit de vitale infrastructuren hun aanpak en middelen zouden kunnen testen. Een whitepaper hierover verschijnt binnenkort.

Veel aandacht bij AlertOnline 2016 (credit: Wilbert Pijnenburg)

Anonieme aanwezigheid op internet

Vervolgens was het podium voor Rolf van Wegberg van TNO, die samen met zijn collega Thymen Verburgh de aanwezigen een inleiding gaf in het Darkweb, en hoe dit door met name criminelen gebruikt wordt om hun nieuwe businessmodellen in de praktijk te brengen. Twee technologieën zijn de drijvende kracht achter het Darkweb: The Onion Router (TOR) en Block Chain Technology (BitCoins). Middels de eerste is een volledig anonieme aanwezigheid op internet mogelijk, middels de tweede kunnen financiële transacties, ook weer volledig anoniem, worden afgehandeld.

Onderzoek van TNO laat zien dat er op dit Darkweb diverse soorten handel plaats vinden, zowel 'Business to Consumer' (veelal gericht op het verkopen van verdovende middelen), als ook 'Business to Business' (waarbij criminelen hun 'diensten' aan andere criminelen aanbieden). Echter ook 'consumenten' weten steeds vaker de weg naar deze 'diensten' te vinden, zo is het gezamenlijk inkopen van een 'DDoS as a Service' een favoriete bezigheid van scholieren in de examentijd. Echter ook meer 'edele' doelen worden gediend met het Darkweb: het is een bescherming voor bijvoorbeeld klokkenluiders en journalisten die hun bronnen willen beschermen. Het verbieden van Darkweb lijkt geen goede optie. Onderzoekers zijn nu wel in staat om te volgen wat daar zoal gebeurt.

Aan de hand van instructies van Rolf en Thymen konden de aanwezigen met een laptop al gauw zelf het Darkweb op, en daar eens rondneuzen. Rolf gaf aan dat het best wel handig kan zijn om daar te zoeken op de naam van je eigen organisatie of bedrijf: een gewaarschuwd mens telt voor twee.

Masterclass Security Awareness

Eindbeoordeling Masterclass sessie (credit: Wilbert Pijnenburg)

Vervolgens werd door Wilbert Pijnenburg en zijn collega Laurens Dijkstra (gedragspsycholoog bij Insite) een (verkorte) Masterclass Awareness Training gegeven. Middels quiz-achtige vragen met behulp van de Menti-tool werden de aanwezigen betrokken bij het ontwikkelen van een security awareness training voor een fictief bedrijf. De belangrijkste boodschap is dat de medewerkers voor wie het awareness programma bedoeld is, daadwerkelijk 'nut en noodzaak' inzien, anders gaat het niet werken. Alhoewel de tijd natuurlijk te kort was om daadwerkelijk diep inzicht te krijgen in het opzetten van een goed security awareness programma, was dit voor de meeste aanwezigen een 'eye opener' om mee verder te werken in hun bedrijf of organisatie.

Carlijn Broekman (Innovation Management Consulant bij TNO) vertelde over haar onderzoek bij TNO naar gepersonaliseerde training. Wanneer de resultaten van dit onderzoek beschikbaar komen, kan dit helpen bij het differentiëren van de security awareness training naar diverse groepen binnen het bedrijf. Immers: 'one size fits all' gaat absoluut niet op voor een goed security awareness programma.

Om te illustreren hoe gemakkelijk de mens als toegang tot de kroonjuwelen van de organisatie gebruikt kan worden, liet Andres Rutkens (Adviseur bij Insite) met een aantal smakelijke voorbeelden zien hoe makkelijk een mens zich door anderen laat beïnvloeden. En zich daarmee dus kwetsbaar maakt voor een 'goed kletsverhaal', waardoor hij/zij (ongewild) anderen met minder goede bedoelingen gevoelige informatie verstrekt.

Social engineering = goed kletsverhaal

Peter Zinn (expert Cybercrime bij KLPD) liet in een flitsende presentatie zien dat het 'einde nabij is', en dat we dit zelf aan het veroorzaken zijn. Niet door overbelasting van het milieu of door uitputting van de grondstoffen, of door een geweldsconflict met inzet van nucleaire middelen, maar gewoon door het Internet of Things. Het gros van de 'dingen' die nu aan internet worden gehangen zijn niet voorzien van goed doordachte beveiliging, en daarmee willig speelveld voor zowel 'state actors' als criminelen. Recentelijk hebben we al het eerste zombienetwerk van IoT-apparaten gezien dat daadwerkelijk een DDos aanval uitvoerde. Waarmee wij als informatiebeveiligers dus allemaal zombiejagers zijn geworden, in de beeldspraak van Peter.

Tot slot ging Jeffrey de Graaf (Sales Manager bij QSight IT) in op de menselijke factor in de ICT. Niet alleen blijkt uit onderzoek dat 10% van de mensen pathologisch niet integer is, zo'n 65% van de bedreigingen voor bedrijven en organisatie komen van 'insiders'. Uit een ander onderzoek blijkt dat 90% van de security incidenten 'mens-gerelateerd' zijn. Daarom is de helpdesk zo'n gewild doelwit van criminelen: de medewerkers zijn over het algemeen graag bereid te helpen en zitten op een heleboel kennis van de organisatie, inclusief de mogelijkheid van toegang tot vrijwel alle pc's en laptops in het bedrijf. Om dit in voldoende mate te kunnen voorkomen wordt 'end point security' steeds belangrijker, niet alleen om pogingen tot toegang te melden, maar ook te blokkeren, en het gedrag van de medewerker vast te kunnen leggen. Dat moet uiteraard niet ontaarden in 'Big brother is watching you', maar middels een gefaseerde, op de afdeling afgestemde aanpak kan dit helpen om risico's in te perken.

Conclusie: dit symposium was vanuit twee oogpunten nuttig. Niet alleen werden er bruikbare kennis en inzichten over het opzetten van een goed security awareness programma meegegeven aan de deelnemers, er was ook voldoende ruimte voor het netwerken tussen de deelnemers onderling. Daarbij bleek dat het niet alleen de 'usual suspects' waren, die op dit symposium afgekomen waren, maar ook veel mensen die security 'er bij doen'. En het is goed dat ook die groep hun skills op een hoger plan kan brengen door middel van dit soort symposia.

Links

The Hague Security Delta (HSD): https://www.thehaguesecuritydelta.com/
HSD Campus: https://www.thehaguesecuritydelta.com/about/hsd-campus
Insite Security: https://www.insitesecurity.nl/diensten/
Qsight Security: https://www.qsight.nl/diensten
TNO: https://www.tno.nl/nl/aandachtsgebieden/defensie-veiligheid/cyber-security-resilience/
The Onion Router (TOR): https://www.torproject.org/

Lex Dunn is adviseur op het gebied van informatiebeveiliging en compliance.
Hij is te bereiken via lex@selexity.nl.

VERSLAG CISO 14

WAAROM ZIJN WIJ NOG NIET VEILIG?

(...en wat hieraan te doen)

Mijn laatste CISO-bijeenkomst op 7 december 2016 stond in het teken van de toekomst. Gerard de Weerd is een van de mensen die vanaf 2017 in mijn plaats, samen met Bart van Staveren, CISO bijeenkomsten gaat voorbereiden. Voor CISO 14 had Gerard een mystery guest beloofd en een discussie die past in de opzet van CISO. Hij zou de vraag aan de orde stellen: 'Waarom zijn wij (nog) niet veilig en verslechtert de situatie zelfs in plaats van dat deze beter wordt.?'

De gast bleek Julian Wynne te zijn, werkzaam bij Ilionx. Zittend op een tafel, zonder sheets of andere hulpmiddel, vertelde hij over zijn achtergrond, ervaringen en zijn persoonlijke missie: weerbaarheid genereren in een cyberomgeving.

Informatiebeveiliging is een onderdeel van de formele wereld waar processen, mensen en technologie met wetten en regels 'in control en compliant' worden gehouden. De informele hacker, de crimineel, heeft hieraan geen boodschap en gaat zijn gang. De digitale wereld van de cyberspace is gebaseerd op een internet dat is ontworpen voor beschikbaarheid voor iedereen zonder aandacht voor betrouwbaarheid en vertrouwelijkheid. En dan is er het grote verschil met de fysieke wereld; in cyberspace is weinig 'te zien'.

Discussie

Inleiding en discussie gingen als vanzelf in elkaar over en concentreerden zich op de crimineel, de mens buiten de organisatie die zijn eigen belangen nastreeft. Julian wees erop dat de fysieke wereld heuristisch is en beperkt, maar overzichtelijk. In de digitale wereld verandert dat door de hoeveelheid variabelen die niet meer te overzien is. Julian merkte op dat wij ons niet eens bewust zijn van de bedreigingen. De schade door cybercriminaliteit is groter dan wij denken. Die schades worden niet erg geopenbaard. omdat de belangen van partijen dat tegenhouden. Bovendien, zij zijn niet zo zichtbaar als de fysieke incidenten.

Wat zijn de opties voor de CISO? Bewegen, waardoor de aanvaller minder tijd heeft, is een mogelijkheid. Blockchain techniek kan een andere zijn. En natuurlijk, men kan ook besluiten de hardware te compartimenteren of data niet langer te ontsluiten. Maar is dat realistisch? Van cryptografie moeten wij het niet hebben, want dat is techniek, zoals zoveel beveiligingsmaatregelen. Technische oplossingen leveren een ratrace op, iedere verbetering nodigt uit voor een volgende. Dus waarom hechten CISO's dan zo aan compliance?

Julian wees op Bruce Schneider die hem in dit verband eens zei dat de enige realistische maatregel tegen cyberaanvallen detectie is.

Dit was mijn laatste CISO. Vele jaren heb ik de bijeenkomsten

Technische oplossingen leveren een ratrace op, iedere verbetering nodigt uit voor een volgende.

De discussie leverde een aantal constateringen en vragen op:

- Wat ik niet ken, kan ik ook niet detecteren.
- De mens kan buiten een systematiek denken, een computer werkt op basis van reeds bekende regels.
- In een private onderneming worden grenzen aan acceptabele risico's gesteld door geld, reactie van de klant en reputatie. Bij de overheid ligt dat anders.
- Hoe digitaler wij worden, hoe kwetsbaarder voor criminelen.
- Zijn wetten doeltreffend als de lasten groot zijn, het effect gering en het toezicht ontbreekt?
- De wet nodigt uit om compliant te zijn. Maar is de situatie dan ook veiliger?
- Moet alles digitaal? Deugen de argumenten?
- Het beveiligen van cyberspace kan alleen met de regels van cyberspace.
- De verantwoordelijkheid voor de weerbaarheid van een organisatie ligt bij de deelnemers. Laat dat dan ook voor cyberincidenten zo zijn.
- Het gebruiken van standaarden is mooi, maar de aanvaller kent die ook.
- De CISO zal het management moeten helpen het adaptievermogen van de organisatie te vergroten.
- De verwachting is dat de budgetten voor IB stijgen, dat biedt mogelijkheden voor het investeren in herstelvermogen.

voorbereid en verslagen. Het begon bij rechtsvoorgangers van PvIB met vertegenwoordigers van organisaties die van elkaar over IB wilden leren, ervaringen wilden uitwisselen en antwoorden wilden verkennen op vragen die breed leven in organisaties. In 2007 besloot het bestuur van PvIB tot de voortzetting hiervan als IBO-bijeenkomst, sinds 2014 CISO-bijeenkomst genoemd. Het werd tijd voor een nieuwe generatie betrokkenen die op een eigentijdse manier de vragen en ontwikkelingen rond IB aan de orde kunnen stellen. Graag geef ik het stokje door met de dank aan de velen die bijdroegen aan spannende gedachtewisselingen, het benoemen van uitdagingen en het bespreken van positieve en negatieve ervaringen. Leren van collega-professionals, het blijft een stimulerende bezigheid die dwingt tot nadenken.

Cees Coumou is sinds medio 2003 gepensioneerd als senior EDP Audit manager bij KPMG. Sindsdien is hij onafhankelijk adviseur en docent aan de IT-Audit Master van de Vrije Universiteit, de opleiding Master of IT auditing van de Universiteit van Amsterdam. Zijn werk op het gebied van organisatieadvisering betrof de laatste decennia met name onderwerpen als risicomanagement, continuiteitsmanagement en informatiebeveiliging. Tussen 2005 en 2012 redigeerde hij voor PvIB acht boeken over trends in IT-beveiliging op basis van gesprekken met vele verschillende professionals.Hij is bereikbaar via cees.coumou@planet.nl.

Artikelen

[A] Artikel
[V] Verslag
[I] Interview
[O] Opinie

Jaaroverzicht 2016

Achter Het Nieuws

In deze rubriek geven enkele IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over de 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 kunt u sturen naar ibmagazine@pvib.nl.

INTERNET DER DREIGINGEN

In de afgelopen periode zijn er meerdere grote DDoS-aanvallen uitgevoerd vanaf botnets bestaande uit Internet-of-Things (IoT)-apparaten, zoals beveiligingscamera's en thuisrouters. Hoewel deze apparaten relatief weinig rekenkracht hebben, worden ze in grote hoeveelheden door kwaadwillenden ingezet om de grootste DDoS-aanvallen tot nu toe uit te voeren. Voorbeelden hiervan zijn de aanvallen op securityjournalist Brian Krebs, hostingprovider OVH en DNS-provider Dyn. Terwijl het allang algemeen bekend is dat de meeste IoT-apparaten slecht beveiligd zijn (standaard wachtwoorden, geen beveiligingsupdates, etc.), wordt er mogelijk te weinig aan gedaan om de situatie te verbeteren. Het lijkt alsof er tegenstrijdige belangen zijn, zoals security, functionaliteit en lage kosten, die ervoor zorgen dat securityaspecten onvoldoende aandacht krijgen. Binnen de private en publieke sectoren en op nationaal en internationaal niveau loopt er discussie over deze toenemende dreiging. Wie wordt het volgende slachtoffer en hoe groot wordt de schade? Wat kunnen we eraan doen en, wellicht de lastigste vraag, wie is de meest geschikte partij om er iets aan te doen? Is de markt in staat om IoT-security te prioriteren of is internationale wetgeving nodig?


Maarten Hartsuijker


Lex Borger

Maarten Hartsuijker

Apparatuur die wordt uitgeleverd met kwetsbare standaard functionaliteit en standaard instellingen is van alle tijden. Google voor wat geschiedenis een keer op 'Phenoelit default password' en je ziet dat het type kwetsbaarheden (zoals makkelijke standaard wachtwoorden) die we nu in IOT-apparatuur zien van alle tijden is. En in zakelijke IT-omgevingen al jaren een bekend verschijnsel is. Dat beperkt zich overigens niet tot apparatuur. Ik kom tijdens audits ook IT-bedrijven tegen die al hun klanten met dezelfde wachtwoorden beheren. Of softwarebedrijven die hun databases overal van dezelfde wachtwoorden voorzien. Gemak dient nu eenmaal de mens. Dit gaan we niet zomaar veranderen.

Het grootste verschil met IOT is wat mij betreft de impact van dit soort kwetsbaarheden. Daar waar de dreiging voorheen vooral individuele bedrijven trof, zien we dat via de consumentenmarkt de stabiliteit van het internet wordt bedreigd. En dat organisaties die denken hun beveiliging goed op orde te hebben, benadeeld worden door mensen waarvoor dat niet geldt.

Hoewel het fantastisch zou zijn als elke leverancier zijn apparatuur standaard in een veilige modus uitlevert (en overheden en bracheorganisaties daar vooral op aan moeten dringen), is dat vermoedelijk een utopie. Hetgeen we bij IOT zien is al decennia een probleem en nog lang niet uitgeroeid. En iedereen speelt hierin zijn eigen rol. De consument, omdat deze te vaak zonder nadenken van alles aansluit. De IOT-leverancier, omdat hij de consument via de gebruikersinterface niet altijd voldoende 'coacht' om een veilige installatie uit te voeren. De telecomprovider, omdat deze niet zelden routers oplevert met UPNP. De IOT-installateur, daar waar hij na de installatie van de zonnepanelen of de alarminstallatie de standaardinstellingen actief laat.

Persoonlijk ben ik geen voorstander van beperkende (wetgevende) maatregelen. Dit leidt te gemakkelijk tot een beperking van vrijheid en digitale mogelijkheden. Maar een plek binnen bewustwordingscampagnes zoals Alert Online verdient dit wat mij betreft zeer zeker.

Lex Borger

Het is niet een kwestie wie het volgende slachtoffer wordt, maar wie de volgende 'dienstverlener' wordt die dit soort aanvallen gaat aanbieden. En dan is er nog een klant nodig die diep genoeg in de buidel wil tasten om alle DDoS-registers open te trekken. We zien aan de sprongen die gemaakt werden in aanvalscapaciteit dat het plafond niet bereikt is. Voordat we het in de gaten hadden, was het maximum verviervoudigd...

Op het moment dat de 'things' bestaan, is het al te laat. De routers, camera's, koelkasten zijn verkocht en staan ergens, verbonden aan het internet met al hun kwetsbaarheden. Er hoeft geen IP-adres gespoofd te worden, er hoeft niet aan reflectie gedaan te worden, er zijn gewoonweg genoeg zombie-bots om een rechttoe-rechtaan aanval te doen. Dit maakt het ook heel moeilijk om een aanval te detecteren.

Dus wie moet hier iets aan doen? De verkoper en koper kun je niet aanpakken, die zitten over de hele wereld verspreid en hebben totaal geen last van de DDoS-aanval. Hetzelfde geldt voor de maker. Die staat onder druk om tegen minimale kosten een functioneel product te leveren in een heftige concurrentiestrijd.

Maar ook (overheids)regulering gaat niet zonder meer werken. Het internet der dingen werkt over landsgrenzen heen. Ik denk dat een firewall bij AMS-IX (Amsterdam Internet Exchange) ook niet echt is wat we willen.

Wat blijft er over? Zelfregulering door de sector? Daar zit de meeste belofte. Als uit maatschappelijke verantwoording of onder druk van potentiële boetes de makers zorgen dat ze alleen veilige apparaten maken, lijkt de enige logische mogelijkheid dat deze apparaten eigen bewaking hebben om te zorgen dat iedereen hier in meegaat. Ook voor dit scenario zullen er veel details uitgewerkt moeten worden...

Het is natuurlijk mogelijk om een joker in te zetten: is bijvoorbeeld met de inzet van blockchain-technologie het Internet of Things te temmen? Het ligt niet voor de hand, maar wellicht zijn er creatieve geesten die een werkend, praktisch ontwerp kunnen maken? En zo eindigt het voorlopig ook net zoals het begon: met een aantal vraagtekens...

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

REDACTIE
Lex Borger (hoofdredacteur, werkzaam bij i-to-i)
e-mail: hr@pvib.nl
MOS bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

Tom Bakker (Digidentity BV)
Kas Clark (NCSC)
Lex Dunn
Maarten Hartsuijker (Classity)
Rachel Marbus (KPN)
Bart van Staveren

ADVERTENTIE-ACQUISITIE
e-mail: adverteren@pvib.nl;
of neem contact op met MOS
T (033) 247 34 00
ibmagazine@pvib.nl

VORMGEVING EN DRUK
VdR druk & print, Nijkerk
www.vdr.nl

UITGEVER
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
F (033) 246 04 70
e-mail: secretariaat@pvib.nl
website: www.pvib.nl

ABONNEMENTEN 2017
De abonnementsprijs in 2017 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

PvIB abonnementenadministratie
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
e-mail: secretariaat@pvib.nl

ISSN 1569-1063

DE KOERIER

Zoals iedere lezer van dit onvolprezen magazine wel weet, vierden we kortgeleden de eerste verjaardag van de Meldplicht Datalekken. Ik heb te weinig ruimte om de gehele regeling aan u uit te leggen, maar het komt erop neer dat het lekken van data in het vervolg gemeld moet worden op straffe van een zeer forse boete. De onderliggende gedachte is dat er voorzichtiger met data wordt omgegaan. Op zich is dat natuurlijk een geweldige gedachte. Dus als je nu een onbeveiligde USB-stick verliest met alle klantgegevens van je webshop, dan ga je naar de Autoriteit Persoonsgegevens (AP). Zij onderzoeken dan of jij onvoorzichtig bent geweest en of je aanpassingen in je IT-omgeving moet doen.

In beginsel klinkt dit goed, het probleem is echter dat als je niets meldt, je geen sancties krijgt. Tenzij je betrapt wordt natuurlijk, dan kom je in aanmerking voor de boete. Wij Nederlanders doen dat nooit, maar helaas gaat onze data weleens de grens over. Dit doen we omdat er zo'n lekkere goedkope hosting-partij in Verweggistan zit. Dan wordt het al veel lastiger oog te houden op de data, zelfs als je de eigenaar bent van deze data.

Er worden natuurlijk contracten afgesloten, maar hoe ben je er honderd procent zeker van dat dit goed gaat? Op 15 december 2016 werden de eerste tussenresultaten bekend. Er werden maar liefst 5500 datalekken gemeld en dat komt neer op ruim vijftien meldingen per dag. De AP is een ambtelijk bedrijf, dus is in het weekend dicht. Dat betekent dat zij twintig gevallen per dag moeten onderzoeken. Ik heb het natuurlijk alleen over de bij het AP gemelde lekken.

Ik moet u eerlijk zeggen dat ik somber was toen deze regeling werd ingevoerd, maar achteraf blijk ík zelfs te optimistisch geweest te zijn. Vijftien meldingen per dag zijn er gedaan, variërend van de verloren USB-stick tot aan een grootschalige diefstal van data van een internetsite af! Ambtenaren van de AP gaan dan naar de locatie toe om onderzoek te doen. Van de 5500 meldingen zijn 4000 meldingen onderzocht of in onderzoek.

Begrijp mij goed, ik vind het een enorm goed initiatief, maar ik heb zeer grote twijfels of deze regelgeving bij gaat dragen aan het beveiligingsniveau van persoonsdata. De nieuwe president van de Verenigde Staten van Amerika is er ook heel duidelijk in: als je belangrijke informatie hebt te bewerken, dan sla je die niet in een computer op. Ook e-mail is volstrekt ongeschikt voor het verzenden van belangrijke informatie. Nee, belangrijke berichten zet je op papier in een brief en die brief verstuur je per koerier. Ik bedenk het niet, meneer de president doet dat.

Ik beschouw deze column niet als belangrijk, dus neem ik de vrijheid deze naar mijn hoofdredacteur te e-mailen. Ik hoop maar dat die actie geen gevolgen heeft.

Berry

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

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

Stappenplan ISO 27001/NEN 7510

Download kosteloos de whitepaper 'Stappenplan naar informatiebeveiliging'

www.dnvgl.nl/whitepapers