iB
INFORMATIEBEVEILIGING
jaargang 17 - 2017
#3

SEGMENTATIE

To segment or not to segment

De kracht van het Privacy Impact Assessment

Interview Masum Mir

Voorbij awareness: grip op cyberveilig gedrag

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

SAFER, SMARTER, GREENER

DNV·GL

VERDEEL EN HEERS

De Titanic was 105 jaar geleden verdeeld in zestien compartimenten en daarom onzinkbaar. Wat betekent dat? Dat het risico van zinken zo goed als nul was. Vier compartimenten konden vollopen en het schip zou blijven drijven. Het was ondenkbaar dat bij een aanvaring zoveel compartimenten lek zouden raken. Een prachtige ontwerp-maatregel: beperk de impact van een incident tot het vollopen van één of twee compartimenten en de schade blijft beperkt tot lokale waterschade.

Zo ook bij moderne netwerken: segmenteer het en aanvallers zullen bij succesvol binnendringen niet het gehele netwerk kunnen binnendringen, hooguit het segment waar ze zitten. 'Heel goed!', denk ik dan, er zijn maar weinig maatregelen die echt impactbeperkend zijn. De meeste maatregelen beperken de waarschijnlijkheid. En met microsegmentatie kunnen we dynamisch duizenden netwerksegmenten hebben. Een enkele doorbraak heeft dan nog maar een micro-effect. En dat micro-effect is zo klein dat één leverancier zelfs spreekt van een 'stealth' effect van micro-segmentatie.

Verdeling in segmenten is één manier om risico te beperken, authenticatie verdelen over meerdere factoren is een ander. 'Two-factor' authenticatie (2FA) is de norm aan het worden en we leren hoe we daar de middelen die de gebruiker zelf al heeft voor kunnen gebruiken. BYOD werkt in dit geval echt kostenbesparend. De gebruiker heeft zijn eigen mobieltje, daar kan een relatief veilige one-time password (OTP) authenticatie mee worden uitgevoerd. We weten hoe het de Titanic is vergaan: een ijsberg die zich achter een mirage verborgen hield kon het schip onopgemerkt aanvallen en zes compartimenten lek slaan. Dat was een te grote impact voor het onzinkbare schip. De aanval was te verdeeld over meerdere segmenten en overheerste daardoor.

Dus is segmentatie gedoemd te mislukken? Ik denk van niet. Maar we moeten wel bedenken dat er nog steeds aanvallen mogelijk zullen zijn die door de segmenten heen kunnen breken. Ruim honderd jaar later weten we dat een gesegmenteerd netwerk niet onhackbaar is. Het is wel véél moeilijker te hacken. Bescherming tegen hackers is een zeer noodzakelijke kwestie van goede hygiëne toepassen. Je hoeft hier geen risicoanalyse op te doen, als je iets aansluit op het internet dien je het te beveiligen. Wie daar aan twijfelt, leest er maar het Cybersecuritybeeld Nederland op na, of het Verizon Data-Breach Investigation Report (DBIR). Van die laatste is trouwens net weer de tiende editie uitgekomen!

Lees in dit nummer artikelen over het ontwerp van netwerksegmentatie, de strategie van Juniper en de visie op OTP van SANS, naast een aantal artikelen over privacy en andere beveiligingszaken.

Lex Borger, hoofdredacteur

In dit nummer

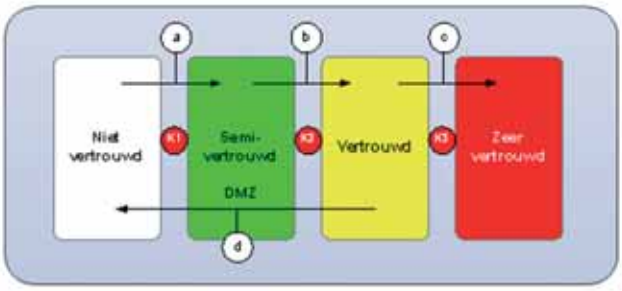
TO SEGMENT OR NOT TO SEGMENT

Een overzicht van nut en noodzaak van netwerksegmentatie

Segmentatie of zonering is geen doel op zich, maar een middel om bedrijfsdoelen te realiseren. Aan welke doelen kan je hierbij zoal denken? Hoe pak je het lastige onderwerp van segmentatie aan en waar begin je mee? Hoe voorkom je over-segmentatie? En wat is segmentatie überhaupt; hebben we het dan over fysieke scheiding of VLANS en moderne (virtuele) Next Generation Firewalls (NGFW's)? Dit artikel wil een overzicht geven van de mogelijkheden en inzicht geven in hoe segmentatie vorm te geven is binnen de eigen organisatie. Het artikel is mede opgesteld naar aanleiding van een informatiesessie zomer 2016 bij SURFnet met meer dan veertig deelnemers van diverse onderwijs- en onderzoeksinstellingen met presentaties van Technische Universiteit Delft, Radboud Universiteit Nijmegen, Wageningen University & Research en Fortinet.

Netwerksegmentatie is het opsplitsen van een netwerk in logische of fysieke gescheiden zones. Dit kan helpen bij het voldoen aan geldende wet- en regelgeving, informatiebeveiligingsbeleid, beperking van risico's en toezicht vereenvoudigen. De termen zonering en segmentatie worden vaak als elkaars synoniem gebruikt dan wel gecombineerd (bijvoorbeeld: 'segmentatie levert zones op').

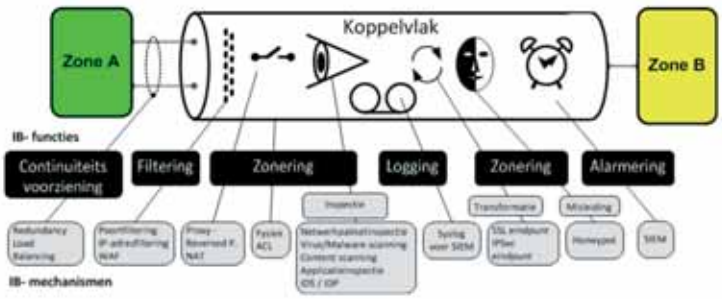
Het NORA-ontwerpkader IT-voorzieningen [1] definieert een zone als een afgebakend netwerk van IT-voorzieningen, waarbinnen gegevens met hetzelfde niveau van beveiligingsmaatregelen indien gewenst en toegestaan vrijelijk kunnen worden uitgewisseld. Informatie-uitwisseling tussen zones verloopt via gedefinieerde koppelvlakken, die de informatiestromen controleren (zie figuur 1).



Figuur 1 - Scheiding van infrastructuur door koppelvlakken [1].

Het informatiebeveiligingsmechanisme van een koppelvlak wordt nader uitgewerkt voor aspecten als logging, filtering, zonering, alarmering en beschikbaarheid (zie figuur 2). Dit zijn allemaal aspecten die relevant zijn bij de nadere inrichting van de verschillende segmenten.

Zonering is mogelijk via diverse technische maatregelen. Fysieke scheiding, VLAN's (Virtual Local Area Network), ACL's (Access Control List), NAC's (Network Access Control) en NGFW's (Next Generation Firewalls) zijn de meest gebruikte mechanismen



Figuur 2 - Overzicht mogelijke maatregelen van een standaard koppelvlak [1].

voor segmentatie. Op basis van het verschil in gevoeligheid tussen twee koppelvlakken ofwel de betrouwbaarheidseisen tussen zones zal voor een bepaalde techniek gekozen worden (zie tabel 1 ter illustratie [2]). VLAN's zijn meer een oplossing voor Traffic Management en het wordt tegenwoordig veelal niet meer geaccepteerd als security-mechanisme [3].

VLAN/ACL
ACL
Orchestration
Security Virtualizer
Virtual Firewall
Virtual Firewall in Appliance
Firewall
Data Diode
Air Gap

Tabel 1 - Segmentatiemaatregelen in volgorde van vertrouwen (van laag naar hoog) [2].

Raoul Vernède is Security Officer bij Wageningen University & Research. Hij is bereikbaar via raoul.vernede@wur.nl.

Segmentatie tussen verschillende zones kan plaatsvinden op basis van onder andere de volgende criteria:

- classificatie van informatie(systemen) ten aanzien van vertrouwelijkheid en integriteit (BIV-classificatie: Beschikbaarheid, Integriteit & Vertrouwelijkheid);
- trustlevel van end-point apparaten (variërend van onbekend tot managed en compliant apparaten)
- organisatiestructuur en geografische locaties van bedrijfsonderdelen;
- systeemstadia (Ontwikkel, Test, Acceptatie & Productie-omgevingen (OTAP) scheiden) en functie (zoals logging en monitoring/auditing).

Redenen voor segmentatie

Segmentatie kan bijdragen aan diverse businessdoelen en meer IT-gerelateerde doelen. Hieronder een nadere uitwerking van nut en noodzaak voor segmentatie. Sommige punten zijn met name relevant in de context van onderwijs- en onderzoeksinstellingen.

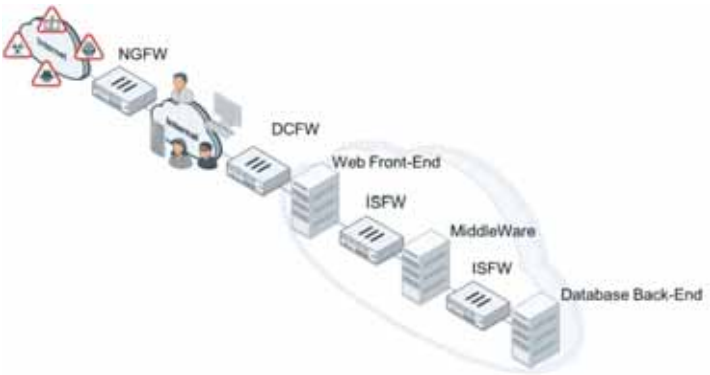
- **Defense in Depth-strategie:** Concept van een centrale firewall – perimeter die al het netwerkverkeer controleert – neemt af; netwerken zijn steeds opener en beveiliging moet meer bij de bron plaats vinden (zie ook de Jericho Geboden uit inmiddels 2007 [4]). Principe van centrale 'kasteelmuur' neemt af en wordt vervangen door Defense in Depth-strategie. Op dit moment is "de muur hard aan de buitenkant en zacht aan de binnenkant en verder eenmaal binnen wordt het verkeer als vertrouwd gezien". Feitelijk moeten we steeds meer uitgaan van een grenzeloze aanvalsoppervlakte (borderless attack surface). Mogelijk eindstation is microsegmentering van individuele hosts met behulp van Next Generation Firewalling (die vanuit governance-optiek idealiter via geautomatiseerde DevOps-achtige processen geborgd worden).
- **Informatiebeveiligingsbeleid:** Binnen het informatiebeveiligingsbeleid van organisaties wordt vaak aangegeven dat, voor de verschillend geclassificeerde informatie, passende beveiligingsmaatregelen genomen dienen te worden. In die beleidslijn is het hierdoor wenselijk om voor geheime en/of vertrouwelijke informatie (wat minimaal alle systemen met persoonsgegevens omvat) segmentatie toe te passen. Specifieke BIA's (Business Impact Analysis) kunnen aanvullend inzicht geven in risico's in relatie tot de genomen controlemaatregelen.
- **Best-practices en compliance:** In diverse best-practices (zoals ISO 27000, BIR, SURF Normenkader) en compliance kaders (zoals PCI) wordt als mogelijke controlemaatregel gesproken over scheiding van netwerken. In het kader van certificering dan wel toezicht zal daarom door een auditor ingegaan worden op de aanwezige zones van een organisatie en of deze een bijdrage leveren in het beschermen van data en identiteiten.
  Het is belangrijk te bedenken dat netwerksegmentatie alleen niet voldoende is voor compliance en dat voor bijvoorbeeld geprivilegieerde beheerders dergelijke scheidingen relatief makkelijk kunnen doorbreken. Dit is mogelijk indien de autorisaties te ruim staan, two-factor-authenticatie mist c.q. functiescheiding ontbreekt (als voorbeeld het signeren van broncode om te voorkomen dat backdoors geïntroduceerd worden).
- **Nieuwe IT-diensten en dienstendifferentiatie:** Door zonering wordt het mede mogelijk om nieuwe dan wel vanuit security en privacy oogpunt meer gedifferentieerde en flexibelere IT-diensten aan te bieden aan de interne gebruikers. Zodoende wordt het bijvoorbeeld mogelijk om Managed Servers aan te bieden met minder stringente security-eisen (meer 'speeltuin-achtige'-omgeving).
  Door segmentatie kan er meer 'maatwerk' worden geboden die voldoet aan de eisen en wensen van de gebruiker, waardoor alternatieven zoals externe clouddiensten en eigen servers (shadow-IT) minder snel nodig zijn voor de gebruiker. Eventueel gebruik van externe diensten dient hierbij natuurlijk altijd ook verder ingekaderd te worden met harde eisen op het gebied van governance en compliance. Segmentatie biedt hiertoe passende mogelijkheden.
- **Campus-ontwikkelingen en Derdenbeleid:** Het gebruik van delen van het netwerk van de universiteitscampus door derde partijen zoals spin-off bedrijven of samenwerkingspartners zal de komende jaren waarschijnlijk verder toenemen. Valorisatie van fundamenteel onderzoek naar de praktijk is een blijvende focus van de overheid. Tevens wil men gebouwen en ruimtes op de campus steeds flexibeler gaan inzetten voor eigen personeel of derden.
  Indien het gaat om werkzaamheden met een potentieel hoge financiële (intellectual property zoals patenten), politiek-gevoelige of militaire onderwerpen moet men serieus rekening houden met APT-achtige (Advanced Persistent Threat) spionageaanvallen van bedrijven en/of statelijke actoren. Afhankelijk van de specifieke situatie is fysieke scheiding onvermijdbaar en kan met behulp van segmentatie de benodigde scheiding binnen een gedeeld netwerk aangebracht worden.
- **Actieve monitoring en beheer:** Door het gebruik van segmenten kunnen monitoring en alerting van verdacht netwerkverkeer met behulp van SIEM-oplossingen (Security information and event management) en Next Generation Firewall-features (denk aan Deep Packet Inspection en IPS), zich richten op een beperkt aantal segmenten met daarin de cruciale systemen en informatie. Zeker voor onderzoeksinstellingen is het vaker ondoenlijk, vanwege de enorme datahoeveelheden en bijbehorende performance-aspecten en licentiekosten, om op de centrale firewall al het netwerkverkeer diepgaand te monitoren en te controleren. Zaken als Data Leakage Prevention en Digital Rights Management zijn voor bepaalde segmenten makkelijker in te richten. Tevens zijn er deels performancevoordelen mogelijk. Het netwerkverkeer wordt efficiënter verwerkt, omdat het niet per definitie door het complete netwerk heen hoeft, maar waar nodig binnen een segment blijft waar het voor bestemd is.
  Het opdelen van het netwerk kan het beheer overzichtelijker maken, doordat de gesegmenteerde delen qua beheer aan diverse personen/teams zijn toe te kennen. Denk bijvoorbeeld aan het datacenter en de campus dat ieder een aparte aanpak vereist.

Best practice implementatierichtlijnen

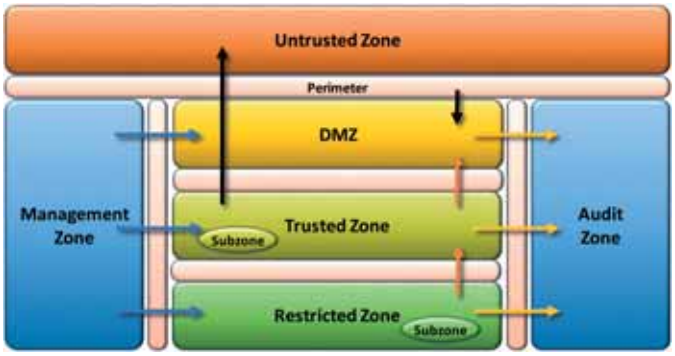
- Elke zone heeft een vastgesteld uniek beveiligingsdoel.
- Elke zone wordt slechts beheerd onder verantwoordelijkheid van één beheerinstantie (m.u.v. onvertrouwde derden).
- Een zone heeft een gedefinieerd beveiligingsniveau. D.w.z. een zone kent een gedefinieerd stelsel van samenhangende beveiligingsmaatregelen.
- De maatregelen van logische toegangsbeperking zijn van toepassing op alle IT-voorzieningen in een zone.
- Uitwisseling van gegevens tussen zones vindt uitsluitend plaats via een gedefinieerd koppelvlak.
- Zones kunnen worden onderscheiden door gebruikmaking van routering van datastromen, verificatie van de bron- en de bestemmingsadressen, door toepassing van verschillende protocollen, encryptietechnologie, partitionering of virtualisatie van servers, maar ook door fysieke scheiding. (BIR 11.4.7)
- Poorten diensten en soortgelijke voorzieningen geïnstalleerd op een computer of netwerkvoorziening die niet speciaal vereist zijn voor de bedrijfsvoering worden uitgeschakeld of verwijderd. (BIR 11.4.4)
- Er zijn aparte zones voor Ontwikkeling, Test, Acceptatie en Productie. (BIR 10.1.4.b)
- Vitale bedrijfsgegevens worden in een aparte zone geplaatst.
- De experimenteeromgeving (laboratorium/sand-box) is een fysiek gescheiden zone.
- Beheer van zones vindt plaats vanuit een eigen zone.
- IT-voorzieningen (zoals mobiele clients en werkstations) die buiten de fysieke toegangsbeveiliging van de gebouwen van de organisatie zijn opgesteld, worden in de externe zone (externe werkplek) gepositioneerd.
- Dataservers waarvoor een hoger beveiligingsniveau geldt dan het basisniveau kunnen in een eigen zone worden opgenomen. (BIR 11.6.2)
- Van werkstations wordt bepaald welke onderdelen tot welke zone behoren, gelet op de risico's van het onbevoegd ontsluiten van data via de verschillende soorten poorten. Om deze reden kan lokale opslag van gegevens op de vaste schijven van werkstations (bijvoorbeeld laptops) en opslag op verwijderbare opslagmedia worden geblokkeerd.
- Interne systemen wisselen gegevens uit met ketenpartners en klanten via een centrale interne zone (DMZ) en een vertrouwde externe zone.
- Voor de uitwisseling van gegevens met derden (niet openbare gegevens) worden besloten externe zones (vertrouwde derden) gebruikt.
- In een DMZ worden alleen openbare gegevens van een organisatie opgeslagen die in het uiterste geval verloren mogen gaan. (BIR 10.9.3.d)

Bron: NORA Katern-Informatiebeveiliging [1] met daarin verwijzingen naar de BIR (Baseline Informatiebeveiliging Rijksdienst) [12].

- **Impactbeperking en formeel bewijs bij datalekken:** Door middel van segmentatie is het mogelijk om de impact en de verspreiding van een incident te beperken (Lateral Spread). Denk hierbij aan bijvoorbeeld een netwerkloop, maar ook ransomware-infecties en datalekken.
  In het kader van de nieuwe Europese privacywetgeving moet bij een datalek aangetoond worden dat de toegang tot vertrouwelijke data beperkt was en er passende preventieve beveiligingsmaatregelen genomen waren. Adequate netwerksegmentatie naast zaken als two-factor-authenticatie, hardening en patchmanagement kunnen hierbij helpen richting de Autoriteit Persoonsgegevens.
- **Legacy-systemen en sand-boxed omgevingen:** Er is behoefte en noodzaak vanuit organisaties om sommige verouderde software operationeel te houden (denk binnen de onderzoekswereld aan dure analyseapparatuur met verouderde besturingssystemen of Java/Flash) dan wel een testomgeving waar een onderzoeker afgeschermd (sand-boxed) kan experimenteren met software. Met behulp van segmentatie zijn hiervoor maatwerkoplossingen in te richten.
- **BYOD en IoT:** De wens van medewerkers om met eigen apparaten (Bring Your Own Devices) te kunnen werken en informatie van binnenuit of van buitenaf te kunnen ontsluiten, is vandaag de dag heel normaal. In tegenstelling tot beheerde clients is van privéapparaten de staat van de security divers. Men moet ervan uitgaan dat een deel van deze apparaten met actuele systemen werken die niet zijn geüpdatet en/of geen virusscanner hebben. Tevens zorgt de opkomst van Internet of Things (userless devices die zijn geprogrammeerd om autonoom te werken dan wel met minimale userinterface) met een groot aantal inherent onveilige onbeheerde apparaten ervoor dat aanvullende maatregelen nodig zijn. Segmentatie kan voor beide ontwikkelingen een



Figuur 3 - Traditioneel vier lagen segmentatiemodel (NGFW: Next Generation Firewall, DCFW: Datacenter Firewall en ISFW: Internal Segmentation Firewall) [6].



Figuur 4 - Gelaagde netwerk architectuur [7].

oplossingsrichting bieden. Zo wordt het mogelijk om dynamische netwerktoegang naar een specifieke zone in te richten op basis van cryptografie en PKI op basis van certificaten (bijvoorbeeld 802.1x-certificaten) of agents (met toets een aantal specifieke security criteria). Hierbij kan men bijvoorbeeld kiezen om drie zones in te richten, te weten Untrusted, Semi-trusted en Trusted, dan wel om de Trusted en Semi-trusted zones samen te voegen.

- **Netwerktoegang IT-leveranciers:** Verdergaande gebruik en integratie van bestaande interne bedrijfssystemen van on-premise en off-premise dienstverlening zorgt voor nieuwe uitdagingen. Denk bijvoorbeeld ook aan de situatie dat een externe dienstverlener (geautomatiseerd) beheer moet kunnen uitvoeren op on-premise-servers. Segmentatie kan hierbij zorgen voor passende logische afscherming naar de andere systemen.

Naast alle genoemde voordelen en kansen zijn er natuurlijk ook een aantal nadelen en risico's. De twee belangrijkste zijn: performance en complexiteit. Indien de performance tussen segmenten beduidend afneemt door ongeschikte segmentatie, zal dit problemen opleveren. 'Slow is broken' is hierbij het adagium. Maar ook een toenemende complexiteit bij het oplossen van incidenten en problemen is een uitdaging. Voorkom over-segmentatie [5] en houd het ontwerp simpel en daardoor beheersbaar. Complexiteit is uiteindelijk de vijand voor beveiliging.

Zoneringsmodellen

Traditioneel wordt vaak gebruikgemaakt van het 'vier lagen-model', waarbij er onderscheid gemaakt wordt tussen het Noord-Zuid-netwerkverkeer (DC: internet-datacentrum) en Oost-West-verbindingen binnen het DC (zie figuur 3 [6]). Tussen elke laag is hierbij een scheiding door bijvoorbeeld een firewall (FW) aangebracht. Binnen het DC wordt op basis van het Three Tier-principe van Web Front-end, Middleware en Database Back-end een zonering aangebracht. Hierbij kan de Front-end enkel met de Middleware verbinden en de Middleware enkel met de Back-end.

Een volgende stap is om, indien de organisatie gebruikmaakt van Software Defined Networking (SDN) voor het DC, zelfs op host-niveau te segmenteren (=microsegmentatie) binnen de virtuele omgeving. En zo ontstaat een beeld van een gelaagde netwerkarchitectuur met gebruikelijke toevoegingen zoals een control/management zone, audit zone en plaatselijke subzones (zie figuur 4 voor een voorbeeld).

Praktische uitwerking

Hoe kan je als organisatie nu praktische invulling geven aan segmentatie en komen tot een passend zonemodel voor je eigen organisatie? Vaak is het bestaande netwerk vanuit het verleden al meer of minder opgedeeld in logische elementen en zal dat als basis dienen voor een toekomstige aanpak. Tevens zal men rekening moeten houden met de in gebruik zijnde clouddiensten en overige integraties (filetransfers, webservices, API-gateways, enzovoorts).

Hieronder een nadere grove uitwerking van de fasen hoe men zou kunnen komen tot hoog niveau ontwerp zonemodel met een aantal praktische tips (deels specifiek onderwijs- en onderzoeksinstellingen). Grofweg wordt onderscheid gemaakt in de volgende fases:

1. Bepalen en prioriteren doelen (welke risico's afdekken of kansen realiseren);
2. In kaart brengen huidige situatie netwerk;
3. Iteratief ontwerpen hoog niveau ontwerp zonemodel;
4. Uitwerken verkeersstromen tussen zones en bepalen technische maatregelen.

Een multidisciplinair team, waarin onder andere de klantorganisatie, securitymanagement, architecten en riskmanagers vertegenwoordigd zijn, start met de specifieke eigen organisatiedoelen (zoals eerder in dit artikel nader uitgewerkt) die men wil realiseren. De onderliggende vraag daarbij is: 'Welke business- en IT-doelen worden met behulp van segmentatie gerealiseerd?'. Segmentatie als controlemaatregel kan helpen om risico's af te dekken dan wel kansen te realiseren. Niet alle doelen zijn even belangrijk en dus specifieke voor de eigen organisatie op basis van een risicoanalyse geprioriteerd moeten worden (cruciaal,

gemiddeld en nice to have).

Aansluitend zal een gedetailleerde inventarisatie van de huidige situatie (IST-situatie) gemaakt moeten worden om de delta te kunnen bepalen. Vaker is de huidige situatie door de jaren heen complexer dan zoals bijgehouden in de documentatie. In kaart gebracht moeten worden onderwerpen als:

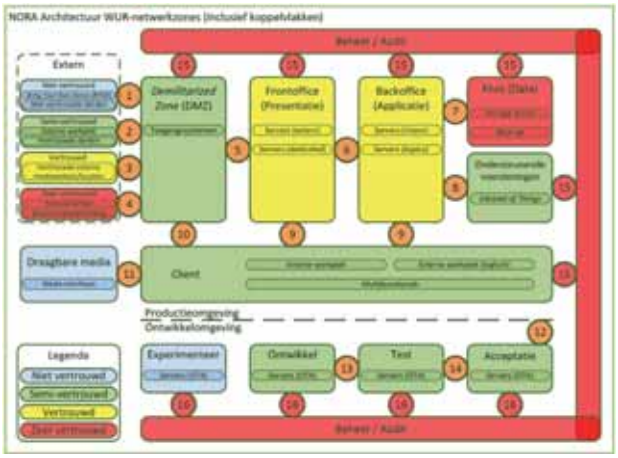
- huidige netwerksegmentatie;
- gebruikersgroepen (medewerkers, gasten, externen, studenten, enzovoorts);
- (Informatie)classificatie van systemen;
- type apparaten (beheerde apparaten, BYOD of IoT zoals koffieapparaten, printers, regelsystemen, presentatieschermen, analytische apparatuur, brandmelders, kassa's, toegangssystemen, domotica, thermostaten, enzovoorts);
- type netwerkstromen (hoeveelheden data en type protocollen).

Op basis van de eerder gedefinieerde must-have doelen, kan vervolgens in een subgroep gestart worden met het iteratief ontwerpen van verschillende mogelijke zonemodellen. Uiteindelijk zal dit divergeren naar een of meerdere scenario's met bijbehorende voor- en nadelen. Het is hierbij cruciaal om de implementatie en het onderhoud van segmentatie realistisch in te schatten en dus de eigen vaardigheden en maakbaarheid van oplossingen niet te overschatten. Bevindingen dienen besproken te worden met het eerdergenoemde multidisciplinaire team en uiteindelijk zal een model gekozen worden dat verder technisch uitgewerkt dient te worden.

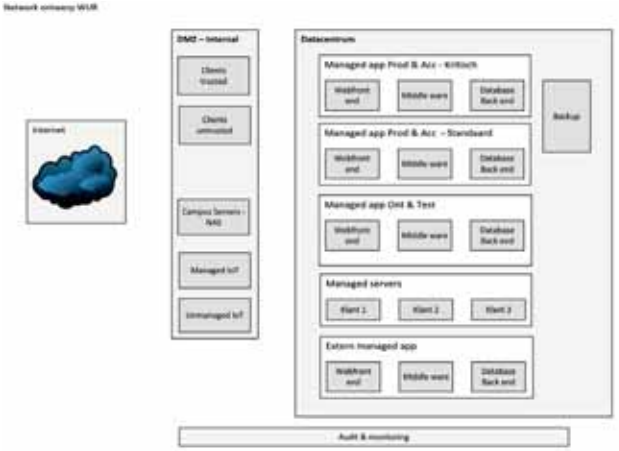
Bij het ontwerpen van een zonemodel kan als basis gebruikt gemaakt worden van de NORA [1] best-practice implementatierichtlijnen uit het kader hieronder (met verwijzingen naar de BIR: Baseline Informatiebeveiliging Rijksdienst). De diverse punten zullen wel verder geconcretiseerd en aangepast dienen te worden naar de eigen organisatie.

Naar aanleiding van de informatiesessie en na bestudering van diverse bronnen (waaronder [8], [9]) zijn de volgende hierop aanvullende algemene maar soms ook zeer specifieke adviezen en tips relevant bij de uitwerking van het een eigen zonemodel en bijbehorende koppelvlakken onderling (in willekeurige volgorde en mede afhankelijk van wat men wil bereiken met segmentatie):

- Probeer het aantal segmenten beperkt te houden; uiteindelijk is complexiteit de vijand van informatiebeveiliging. Begin klein maar creëer ruimte om op termijn te groeien (eventueel zelf naar micro-segmentatie).
- Richt per niveau informatieclassificatie minimaal één segment in. Zo dienen bijvoorbeeld informatiesystemen voor de elektronische afname van examens gescheiden te zijn van andere netwerksegmenten.
- Denk na over de consequenties voor het netwerkontwerp van een toekomstige invoering van IPv6 (zeker bij dual stack oplossingen).
- Houd servers en werkplekken apart. Servers bevatten over het algemeen meer vertrouwelijke data en zijn interessanter voor misbruik. Ze dienen dan ook beter afgeschermd te worden en regelmatig gescand te worden op kwetsbaarheden.
- Houd rekening met de mogelijkheid voor een dynamische segmentatie via NAC (network access control) van end-points op basis van bijvoorbeeld de aan- of afwezigheid van een 802.1x client certificaten of agents. Denk bijvoorbeeld aan eigen beheerde apparaten versus BYOD of IoT.
- Houd ook rekening met de performance indien grotere datastromen tussen segmenten afgewikkeld dienen te worden.
- Maak niet zo zeer onderscheid in type gebruikers of bedraad versus draadloze netwerkverbindingen. De betrouwbaarheidsniveaus van verschillende end-points van gebruikers zijn meer divers (bijvoorbeeld BYOD versus managed client) en daardoor meer bepalend voor de inrichting van segmenten. Absoluut gezien blijft draadloos natuurlijk kwetsbaarder dan bedraad.
- Richt geen aparte segmenten voor VPN of tunneling in het algemeen. Dit is een maatregel, die tussen elke zone door de koppelvlakken in geregeld kan worden.
- SSL/TLS off-loading voor Deep Packet Inspection van encrypte web-verbindingen op de firewall dan wel loadbalancer is niet wenselijk. Door het off-loaden zullen browsers certificaat foutmeldingen geven bij de gebruikers. Het lijkt beter om op de clients zelf passende preventieve en detectieve tools te installeren. Voor eigen beheerde apparaten is de installatie hiervan eenvoudig en voor BYOD zou dit via een onboarding proces kunnen verlopen. Wil men wel centraal Deep Packet Inspection uitvoeren en zaken als Perfect Forward Secrecy afdwingen, dan zal men gebruik moeten maken van SSL-offloaders en Reverse Proxies.
- Houd IoT- en gebruikersverkeer apart. IoT-verkeer (vaak niet gekoppeld aan specifieke gebruiker waardoor de herleidbaarheid lastiger is) is veel homogener en abnormaliteiten kunnen makkelijker gedetecteerd worden.
- Richt aanvullende controlemaatregelen, zoals two-factor-authenticatie, in voor de toegang van hoog geprivilegieerde beheerders tot specifieke netwerksegmenten.
- Regel voor uitgaand verkeer minimaal Reputation Filtering in, waarbij er gezorgd wordt dat er geen connecties met bijvoorbeeld kwaadaardige command-and-control-servers gemaakt worden. Beperk uitgaand verkeer verder weinig voor het client-segment. Voor serversegmenten is aanvullende analyse van uitgaand verkeer wel wenselijk (bijvoorbeeld anomaliedetectie). Laat database-servers uitsluitend verbinden met bekende interne servers op basis van IP-nummers/ranges.
- Gebruik een generieke Proxy of Reversed Proxy, al dan niet in de vorm van een WAF (Web Application Firewall), als beschermingslaag voor kwetsbare webapplicaties. Regel de bescherming van de webapplicaties niet op iedere service apart in.
- Sta het pingen (ICMP-verkeer) van servers overal toe; dit is cruciaal voor beheer om te checken of systemen beschikbaar zijn. Als dit niet kan, richt dan in dat systemen zich via een heartbeat melden



Figuur 5: Concept ontwerp netwerksegmentatie Wageningen University & Research [10].



Figuur 6: Concept ontwerp netwerksegmentatie Wageningen University & Research [10].

bij een centraal logsysteem of SIEM.
- Denk goed na welke managementtooling bij welke apparaten en systemen moet kunnen komen. Zo wil Altiris bijvoorbeeld toegang tot de beheerde werkplekken.
- Voer binnen belangrijke segmenten regelmatig Discovery Scans uit en bepaal eventuele verschillen met de CMDB (Configuration Management Database).

Hieronder een tweetal eerste conceptuele uitwerkingen voor netwerksegmentatie voor Wageningen University & Research (zie figuur 5 en 6). Het eerste ontwerp is met name gebaseerd op de NORA-aanpak en de tweede is een nieuw ontwerp.

Indien men intern overeenstemming heeft kunnen vinden over het high level design is de volgende stap het opstellen van een van-naar verkeersmatrix [11]. Hierbij wordt per segment aangegeven welk netwerkverkeer toegestaan is dan wel geweerd wordt en welke aanvullende controlemaatregelen (monitoring, IPS/IDS, enzovoorts) noodzakelijk zijn. De gekozen maatregelen dienen als baseline en zullen door de tijd heen risk-gebaseerd geëvalueerd moeten worden om te bepalen of ze nog steeds afdoende zijn.
Verder is het belangrijk om na te denken over het centrale beheer en de governance van de segmentatieregels. Zijn er passende procedures voor wijzigingsverzoeken en bestaan er passende exportmogelijkheden om overzicht te behouden en audits kunnen uitvoeren?

Aansluitend kan een technisch ontwerp gemaakt worden en overgegaan worden tot geleidelijke implementatie binnen de organisatie.

Conclusie

Netwerksegmentatie biedt kansen om informatie passend te beschermen en doelstellingen van de primaire business te realiseren. De inrichting van de segmentatie dient hierbij goed aan te sluiten bij het type organisatie en de business-sector waarin het opereert. Tevens is de volwassenheid van de IT-beheerorganisatie bepalend voor een succesvolle implementatie en onderhoud van netwerksegmentatie. Er dient een balans gevonden te worden tussen geen of te beperkte segmentatie en een te complexe en lastig beheerbare over-segmentatie. Sec segmentatie inrichten zonder verdere inbedding met andere securitymaatregelen is onvoldoende. Er zal invulling gegeven moeten worden aan zaken als netwerkverkeer monitoring en alerting; policy management, auditing en two-factor-authenticatie voor toegang van geprivilegieerde beheerders tot specifieke netwerksegmenten.

Referenties

[1] NORA Katern–Informatiebeveiliging - Ontwerpkader IT-voorzieningen Versie 0.11 2013: http://bit.ly/2q1QiSQ
[2] Best Practices in Network Segmentation for Security door Greg Young - 2016 – Gartner
[3] Virtual LAN Security: weaknesses and countermeasures – SANS – 2003: http://bit.ly/20YpXh2
[4] Jericho Commandments – 2007 – Open Group: http://bit.ly/1mci81k
[5] Avoid These "Dirty Dozen" Network Security Worst Practices door Andrew Lerner & Jeremy D'Hoinne – Gartner – 2015
[6] Fortinet presentatie – Ton Sips – 2016
[7] Adaptive Zone Defense: http://bit.ly/2pdtU61
[8] Zonering - Zonemodel voor de Radboud Universiteit door Harrie Harings – 2015 (niet openbaar)
[9] Network segmentation and segregation – Australian Government Department of Defence – 2012: http://bit.ly/2oOKed2
[10] Stageverslag – Netwerksegmentatie bij Wageningen University & Research door Mike Slotboom – 2016 (niet openbaar)
[11] AlgoSec video presentaties: http://bit.ly/2oG6kgz & http://bit.ly/2pZTFXw
[12] BIR: http://bit.ly/2oHMeDa

Mr. Rachel Marbus
@rachelmarbus op Twitter

DE PRIVACYMALLOOT

Er is een speciaal soort privacyadviseur opgestaan en deze heeft zich de afgelopen tijd goed vermenigvuldigd. Ik noem het de privacymalloot. Mind you, ze zijn er eigenlijk altijd wel geweest hoor, maar dat was een verdwaalde privacymalloot (zoiets als een fan van Nickelback; ze zijn er, maar niet zoveel en het is toch een beetje schaamtevol). Iedereen 'in the scene' wist wel wie deze malloten bij naam en toenaam waren, zodat al te grote bedrijfsongelukken vermeden konden worden. Leven en laten leven, maar niet aannemen om je klussen op te knappen.
De aanstaande Algemene Verordening Gegevensbescherming (AVG) heeft ervoor gezorgd dat inmiddels heel veel mensen ineens privacyspecialist zijn geworden, sterker nog, er zijn ook allemaal Privacy Officers volgens cv's, LinkedIn en verwante momenten waar je met (gefingeerde?) kennis en kunde kunt strooien. Het is ook best lastig om het kaf van het koren te scheiden als je er zelf niet enorm veel verstand van hebt – je wil vaak namelijk iemand inhuren/aannemen juist omdat het je zelf aan kennis ontbeert. En het beroep Privacy Officer is geen beschermd beroep. Een echte opleiding is er ook niet, alhoewel je inmiddels op een heel aantal plekken wel echt erg goede cursussen hebt over privacy.

Je hebt ze in alle kleuren en smaken overigens, die malloten. Zo had ik er laatst nog een aan de telefoon die me iets wilde verkopen zodat ik "beter kon omgaan met het proces rondom datalekken want die moest ik toch gaan melden onder de AVG". Die persoon toch maar verteld dat de Telecomsector al jaar en dag een meldplicht kent en dat die zo'n beetje het licht hebben uitgevonden als het gaat om het melden van datalekken. En dat iedereen in Nederland dat al moet sinds januari 2016. Het gesprek duurde niet lang meer daarna. Een andere malloot had een clubje op het cv staan waarvan de titel deed suggereren dat het een vereniging was (waarvan deze boardmember was) waar (alle?) Data Protection Officers lid van zijn. U begrijpt, ik heb connecties in deze wereld… dus vroeg ik aan alle mij bekende Privacy Officers of zij ooit van die club gehoord hadden. Wat denkt u? Niemand!

Er is al een tijdje een schrijnend tekort aan goede privacyspecialisten, de meesten zitten prima waar ze inmiddels zitten en het is niet een enorm grote beroepsgroep. Zeker niet daar waar het mensen met tien jaar (en meer) ervaring betreft. En veel organisaties hebben dringend behoefte aan privacyspecialisten. Sterker nog, veel gaan ook echt wettelijke Privacy Officers nodig hebben (de Functionaris Gegevensbescherming). Voor de beroepsgroep natuurlijk geweldig, iedereen weet wat er gebeurt als de vraag hoog is en het aanbod laag. Maar, de keerzijde is dus ook dat er meer privacymalloten de markt vervuilen. Wat ik nu ga zeggen, lijken allemaal open deuren. Maar gezien de enorme toestroom op de arbeidsmarkt, is het niet overbodig. Een aantal tips als je privacyadviseurs gaat aannemen:

1) **Staar je niet blind op het cv, iedereen kan cursussen privacy volgen, maar niet iedereen kan privacy toepassen in de praktijk. Vraag dus door en leg desnoods wat kleine inhoudelijke vragen voor.**
2) **Vraag om referenties en bel die op.**
3) **Vraag een beetje om je heen of de persoon bekend is in het veld.**

En hopelijk kun je zo de grootste privacymalloten vermijden.

PRIVACY BY DESIGN EN PRIVACY BY DEFAULT IN DE AVG

In de Algemene Verordening Gegevensbescherming (AVG) worden privacy by design en privacy by default verplicht gesteld voor aanbieders van producten en diensten die persoonsgegevens verwerken. Het idee is dat organisaties in een vroeg stadium zowel technisch als organisatorisch een zorgvuldige omgang met persoonsgegevens afdwingen en privacyvriendelijke standaardinstellingen hanteren. In dit artikel zal ik dieper ingaan op deze twee begrippen en de impact die ze met zich brengen voor organisaties.

Het begrip privacy by design is niet nieuw. In de jaren '90 is privacy by design voor het eerst gebruikt door Ann Cavoukian, indertijd informatie & privacy commissaris in Canada. Het concept is door haar ontwikkeld om tegenwicht te kunnen bieden aan de groei van informatie- en communicatietechnologieën alsmede grootschalige netwerksystemen die data verwerken en de hiermee gepaard gaande privacyrisico's [1]. Rond diezelfde periode is in 1995 de huidige Europese Privacyrichtlijn [2] tot stand gekomen, ook vanwege de noodzaak om in het licht van de toegenomen informatie- en communicatietechnologieën persoonsgegevens adequaat te beschermen. Artikel 17 van de Privacyrichtlijn omvat de verplichting voor organisaties om passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen. Hoewel dit artikel niet expliciet de verplichting bevat om al bij de inrichting van informatiesystemen rekening te houden met gegevensbescherming, is overweging 46 van de Privacyrichtlijn hier concreter over: "Overwegende dat de bescherming van de rechten en vrijheden van de betrokkenen in verband met de verwerking van persoonsgegevens zowel bij het ontwerpen als bij de uitvoering van de verwerking passende technische maatregelen vergt, in het bijzonder om de veiligheid te waarborgen en zodoende elke ongeoorloofde verwerking te verhinderen (…)".

Deze verplichting uit de Privacyrichtlijn om passende beveiligingsmaatregelen te treffen, is vertaald in artikel 13 van de Nederlandse Wet Bescherming Persoonsgegevens [3]. In 1999 is dit artikel uitgebreid naar aanleiding van een amendement inzake 'privacy enhancing technologies'. De toelichting bij dit amendement maakt duidelijk dat de beveiligingsverplichting van artikel 13 zich uitstrekt tot alle onderdelen van het proces van gegevensverwerking. Juridische (beveiligings)normen moeten worden vertaald in de feitelijke inrichting en verdere ontwikkeling van informatiesystemen [4]. Ook deze toelichting maakt duidelijk dat al bij de inrichting van informatiesystemen de normen omtrent gegevensbeveiliging moeten worden nageleefd.

Zowel uit de Europese Privacyrichtlijn als de Nederlandse Wet Bescherming Persoonsgegevens vloeit impliciet al de verplichting voort om bij de inrichting van informatiesystemen rekening te houden met gegevensbescherming [5]. We leven inmiddels in een nóg meer digitale wereld dan in de jaren '90, waarin privacy by design als een belangrijk speerpunt voor privacybescherming wordt gezien. Privacy by design en privacy by default zijn daarom nu expliciet opgenomen in de Algemene Verordening Gegevensbescherming waar zij in de Nederlandse vertaling 'gegevensbescherming door ontwerp' en 'gegevensbescherming door standaardinstellingen' heten.

Privacy by design

Privacy by design is de plicht voor organisaties om reeds in de ontwikkelfase van informatiesystemen en diensten privacyverhogende maatregelen te treffen, zogeheten privacy enhancing technologies. Systemen moeten daarom technisch op een dusdanige wijze worden ingericht dat bijvoorbeeld passende bewaartermijnen worden nageleefd, rekening wordt gehouden met dataminimalisatie en zo veel mogelijk persoonsgegevens worden geanonimiseerd of gepseudonimiseerd. Privacy by design biedt tegenwicht aan de groeiende toegankelijkheid en herleidbaarheid van persoonsgegevens. Organisaties treffen in een vroeg stadium technisch afdwingbare

maatregelen die bijdragen aan een verantwoorde omgang met persoonsgegevens. Dit zorgt ervoor dat privacyrisico's worden gemitigeerd. Tegelijkertijd wordt privacy een kerncomponent van producten of diensten. Belangrijker nog is dat het gebruik van privacy by design bijdraagt aan een correcte verwerking van de persoonsgegevens van individuen. Het niet hanteren van privacy by design tijdens de ontwikkeling van producten en diensten kan ertoe leiden dat een organisatie in een later stadium alsnog kostbare aanpassingen moet doen om privacy by design met terugwerkende kracht door te voeren ('privacy by re-design') of dat bij bepaalde innovaties of trajecten zelfs volledig de stekker eruit getrokken moet worden.

Privacy by default

Privacy by default houdt in dat de standaardinstellingen en -functies van een programma of dienst op de meest privacyvriendelijke stand zijn ingesteld. De gebruiker krijgt zelf de regie in handen over het gebruik van zijn persoonsgegevens: dus opt-in in plaats van opt-out en persoonsgegevens worden alleen gedeeld na toestemming van de gebruiker. Het gaat echter niet alleen om instellingen en functies. Ook algemene voorwaarden moeten privacyvriendelijk zijn geschreven, zonder verstopte privacyonderwerpen op een plaats waar ze niet thuishoren. Diensten zoals sociale netwerken zullen veel met privacy by default te maken krijgen. Gebruikers delen hun persoonsgegevens op sociale netwerken, waarbij zij zelf de zichtbaarheid van hun gegevens kunnen instellen. Sociale netwerken willen daarnaast graag zo veel mogelijk interessante informatie ontvangen van hun gebruikers, om de voor de hand liggende reden dat deze informatie vanuit commercieel oogpunt waardevol is. Deze diensten hebben dan ook baat bij standaardinstellingen die zijn gericht op het delen en verschaffen van zo veel mogelijk informatie. Gebruikers accepteren deze standaardinstellingen veelal blindelings, zonder zich te verdiepen in de lange en vaak onleesbare voorwaarden. Veel gebruikers zijn zich er daarom vaak niet van bewust welke privacyinstellingen ze hebben geaccepteerd. Ter bescherming van deze gebruikers dienen de standaardinstellingen privacyvriendelijk en veilig te zijn. Privacy by default geldt echter niet alleen voor sociale netwerken. Alle diensten die standaard privacyinstellingen gebruiken zullen privacy by default moeten omarmen.

Ter vergelijk

Beide begrippen zijn verwant aan elkaar, ze beogen allebei privacy vanaf de ontwikkelfase maximaal te integreren in producten en diensten en betrokkenen controle te geven over het gebruik van hun persoonsgegevens. Privacy by default kan als een onderdeel van privacy by design worden gezien. Het grote verschil tussen beide begrippen is dat privacy by design vooral van toepassing is op de ontwikkeling van nieuwe producten en diensten, terwijl privacy by default in het leven is geroepen voor producten en diensten waarbij gebruikers zelf de mogelijkheid hebben hun persoonsgegevens te ontsluiten, zoals bij sociale netwerken.

Wat leveren privacy by design en privacy by default mij op als organisatie?

Het ideale scenario is dat informatiesystemen na toepassing van privacy by design en privacy by default dusdanig zijn ingericht dat de privacy van betrokkenen conform de privacywetgeving wordt beschermd. Toepassing van privacy by design staat niet per definitie in de weg van de ontwikkeling van informatiesystemen waarin persoonsgegevens worden verwerkt. Het kan wel implicaties hebben voor de inrichting van dergelijke systemen. Een organisatie die privacy by design en privacy by default in een vroeg stadium van de implementatie van informatiesystemen en standaardinstellingen hanteert, zal hier voordeel uithalen vanuit een compliance oogpunt. Deze aanpak stelt organisaties in staat om hun wettelijke verplichtingen na te leven, doordat potentiële problemen vroegtijdig zullen worden gesignaleerd. Corrigerende maatregelen zullen hierdoor minder impactvol zijn. Ook kunnen organisaties concurrentievoordeel behalen door het naleven van privacy by design. Organisaties zullen wel moeten, klanten zullen hier straks expliciet om gaan vragen. Privacy by design en privacy by default horen daarom tot in het DNA van organisaties door te dringen.

Referenties

[1] Ann Cavoukian. 'Privacy by design: The 7 foundational principles.' Information and Privacy Commissioner of Ontario, Canada, 2009.

[2] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

[3] Elke Europese lidstaat heeft op basis van de Europese Privacyrichtlijn zijn eigen privacywet opgesteld. De implementatie van deze Privacyrichtlijn in de Nederlandse wetgeving heeft geresulteerd in de Wet Bescherming Persoonsgegevens.

[4] Kamerstukken II, 1999-2000, 25892, nr. 22.

[5] J.B. Schmaal, 'Privacy by design', Juridisch up to date 2010, nummer 5, p. 23.

Zakaria Abassi is Legal Counsel bij Pon. Hij is bereikbaar via zakaria.abassi@pon.com.

DE KRACHT VAN HET PRIVACY IMPACT ASSESSMENT

Met nog ruim een jaar te gaan tot de Algemene Verordening Gegevensbescherming (AVG) van toepassing wordt, zijn de meeste organisaties als het goed is begonnen met (het voorbereiden van) de implementatie er van. Met het van kracht worden van de AVG moet elke organisatie verplicht op relevante bedrijfsprocessen en informatiesystemen een Privacy Impact Assessment (PIA) uitgevoerd hebben. Maar wat is nou eigenlijk zo'n assessment? En wat is een goede manier om (op een pragmatische wijze) met een PIA te starten?

Een Privacy Impact Assessment is een gestructureerde manier om na te denken over het op de juiste wijze verwerken van persoonsgegevens binnen een organisatie. Een PIA helpt je in kaart te brengen welke gegevens verwerkt worden, hoe gevoelig de gegevens zijn en wie er bij de verwerking betrokken is. Vervolgens helpt een PIA je om zicht te krijgen op zaken als afspraken met derden, de beoogde wijze van het verzamelen en gebruiken van persoonsgegevens, transparantie naar de betrokkenen, het beperken van de risico's voor de organisatie en de betrokkenen en natuurlijk de beveiliging van de gegevens.
Door een PIA uit te voeren, de juiste aandachtspunten te benoemen en vervolgens te adresseren, wordt een organisatie geholpen om op een overzichtelijke manier aan de privacywetgeving te voldoen.

Modellen

In Nederland zijn een aantal bekende PIA-modellen gepubliceerd. Zo heeft SURF een PIA-model en -tool (in Excel) beschikbaar gesteld aan aangesloten instellingen. Binnen de Rijksoverheid is een toetsmodel opgesteld waarmee de uitvoering van een PIA wordt ondersteund. Daarnaast heeft NOREA (de beroepsorganisatie van Register EDP Auditors) samen met onder andere de Auditdienst Rijk een PIA-model ontwikkeld en ter beschikking gesteld. Het NOREA-model is voorzien van een praktische en uitgebreide vragenlijst die elke organisatie in staat stelt om een goede PIA uit te voeren.

PIA als gespreksmodel

Een Privacy Impact Assessment is bedoeld om bij de ontwikkeling van een product of dienst op passende wijze aandacht te besteden aan het op een juiste manier verwerken van persoonsgegevens. De PIA dwingt een organisatie om grondig na te denken over de wijze waarop de betrokken persoonsgegevens verwerkt worden. De discussies die hierdoor ontstaan, helpen om in de breedte over een nieuw product of dienst na te denken. Welke gegevens heb ik eigenlijk nodig om mijn doel te bereiken? Hoe belangrijk zijn de juistheid en de vertrouwelijkheid van de gegevens daarbij voor de organisatie? En hoe wissel ik de gegevens veilig uit? Het komt niet zelden voor dat de PIA de aanleiding is om grondiger over dit soort vragen na te denken. En hoe eerder je dit in een project met alle betrokkenen doet, hoe efficiënter iedereen er in zijn werkzaamheden rekening mee kan houden. Hiermee heeft de PIA een veel breder nut dan privacy alleen. Want iets direct op de juiste wijze uitvoeren, is goedkoper dan iets achteraf corrigeren. Het uitvoeren van een PIA verdient zichzelf hierdoor vrijwel altijd terug en wordt over het algemeen door de meeste betrokkenen als zeer nuttig ervaren.

Betrokkenen

Bij het uitvoeren van een PIA is het belangrijk dat medewerkers met de juiste kennis van het product of de dienst aan tafel zitten met medewerkers die over de juiste technische kennis beschikken. Daarnaast is het belangrijk om een goede risicoweging van de benoemde aandachtspunten te kunnen uitvoeren en om acties direct toe te kunnen wijzen. Vraag daarom altijd de eindverantwoordelijke/budgethouder van een product of dienst om bij de impact analyse aanwezig te zijn. Daarnaast kunnen productontwikkelaars, business analisten en/of (IT) architecten vaak veel toegevoegde waarde leveren. De rol van de security officer en/of privacy officer is over het algemeen bij voorkeur ondersteunend.

Succesfactoren

Hoewel de kwaliteit van het model erg belangrijk is om een goede PIA uit te voeren, zijn er ook andere factoren die bijdragen aan het succes. Zo is het met de PIA van NOREA eenvoudig om aan de hand van een ja/nee vragenmodel tot adviezen te komen die helpen om verantwoord met persoonsgegevens om te gaan en om daarmee invulling te geven aan de privacywet. Maar afhankelijk van de dienst of het product waar het assessment betrekking op heeft, kan het feitelijke bedrijfsrisico natuurlijk verschillen. Door tijdens het

Maarten Hartsuijker is redacteur bij IB-Magazine, security consultant en tevens de bouwer van het Online Privacy Impact Assessment van Classity. Maarten is bereikbaar via pvib@classity.nl.

Classity heeft op basis van het NOREA-model een online tool gemaakt waarmee het makkelijker wordt om van de PIA een succes te maken

assessment tevens een goede risicoweging (kans x impact) mee te nemen, kunnen de resultaten van de PIA eenvoudig tot gewogen besluiten leiden. Afhankelijk van het risico kan er bijvoorbeeld gekozen worden om risico's te accepteren, te reduceren, volledig weg te nemen of om eventuele gevolgschade te verzekeren. Daarnaast is het verstandig om tijdens een PIA niet alleen de privacy-impact in kaart te brengen, maar om vervolgacties direct zo goed mogelijk toe te wijzen aan betrokken personen. Hiermee wordt voorkomen dat aan het eind van een uitgevoerd assessment weliswaar bekend is waar de uitdagingen liggen, maar nagelaten wordt om tot concrete opvolging te komen.

Het is ook aan te raden om direct na het afronden van een PIA af te spreken wie de opvolging van de PIA gaat bewaken en wanneer de voortgang van de opvolging wordt besproken. Dit geeft de actiehouders een datum om naar toe te werken en voorkomt dat de PIA leidt tot ambities zonder vervolg. Het is verleidelijk om actiepunten uit de PIA te beleggen bij een security of privacy officer. Het is echter vaak verstandiger om deze functionarissen de PIA te laten ondersteunen met kennis en advies. Het goed opvolgen en prioriteren van acties werkt vaak het beste als de verantwoordelijkheid voor de opvolging zo dicht mogelijk bij de business-/systeem-/proceseigenaar wordt belegd. Na de opvolging van de aandachtspunten uit de PIA kunnen de security en privacy officer waar relevant nog een eindcontrole uitvoeren om vast te stellen dat het resultaat aan alle uitgangspunten van de organisatie en de privacywet voldoet.

Classity heeft op basis van het NOREA-model een online tool gemaakt waarmee het makkelijker wordt om van de PIA een succes te maken. De tool helpt om op een eenvoudige en gestructureerde wijze tot een geautomatiseerde PIA-rapportage te komen. Hiermee komt het zelf uitvoeren van een PIA voor iedereen binnen bereik en daarnaast neemt de uitvoeringstijd (en met name de rapportagetijd) er mee af.

Veranderende aandachtspunten door de AVG

De Algemene Verordening Gegevensbescherming introduceert verschillende nieuwe aandachtspunten die nog niet (volledig) in de huidige, vrij beschikbare, PIA-modellen zijn geïntegreerd. Privacy-bewuste ontwerpprincipes ('by design' en 'by default') zijn nadrukkelijker gepositioneerd. Ook geeft de AVG betrokkenen diverse nieuwe rechten, zoals het recht op overdraagbaarheid, het recht op beperking van de gegevensverwerking, het recht om niet te worden onderworpen aan profilering en het recht om vergeten te worden. Daarnaast dient een organisatie een register van de verwerkingsactiviteiten op te zetten. Dit is een documentatieplicht die ter vervanging van de aanmelding van een verwerking bij de Autoriteit Persoonsgegevens is geïntroduceerd. De impact van sommige veranderingen die met de AVG van kracht worden, is erg groot. Zo kan het beperken van de gegevensverwerking van een individuele betrokkene binnen een specifiek informatiesysteem erg complex zijn. Organisaties doen er daarom goed aan om ook dit soort aandachtspunten al ruim voor het van toepassing worden van de AVG mee te nemen in de ontwikkeling van nieuwe producten en diensten (of om noodzakelijke aanpassingen door te voeren in bestaande producten en diensten).

Begin dus op tijd

De Algemene Gegevensverordening is vorig jaar in werking getreden. Organisaties hebben tot eind mei 2018 om hun producten en diensten aan deze nieuwe wet te laten voldoen. Op dat moment wordt de AVG volledig van toepassing en kan de naleving worden gehandhaafd. Stel het uitvoeren van een Privacy Impact Analyse daarom niet te lang uit en breng in kaart op welke punten de privacy van producten en diensten verbeterd kan worden. Dit maakt de kans kleiner dat de verwerkte persoonsgegevens (met het in werking treden van de AVG, maar natuurlijk ook nu al) niet op passende wijze verwerkt en beschermd worden.

Melanie Rieback, één van de sprekers tijdens voorgaande edities van SS@TB.

Netwerken, inspirerende sprekers en een relaxte omgeving op Security Summit @ The Beach

Sinds twee jaar is er een kleinschalig evenement waarbij het nuttige (netwerken, informatie uitwisselen, inspirerende spreekgasten) met het aangename (relaxte omgeving, goed glas wijn, smakelijk diner) gecombineerd wordt: Security Summit @ The Beach oftewel SS@TB. Op 29 juni 2017 vindt de derde editie plaats op het strand van Scheveningen in de Carlton Beachclub.

Naast het bijspijkeren van je vakkennis, is SS@TB ook om te netwerken, oude bekenden weer te zien en nieuwe contacten te leggen. Meteen na de ontvangst is er ruim gelegenheid om je te mengen onder de aanwezigen onder het genot van een drankje. Een voortreffelijke barbecue vloeit geruisloos over in de eerste van de gemiddeld drie presentaties op een avond. Na afloop is er gelegenheid om nog met elkaar van gedachten te wisselen, gegevens uit te wisselen en nog een laatste versnapering. Dit jaar wordt er voor het eerst afgesloten met een spetterend optreden van de band Detonics. Dit is de bluessensatie van het jaar die Nederland vertegenwoordigde in Memphis bij de International Blues Challenge. Dat wordt een feestje, zowel inhoudelijk als qua entertainment. Schrijf je in voor SS@TB op 29 juni 2017 via www.ssatb.nl en ervaar een ander security event....at the beach.

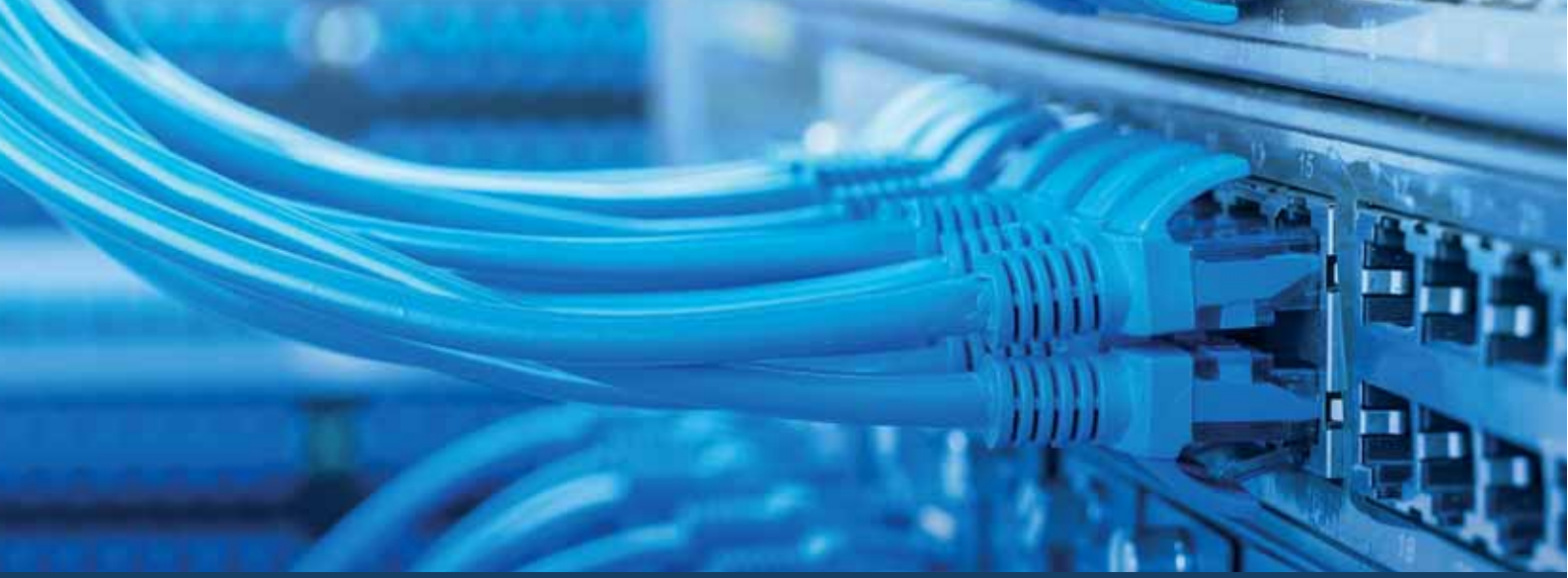
Openingspagina van de expertbrief

PvIB Expertbrief SOC

In mei 2017 is door het PvIB de nieuwe expertbrief SOC gepubliceerd. Deze expertbrief kreeg het bijschrift en titel 'Een proactief business Cyber Security Operations Center - Een wendbaar SOC is mensenwerk'.

De auteurs van de nieuwe expertbrief SOC.

De openingsalinea van de brief beschrijft welke vraag er beantwoord wordt: "De afgelopen jaren hebben veel organisaties een Security Operations Center (SOC) ingericht of als dienst ingekocht. Organisaties werden hierbij veelal gedreven vanuit strenger wordende wet- en regelgeving (compliance-driven) en vanuit de wens om (potentie?le) dreigingen in een vroegtijdiger stadium te ontdekken. SIEM (Security Information & Event Management) neemt binnen een traditioneel SOC een centrale plaats in. Dit maakt een traditioneel SOC bij uitstek reactief. Een probleem wordt gedetecteerd, dit wordt gerapporteerd en er wordt actie ondernomen. Terwijl de snelle veranderingen in de wereld om ons heen, en de cyberwereld in het bijzonder, vragen om een proactief SOC. Wat is er nu nodig om van een traditioneel reactief SOC (r-SOC) te groeien naar een modern proactief SOC (p-SOC)? Hoe ziet een hedendaags p-SOC eruit dat is voorbereid op de toekomst?"
De expertbrief SOC is te downloaden op onze website, www.pvib.nl.



Interview Masum Mir

HET OPEN ECO-SYSTEEM VAN NETWERKEN

Hoofdredacteur Lex Borger sprak Masum Mir, VP Product Management, Solutions & Technical Marketing bij Juniper, op 15 maart 2017 voordat Mir voor zijn keynote het podium opging op het SecureLink Security Bootcamp. Ze spraken over de visie op netwerkbeveiliging van Juniper.

Wat is de uitdaging voor netwerktechnologie vandaag?
"In het zakenleven vandaag de dag bestaat geduld niet meer. Alles moet snel, wat het ook kost. We bieden megaservices aan, waarin een heleboel informatie verwerkt wordt. Het is allemaal verbonden met netwerken en alles is digitaal. Het netwerk verbindt mensen, bedrijven en computers. We kunnen spreken van 'A2A' connecties, anything-to-anything.

De plaats van interactie of informatie staat niet meer vast. Je kunt het niet meer afsluiten of omsluiten. Wat je nodig hebt om veilig informatie te verwerken, is een alom veilig netwerk. En een veilig netwerk hebben, betekent niet meer firewalls plaatsen, of de volgende 'next generation' firewall gebruiken."

Ok, geen firewall, dat is traditionele perimeterbeveiliging. De aanvaller is al binnen. Hoe kun je hier dan toch veilig gebruik van maken?
"Het beheren van het netwerk in zijn geheel is complex. En daar moeten dan voor beveiliging nog eens firewallregels aan toegevoegd worden. Dit moet eenvoudiger kunnen. In plaats van het schrijven van firewallregels, zouden we bedrijfsmatige regels (business intent) moeten beschrijven, in termen van wat snel moet kunnen en wat volgens compliancy, security of privacy niet mag. De techniek moet de vertaling maken van bedrijfsintenties naar technische regels, waar en hoe nodig, overal in het netwerk, ongeacht de locatie. Dit kan in een datacenter zijn of in de cloud.

Daar moet het niet bij blijven. Er is feedback nodig uit analyse van meetgegevens. Als we ervan uitgaan dat je continu gehackt wordt, dan gaat het om snel te reageren op indicators of compromise. De meeste analysetools geven je duizenden triggers om actie uit te halen. Dat werkt niet. Het netwerk is echter uitermate geschikt om compromise te detecteren én daar ook snel op te reageren. Waarom? Omdat alle informatie over het netwerk gaat. Het stelt je in staat meetinformatie te krijgen uit verschillende bronnen. Het netwerk kan bepalen wat normaal is en wat niet."

Dan zie je iets dat niet normaal is, maar wat moet je daar dan mee?
"Omdat het netwerk overal is, kan het ook snel reageren, namelijk door dicht bij de bron in te grijpen, of die nu binnen probeert te komen of al binnen is. En omdat het netwerk dynamisch is, moet hier ook rekening mee gehouden worden. Een eenmaal besmette container duikt iedere keer weer ergens besmet op als je er niets aan doet."

Dus het netwerk wordt actiever?
"Het netwerk van de toekomst ziet er anders uit. Wij gaan internetdiensten nog verder uitbreiden. Neem bijvoorbeeld de service UberEATS [1]. Deze dienst combineert de taxi-service van Uber met een maaltijdbezorgdienst. Het is ook in Amsterdam beschikbaar. Om deze dienst uit te voeren dienen een heleboel computers gegevens met elkaar uit te wisselen. En hier komt bijna geen mens aan te pas. En we gaan veel meer systemen verbinden met het internet. Er komen in de komende jaren meer dan 20 miljard apparaten aan het internet te hangen.
De toepassing van software-defined networking zal helpen om ze van elkaar te isoleren. Om dit te kunnen doen, zal de kennis zoals die al in het netwerk bekend is, gebruikt moeten worden. En dit kan door twee stappen te nemen: gebruik de netwerkapparatuur als sensors en gebruik machine learning om verkeer in realtime te analyseren. Het is onmogelijk dit te doen met leverancier-eigen techniek, of dit nu Juniper is of een andere netwerkleverancier. De apparatuur zal de gegevens in een standaardformaat moeten leveren, zodat machine learning systemen deze informatie allemaal kunnen verwerken."

Is dat lastig?
"Software-defined networking heeft een karakteristiek verschil met traditioneel netwerken: het netwerk verandert meer en sneller. Dit kan niet gedaan worden zonder aanpassingen in de infrastructuur. We hebben automatisering nodig in de softwareontwikkelingstools en netwerkdiensten. Analyse van netwerkverkeer, waarbij bij verdacht gedrag het misdragende netwerkcomponent niet alleen geïsoleerd wordt in zijn omgeving, maar in een soort honeypot wordt gezet om het gedrag verder te kunnen analyseren en daar dus van te leren. Hebben we alle kennis en kunde om dit nu te kunnen doen? Nee, het is een reis. Vergelijk het met de zelfrijdende auto. De specialisten zijn daar een heel eind mee gevorderd, maar voor veiligheid moet er nog een bestuurder bij zitten. We zijn zover gekomen door aandacht te hebben gehad voor veiligheid van de inzittenden en de andere weggebruikers. We hebben babystapjes genomen, met eerst cruise-control en lane-assist. En terwijl dit alles ontwikkeld wordt, rijden er ook nog traditioneel bestuurde auto's op de weg."

Vooral dat laatste is iets om rekening mee te houden.
"Ja, dat moeten we dus ook doen in de netwerktechnologie. We moeten leren hoe we netwerkconfiguratie automatiseren, standaardiseren in een open eco-systeem en hoe we de meetgegevens verkrijgen en analyseren. En dit alles terwijl de nieuwe netwerken kunnen werken met de huidige netwerken. Dit vergt dat we niet alles opnieuw gaan uitvinden, maar gaan werken met wat we al hebben, bijvoorbeeld op aanpalende gebieden zoals softwareontwikkeling.
De beheerder moet voor het netwerk op een simpele manier kunnen beschrijven hoe het netwerk zich moet gedragen. Een soort if-this-then-that voor het netwerk. IFTTT [2] is in dit opzicht een interessante applicatie. Deze kan alleen werken als het platform open is. Juniper wil een open platform voor netwerkbeheer zijn, daar mogen onze klanten ons aan houden. Daarom investeren we in machine learning, daarom hebben we een partnership met VMware, daarom moet analyse van het netwerk en de applicaties samenkomen. Ons motto is 'Develop systems thinking', want dat hebben we nodig."

Referenties

[1] https://www.ubereats.com/amsterdam/
[2] https://ifttt.com/

Lex Borger is hoordredacteur van IB-Magazine, security consultant bij i-to-i en docent security aan de Hogeschool Utrecht. Lex is te bereiken via l.borger@i-to-i.nl.

CAPABLE

There have been numerous media reports in recent times about the cyber-attack capabilities of nation states hostile to Western political and business interests. That of course raises the debate about our cyber-defence capabilities and what they should be in this emerging threat landscape. In particular some commentators have raised the issue of the purpose and motive on the part of the attackers – what do they want to achieve? What are their goals?

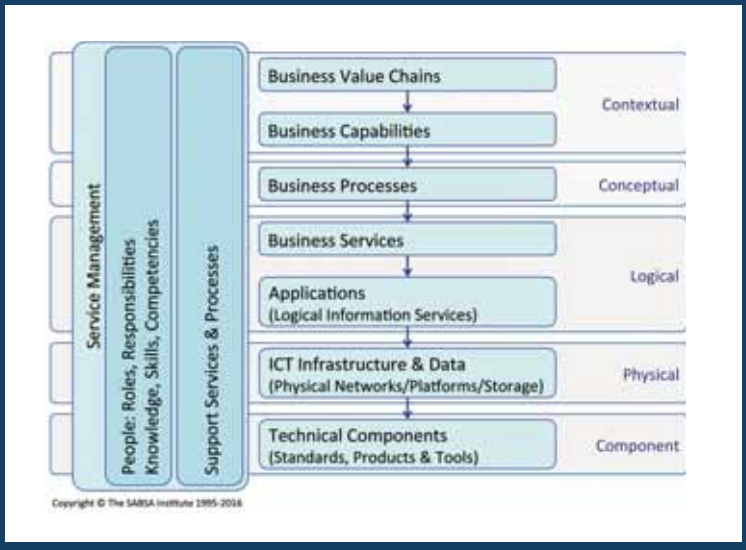


Figure 1 - The SABSA Business Stack.

The more insightful commentators have pointed out that in the Western world we seem to be stuck in a relatively immature state of mind, believing that it's all about theft of information, fraudulent money transactions, denial of service associated with ransom demands and the like – all very tactical and short term. Yet it's clear that there are many hostile operators with much more strategic goals. It has been suggested, and there seems to be much evidence (although not necessarily in the public domain) that there is intent to disrupt and indeed destabilise entire Western societies and nation states. The suggestion that there has been interference in the democratic electoral processes associated with the US presidency and the Brexit referendum are examples of such long-term hostile strategies. There have also been suggestions that disruption of world banking systems is a potential goal – undermining confidence in the economic capabilities of Western nations. Is this credible? The Attributer thinks that it is.

If there is immaturity of thought in Western society, it is because we are hooked on technical capabilities rather than the 'business' capabilities that technology delivers. Maybe it's because we collectively invented the Internet and WWW-technology that we are still looking proudly at those

So it is the same with cyber technology, and it seems that maybe those who are the 'settlers' rather than the 'pioneers' of this technology are more likely to see the true potential capabilities that it enables

achievements instead of looking at what value-creation capabilities they enable, whether economic or political.

SABSA says differently, but the traction of this thinking is somewhat limited as yet. The SABSA Business Stack model makes it clear that technological capabilities are merely the means to achieve value-creation capabilities (see Figure 1). Every enterprise (on a scale from a personal level up to huge commercial or government enterprise level) has a set of value propositions that drive its efforts going forward. It has a value chain, whereby value is developed and increased for the benefit of the enterprise. The value chain is supported at the next layer of the stack by capabilities to create, protect and sustain value. The technical capabilities appear much lower down in the stack layers and should not be confused with those at the higher level.

Let's take a simple analogous example to illustrate this concept. Some years ago, Bosch, the European power tool manufacturer, realised that marketing power drills as tools was not the best way to sell them. They were really selling the capability to make holes of various sizes in various materials. Smart thinking, but still not all the way there. The Attributer is the proud owner of a hi-tech combi-drill/driver power tool (as it happens from a different manufacturer). It has many features such as: cordless; two-speed drill setting, hammer setting, 17 different torque settings for driving, forward and reverse, keyless self-tightening chuck, two interchangeable batteries for continuous working… impressive eh?

The Attributer, being a married man, is keen to impress The Attributer's Wife, by bringing added value into her life. Do you think that showing her the combi-drill does that? She might feign interest and smile indulgently, but what will really impress her are The Attributer's capabilities to fix things in the house and garden.

Figure 2 - The SABSA Lifecycle.

Does the technology alone do that? Of course not. It requires someone to plan what is needed to further the household enterprise strategy, to plan some projects, to design some solutions, to do the implementation work and to monitor the success and maintain the state of repair over the future. Does that remind you of the SABSA Lifecycle? (See Figure 2).

What this simple domestic example demonstrates is that technology alone is nowhere near enough to achieve value creation. What is needed is a complex combination of people, process and technology. The technology itself is important but not significant in creating valuable capabilities unless used by skilful, competent people following robust processes.

So it is the same with cyber technology, and it seems that maybe those who are the 'settlers' rather than the 'pioneers' of this technology are more likely to see the true potential capabilities that it enables. If we remain stuck with the purely technical view we run the risk of being incapable of analysing the way in which we may be attacked, because we are missing the analysis of what motivates our potential enemies, what their goals are and the strategies they are developing to further those goals.

SABSA-thinking will help us to comprehend more fully the future of the digital world based on the Internet of Everything. We need always to think in terms of the value chains (both our own and those of our opponents) and the capabilities that enable them. We need to be fully capable at the highest level of enterprise extraction.

The Attributer

6

Zes vragen

Je leest het eerste artikel in een nieuwe rubriek, 'zes vragen'. In deze rubriek worden experts een aantal vragen gesteld om een inzicht te krijgen in een ontwikkeling op het gebied van informatiebeveiliging.

HET NIEUWE AUTHENTICEREN

Johannes Ullrich is Dean of Research bij SANS Institute. Hij is oprichter en Director van het Internet Storm Center, het internet-waarschuwingssysteem waar nieuwe aanvallen vaak als eerste worden opgemerkt. Hij is op Twitter te vinden: @johullrich. Lex Borger stelt hem zes vragen.

Voor welk gebruik zullen de OATH-verificatiestandaarden de standaard worden voor verificatie op internet?

"Het belangrijkste voordeel van OATH-gebaseerde tokens is dat ze makkelijk en goedkoop zijn om te implementeren. OATH-compatibele soft tokens zijn beschikbaar voor bijna elk platform en gebruikers zijn meestal bekend met hen. OATH soft tokens bieden een significante verbetering ten opzichte van alleen gebruikersnamen en wachtwoorden. Ze hebben ook geen last van sommige aanvallen op sms-berichten, als er een speciale applicatie wordt gebruikt om de token te genereren. Dit maakt ze ideaal voor websites zoals e-commerce sites, waar extra authenticatiestappen reden voor shoppers zijn om hun winkelwagentje te verlaten, of gratis web mail systemen. Kleine bedrijven kunnen OATH ook gebruiken om verbinding te maken met interne applicaties. "

Zal het gebruik van soft tokens voor verificatie (mobiele device authenticators) het gebruik van hard tokens domineren? Wat zijn de drivers voor het gebruik van een hard token? Wat zijn de drivers voor het gebruik van een soft token?

"Ja. Soft tokens zullen hard tokens gaan domineren. De belangrijkste reden is prijs en gemak. Bij soft tokens kan de gebruiker gemakkelijk verschillende tokens voor meerdere sites op een apparaat of zelfs in een app beheren (als een standaard zoals OATH gebruikt wordt). Harde tokens zijn duurder, en moeilijker te beheren. Ook zou een gebruiker voor elke site die ze bezoeken een ander token nodig hebben, wat niet haalbaar is.

Het grootste nadeel van soft tokens in het algemeen (niet alleen OATH) is echter dat ze slechts zo veilig zijn als het apparaat waarop ze zijn opgeslagen. Elk token vereist een uniek 'secret' dat op het apparaat is opgeslagen. Hoewel er methoden zijn om deze tokens veilig op te slaan in moderne mobiele apparaten, zal vermoedelijk niet in alle software deze best practises geïmplementeerd worden. Tijdens het opzetten van een token moet de gebruiker het secret in de toepassing invoeren. Dit gebeurt vaak via QR-codes. Als de gebruiker een image van de token op een onveilige locatie opslaat, is het token in gevaar en kan het worden gestolen zonder dat de gebruiker dat weet. Beveiligde hardware-tokens zijn veel moeilijker of onmogelijk om ongemerkt te kopiëren. Applicaties

met zware beveiligingseisen, zoals financiële gegevens of bedrijfsapplicaties, kunnen nog steeds hardware-tokens verkiezen.

Zakelijke authentication, of federated identity, waarbij gebruik wordt gemaakt van de leverancier om bij verschillende oplossingen in te kunnen loggen is een onderwerp dat in discussies rondom new authentication ook naar boven komt. Hier hangt het vertrouwen samen met het vertrouwen dat organisaties in de leverancier hebben en welke best practises zij hebben geïmplementeerd. Ook hier geldt dat er voor applicaties die zware beveiliging vereisen zoals financiële systemen, hard tokens blijven worden ingezet."

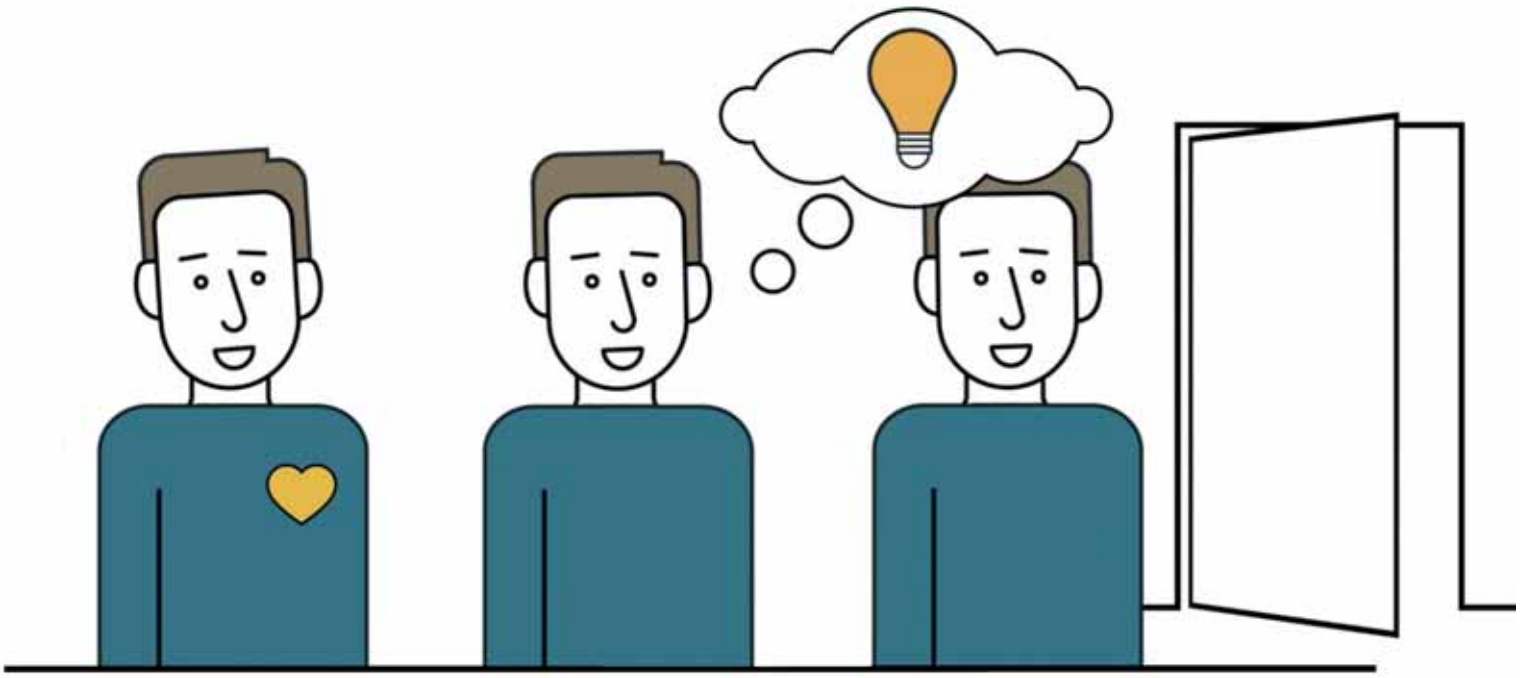
Hoe kunnen deze authenticatie tokens worden gebruikt in de productie van sterke digitale handtekeningen? Zullen zij in de nabije toekomst over PKI-tokens domineren?
"Tokens zoals OATH worden meestal niet gebruikt voor digitale handtekeningen, maar ze kunnen een gebruiker authenticeren naar een systeem dat de digitale handtekening genereert. Voor dit doel zullen PKI-tokens in gebruik blijven. PKI-tokens kunnen ook worden gebruikt voor gebruikersauthenticatie, maar implementatie en sleutelbeheer lijken complexer te zijn dan voor OATH-gebaseerde soft tokens."

Wat zijn de waarschijnlijke scenario's omtrent het gebruik van externe identiteit dienstverleners? (Zullen we allemaal alleen met Google of Facebook authenticeren?)
"Het voordeel van externe identiteitsverleners is het gebruiksgemak. Maar privacy is een groot probleem, aangezien die dienst die de identiteit van de gebruiker levert ook weet met welke site de gebruiker connectie maakt. Bovendien werken deze diensten alleen voor online /verbonden toepassingen, niet voor applicaties in privé-netwerken. Vertrouwen is een ander belangrijk probleem. Als de identiteitsaanbieder is gehackt, kan iemand het gebruiken om gekoppelde accounts aan te vallen. Het onderliggende idee van deze identiteitsverleners is om het gebruiksgemak van single-sign-on (SSO) en identiteitsmanagement naar publieke systemen te kopiëren. Tot nu toe is SSO en ID-management meer gebruikt in private/gesloten systemen. Aangezien de huidige systemen op internet zijn gebaseerd, kennen ze ook een aantal van de beveiligingslekken die inherent zijn aan webapplicaties (bijvoorbeeld problemen zoals phishing, CSRF (cross-site-request forging) en click jacking met systemen zoals OAUTH). Let op: OAUTH moet niet verward worden met OATH. "

Gewoonlijk moet een gebruiker een wachtwoord, een gebruikers-id, kiezen en het e-mailadres verifiëren om zich aan te melden

Wat zijn de drivers voor het gebruik van een externe identiteit dienstverlener?
"Gemak en daarmee minder weerstand om als gebruiker in te schrijven. Gewoonlijk moet een gebruiker een wachtwoord, een gebruikers-id, kiezen en het e-mailadres verifiëren om zich aan te melden. Dit is een proces met meerdere stappen en als een stap (bijvoorbeeld de e-mailverificatie) mislukt, kan de gebruiker zich niet aanmelden. Inloggen via sociale media-accounts zoals Facebook gaat veel gemakkelijker. In sommige gevallen kan er ook meer inzicht over de gebruiker verzameld worden als gebruikers ermee akkoord gaan om gegevens uit hun sociale mediaprofiel te delen."

Is er een onderwerp dat in de discussie onderbelicht blijft?
"Het risico van gekopieerde tokens noemde ik al, maar wat vaak over het hoofd wordt gezien in de discussie rondom OATH is het risico die reset services met zich meebrengen. Dienstverleners moeten echt aandacht besteden aan de manier waarop ze het resetten van tokens, ingeval je die bent vergeten, of het token is gehackt, inrichten. Net als bij het resetten van wachtwoorden heb je niets aan een sterk wachtwoord als je met een eenvoudig te achterhalen vraag het password kan resetten. Dit geldt ook voor tokens. Providers kijken hiervoor het liefst naar selfservice processen, maar er is nog geen best practise standaard ontwikkeld voor het resetten van tokens via een self-serviceproces. Hier moet de markt echt aandacht aan besteden. Want hoe veilig is een token die je met alleen een e-mailadres kunt resetten of uitschakelen?"



Figuur 1 - Gedrag = motivatie + capaciteit + gelegenheid.

VOORBIJ AWARENESS

Grip op cyberveilig gedrag

Cyberdreigingen worden steeds geavanceerder. Dit geldt niet alleen op technisch vlak, maar zeker ook op menselijk vlak. Social engineering-technieken worden steeds vernuftiger en het vraagt steeds meer van de mens om daar weerbaar tegen te zijn. Tijd voor een nieuwe strategie! In dit artikel wordt het weerbaar maken van medewerkers van organisaties besproken vanuit een psychologisch perspectief. Wat zegt de psychologie over gedragsverandering, hoe kan dat ingezet worden en waarom bereiken de huidige awarenessprogramma's vaak niet het gewenste resultaat?

Waar vroeger de dreigingen in het cyberdomein nog relatief behapbaar waren, neemt de complexiteit vandaag de dag sterk toe. Niet alleen ICT-systemen zijn onderwerp van aanval, maar steeds vaker de medewerkers die deze systemen bedienen en toegang hebben tot kritieke bedrijfsinformatie of -applicaties. CEO-fraude is daar een goed voorbeeld van. Op een slimme, mensgerichte manier wordt geprobeerd om via een medeweker van een financiële afdeling geld te ontvreemden door het proces van de organisatie te passeren of te misbruiken. Zo komt het voor dat er honderdduizenden euro's op relatief simpele wijze in handen van kwaadwillenden terechtkomen. Iets breder kan gesteld worden dat de gevolgen van een cyberaanval zijn verbreed. Te denken valt aan imago- en reputatieschade, verlies van klanten of van inkomsten of diefstal van financiële tegoeden.
Een andere ontwikkeling is de koppeling van de fysieke aan de digitale wereld. Daar waar beveiliging vroeger alleen bestond uit het beveiligen van een zakelijk pand, moeten nu ook de digitale dreigingen worden meegenomen en zijn er meer toegangspoorten te beschermen dan alleen de fysieke toegang. In feite is iedere werknemer een toegangspoort geworden tot een organisatie, mede door het gebruik van smartphones, tablets en laptops die op afstand verbinding leggen met een bedrijfsnetwerk. Het is dus niet vreemd dat kwaadwillenden zich steeds vaker richten op de medewerker om via hen ongewenste toegang te verkrijgen tot informatiesystemen van een organisatie. Het is daarom in toenemende mate belangrijk om aandacht te besteden aan de weerbaarheid van medewerkers.

Motivatie refereert naar of iemand het gedrag wil vertonen; welk doel vindt iemand eigenlijk belangrijk? Bijvoorbeeld iemand die veiligheid zeer belangrijk vindt, zal meer gemotiveerd zijn om een ingewikkeld wachtwoord te bedenken dan iemand die snelheid en gemak belangrijk vindt.
Capaciteit verwijst naar iemands kennis en kunde: de mate waarin iemand in staat is om bepaald gedrag te vertonen, gegeven zijn eigenschappen, vaardigheden en instrumenten.
Gelegenheid is de mate waarin de omstandigheden het gedrag bevorderen of belemmeren. Hierbij kan gedacht worden aan fysieke omstandigheden (omgeving: is je kast af te sluiten?), sociale omstandigheden (is het in de bedrijfscultuur geaccepteerd om een onbekende aan te spreken?) en technologie (is het mogelijk om je wachtwoord regelmatig te wijzigen?).

Deze menselijke kant van cyberaanvallen wordt de laatste jaren steeds breder onderkend. Zo bleek uit een recent onderzoek door het Ponemon Institute onder 450 IT- en IT-securityspecialisten dat de 'menselijke fout' de grootste barrière is voor het bereiken van een cyberveilige organisatie [1]. In lijn hiermee liet een PWC-survey [2] zien dat zowel in 2014 als in 2015, werknemers het belangrijkste risico zijn. Dit blijkt ook uit het Cybersecuritybeeld Nederland [3], waarin werd geconcludeerd dat phishing (in het bijzonder spearphishing) hét middel is voor gerichte aanvallen. Deze ontwikkelingen pleiten voor de introductie van een nieuwe discipline in het cybersecurity werkveld: gedragspsychologie. De psychologie achter mensgerichte cyberaanvallen wordt namelijk geavanceerder van aard, dus sociaalpsychologen inzetten om personeel te 'wapenen' lijkt een mooie volgende stap.

Psychologie & cybersecurity

Wat brengt het dan, als we psychologie toevoegen aan cybersecurity? De laatste jaren zijn steeds meer organisaties zich bewust van de ingang die cybercriminelen zoeken bij het personeel. Als antwoord hierop, bleek uit een grote steekproef in 2015 dat 53% van de Nederlandse organisaties een awarenessprogramma heeft (PWC 2016). Dit creëren van awareness bij medewerkers heeft als doel ze kennis te geven over de aanvalsmanieren en ze daarmee weerbaar te maken. Echter, dat is alleen maar een oplossing als het ontbreken van deze kennis het probleem is. Mensen moeten zich bewust zijn van bepaalde dreigingen om ze te herkennen, absoluut. Er zijn alleen talloze voorbeelden waaruit blijkt dat in veel gevallen deze kennis niet leidt tot een verandering in het gedrag en dus niet het

Dr. Inge Wetzer is sociaalpsycholoog cybersecurity Hoffmann Cybersecurity. Ze heeft economische psychologie gestudeerd en is gepromoveerd in de sociale psychologie. Vervolgens heeft ze bijna tien jaar bij TNO gewerkt, waar ze psychologisch onderzoek verrichtte in het domein Defensie & Veiligheid. Sinds 2016 werkt zij bij Hoffmann als sociaalpsycholoog cybersecurity. Haar opdracht is om haar kennis en ervaring op gebied van menselijk gedrag te koppelen aan het domein cybersecurity om zo werknemers van organisaties beter te beschermen tegen cyberaanvallen. Inge is te bereiken via i.wetzer@hoffmannbv.nl.

probleem is! Neem wachtwoorden: haast iedereen weet tegenwoordig dat een lang ingewikkeld wachtwoord veiliger is. Veel mensen gebruiker echter tóch de naam van hun kind, hun verjaardag of een jaartal als wachtwoord. Hieruit blijkt dat awareness slechts een eerste stap is naar wat het eigenlijke einddoel zou moeten zijn, namelijk cyberveilig gedrag. Verschillende studies tonen aan dat awareness zeker niet altijd leidt tot de gewenste cyberveilige gedragingen [4].

Gewenst gedrag	Motivatie	Capaciteit	Gelegenheid
Wachtwoord regelmatig wijzigen	Hoe belangrijk vindt iemand het om het wachtwoord regelmatig te wijzigen? Hoe verhoudt het belang dat iemand hieraan toekent tot andere drijfveren zoals gemak?	Weet iemand hoe het wachtwoord gewijzigd moet worden en is hij in staat om deze handelingen uit te voeren?	Staat de technologie het toe om het wachtwoord te wijzigen en is er uitleg beschikbaar hoe dit werkt?
Openbare netwerken vermijden voor zakelijk gebruik	Hoe belangrijk vindt iemand het om openbare netwerken te vermijden? Hoe verhoudt dit belang zich ten opzichte van andere drijfveren zoals pragmatisme en snelheid?	Is iemand zich bewust van de risico's van het gebruik van openbare netwerken? Kent iemand de alternatieven voor het gebruik van openbare netwerken en kan hij die uitvoeren?	Heeft iemand andere mogelijkheden om in dringende gevallen toch op een veilige manier verbinding te kunnen maken met het bedrijfsnetwerk?
Tegenhouden van een onbekende die mee het bedrijfspand wil inlopen	Hoe belangrijk vindt iemand het om onbekenden buiten te houden? Hoe groot schat hij de kans dat dit een risico vormt?	Is iemand zich bewust van de risico's van onbekenden in het bedrijfspand? Weet iemand hoe hij een onbekende kan tegenhouden op een manier die hij ook kan en durft uit te voeren?	Staat de bedrijfscultuur toe dat werknemers onbekenden durven aan te spreken? Is er een goed alternatief waarnaar men de onbekende kan verwijzen?

Tabel 1 – Voorbeelden van motivatie, capaciteit en gelegenheid.

Het antwoord hoe de kloof tussen awareness en gedrag kan worden overbrugd, kan gevonden worden in de psychologie. Om te begrijpen hoe gedragsverandering plaats kan vinden, is het belangrijk om eerst gedrag beter te begrijpen. De gedragstheorie van MacInnis, Moorman & Jaworski [5] ontleedt gedrag in componenten. Specifieker betekent dit dat gedrag kan worden gezien als resultaat van drie factoren: motivatie, capaciteit en gelegenheid. Met andere woorden: wíl iemand het doen, is hij in staat om het te doen en krijgt hij de kans om het te doen?

Als deze drie factoren alle drie in voldoende mate aanwezig zijn, zal gedrag plaatsvinden. Als één van deze factoren (deels) ontbreekt, is de kans op gedrag een stuk kleiner. Maar wat is dan 'gedrag'?

In het kader van gedragsverandering leert de psychologie ons dat gedrag, om veranderd te kunnen worden, heel specifiek gedefinieerd moet worden. Immers, 'veilig gedrag' is zo'n breed begrip dat het niet meetbaar of grijpbaar is. Daarom zal een psycholoog altijd vragen naar concreter gedrag: wat is het precieze gedrag dat u wilt veranderen? Wat is het gewenste gedrag dat u graag zou zien? In het domein van cybersecurity zien we hier een relatief groot aantal gedragingen die haast voor elke organisatie van toepassing zijn. Hierbij kan gedacht worden aan het locken van een pc als iemand zijn of haar werkplek verlaat, het kiezen van een complex wachtwoord, het niet delen van het wachtwoord met collega's en anderen, enzovoorts. Echter, onze ervaring leert ook dat de gedragingen die gewenst zijn in het kader van cybersecurity soms zeer specifiek kunnen zijn voor een bepaalde organisatie. Bijvoorbeeld het aanspreken van onbekenden die zonder begeleiding door een zwaarbeveiligd gebouw lopen of het niet spreken over vertrouwelijke dossiers van een opdrachtgever in publieke ruimten. Wanneer het gewenste gedrag duidelijk is gedefinieerd, kan worden onderzocht hoe het staat met de motivatie, capaciteit en gelegenheid van de doelgroep om het gewenste gedrag te vertonen. Ter illustratie worden in tabel 1 een aantal voorbeelden getoond van motivatie, capaciteit en gelegenheid voor concrete gedragingen in het specifieke domein van cyberveilig gedrag.

Door gedrag zo duidelijk onder te verdelen in deze drie componenten, geeft deze theorie ook meteen inzicht in de maatregelen die genomen kunnen worden om bepaald gewenst gedrag te laten optreden. Het gegeven dat gedrag uit verschillende componenten bestaat, maakt inzichtelijk waarom awareness programma's vaak niet tot het gewenste resultaat leiden. Awareness gaat over capaciteit. Dat gedrag niet optreedt vanwege een gebrek aan kennis erover is namelijk een aanname! Het kan net zo goed ontbreken aan motivatie of aan gelegenheid om het gedrag te vertonen.

Referenties

[1] Ponemon Institute (2016). The Cyber Resilient Organisation in the United Kingdom: Learning to Thrive against Threats

[2] PWC (2016). Turnaround and transformation in cybersecurity. Key findings from The Global State of Information Security Survey.

[3] NCSC (2015). Cybersecuritybeeld Nederland (2015). Nationaal Cyber Security Centrum (NCSC).

[4] Wijn, R., Van den Berg, H., Wetzer, I. M., & Broekman, C. C. M. T. (2015). Supertargets: Verkenning naar voorspellende en verklarende factoren voor slachtofferschap van cybercriminaliteit. TNO-rapport R11499.

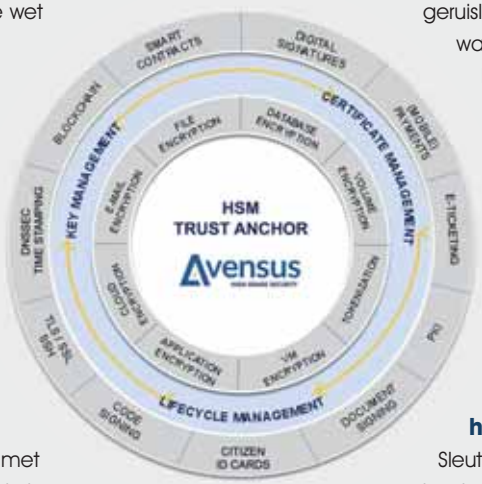
[5] MacInnis, D. J., Moorman, C., & Jaworski, B. J. (1991). Enhancing and Measuring Consumers' Motivation, Opportunity, and Ability to Process Brand Information from Ads. Journal of Marketing, 55, 32-53.

DE ESSENTIËLE ROL VAN VERSLEUTELING EN SLEUTELBEHEER

ICT verandert exponentieel en innovaties als IoT, cloud, blockchain en Big Data zijn een feit. We opereren in een open omgeving en hebben minder controle over waar onze data zich bevindt, zich naartoe verplaatst en wie het in gebruik heeft. Het creëren van vertrouwen in het digitale tijdperk is nu meer dan ooit essentieel, vindt Pasqualle Verwoerdt, Business Manager bij Avensus High Grade Security.

Pasqualle Verwoerdt

Onze maatschappij en de wetgever stellen hoge eisen aan digitalisering en privacy. Na de wet Meldplicht Datalekken en de EU eIDAS-verordening stevenen we nu af op de AVG / GDPR. De consequenties voor bedrijven die niet voldoende controle hebben over hun informatiebeveiliging worden groter: forse boetes, reputatieschade, vertrouwensbreuk en nadelig effect van dit alles op de aandelenkoersen.



Hiernaast is het Avensus High Grade Security ecosyteem te zien, waarbij encryptie en sleutelbeheer onlosmakelijk met elkaar is verbonden. Ik vind dat men regulering ook kan beschouwen als een kans; zie het als concurrentievoordeel om je op het gebied van informatiebeveiliging te onderscheiden. De recente internationale Ransomware-uitbraak toont de zwakke plekken in onze samenleving; maar zijn dat wel onze grootste bedreigingen? Ieder zichzelf respecterend bedrijf heeft de juiste back-up in huis en maakt medewerkers bewust op de risico's. De echte bedreidingen waar we mijns inziens alert op moeten zijn, zijn cyberspionage, datalekken, gerichte attacks en de bewust of onbewust onbekwame medewerker.

De breach is een kwestie van tijd; zorg voor controle

Kijkend naar innovaties, bedreigingen en regelgeving, moeten we ons afvragen of de traditionele NextGen Security Intelligence Solutions wel de juiste richting is om in te slaan. Is het niet tijd om te schakelen van het voorkomen van security breaches naar het beveiligen van de breach an sich? Als we onze informatie weten te classificeren - uitgaande van vertrouwelijkheid, integriteit en beschikbaarheid – kunnen we ook preventieve maatregelen nemen. Zelfs als men níet in staat is om alle informatie te classificeren, dan nog kan encryptie de informatie beschermen. De wetgever stelt niet voor niets dat privaygevoelige data alleen door gebruik van encryptie op de best mogelijke manier beschermd is; alleen dan bent u compliant en vindt de overheid dat u aan uw plicht tot bescherming van privacygevoelige data heeft voldaan. Maar encryptie leidt toch tot vermogensverlies en hoge kosten? Dat is al lang niet meer valide. We beschikken over een range aan transparante versleutelingsoplossingen die een minimaal processorverlies met zich meebrengen en geruisloos aansluiten op de omgeving waarbinnen ze worden toegepast. Ook hoeft men minder te investeren in generieke beveiligingsoplossingen om toch gewoon zaken te blijven doen. Kosten verschuiven als het ware. Daarbij moet men zeker het risico op bedrijfscontinuïteit, boetes en reputatieschade meenemen bij de overweging tot investering in encryptie.

Sleutelbeheer is essentieel voor het succes van encryptie

Sleutelbeheer is een kritische succesfactor en net zo belangrijk als de versleuteling zelf. Naast de processen is de juiste apparatuur ook een belangrijk gegeven. Wordt er een systeem voor sleutelbeheer gebruikt? Worden de sleutels gemaakt, beschermd opgeslagen, gedistribueerd, verwisseld en vernietigd? Wordt er gebruik gemaakt van software of van gecertificeerde hardware (Hardware Security Modules)? Het is helemaal raadzaam om informatie in de cloud te versleutelen en daarbij de sleutels zelf goed te beheren (beleid, processen en apparatuur): Encrypt all and Manage the keys yourself! Het is de enige manier om controle over informatie te behouden. De vraag die veel relaties mij stellen is: investeren we op de juiste gebieden? Hebben we ons laten overdonderen door commerciële oplossingen? Op 15 juni a.s. organiseren we ons High Grade Security Kennisevent. Verschillende stakeholders delen kennis en inzichten over nieuwe vormen van versleuteling en het beheer ervan. Aanmelden kan via sstoetszer@avensus.nl.
Het wordt een interessante digitale toekomst voor ons allemaal.

VERSLAG CISO 16

ASPECTEN VAN INFORMATIEBEVEILIGING

Er was weer volop gelegenheid voor netwerken en discussie tijdens de CISO-bijeenkomst in nieuwe setting. Deze vond plaats op 29 maart in het BOVAG-huis in Bunnik en werd begeleid door Cees in 't Veld van Focus op verbeteren.

Bart van Staveren opende de bijeenkomst met een verwijzing naar Gerard de Weert en Pim van den Hoff die samen met hem de CISO-bijeenkomsten voorbereiden. Daarna introduceerde hij van Cees in 't Veld.

Cees in 't Veld is consultant bij Focus op verbeteren op het gebied van governance; bestuur, control, verantwoorden en toezicht. Als partner van Next Level MKB verzorgt Cees het onderdeel financiën en risicomanagement van de Masterclass 'Goed bestuur in het MKB' en als docent bij LLM Legal geeft hij trainingen in jaarrekening lezen, risicomanagement en toekomstgericht denken. Verder is hij parttime docent Corporate Governance aan de Nyenrode Business Universiteit en Hogeschool Utrecht en gastspreker governance en risicomanagement bij Wageningen University & Research.

Cees had zijn presentatie ingedeeld in drie deelgebieden: governance, risicomanagement en informatiebeveiliging.

Governance

Governance richt zich op besturen, verantwoording, toezicht en beheersen. Om 'in control' te zijn, moet een organisatie de interne en externe onzekerheden (risico's) die de realisatie van de doelstellingen in gevaar kunnen brengen onderkennen en maatregelen nemen om de gevolgen hiervan te beperken.

Daarbij zijn van belang:

- Een integrale kijk op de eigen organisatie;
- Kennis van de externe omgeving;
- Het anticiperen op toekomstige ontwikkelingen.

Het gaat er dan om dat de juiste discussie op het juiste moment op het juiste niveau wordt gevoerd zodat (indien nodig) bijgestuurd kan worden om zo de doelstellingen te realiseren. De organisatie moet dus zodanig ingericht zijn, dat goed bestuur mogelijk is.

Risicomanagement

Te beginnen met (de definities vanuit) COSO komt Cees tot de slotsom dat het onmogelijk is om alle risico's op een bepaald moment te kennen, laat staan deze volledig te beschrijven en te beheersen. Daarom richt het risicobeheersing- en controlesysteem zich op de belangrijkste risico's. Cees pleit ervoor om te beginnen met een organisatiebrede risicoanalyse/inventarisatie het Interne Controle Raamwerk (ICR) vast te leggen. Hij komt zo'n vastlegging in de praktijk nog weinig tegen. Maar het blijkt ook in de praktijk dat daarmee risico's bespreekbaar worden. Vanuit het besef dat risicomanagement een proces is met een P-D-C-A-cyclus is het nodig die inventarisatie (minimaal) jaarlijks, bijvoorbeeld in verband met de begroting, te actualiseren.

Voor het beheersen van risico's verwijst Cees naar het model van Bedrijfsvitaliteit/Van Heeswijk.

Aan de hand van het INK-model laat Cees zien hoe een ICR gevuld kan worden. Een ICR dwingt om de interne controle te beschouwen, maar is vooral een goed instrument bij de communicatie met bestuurders, MT-leden en adviseurs/commissarissen/toezichthouders en verbetert daar de

'awareness' van met name risico's met Kans Hoog, Effect Hoog. Eenmaal opgesteld, is het makkelijk te onderhouden en kan de kennis in het MT actueel blijven.

Informatiebeveiliging

Als inleiding op dit onderdeel laat hij het filmpje zien van Jose Esteves uit 2016 [1] over de snelheid van de ontwikkeling van data en consequenties ervan. Volgens Cees komt uit onderzoek naar voren dat bij bestuurders en commissarissen zowel het onderkennen van het belang van ICT als de kennis van ICT in totaliteit bezien bij beide groepen vaak ver onder de maat blijkt. En omdat de komende vijf jaar sprake is van een verwachte golf van innovaties in de nanotechnologie, de medische technologie en de biotechnologie en de opkomst van verregaand gedigitaliseerde exponentiële organisaties [2]. Waardoor het belang van informatiebeveiliging nog groter is geworden.

Daarbij is de mens de zwakke schakel bij de beheersing van risico's, waardoor het aankomt op gedrag en cultuur, normen en waarden. Via het een variant op het Johari-venster, door Cees vertaald in het groeiproces van onbewust onbekwaam via bewust onbekwaam en bewust bekwaam naar onbewust bekwaam, komt Cees uit bij een INK-model voor de ICT. Hij komt ertoe dat je dit ook per blok moet uitschrijven in het ICR.

Met de snelle ontwikkelingen geldt dat denken in risico's vanuit opgedane ervaringen daarom niet per definitie alle risico's dekt! Toekomstgericht denken wordt essentieel onderdeel van risicomanagement en informatiebeveiliging en moet dan ook binnen de organisatie belegd worden als kernattitude.

Daarmee komt Cees terug bij risicomanagement en met een stappenplan daarvoor:

1. Beleg risicomanagement bovenin uw organisatie.
2. Introduceer een risicomanagementmodel dat passend is voor uw organisatie.
3. Ontwikkel op een gestructureerde wijze toekomstgericht denken in uw organisatie.
4. Integreer risicomanagement in uw bestaande planning & control cyclus
5. Evalueer periodiek uw verzekeringsportefeuille.
6. Beschrijf het Interne Controle Raamwerk, actualiseer dit periodiek en neem gestructureerd actie.
7. Besteed in het Interne Controle Raamwerk specifiek aandacht aan afwijkende organisatie-onderdelen.
8. Zorg voor goede 'soft controls'.

Na een eerste aanzet over de eisen van wet- en regelgeving (BIR/BIG) waar je in ieder geval aan moet voldoen en waar een hoop werk uit voortvloeit, werd door Cees verwezen naar 'de verdraaide organisatie' van Wouter Hartjes [3]. Daarbij ging de discussie ook over hoe ver de normenkaders gaan. Daarna volgde een verdieping over of we nog voldoende het doel van Informatiebeveiliging in het vizier hebben en kunnen houden, gezien de snelle ontwikkelingen rond de cloud en de recente besluitvorming in Amerika. De zaal was het vrij unaniem eens over het belang van het blijven werken aan awareness en gedrag, waarbij het kan helpen de medewerkers jaarlijks te vragen een statement over (beveiligings)gedrag te laten ondertekenen.

Op de vraag van Bart van Staveren wat de beroepsgroep maatschappelijk nog meer kan betekenen, gaf Cees aan ons meer te richten op de politiek. Dit ook omdat het moeilijk is dit direct het midden- en kleinbedrijf te bereiken. Hij stelde voor belangenbehartiging uit te dragen door whitepapers en positionpapers naar de Tweede (en Eerste) Kamerleden te sturen.

Met een verwijzing naar de komende Esmeraldalezing (6 juli) en verdere CISO-bijeenkomsten sloot Bart van Staveren de bijeenkomst.

De gepresenteerde sheets en casussen zijn te bekijken op het besloten ledengedeelte op de PvIB website (agenda-archief) www.pvib.nl/actueel/evenementen/ciso-16.

Referenties

[1] www.youtube.com/watch?v=uqZiIO0YI7Y
[2] Yuri van Geest van de Singularity University (SU) schree,f samen met Salim Ismael, Exponentiele organisaties (ExO's).
[3] Whitepaper aan te vragen op http://www.eventverdraaideorganisaties.nl/whitepaper

Geert Martens is sinds 1 februari gepensioneerd als senior ICT/OA- auditor en senior controller bij UWV. Zijn werk bestond de laatste jaren in het inrichten van de control, AO/IB en risicomanagement op de grote geldstroom. Tijdens zijn tijd bij de accountantsdienst van UWV heeft hij het ISO-traject getrokken. Hij is bereikbaar via gjm.martens@hccnet.nl.

ARTIKEL VAN HET JAAR 2016

Jaarlijks reikt de redactiecommissie de prijs uit voor het 'Artikel van het Jaar', terugblikkend op het afgelopen jaar. Met een paar uitzonderingen dingen alle artikelen mee naar deze prijs. De redactie maakt een eerste selectie van ongeveer tien artikelen, een jury bepaalt hieruit de prijswinnaars. De jury bestond dit jaar weer uit Renato Kuiper van VKA, Ellen Wesselingh van de Haagse Hogeschool en Jurgen van der Vlugt van Maverisk.

De uitreiking vond dit jaar plaats op 18 april, tussen de ALV en de daaropvolgende avondbijeenkomst. Renato Kuiper presenteerde het juryrapport. Verder daagde hij de zaal en de redactiecommissie uit de leden directer te betrekken bij de verkiezing van het Artikel van het Jaar. Stof om over na te denken.

Juryrapport

De jury was het dit jaar snel eens: de kwaliteit van te jureren artikelen was weer hoger dan vorig jaar, en meer divers. Hierdoor was enige stevige discussie nodig om uit de voorselectie van tien artikelen eerst de top-drie shortlist en vervolgens daaruit de winnaar te kiezen. Dit lukte uiteindelijk door bij het bestuderen op structuur en inhoud van de artikelen nog kritischer te zijn en de harde en zachte criteria nog preciezer onderbouwd te scoren. Ook de onderlinge discussie kreeg meer weg van een inhoudelijk verkiezingsdebat dan een snel gevonden consensus.

De juryleden hebben eerst ieder voor zich de hele beoordeling met argumentatie gedaan en de eigen voorkeursvolgorde opgesteld. Nodeloos te zeggen dat daar nogal verschillende ijstjes uitkwamen. De discussie ging dan ook al snel over de specifieke voor- en tegenargumenten en de weging hiervan. Een vruchtbare discussie, die zoals het hoort soms ook de eigen beoordeling op losse schroeven zet! Uiteindelijk kwam dan overigens 'toch nog onverwacht snel' een eensluidende conclusie uit de bus.

Door de artikelen naast elkaar te leggen, komen een paar generieke zaken naar voren die, als het gaat om de kwaliteit van de artikelen, als advies voor auteurs kunnen worden meegenomen. Een belangrijke daarvan is dat opsommingen nuttig kunnen zijn, maar als overzicht van kennis tekortschieten in het vasthouden van de aandacht van de lezer. Te veel nadruk op opsommingen brengt ook het risico met zich mee dat in vorige jaren reeds was gesignaleerd: te veel methodologisch

Criteria Artikel van het Jaar

Wederom is bij het jureren gekeken naar, onder andere, de volgende criteria:

1. Opzet artikel – Is de opzet van het artikel juist voor de soort (inhoudelijk of opiniestuk)?
2. Leesbaarheid – Is het artikel helder en begrijpelijk geschreven, met passende illustraties? Is de stijl consistent, zoals serieus of satirisch? Of het nu een praktijkbeschrijving is of een wetenschappelijke beschouwing betreft, is de leeservaring prettig?
3. Benadering van de doelgroep – Is het duidelijk wat de doelgroep is voor het artikel? Is het artikel te volgen voor een lezer buiten de subgroep?
4. Vernieuwend gehalte – Heeft het artikel aspecten die getuigen van visie bij de auteur en/of nieuwe gezichtspunten op een onderwerp? Levert het de lezer nieuwe kennis op?
5. Zet het de doelgroep aan het denken? – Is het artikel een verslag van uitgevoerde werkzaamheden waarbij de lezer denkt 'fijn, weet ik weer, nu verder', of benoemt het aspecten of zelfs open eindjes waarmee de lezer wordt geprikkeld om de argumenten, aspecten en kanttekeningen eens wat langer in gedachten te houden?

correcte algemene aanduiding van oplossingsrichtingen, maar weinig concrete handvatten. Hierdoor kwam met enige regelmaat de opmerking terug: "Ziet er allemaal verantwoord uit, maar nu weet ik nog niet wat ik moet…".

En waar een op zich uitstekende analyse of confrontatie van these en antithese wordt gegeven, ontbreekt regelmatig dan nou net de synthese, de volgende stap die de theorie – en de praktijk – vooruit kan helpen.

Renato Kuiper presenteerde het juryrapport.

Winnaars

De winnaar van dit jaar is er een die wat dat betreft op alle punten scoort, en meer nog juist enthousiasme oproept om van alles toegevoegd te willen zien. Jammer dat allerlei spontane ideeën voor uitbreiding die bij ons opkwamen, zoals over het langere-termijn meten van resultaten, er niet al in stonden. Maar misschien was een en ander dan wel te lijvig geworden voor een artikel en had de focus verloren gegaan. Desalniettemin is duidelijk: Marijke Stokkel heeft met haar artikel 'Security-Awareness: Zo wordt het een succes' een eersteprijswinnaar neergezet. We zien uit naar vervolgartikelen!

Op slechts een paar banddiktes afstand volgt Matthijs Koot met 'Apple vs. FBI: De feiten op een rijtje'. De jury was unaniem over de toegevoegde waarde van de uiteenzetting en vond deze zowat de eerste die een zo helder maar toch nauwkeurig en volledig beeld geeft van de problematiek. Een prima voorbeeld van hoe een casestudy moet zijn: de case als instantie van een generiek issue, als voorbeeld en als mogelijk juridisch precedent. Alleen ontbrak nog de relevantie voor de Nederlandse situatie, juist nu de nieuwe hackwet erdoor is, maar we kijken uit naar meer van dit soort case-besprekingen.

Nummer drie dit jaar is Peter Kampman met het artikel 'Risicoanalyse: Privacy versus informatiebeveiliging'. Een prima kort en bondige bespreking van de IB-Risico-Analyse (IBRA) versus de Privacy Impact Analyse (PIA). De conclusie dat beide slechts moeizaam te combineren zijn, werd in de jury lustig bediscussieerd – we hadden graag gezien dat er een oplossing tot samenwerking tussen IBRA en PIA was geforceerd… Laten we hopen dat Peter of een vakgenoot ons binnenkort verblijdt met zo'n vervolgstap.

Aan alle auteurs en lezers: hartelijk dank, blijf schrijven en lezen, en laten we de wereld veiliger maken.

Winnaars

1. Marijke Stokkel, Security-Awareness: Zo wordt het een succes, IB 4, 2016.
2. Matthijs Koot, Apple versus FBI: De feiten op een rijtje, IB 5, 2016.
3. Peter Kampman, Risicoanalyse: Privacy versus informatiebeveiliging, IB 8, 2016.

Renato Kuiper, namens de jury van de verkiezing 'Artikel van het Jaar 2016'. Renato is te bereiken via renato.kuiper@vka.nl.

AANVALLENDE OVERHEDEN: VALT ER NOG TEGENAAN TE BEVEILIGEN?

In 2010 maakten we kennis met Stuxnet, een complexe worm die zichzelf verspreidt door misbruik te maken van verschillende typen kwetsbaarheden. In 2013 volgde Edward Snowden en maakten we kennis met achtergehouden kwetsbaarheden in Cisco-apparatuur en diverse andere manieren om gebruik te maken van kwetsbaarheden in infrastructuren. Begin dit jaar kwam WikiLeaks met de 'Vault 7 Leaks', waarin we kennis maakten met diverse manieren waarop de CIA inbreekt op computersystemen en werden we wederom overspoeld met achtergehouden kwetsbaarheden die ons vatbaar maken voor misbruik. Als je als informatiebeveiliger dit soort nieuws volgt, kan de moed je af en toe in de schoenen zakken. Tegen de enorme offensieve capaciteit die wordt ingezet om kwetsbaarheden te (laten) vinden en geheim te houden, valt bijna niet op te beveiligen. Wat kunnen we als informatiebeveiligers leren van dit soort nieuwsberichten? Kunnen we onze informatie nog wel passend beschermen? Of is deze wedstrijd eigenlijk al verloren? En is het verstandig dat overheden kwetsbaarheden geheimhouden voor eigen gebruik, of zijn we er als maatschappij meer bij gebaat als overheden bijdragen om informatie(systemen) zo veilig mogelijk te houden?

Maarten Hartsuijker

Er is veel veranderd in ons werkveld de afgelopen jaren. Waar we voorheen veronderstelden dat we met snel patchen de belangrijkste kwetsbaarheden in onze software wegnamen, weten we nu dat het vinden, verkopen en geheimhouden van kwetsbaarheden een nieuwe bedrijfstak is geworden. Daar waar we er vroeger van uitgingen dat Safe Harbor de privacy van onze gegevens in de V.S. zou waarborgen, houden we er nu rekening mee dat het Privacy Shield vooral een lekker klinkend marketinginstrument is. En daar waar we er voorheen redelijk zeker van konden zijn dat verbindingen tussen datacenters geen extra versleuteling nodig hadden, moeten we er nu rekening mee houden dat ze afgetapt worden.

Als informatiebeveiliger ben je gewend om rekening te houden met een aanvallende tegenstander. Om je te beschermen tegen criminelen die in je financiële administratie willen inbreken of je af willen persen met ransomware. Maar tegen de enorme budgetten van aanvallende overheden valt eigenlijk niet meer op te beschermen. En de noodzaak om continu rekening te moeten houden met 'goede' of 'foute' cloud-omgevingen is niet bevorderlijk voor de innovatiekracht en efficiëntie van bedrijven.

Momenteel zien we in de regelgeving binnen ons werkveld steeds meer tegenstrijdigheden ontstaan. Aan de ene kant wordt in alle openheid privacywetgeving verscherpt en gevraagd van bedrijven om de beschermingsteugels strakker aan te trekken. Aan de andere kant buitelt men in schimmige hoekjes over elkaar heen om (zelfs 'onder vrienden') in te breken


Maarten Hartsuijker


Lex Dunn


Lex Borger

in elkaars vitale infrastructuren op jacht naar 'de beste data'. Steeds vaker worden er proefballonnetjes opgelaten om in de slipstream van een incident (never waste a good crisis) draagvlak te zoeken voor wetgeving die onze digitale veiligheid verzwakt in plaats van versterkt. We leven op alle fronten in een datagedreven maatschappij, maar voor veiligheid en betrouwbaarheid is het belangrijk om erop te kunnen vertrouwen dat tenminste de wetgever die jou vraagt om veiligheid en privacy te borgen geen baat heeft bij zwakheden in de IT-omgevingen die jij moet beschermen.

Lex Dunn

Er blijkt al jaren een 'rat-race' aan de gang te zijn, waarbij diverse partijen jagen op 'zero day-kwetsbaarheden' in zo ongeveer alles dat aan het internet hangt. Security-onderzoekers kunnen zowel op de zwarte als op de witte markt behoorlijke bedragen scoren voor zo'n gevonden kwetsbaarheid. Die kwetsbaarheden worden 'geheim' gehouden, en actief ge-/misbruikt. Daarbij gaat het om criminelen die de kwetsbaarheid misbruiken om toegang te krijgen tot systemen en applicaties. In het algemeen voor geldelijk gewin door diefstal en steeds vaker afpersing. Uit de Snowden-onthullingen en latere berichten (zoals recentelijk nog vanuit The Shadow Brokers) blijkt dat dit soort gaten ook door allerlei overheidsinstanties wordt gebruikt. Enerzijds om criminele, maar vooral terroristische, activiteiten op te sporen, bloot te leggen en te kunnen vervolgen. Maar anderzijds ook om spionageactiviteiten uit te voeren. Daarbij wordt, lijkt het wel, geen onderscheid meer gemaakt tussen bevriende naties, en 'de anderen'. Elke staat heeft haar eigen nationale inlichtingen- en veiligheidsdienst(en), die veelal zeer ruime operationele kaders hebben meegekregen. Veelal gaat het daarbij om economische spionage, maar ook cyber oorlogvoering speelt een steeds belangrijkere rol. De afgelopen tijd hebben we gezien dat het niet noodzakelijkerwijs gaat om het toebrengen van fysieke schade, het simpel verspreiden van 'nep-nieuws' blijkt ook al een effectieve beïnvloedingstactiek. Maar nu terug naar die 'geheime' kwetsbaarheden: het moge duidelijk zijn dat deze slechts 'waarde' hebben zolang de kwetsbaarheid nog niet publiekelijk bekend is gemaakt. Zo gauw het gat bekend is, kan er door de ontwikkelaars een 'pleister' voor gemaakt worden, waarmee het gat gedicht kan worden. Jammer genoeg hebben de bovengenoemde partijen geen enkele drijfveer om die (duur betaalde) kwetsbaarheden publiek te maken om zo het internet een beetje veiliger te maken. Criminelen niet, want zo lang de kwetsbaarheid bestaat kunnen ze er geld mee 'verdienen'. En overheden niet, omdat ze zo toegang hebben tot criminele en/of terroristische netwerken, of economisch interessante informatie. Alhoewel we er met z'n allen zeker bij gebaat zouden zijn als dit soort kwetsbaarheden zo snel mogelijk bekend gemaakt zou worden, gaat dat gewoon niet gebeuren. Althans niet door de bovengenoemde partijen die de kwetsbaarheden 'inkopen'. Gelukkig doen ook grote bedrijven als Google, Microsoft en Facebook steeds vaker een (flinke) duit in het zakje om kwetsbaarheden aan te kopen. Die worden dan (over het algemeen) binnen redelijke tijd gedicht. De enige hoop die ik als informatiebeveiliger wat dit betreft heb, is dat er gelukkig nog steeds security onderzoekers zijn, die niet zwichten voor het grote geld, en de door hun gevonden kwetsbaarheden publiekelijk bekend maken (uiteraard via Responsible Disclosure). Of we die race ooit zullen winnen: ik betwijfel het. Maar gelukkig zijn er klokkenluiders zoals Snowden.

Lex Borger

We moeten er van uitgaan dat er onontdekte kwetsbaarheden zijn die bij aanvallers bekend zijn. En ons ervan bewust zijn dat er aanvallers zijn die veel tijd en geld willen investeren om ons te infiltreren en eventueel jarenlang stil verborgen in de bosjes te zitten. Passende bescherming is zeker wel mogelijk, met toepassing van een paar aloude beveiligingsprincipes: pas meerlaagsbeveiliging toe, faal veilig en meten is weten. Stomweg alleen een preventieve maatregel nemen, is er niet meer bij. Honderd procent veilig kunnen we het niet maken. Vroeger niet, nu ook niet.
Ik blijf een eeuwige optimist, die blijft geloven in onze eigen weerbaarheid. Uiteindelijk kunnen we als maatschappij veel doen als het moet. Een voorbeeld dat ik aan kan halen, is de recente focus op PFS, perfect forward secrecy. Na de onthullingen van Snowden is de toepassing van PFS in TLS-verkeer ineens helemaal 'hot' en is je TLS-tunnel minderwaardig als jouw webserver geen PFS toepast bij TLS-verkeer. Daarvoor was er nauwelijks aandacht voor. Kwetsbaarheden geheimhouden voor eigen gebruik heeft twee kanten. De geheime diensten hebben er baat bij als aanvaller gebruik te kunnen maken van 0-days. Je kunt er echter nooit van uitgaan dat je tegenstander de kwetsbaarheid niet kent. Als ze die wel kennen, kunnen ze jou voor gek zetten en diezelfde kwetsbaarheid tegen jou gebruiken. Een groot risico. Als maatschappij willen we veilig zijn en dus onze verdediging zoveel mogelijk op orde hebben. Hier hoort bij dat kwetsbaarheden die je kent ook verholpen zijn.

Deze editie van Achter het Nieuws bleek bij het ter perse gaan zeer actueel: op 12 mei 2017 brak WannaCry uit.

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

LET OP JE WOORDEN

We zaten laatst met een aantal vrienden mijn nieuwe smart-tv van Samsung te bewonderen en ik liet trots alle mogelijkheden zien. De vrienden waren allemaal onder de indruk, vooral nadat ik ze de prijs had verteld. Verbluft waren ze, dat je voor betrekkelijk weinig geld zoveel techniek in huis kunt halen. Een paar biertjes later vertelde één van de aanwezigen dat als we met zijn allen ter plekke het merk van onze biertjes zouden benoemen, ik binnen een aantal weken op websites die ik bezoek bedolven zou worden onder de advertenties van het betreffende biermerk. We keken hem aan met een blik vol ongeloof over dat je na twee biertjes al zulke rare dingen kan zeggen.

Hij stond op en pakte de afstandsbediening van de tv. Hij deed de televisie aan en zei iets. Ik zag inderdaad een microfoonicoontje op het scherm verschijnen. We werden allemaal stiller en mijn vriend zei dat Samsung het recht had om de geluiden te ontvangen op hun servers en vervolgens te analyseren. Ik voelde mij niet blij en zag de televisie graag weer uitgaan. Ik was een beetje stil en besloot het onderwerp om te buigen naar de pop die ik kocht voor mijn kleindochter. Ik waande mij volledig veilig tot dezelfde man gretig om het merk vroeg van de pop. Ik voelde het hart in mijn keel kloppen toen ik een herkennende knik van hem zag toen ik het merk noemde.

Ik besloot in een wilde poging om het onderwerp weer van tafel te krijgen eenieder te vragen of ze nog iets te drinken wilden. Ik stond op om een paar biertjes te pakken en opende ze aan tafel. Ik zat nog niet of meneer begon weer over die stomme poppen. Hij vertelde een vergelijkbaar verhaal als over mijn tv, maar dit kwam nog een slagje enger over. Kinderen praten tegen de pop en de pop ontvangt die gegevens om ze vervolgens via het internet te laten analyseren en de pop een passend antwoord te laten geven. Volgens de verpakking was de pop in staat om de stemming van de kinderen te herkennen. Gelukkig zaten de batterijen er nog niet in, anders zou de pop rode koontjes krijgen als hij mijn stemming wist te herkennen. Mijn vriend bleef maar doorgaan en gaf aan dat de data niet direct weggegooid werd, maar gebruikt zou kunnen worden om de kinderen via de pop reclame aan te bieden.

Ik besloot mijn biertje te laten staan en over te gaan op een glas water. Ik was met mijn hoofd niet meer bij het gesprek en probeerde mijn boosheid niet te laten blijken. Gelukkig was het laat geworden en besloten mijn vrienden naar huis te gaan. Nadat ik ze gedag had gezegd, ging ik weer zitten met de doos waarin de pop zat. Ik heb de batterijen eruit gehaald toen mijn vrouw binnenkwam. "Zo, dus jij bent met de pop van je kleinkind aan het spelen?" Ik vertelde dat ik hem nog eens wilde bekijken. Ze vroeg of ik me goed voelde. Ik speelde de vrolijke man en vroeg haar waarom ze dat dacht. "Omdat je je biertje niet op hebt gedronken." Ik deed er maar het zwijgen toe.

Berry

SECURITY ACADEMY

NIEUW

SECURITY AUDITING
PRACTITIONER

Leer in vijf dagen de belangrijkste elementen van auditing
en behaal uw S-SAP titel van SECO-Institute

De opleiding **Security Auditing Practitioner** leert u nu eens echt hoe u een audit uitvoert. Hierbij wordt bijzondere aandacht gegeven aan security aspecten zoals bijvoorbeeld security normen (ISO27001, 27002), systeemontwikkeling, beheer en business continuity. De opleiding wordt afgesloten met het **officiële SECO-Institute examen** waarmee u uw internationale **S-SAP audittitel** kunt behalen.

Theorie en toepassing gaan hand in hand in deze opleiding door het veelvuldig gebruik van **praktijkcasussen**. Zo ontwikkelt u uw kennis, kunde en vaardigheden op het gebied van **(security-)auditing**. Na het volgen van deze opleiding bent u in staat zelfstandig een audit van een gemiddelde complexiteit uit te voeren.

Deze opleiding is bedoeld voor de **beginnende (security) auditors** die zich verder wil ontwikkelen in het audit-vakgebied en hun kennis en kunde willen uitbreiden en verdiepen ook richting **IT-security**. Deze opleiding is tevens zeer geschikt voor **informatiebeveiligers** die zich willen verdiepen in het audit vak.

De Security Academy biedt naast de **Security Auditing Practitioner** van SECO-Institute ook andere SECO-tracks aan waar u een internationale titel mee kunt behalen:

SECO CERTIFIED OFFICER — INFORMATION SECURITY

SECO CERTIFIED OFFICER — IT-SECURITY

SECO CERTIFIED OFFICER — PRIVACY & DATA PROTECTION

SECO CERTIFIED LEADER — ETHICAL HACKING

SECO CERTIFIED LEADER — SECURE SOFTWARE

SECO CERTIFIED OFFICER — CRISIS MANAGEMENT

SECO CERTIFIED OFFICER — BUSINESS CONTINUITY

www.securityacademy.nl info@securityacademy.nl +31(0)348-40 80 61