iB
INFORMATIEBEVEILIGING
jaargang 16 - 2016
#6

privacy

Privacy by design

Security standaarden

Versleuteling en sleutelbeheer

Verslag The Next Web

Waarom we een CISO en een Information Security Specialist zoeken

www.pggm.nl/werkenbij

We werken aan de toekomst van 2,7 miljoen mensen. We beheren ruim 185 miljard aan pensioenvermogen. Dat vereist uiterste zorgvuldigheid. We willen informatiebeveiliging nu naar een nog hoger niveau brengen. Onze nieuwe CISO en Information Security Specialist moeten ons Security en Quality Office daarbij gaan versterken.

CISO

Je stelt PGGM's beveiligingsstrategie op. Je monitort de processen en geeft vorm aan het Security & Quality Office. Als partner van de business verhoog je het risicobewustzijn van de hele organisatie.

Information Security Specialist

ICT security is je kerntaak. Je borgt het beleid, voert assessments uit en optimaliseert het incidentproces. Je beoordeelt de beveiliging bij leveranciers en ondersteunt onze managementteams.

Wat we nog meer van onze nieuwe CISO en security specialist verwachten, lees je op pggm.nl/werkenbij

PGGM

Voor een waardevolle toekomst

THEATERVOORSTELLINGEN

Dezer dagen kom je bij het reizen veel beveiliging tegen. Bruce Schneier noemt het 'security-theater', omdat het ontworpen is om er veilig uit te zien, niet omdat het per se veilig is. Ik heb deze zomer ook veel security-theater gezien. De e-reader die ik op eBay kocht, is opengemaakt onderweg. De envelop is opengescheurd, en er zit een sticker op: 'Dangerous goods inspection'. Nergens treedt het security-theater duidelijker op dan op Schiphol. Twee kilometer file op de A4 omdat we de afrit Schiphol beveiligen... Ga je vanaf Badhoevedorp of Hoofddorp binnendoor naar Schiphol dan hoef je niet langs zo'n controle, want je gaat niet langs het podium. Het is niet voor niets een theater, toch?
Dus ik verwachtte dat het in de Verenigde Staten nog erger zou zijn. Het theater daar is zeker gericht om bezoekers te controleren bij binnenkomst. Daarna is het eigenlijk heel relaxed. Geen dreigend uitziende mannen met automatische wapens, je voelt je vrij, op de controles bij de ingang van attracties na. Maar ook die controles stellen niets voor vergeleken met de screening bij Schiphol.
In Central Park is er helemaal geen beveiliging te zien, ook al is er dat weekend een wielersport-event. Aparte belevenis, zo'n groot park met wilde gebieden midden in een wereldstad. En bij de zuidelijke ingang aan 5th Avenue was er elke avond een hele samenscholing van Pokémon-spelers [1]. De paar politiemensen die erbij waren, zagen de beren broodjes smeren, meer niet.
Is er dan gewoon geen aandacht voor de veiligheid op straat? Zeker wel. Als je goed rondkijkt zie je overal op straat de verkeersagenten. Het lijkt wel of ieder kruispunt er een heeft staan om het verkeer zo soepel mogelijk door te laten stromen. Die mannen en vrouwen zien natuurlijk alles. En omdat ze continu met hun omgeving bezig zijn ontgaat ze niets. Het komt alleen helemaal niet dreigend over. Het is waarschijnlijk wel een effectievere detectiemaatregel.
Eén plaats had wél een duidelijke aanwezige beveiliging: Trump Tower. Politie, FBI en civiele beveiligingsklerenkasten staan voor het gebouw geposteerd, samen met nieuwsploegen die zich trouw elke dag weer opstellen. En dat terwijl Donald er zelf niet eens was, die had afspraken in Cleveland. Toch wel knap dat die fan van Trump een paar weken later buiten tegen het gebouw omhoog kon klimmen [2]. Kennelijk was hier toch weer sprake van security-theater.
Zo zie je maar: beveiliging hoeft niet security-theater te zijn, integratie met de dagelijkse werkzaamheden heeft wellicht betere beveiliging tot resultaat.

Lex Borger, Hoofdredacteur

Links

[1] https://www.youtube.com/watch?v=0eloPUvcC6U
[2] http://www.nytimes.com/2016/08/11/nyregion/man-climbs-trump-tower.html

In dit nummer

PRIVACY BY DESIGN
IS EEN BUSINESS VRAAGSTUK

'Privacy by design', het begrip klinkt logisch en eenvoudig. In de praktijk is geen van beide waar. Een grote misvatting is dat Privacy by Design wordt gezien als een technisch vraagstuk en dat al snel kan worden volstaan met anonimisering en versleuteling. Privacy by Design is veel meer dan dat: het is vooral een vraagstuk voor procesontwerp en -beheer. Renato Kuiper en Frank van Vonderen beschrijven in dit artikel wat zij zien als 'Privacy by Design' en hoe organisaties dit kunnen vertalen naar de eigen bedrijfsvoering.

Wat is Privacy by Design? Het antwoord op deze vraag is niet eenduidend. Privacy by Design wordt allesbehalve eenduidig beschreven. Vaak wordt verwezen naar de 7 foundational principles van Ann Cavoukian [1], of de publicatie van Enisa [2]. Daarbij valt op dat de interpretaties onderling nogal verschillen. Dichter bij huis geeft de Autoriteit Persoonsgegevens de volgende toelichting: "Privacy by Design" houdt in dat u als organisatie al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) ten eerste aandacht besteedt aan privacy-verhogende maatregelen, ook wel Privacy Enhancing Technologies (PET) genoemd [3]. Ten tweede houdt u rekening met dataminimalisatie: u verwerkt zo min mogelijk persoonsgegevens, dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking. Op deze manier kunt u een zorgvuldige en verantwoorde omgang met persoonsgegevens technisch afdwingen."
Privacy by Design houdt dus twee dingen in, al zouden wij de volgorde liever omdraaien omwille van efficiëntie: 1. het zo min mogelijk verwerken van persoonsgegevens en 2. het vervolgens 'inbouwen' van privacy door het inzetten van technologieën die de persoonsgegevens beschermen.

Maar hoe maak je dit nu concreet? Dit beschrijven we hierna, aan de hand van de acht OECD-principes voor privacy [zie kader]. We kiezen voor de OECD-principes, omdat deze als generiek framework beter passen bij de doelstellingen die de privacy-wetgeving nastreeft.

The OECD Privacy Principles

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

Bron: OECD Privacy Principes [4]

Collection Limitation-principe

Het Collection Limitation-principe betekent feitelijk dat je alleen die persoonsgegevens verzamelt die je nodig hebt. Maar wat heb je minimaal nodig om je werk goed te kunnen doen. En welke informatie verzamel je vooral om de klant beter te kunnen helpen.
Vertaling naar de praktijk: een bekend voorbeeld zijn aanvraagformulieren, waarbij je het hemd van het lijf wordt gevraagd, waarbij je je afvraagt waarom men bepaalde gegevens eigenlijk nodig heeft. Bij administratieve processen staat het Collection Limitation-principe op gespannen voet met het principe van eenmalige gegevenscollectie. Bij dit laatste is de gedachte dat een administratief proces uit verschillende stappen bestaat, maar dat bij de eerste stap alvast alle gegevens voor alle stappen worden opgevraagd om te voorkomen dat een persoon verschillende keren langs het (digitale) loket komt om steeds aanvullende stukjes informatie te verschaffen.
In dit geval moet een organisatie dus een keuze maken tussen ofwel zo min mogelijk gegevens verzamelen en later de klant vragen om aanvullende informatie, of alles in één keer vragen waarbij je ook gegevens ontvangt die je niet altijd zult gebruiken. Dit vraagt per case om een eigen afweging: welke hoeveelheid data wordt mogelijk te veel verzameld en hoe lastig is het om de klant later nogmaals te benaderen voor aanvullende informatie.
Een verdere vrije interpretatie van het principe van 'collection limitation' is de vraag: welke informatie heb je eigenlijk nodig. Regelmatig is zichtbaar dat organisaties een bepaalde toets willen doen en daarbij meer persoonsgegevens vragen dan nodig is. Voorbeelden:
Bij een inkomenstoets wordt gevraagd naar het inkomen van een betrokkene (een absolute waarde, met enige gevoeligheid), in plaats van dat wordt gevraagd of iemand meer of minder dan drempel x verdient (een ja/nee waarde, met lagere gevoeligheid)
Bij het bepalen van het kortingspercentage voor toegang van kinderen wordt gevraagd naar de geboortedatum van een bezoeker (enige gevoeligheid). Alternatief zou kunnen zijn: is of de bezoeker geboren voor of na datum XYZ (veel lagere gevoeligheid).
De vraag bij dit soort voorbeelden is dus: heb je letterlijk deze informatie nodig, of gebruik je deze informatie om een


Frank van Vonderen is management consultant bij Verdonck, Klooster & Associates en bereikbaar via frank.vanvonderen@vka.nl.
Renato Kuiper is security architect bij Verdonck , Klooster & Associates en bereikbaar via renato.kuiper@vka.nl.

Privacy by Design: zo min mogelijk verwerken persoonsgegevens en inzetten beschermende technologieën

afweging te maken en zou het ook volstaan om de afweging aan de betrokkene te vragen?

Wat ons betreft past ook het tijdig en gestructureerd verwijderen van persoonsgegevens binnen het principe van collection limitation. Het simpele uitgangspunt is hierbij: als (persoons)gegevens niet langer nodig zijn en wettelijk gezien niet moeten worden bewaard, moeten deze worden verwijderd. Tegelijkertijd leert de praktijk dat dit niet eenvoudig is. Met de digitalisering van archieven en de lage kosten voor opslag is nooit structureel rekening gehouden met het tijdig verwijderen. In veel organisaties worstelt men met het zowel voldoen aan de archiefwetgeving of bewaarplicht in relatie tot privacy.
Vertaling naar de praktijk: de exacte kaders voor de bewaarplicht zijn vaak niet helder (hoe lang, welk deel van de informatievoorziening). Gevolg is dat vaak niet goed wordt nagedacht over wat moet worden bewaard en waarom. Het selectief bewaren van kerndocumenten uit een dossier (in plaats van een compleet dossier) of het onleesbaar maken van gevoelige persoonsgegevens (bijvoorbeeld het na x aantal jaren weghalen van BSN's bij contracten en dan wel de akten bewaren) is vaak bij de dossiervoering en archiveringsprocessen niet ingebouwd. Daarnaast zijn veel stukken zodanig gedigitaliseerd, dat de stukken niet meer kunnen worden doorzocht op specifieke kenmerken zoals persoonsgegevens. Simpel gezegd zijn veel documenten gescand als 'plaatje' en niet als tekstbestand. Dit belemmert het zoeken én belemmert de mogelijkheden tot anonimisering of het efficiënt zoeken en uitvlakken van persoonsgegevens in archieven.

Bij het ontwerpen van een gegevenshuishouding moet dan ook gekeken worden naar:

1. Het bepalen van de bewaartermijn. Hoe lang moet worden bewaard en wat moet worden bewaard (bijvoorbeeld alleen een instemming, of een volledig dossier)?
2. Het vernietigen, zodanig dat tijdens het vernietigen niets lekt of onbedoeld achterblijft.

Data Quality-principe

Het Data Quality principe is niet specifiek voor privacy. Data Quality is een principe dat vooral in het Business Intelligence (BI) vakgebied is uitgewerkt. Het begrip Data Quality bestaat voor BI uit de volgende aspecten [5]:
Volledigheid – Dit geeft aan dat de volledige verwachte dataset aanwezig moet zijn. Bij consolideren van data uit verschillende bronnen, kan dit wel eens een uitdaging zijn. Het volledigheidsaspect heeft wel een mogelijke relatie voor privacy. In dit geval kan door een gebrek aan informatie een verkeerde conclusie worden getrokken. Met meer context gerelateerde informatie kan een gegeven anders worden geïnterpreteerd.
Consistentie – Dit aspect heeft ermee te maken dat door het hele systeem consistente data is opgenomen. Zo kunnen er geen rekeningen worden betaald door iemand die niet heeft besteld, of kan er geen salarisstrook worden aangemaakt voor iemand die niet meer in dienst is. Voor dit aspect zie ik geen specifieke relatie met privacy, behalve dat inconsistentie een relatie zal hebben met de accuraatheid of volledigheid van de gegevens.
Conformiteit – Dit aspect heeft ermee te maken dat door het hele systeem dezelfde coderingen en verwijzingen gebruikt worden (bijvoorbeeld dd/mm/yyyy als standaard notitie voor een datum). Voor dit aspect zien we geen specifieke relatie met privacy, behalve dat inconsistentie een relatie zal hebben met de accuraatheid of volledigheid van de gegevens.
Accuraatheid – Dit geeft aan in hoeverre de data de werkelijkheid weergeeft. Ook dit aspect heeft een relatie met privacy. Door verkeerde informatie kan een verkeerde conclusie worden getrokken. Als bijvoorbeeld ergens is vermeld dat de bewoner van Dorpsstraat 48 een strafblad heeft voor een zedendelict, maar als dat de Stationsstraat 38 had moeten zijn kan dit tot ongewenste effecten leiden.
Integriteit – Het aspect integriteit heeft binnen het vakgebied Business Intelligence een eigen, wat meer technisch georiënteerde betekenis. Het gaat hier niet over de persoonlijke integriteit, maar over de validiteit van de data en het feit dat de relatie tussen de data klopt. Zo bestaat er een vaste relatie tussen een postcode en een straatnaam / huisnummer. Als deze twee niet met elkaar in overeenstemming zijn, is dit een integriteitsissue.
Tijdigheid – Dit is de mate waarin data op tijd aanwezig is. Bijvoorbeeld: In een datawarehouse omgeving, waarin de gefactureerde omzet elke nacht wordt geladen, moet deze data elke morgen volledig beschikbaar zijn. Bij privacy wordt vaak het eerst gedacht aan vertrouwelijkheid naar persoonsgegevens, daarna gevolgd door de juistheid ervan. Ook de (tijdige) beschikbaarheid van persoonsgegevens is echter een onderdeel van privacy. Op dit punt ligt dan ook een de relatie.

Hoe kan principe Data Quality nu het beste naar de praktijk worden vertaald? Discussies over welke informatie betrouwbaar is kunnen worden voorkomen door het bieden van de "single point of truth" of "Authentiek bronregister". Dit houdt in dat zoveel mogelijk gebruik wordt gemaakt van één goed georganiseerde bron voor de data en dat kopieën en afgeleiden (die vaak minder goed en frequent worden onderhouden) worden voorkomen. Zo min mogelijk kopieën van databases of exports naar Excel dus. Naast het vergroten van de kwaliteit van de persoonsgegevens verbetert het de transparantie en vereenvoudigt dit de beveiliging.

Use Limitation-principe

Het Use Limitation-principe houdt in dat de persoonsgegevens niet anders mogen worden gebruikt dan voor het oorspronkelijke doel, zoals dit oorspronkelijk is vastgesteld. Aanvullend gebruik mag alleen als hiertoe een wettelijke grondslag is, of als de gebruiker hiermee instemt. Mochten gegevens door een organisatie anders worden gebruikt dan oorspronkelijk is bedoeld, dan is de kans groot dat men hiervoor (expliciet) de aanvullende goedkeuring van de betrokkene moet vragen. Wat betekent dit in de praktijk? Bij de ontwerp van een bedrijfsproces moet worden gekeken waar de gebruikte gegevens vandaan komen en wat de grondslag is.
Vertaling naar de praktijk: organisaties hebben hiermee bijvoorbeeld te maken bij het gebruik van kernregistraties (zoals de Basisregistratie Personen) en bij het gebruik van het Burger Service Nummer (BSN). Het feit dat je toegang hebt tot deze persoonsgegevens, betekent niet dat je ze overal voor mag gebruiken. Een voorbeeld van dat laatste: in een personeelssysteem is het BSN opgenomen ten behoeve van fiscale verplichtingen. Dit BSN mag dan alleen worden gebruikt voor de fiscale verantwoording, niet op de verlofbriefjes, in de HR-rapportages of bij de informatieuitwisseling rondom de ziekmeldingen.
Er zijn twee bekende uitdagingen, waarbij er een behoefte bestaat om persoonsgegevens breder te gebruiken. De eerste bekende uitdaging voor organisaties is dat men gegevens uit bronsystemen wil combineren om bepaalde analyses te doen die de kwaliteit of de efficiëntie van de dienstverlening kunnen verbeteren. Dit soort initiatieven wordt vaak Big Data of Business Intelligence genoemd. Bij deze toepassingen is het zaak om gegevens zodanig aan te bieden aan omgevingen dat deze zijn ontdaan van persoonsgegevens (anonimiseren) of dat gebruik wordt gemaakt van pseudonimisering. Pseudonimisering is het vervangen van de identificerende gegevens door een pseudoniem waardoor gegevens niet meer te herleiden zijn tot de persoon. Voor beide blijft echter een restrisico bestaan, namelijk dat door het combineren van meer data uiteindelijk zoveel attributen van personen bekend zijn dat hun identiteit daar makkelijk uit kan worden afgeleid.
De tweede uitdaging is dat de ICT-afdeling ten behoeve van systeemontwikkeling en probleemanalyse graag, en soms noodzakelijkerwijs, gebruik maakt van representatieve testgegevens. Met deze testgegevens kan men de actualiteit naspelen en de gangbare mening is dat hoe waarheidsgetrouwer deze data is, hoe beter de test ook is. Het gebruiken van 'een kopietje van de productiedatabase' is echter ongewenst en ook vrijwel altijd onnodig. Voor het ontwikkelen en uitvoeren van functionele testen kan worden volstaan met een nagemaakte set van testgegevens, bijvoorbeeld 'Jan Jansen uit Lutjebroek'. Er zijn intussen ook technische oplossingen beschikbaar die fictieve testgegevens kunnen genereren, of bestaande gegevens kunnen anonimiseren of pseudonimiseren. Meestal is pas bij een allerlaatste functionele test kan het nodig zijn dat productiegegevens (echte gegevens) worden gebruikt. Indien dit echt noodzakelijk is, kan de verstrekking daarvan incidenteel worden gefaciliteerd binnen een geconditioneerde situatie. In onze ervaring blijkt in de grote meerderheid van de testwerkzaamheden het uiteindelijk helemaal niet nodig is om persoonsgegevens te verstrekken voor testdoeleinden.

Purpose Specification-principe

Met deze laatste voorbeelden wordt ook de uitdaging voor voorgaande principe, Purpose Specification, helder. Dit principe vraagt dat het doel van de gegevensverzameling bij de aanleg van de verzameling bekend is en dat het doel niet achteraf wordt aangepast. De suggestie om gegevens op te nemen in een BI-omgeving of ze tijdens testen te gebruiken is zelden initieel bedacht, maar iets waaraan gaandeweg de behoefte groeit. Het ontdoen van de specifieke persoonsgebonden kenmerken voorkomt ook frictie met dit principe, net als bij Use Limitation. Aan de andere kant kan bij de definitie van de 'purpose specification' ook rekening gehouden met een breder gebruik van gegevens, ook bijvoorbeeld ten behoeve van de BI-analyses op metaniveau.

Security Safeguards-principe

Het bepalen van de Security Safeguards is een vakgebied op zich. De keuze van de juiste security-maatregelen hangen sterk samen met de technologie (hardware, applicaties) waarbinnen de persoonsgegevens worden verwerkt. Bovendien staat de kwaliteit van de maatregelen in relatie tot de stand van de techniek. Met de huidige stand van de techniek (anno 2016) worden de volgende maatregelen doorgaans als passend gezien [6]:

1. Authenticatie op een vertrouwde locatie, zoals een werkplek binnen een beveiligd kantoor en op een beveiligd netwerk, vindt minimaal op basis van een kenniskenmerk

(wachtwoord) plaats.
2. Authenticatie op een niet-vertrouwde locatie, zoals een werkplek thuis of in een openbare ruimte, of via een niet vertrouwd netwerk, vereist naast het kenniskenmerk ook een bezitskenmerk.
3. Persoonsgegevens die worden verstuurd over het bedrijfseigen beveiligde netwerk worden bij voorkeur versleuteld; buiten het eigen beveiligde netwerk, zoals internet, worden ze altijd versleuteld. Dit geldt ook op draagbare media.
4. Services die persoonsgegevens verwerken of aanbieden zijn niet te benaderen zonder autorisatie en authenticatie, bijvoorbeeld door het gebruik van certificaten.
5. Fysieke en logische maatregelen schermen de verwerking van de persoonsgegevens af, bijvoorbeeld door servers in afgesloten ruimtes te plaatsen en systemen/componenten te 'hardenen'.
6. De toegang tot persoonsgegevens door systeembeheerders wordt vastgelegd (tijd en raadpleger worden gelogd).
7. De toegang en het gebruik wordt vastgelegd (tijd, raadpleger, proces, en resultaat worden gelogd). In aanvulling op de maatregelen voor de 'gewone' persoonsgegevens worden de volgende maatregelen voor bijzondere persoonsgegevens doorgaans als passend gezien:
8. Authenticatie vindt naast het kenniskenmerk altijd ook op basis van een bezitskenmerk plaats.
9. Bijzondere persoonsgegevens worden, ook als ze verstuurd worden over het bedrijfseigen beveiligde netwerk, versleuteld.

Openness-principe

Het Openness-principe vereist dat organisaties open en transparant zijn in de omgang met persoonsgegevens. Wij zien niet hoe de toepassing van Privacy by Design kan helpen bij een betere openness. Wel andersom: als organisaties effectief zijn in Privacy by Design, kan dit worden gebruikt in uitingen (denk aan beleid, presentaties) waardoor men zich als verantwoordelijke organisatie kan onderscheiden en vertrouwen kan winnen.

Individual Participation-principe

Het Individual Participation-principe vraagt om mogelijkheden om te kunnen voldoen aan inzage, correctie en wijzigingsvereisten. Een organisatie moet in staat zijn om binnen de eigen informatievoorziening te kunnen nagaan welke gegevens van een persoon bekend zijn en deze daar waar nodig aan te passen en te verwijderen.

Indien gegevens moeten worden aangepast, moeten de gegevens niet alleen worden aangepast in de authentieke bron (de eerder genoemde 'single point of truth'), maar ook in de afgeleide kopieën ervan. Wanneer gebruik wordt gemaakt van het recht van verwijdering geldt voor een deel hetzelfde: de gegevens worden verwijderd in de authentieke bron én in afgeleide kopieën. Daarbij moet de verwijdering permanent zijn. Dit klinkt op zich logisch, ware het niet dat in databases soms een gegeven niet kan worden verwijderd, maar hoogstens als 'inactief' wordt gemarkeerd.

Het feit dat in een informatiesysteem de rechten van individuen moet kunnen worden uitgeoefend moet worden vertaald naar een functionele eis en (bij voorkeur) bij oplevering ook worden getoetst.

Accountability-principe

Volgens het Accountability-principe moet de verantwoordelijke zorgen dat aan alle principes is voldaan. Bij Privacy by Design zou dit moeten betekenen dat bij een oplevertoets moet worden vastgesteld dat alle principes adequaat zijn gevolgd. Dit zou bijvoorbeeld kunnen in de vorm van een bijdrage aan de acceptatietest werkzaamheden door een betrokken privacy-adviseur.

Conclusie

Privacy by Design is meer dan versleutelen of anonimiseren. Privacy by Design vraagt om een gestructureerde aanpak, waarbij op basis van bedrijfsprocesanalyse verstandig gebruik wordt gemaakt van persoonsinformatie. Daarmee is Privacy by Design vooral een vak voor bedrijfskundigen, informatieanalisten en procesarchitecten.

Links

[1] 7 foundational principles van Ann Cavoukian: https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf
[2] Enisa, Privacy and Data Protection by Design: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport
[3] AP, Privacy by design: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacycheck/privacy-design
[4] OECD Privacy Principes http://oecdprivacy.org/#principles
[5] 6 Dimensions of Data Quality: http://smartbridge.com/data-done-right-6-dimensions-of-data-quality-part-1/
[6] CIP, Handleiding Privacy by Design, conceptversie: http://www.cip-overheid.nl/wp-content/uploads/2016/03/20160223_Handleiding_Privacy_by_Design_v08.pdf

Wij feliciteren
onze studenten met hun S-CISO titel!

De afgelopen jaren hebben wij vele professionals mogen opleiden met onze **Post-HBO Information Security Management Professional** opleiding. Met het voltooien van deze geaccrediteerde Post-HBO opleiding is de titel **ISMP** behaald. Iedereen die deze ISMP titel heeft behaald en tevens over voldoende werkervaring beschikt, heeft hiermee aangetoond op het SECO-Institute Certified Officer niveau te kunnen acteren. Vanaf heden mag men dan ook de internationaal erkende Certified Information Security Officer **(S-CISO)** titel voeren.

De S-CISO titel wordt uitgegeven door **SECO-Institute** en is de hoogst haalbare internationaal erkende certificering in Information Security Management. Met deze titel toont u aan dat u op management-level het informatiebeveiligingsproces kunt implementeren, borgen en onderhouden.

Wilt u kijken of u ook in aanmerking komt voor deze S-CISO titel? Ga dan naar **www.seco-institute.org/claim-your-title**

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

SECO CERTIFIED OFFICER — IT-SECURITY

SECO CERTIFIED LEADER — ETHICAL HACKING

SECO CERTIFIED OFFICER — BUSINESS CONTINUITY

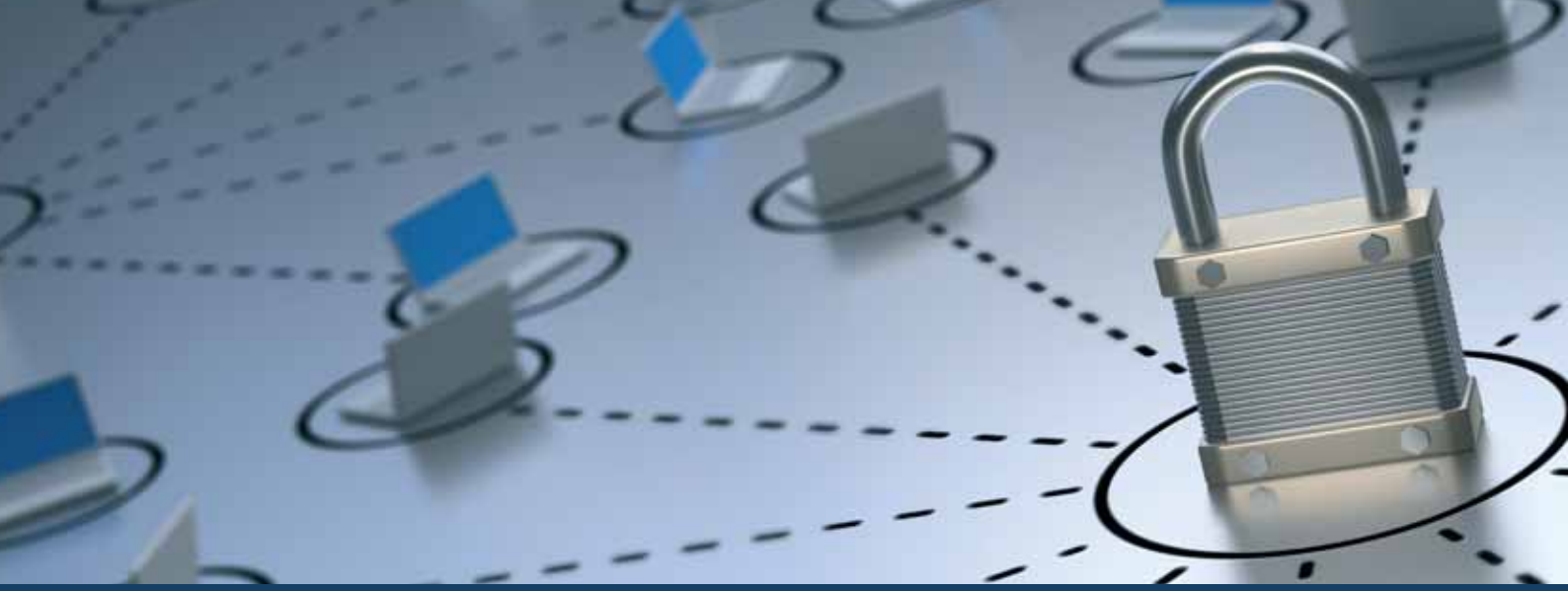
SECO CERTIFIED OFFICER — PRIVACY & DATA PROTECTION

SECO CERTIFIED LEADER — SECURE SOFTWARE

SECO CERTIFIED OFFICER — CRISIS MANAGEMENT

Voor meer informatie kunt u terecht op onze vernieuwde website of neem contact met ons op per mail of telefoon.

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



VOER JE NETWERK-SECURITY NIET OP

Creëer een veilig netwerk

Security-professionals hebben een probleem. Organisaties worden geconfronteerd met een oneindige stroom van cyberaanvallen en moeten die met man en macht zien te bevechten. In een poging om de beveiliging op te voeren schaffen zij maar al te vaak lukraak security-oplossingen aan. Door meer security-lagen aan hun netwerk toe te voegen hopen zij cyberbedreigingen de baas te kunnen blijven.

Dit heeft geresulteerd in een onbeheerbare lappendeken van security-oplossingen die stuk voor stuk beweren het netwerk veilig te houden.
Organisaties duwen hiermee in feite het 'verdediging in de diepte'-model naar het uiterste. En dat gaat tegen hen werken. Ze zijn zo veel tijd en geld kwijt aan het bijwerken van een breed scala aan security-voorzieningen, waardoor ze onvoldoende tijd overhouden voor het inrichten van een netwerk dat écht veilig is. In plaats van meer zekerheid resulteert dit in zorgwekkende complexiteit.
We worden tegenwoordig bestookt met nieuwe appliances die beloven om ons netwerk veilig te houden voor allerlei specifieke bedreigingen. Maar als we voor elke nieuwe bedreiging een nieuwe security-laag toevoegen, maakt dat ons niet veiliger. Integendeel: we komen daarmee te zitten met talloze geïsoleerde eilandjes van technologie die in de laatste instantie onvoldoende effectief zijn.
Feit is dat er een fundamentele verandering nodig is in de manier waarop we de beveiliging benaderen. We moeten onze prioriteiten herzien en onze focus verschuiven van het opvoeren van beveiliging van het netwerk naar het creëren van een veilig netwerk. Hoewel het belangrijk is om met verschillende beschermingslagen te werken, moeten organisaties grotere nadruk leggen op de manier waarop zij hun security-oplossingen integreren, up-to-date houden en beheren.
Automatisering en beheer zouden voorop moeten staan bij de beveiliging van netwerken. Er zouden ook op andere punten binnen het netwerk dan de firewall-regels moeten worden

toegepast om bedreigingen een halt toe te roepen. Verder is een effectievere integratie nodig van informatie over bedreigingen uit diverse bronnen. De analyse van deze verzamelde bedreigingsinformatie moet vervolgens worden geautomatiseerd. Daarna is het de taak aan de organisaties, die moeten zorgen voor centraal beheer en aanpassing van de security-regels. Deze regels moeten op een zo breed mogelijke schaal worden afgedwongen binnen de bedrijfsbrede ICT-infrastructuur.

We moeten op een nieuwe manier gaan nadenken over het detecteren van bedreigingen en het definiëren en toepassen van beleidsregels. Organisaties kunnen verschillende maatregelen treffen om een veilig netwerk te creëren in plaats van de netwerksecurity voortdurend op te moeten voeren.

1) Maak gebruik van een policy engine op basis van open standaarden: De security-branche spreekt al decennialang over de noodzaak van universele regels en policy engines. Het vertalen van beleidsregels en zones tussen policy engines wordt steeds moeilijker. De reden hiervoor is dat CISO's en CIO's minimaal drie generaties aan apparaten hebben geërfd waarvoor weinig documentatie beschikbaar is. Dit vergroot het belang van een geautomatiseerde en geïntegreerde policy engine die het mogelijk maakt om security-regels uit te wisselen op basis van open standaarden. De branche zou open source-specificaties voor de uitwisseling van informatie over cyberbedreigingen moeten omarmen, zoals TAXII™, STIX™ en CybOX™. Een volledig overzicht van deze specificaties is te vinden op de website van het Computer Emergency Readiness Team van de Amerikaanse overheid (US-CERT) [1].

Van deze drie specificaties is STIX™ het meest gericht op de uitwisseling van bedreigingsinformatie. Dit kader kan bijdragen aan een nieuwe aanpak van cyberbedreigingen en de detectie van kwaadaardige activiteiten.

2) Zorg voor netwerkbrede detectie: We zouden in staat moeten zijn om de laatste technologie in te zetten om de activiteiten van cybercriminelen sneller op te merken. Net als met STIX™ zouden we alle bruikbare realtime informatie moeten inzetten voor het identificeren van bedreigingen. Met de uitwisseling van bedreigingsinformatie op basis van open standaarden zou elke organisatie over alle informatie moeten beschikken die nodig is om bekende bedreigingen stop te zetten. Maar zelfs binnen organisaties die gebruikmaken van de beste firewalls en beveiligingsregels voor de netwerkperimeter worden er nog altijd bedreigingen in het local area netwerk gedetecteerd. Helaas worden deze malware en hackers meestal handmatig opgemerkt, en vaak pas nadat er zich een beveiligingsincident heeft voorgedaan. In plaats van het netwerk af te speuren op bedreigingen, zouden we het netwerk zelf moeten inzetten voor het detecteren van kwaadaardige activiteit en het direct in quarantaine zetten of blokkeren van malware.

3) Pas beleidsregels overal binnen het netwerk toe: Als u in staat bent om bedreigingen overal binnen het netwerk te detecteren, zou het ook mogelijk moeten zijn om die een halt toe te roepen. De securitybranche heeft zich van meet af aan gericht op de beveiliging aan de netwerkperimeter. Het probleem is echter dat mobiliteit, BYOD en IoT ervoor hebben gezorgd dat deze perimeter is verdwenen of zo u wilt, overal aanwezig is. Het is financieel geen haalbare kaart en ook vanuit beheeropzicht onwenselijk om op elk punt binnen het netwerk een nieuwe security-laag aan te brengen. Waarom zou u het netwerk zelf niet gebruiken? Het security-budget van veel CISO's varieert van 10 procent tot 25 procent van het totale ICT-budget. Waarom zouden zij slechts een kwart van dit budget gebruiken om de laatste ontwikkelingen bij te benen en de andere driekwart gebruiken om het netwerk te beschermen? Het netwerk zelf inzetten voor de beveiliging is de meest (kosten)efficiënte methode voor het opsporen van bedreigingen en toepassen van security-regels.

Het security-landschap verandert. Het is hoog tijd om af te stappen van een traditionele benadering van netwerksecurity. Professionals die zich hiermee bezig houden moeten elk onderdeel van het netwerk gaan zien als een strategisch punt voor het detecteren van bedreigingen en toepassen van beveiligingsregels. Alleen met een dergelijke aanpak kunnen we voor een werkelijk veilig netwerk zorgen.

Links

[1] US-CERT - Information Sharing Specifications for Cybersecurity: https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

Nico Siebelink is werkzaam bij Juniper Networks, waar hij op Europees niveau verantwoordelijk is voor de Service Provider- en Enterprise-markt. Nico is te bereiken via nsiebelink@juniper.net.

SECURITY STANDAARDEN

Toen ik voor mezelf de taak bedacht om als vakantieproject een overzicht te maken van security-standaarden had ik niet gedacht dat dit een zwaar onderwerp zou zijn. Ik heb de interactie opgezocht met collega's. En het blijkt dat we het over veel zaken eens zijn. Maar één ding kan altijd breder: de scope. Ik roep wel eens gekscherend dat een architect van alles een beetje moet weten en een expert van een beetje alles moet weten. Maar een security-professional moet kennelijk van alles op het gebied van security veel weten. Ik kreeg veel verwijzingen naar standaarden die voor mij nieuw waren. Het gaf me ook te denken wat ik als security-standaard wilde accepteren. Ik wilde daar toch een aantal kenmerken bij toetsen: brede gedragenheid, uitstraling als standaard en een duidelijk beheer van het document. Dat had wel tot gevolg dat ik vele bronnen die mij aangedragen werden niet opgenomen heb in dit artikel. En ik ben blij toe, want met deze beperkte scope is het toch een lijvig artikel geworden.

Tijdens mijn onderzoek kwam ik ook nog een interessante kritiek tegen op een detail van wachtwoordbeheer dat in verschillende standaarden: de specificatie van een minimum wachtwoord-leeftijd, zijnde de tijd waarbinnen een wachtwoord niet veranderd mag worden. Vele experts vinden dit geen security-aspect. Toch zit dit attribuut ingebakken in het wachtwoordbeheer van bijvoorbeeld Microsoft Windows. Dit is er ingekomen toen Windows NT 4.0 eind 90-er jaren een C2 security certificatiestempel kreeg [1]. En waarom? Omdat er een boek was in de zogenaamde 'Rainbow Series' die dit als aanbeveling gaf. Het was een best practice die de certificerende consultants bij een eerdere certificatie in 1986 opgehaald hadden. Dit was de certificatie van een lijn van mainframes, Unisys A Series MCP versie 3.7.
En hoe weet ik dit? Een software-engineer had dit als oplossing bedacht om wachtwoord recycling tegen te gaan op een systeem dat weinig capaciteit had om een reeks oude wachtwoorden op te slaan. Vandaag de dag is het moeilijk voor te stellen dat dit soort zaken zulke beperkingen hadden, maar de definitie van een gebruiker werd in 300 byte chunks ingelezen. Ik wilde zorgen dat alle informatie van een gebruiker meestal in die buffer paste, zodat het ophalen slecht één leesactie vergde. En dat moest dus inclusief de historie aan wachtwoordhashes zijn die we aan het toevoegen waren. Een logische ontwerpbeslissing in die tijd…
Dit was een belangrijke realisatie voor mij: standaarden moeten vooral op het goede abstractieniveau zitten. In dit geval was een specifieke maatregel van meer dan tien jaar oud in de standaarden blijven hangen. Volgens de wet van Moore waren computers 32 keer zo snel geworden. De snelheid van lezen en schrijven naar de harde schijf zeker een factor 100 en de capaciteit van harde schijven zo'n 1000 keer. De wereld was dus danig veranderd.

Met deze wetenschap ben ik ook vooral op zoek gegaan naar praktisch toepasbare standaarden. Ik heb ze naar thema gerangschikt en ook weggestreept. Tot de laatste avond van het uitwerken toe. En hierdoor zijn raamwerken als COBIT en standaarden als PCI-DSS op de vloer van knipselafval beland. Dat wil niet zeggen dat ze niet relevant zijn, maar het laat meer zien hoe rijk de informatie was, dat de lat zo hoog gelegd moest worden om dit behapbaar te houden.
Nog een speciale vermelding wil ik doen van Bob Hulsebosch, die mij attendeerde op een studie van hem, gepubliceerd door het WODC met de titel 'Inventarisatie en classificatie van standaarden voor cybersecurity' [2]. Het is een onderzoek dat een hele andere dimensie van de wereld van standaarden belicht. Voor wie meer wil lezen, kan ik het aanbevelen.

Security-strategie

Ik begin met dit onderwerp omdat hier de wortels van een goede beveiliging liggen. Security moet uiteindelijk de bedrijfsdoelen ondersteunen en niet tegenwerken. Goede beveiliging moet het voor het bedrijf mogelijk maken kansen te benutten onder acceptabele restrisico's. Zonder die beveiliging zouden die kansen niet benut zouden kunnen worden. Dus moet ik ook beginnen met het noemen van twee standaarden die niet door iedereen gezien zullen worden als security-standaarden, maar wel een cruciale rol hebben hierin: TOGAF [SS.1] en Archimate [SS.2]. Archimate noem ik vooral met een beetje Nederlandse trots, hier zijn ook andere kandidaten te noemen, zoals UML. Het belangrijkste is dat er een enterprise-architectuurmethode moet zijn die aandacht heeft voor beveiliging en een standaard representatie die daarmee gepaard gaat. Ik besef me dat ik strategie belicht vanuit het oogpunt van een architect, maar dat is dan ook het oogpunt dat ik gewend ben.
Om die enterprise-strategie door te kunnen vertalen naar de hele inrichting en uitvoering van security in de organisatie heb je een allesomvattend raamwerk nodig. In dit verband weet ik eigenlijk alleen maar SABSA [SS.3] te noemen. SABSA is een raamwerk dat ontstaan is parallel aan COBIT. Het mooie van SABSA is dat het, anders dan COBIT, niet bedrijfsbreed geadopteerd hoeft te worden om effectief gebruikt te worden door architecten. Maar eigenlijk is dat ook tegelijk het nadeel. Doordat deze adoptie niet noodzakelijk is, is het gebruik van SABSA vaak maar beperkt tot een aantal enthousiastelingen binnen een bedrijf.

Risk Management

Voor veel informatiebeveiligers is risicoanalyse het belangrijkste aandachtsgebied. Alle informatiebeveiligers dienen dit domein te kennen. Er zijn veel bronnen voor allerlei aspecten van risico, maar ik wil me in het kader van dit artikel beperken tot standaarden die het risicomanagement proces zelf beschrijven. Ik begin met het ISF. Toen ze nog ESF heetten kwamen ze met

Lex Borger is hoofdredacteur van dit magazine en bereikbaar via hr@pvib.nl

de Sprint standaard, dit is uitgegroeid tot IRAM2 [RM.1]. Helaas alleen beschikbaar voor leden, maar dan heb je ook een standaard ondersteund met vele instrumenten en beschrijvingen van best practices.
Hiernaast is er ook de ISO-standaard ISO/IEC 31000 [RM.2], die ik in de beveiligingspraktijk steeds vaker tegenkom.
Het is een gebied dat ik zelf ook nog graag verder zou willen uitdiepen, want ik zie nog te vaak dat er risico's worden geaccepteerd die niet op een structurele wijze bepaald zijn.

Security Management

In mijn vooronderzoek was er al snel een ding duidelijk: de 'Code voor Informatiebeveiliging' is onbetwist security-standaard nummer één! Iedereen kent deze standaard wel in een van zijn verschijningsvormen, maar dat zijn er helaas wel heel erg veel: De officiële internationale versie zijn de IEC/ISO 27001 en 27002 standaarden, ondersteund door de andere standaarden in de IEC/ISO 27000 Series [SM.1]. De historie van deze documenten is vrij direct terug te traceren naar voorgangers: de IEC/ISO 17799 en het tandem de BS 7799 / NEN Code voor Informatiebeveiliging, opgezet onder leiding van David Lacey en Pieter van Dijken. Maar daar stopt het niet. Er zijn verschillende afgeleiden gemaakt van 'de Code'. De NEN 7510 [SM.2] voor de sector gezondheidszorg, en een serie baselines voor verschillende overheidstakken, waarvan de BIR [SM.3] voor rijksdiensten en de BIG [SM.4] voor gemeenten. Al deze standaarden hebben een eigen progressie, een gezamenlijk verleden en persoonlijk vind ik het jammer dat er de laatste jaren zoveel aftakkingen zijn.
Er zijn naast de 27000 Series toch ook wat andere standaarden op het gebied van security-management die het noemen waard zijn:

- ISF publiceert de 'Standard of Good Practice in Information Security' [SM.5];
- NIST publiceert het Cybersecurity Framework [SM.6];
- IETF publiceert RFC 2196 Site Security Handbook;
- AICPA publiceert de SSAE 16 - gericht op outsourcing;
- CSA publiceert de Cloud Controls Matrix - gericht op cloud-diensten.

Al deze standaarden hebben weer hun eigen inzichten en accenten, wat ze bruikbaarder maakt voor bepaalde organisaties of op bepaalde vlakken. Om dat goed te beschrijven kan er een heel apart artikel geschreven worden. Ik volsta hier met het opnoemen van de standaarden.

Security-technologie

Dit is misschien wel het makkelijkste thema om standaarden bij te noemen, maar tegelijk het moeilijkste thema om dan ook een gevoel erbij te geven dat je structureel de belangrijkste standaarden benoemd hebt. Dus laten we dicht bij huis beginnen: het NCSC publiceert een hele serie whitepapers [ST.1] die grotendeels over technologie-onderwerpen gaan. Als ik even kijk naar de meest recent gepubliceerde whitepapers: legacysystemen, detectie-oplossingen, webapplicaties, TLS, IPv6… Hiermee worden toch al meer dan de helft van de security-problemen van de hedendaagse projecten geraakt.
Mocht je verder willen kijken, dan zijn de 'Special Publications 800' van het NIST [ST.2] een goede plaats om te kijken. Ook hier kun je richtlijnen vinden voor de toepassing van vele verschillende technologieën. Het is wat meer zoeken, dat komt omdat het NIST de publicaties op nummer zet, maar de nummers wel gelijk houdt bij updates. Hierdoor is er geen historische structuur, noch een inhoudelijke. Ze zijn bij NIST ook begonnen aan een SP 1800 Series, over cybersecurity.
Het NIST kan soms vooruitstrevend zijn. NIST's conceptversie voor SP 800-63-3 'Digital Authentication Guideline' was afgelopen mei nog in het nieuws omdat hier afgerekend wordt met een aantal diepgewortelde overtuigingen over de kwaliteit van wachtwoorden. Dit concept beveelt aan wachtwoorden niet langer periodiek te laten verlopen en rekent af met SMS als een tweede factor.
En dan komen we bij een andere grossier in internet-standaarden, waarvan vele een security-tintje hebben: het IETF (Internet Engineering Taskforce). Het IETF heeft maar een handjevol echte standaarden, zoals HTTP en HTML. Maar onder de standaarden zit een hele laag aan RFC (Request for Comments)-documenten. Dit zijn feitelijk standaarden. Het zoeken naar specifieke onderwerpen is moeilijker dan bij de NIST SP 800 Series, en hierbij komt het dat het niet alleen om security- standaarden gaat, alle onderwerpen staan bij elkaar. Nieuwe versies krijgen een nieuw nummer, dus je moet oppassen als je op nummer een document ophaalt. Gelukkig is de IETF er goed in om aan te geven als je een verlopen versie opvraagt.
Eén RFC-document licht ik er uit, omdat het security-technieken op een meta-niveau beschrijft: RFC 3631 'Security Mechanisms for the Internet' [ST.4]. Verder kun je geen internettechnologie noemen waarvoor geen RFC bestaat. Voor het onderwerp email-security heb je bijvoorbeeld SPF (RFC 4408), DKIM (RFC 6376) & DMARC (R7489) en voor connection-security bijvoorbeeld TLS (RFC 5246), Public key pinning (RFC 7469) & HSTS (6797).
Nog een uitsmijter: de standaarden voor digitale handtekeningen van het ETSI [ST.5]. Met de aandacht voor standaardafhandeling van digitaal tekenen staan deze standaarden voorlopig even in het spotlicht, zeker totdat dit soort activiteiten gewoon gemeengoed geworden zijn.

Veilige Software

Bij het thema 'veilige software' denk ik gelijk aan OWASP. Niet echt een standaard, maar wel een organisatie met een hele verzameling praktische richtlijnen, en toch ook een standaard in

haar portfolio: de OWASP Application Security Verification Standard [SW.1]. Versie 3 is net uitgekomen.
En daarnaast is OWASP heel bekend door de OWASP top 10 [SW.2], een lijst van de tien meest voorkomende web-applicatie-problemen. Deze lijst wordt elke drie jaar vernieuwd, en deze vernieuwing staat er ook weer aan te komen! Sinds 2010 is de top drie injection, broken authentication & session management en cross-site scripting (XSS).
Vergelijkbaar met de OWASP top 10 is de 'SANS top 25 Most dangerous software errors' [SW.3]. De huidige lijst is uit 2011 en is wat meer op het voortbrengingsproces gericht dan op de programmeertechniek.
Dat brengt ons ook bij de laatste standaard die ik noem op dit vlak, een Nederlandse standaard: Grip op SSD [SW.4] van het CIP. SSD staat voor 'secure software development'. Grip op SSD is een collectie van standaardeisen en normen voor het ontwikkelingsproces. Het wordt vooral bij de overheid gebruikt en de leveranciers in deze sector hebben het werken op deze manier omarmt.

Cloud Security

Op het gebied van Cloud Security zijn er verschillende standaarden. De eersten die ik noem komen van de Computer Security Alliance (CSA). De CSA is toch wel de meest bekende organisatie op dit gebied die standaarden uitgeeft. Daar waar anderen steevast refereren naar bestaande standaarden en volharden in het standpunt dat cloud niets anders is dan oude wijn in nieuwe zakken, weet het CSA exact de vinger te leggen op wát er dan wél anders is en dát juist te beschrijven.
Als eerste noem ik de CSA Security Guidance [CS.1]. Deze richtlijn bevat richtlijnen in 14 domeinen, verdeeld over de thema's architectuur, bestuur (governance) en operationeel. Het bevat een schat aan definities, normen en best practices en is van harte aan te bevelen aan eenieder die professioneel met cloud en security te maken heeft.
Iets minder bekend, wat meer gespecialiseerd, maar daardoor niet minder waardevol zijn de tien (!) CSA SecaaS Implementation Guidance documenten [CS.2]. Omdat de CSA zelf geen verzamelpagina heeft om deze documenten bij elkaar te presenteren, verwijs ik hierbij naar een blog van Kevin Fielder, die ze bespreekt en doorlinkt.

Privacy

Op het gebied van privacy is er één autoriteit in Nederland: de Autoriteit Persoonsgegevens (AP) De AP publiceert veel documenten op haar website, velen daarvan zijn onderzoeken en adviezen, geen standaarden of richtlijnen. Wel zou je de 'richtsnoeren' als zodanig kunnen beschouwen. Het belangrijkste

richtsnoeren-document is "Richtsnoeren beveiliging persoonsgegevens" [P.1].
In de Richtsnoeren zelf wordt dan wel weer nadrukkelijk benoemd dat de erkende informatiebeveiligingsnormen een afdoende basis vormen om te voldoen aan de eisen uit de Wbp met betrekking tot beveiliging, maar dat het tevens slechts een onderdeel ervan is.
Daarnaast zijn er ook de "Beleidsregels meldplicht datalekken" [P.2], die in conceptvorm nog 'richtsnoeren' genoemd werden. Deze beleidsregels zijn eerder te kwalificeren als een soort van memorie van toelichting bij de wet dan als een standaard of richtlijn, maar dat is het niet. Het AP heeft in dit document beleid opgeschreven wat veel verder gaat dan de wetstekst en aangegeven dat er gehandhaafd wordt aan de hand van wat in het document staat. In die zin legt het dus wel normen neer in de vorm van regels.

Security Documentatie & Audit

Op het oog lijkt het vreemd deze twee onderwerpen met elkaar te combineren. Toch kwam ik er instinctief iedere keer op uit. De connectie is dat vanuit het perspectief van een beveiliger niet alleen maatregelen genomen moeten worden, maar ook aangetoond moet kunnen worden dat deze maatregelen genomen zijn en goed werken. Een groot onderdeel daarvan is de security-documentatie. De een doe je voor het ander, vandaar dat ik deze onderwerpen combineer.
Recentelijk heb ik nog in dit blad het boek SIVA [DA.1] van Wiekram Tewarie besproken. Het wordt onder andere gebruikt om NCSC-normen te beschrijven. Ik volsta in dit artikel om te verwijzen naar twee artikelen [DA.2] van auditors over dit gedachtegoed.
Er is op dit vlak voor mijn gevoel nog meer te halen dan nu beschikbaar is. Wat ik zie in de markt is dat elke partij die een brede portfolio voor securitydocumentatie nodig heeft dit wiel zelf moet uitvinden. Dit is natuurlijk goed nieuws voor de security-consultants die zich specialiseren op dit vlak, maar het is niet effectief. Als er eerst bepaald moet worden wat een norm, standaard, richtlijn en handreiking is, welke er intern gemaakt kunnen worden, welke er extern geadopteerd kunnen worden en dan vervolgens de opzet van deze documenten weer vastgesteld moet worden, dan weet je dat het lang gaat duren en er waarschijnlijk niet een praktisch document uitkomt. Het wordt tijd om hier een standaard voor te hebben.

Security Certificaties

De beveiligers zelf moeten ook aan standaarden voldoen om hun capaciteiten op een gestandaardiseerde wijze aan te kunnen tonen. Ik begin met een ontwikkeling waar het PvIB nauw bij betrokken is: de Beroepsprofielen Informatiebeveiliging [SC.1]. Deze vier profielen geven een duidelijke visie hoe de markt van security professionals ingedeeld kan worden. Het geeft voldoende differentiatie dat een richting gekozen kan worden, zonder te verdwalen in een woud van mogelijkheden. De beroepsprofielen zijn in 2014 voor het eerst gepubliceerd, dus eigenlijk staan we nog aan de bakermat van deze ontwikkeling.
Naast deze profielen zijn er ook nog certificaten te behalen. De wereld van certificeren is internationaal, de meeste certificeringen zijn Amerikaans van oorsprong. Nu zijn er veel certificeringstrajecten. Ik ga ze niet allemaal noemen, want vele certificeringen zijn zo zeldzaam in de markt dat het onduidelijk is wat de exacte meerwaarde is. Ik beperk me tot de bekende certificeringen die een overwicht in de markt hebben. De meeste certificaten eisen dat je een examen haalt, een initieel niveau van ervaring aantoont en je kennis bijhoudt met doorlopend kennis vergaren. Kennis vergaren wordt opgedaan door CPE-punten te verdienen, bijvoorbeeld een cursus te doen, een conferentie te bezoeken, een boek te lezen of een artikel te schrijven.
Als eerste noem ik de CISSP-certificering [SC.2] van ISC2. Wat begon als een vrij technisch certificaat is nu meer richting de proceskant getrokken, waarbij minder relevante technische kennis (in het fysieke domein) minder belangrijk geworden is. Het omgekeerde is aan de gang bij de tegenhanger hiervan is de CISM-certificering [SC.3] van ISACA. Dit had een vrij procesgericht zwaartepunt, maar meer en meer komen ook hier technische details aan bod.
En dan is er de Britse SABSA-certificering [SC.4] voor enterprise-security-architecten. Het belang van SABSA komt vooral voort uit de integratie in TOGAF (zie ook Security Strategie, eerder in dit artikel) en de enthousiaste kern van beoefenaren.
Cloud-security is de opkomende ster, dus ik wil het rijtje afsluiten met twee certificaties op dit vlak, die vergelijkbaar zijn, aangeboden door verschillende instituten: CCSK-certificaat van de CSA en het CCSP certificaat van ISC2. Het is nog te vroeg om te zeggen of een van deze twee de overhand krijgt, dus een gok is het wel.

Conclusie

Veel security-experts zullen 80% van de hiervoor genoemde standaarden goed kennen. Voor hen hoop ik dat er wat pareltjes tussen zitten die het toch het lezen waard maken. Voor de minder ervaren security-professionals hoop ik dat dit bijdraagt aan hun kennis van security-standaarden. Voor iedereen kan het fungeren als een referentielijst naar standaarden. Verder is het wat mij betreft een levend document. Ik zal vast wel een favoriete standaard gemist hebben of een detail verkeerd hebben uitgespeld. Graag hoor ik op- en aanmerkingen, dan zorg ik dat de levende versie ergens een goed thuis krijgt.

Links

[1] Microsoft Windows NT 4.0 C2 Certificatie: https://msdn.microsoft.com/en-us/library/cc767092.aspx

[2] WODC Inventarisatie en classificatie van standaarden van cybersecurity: https://www.wodc.nl/onderzoeksdatabase/2552-inventarisatie-van-standaarden-en-normen-voor-cyber-security.aspx?cp=44&cs=6837

Referenties

Security Strategie

[SS.1] TOGAF: http://w1.opengroup.org/subjectareas/enterprise/togaf

[SS.2] Archimate: https://www2.opengroup.org/ogsys/catalog/W150

[SS.3] SABSA: http://www.sabsa.org/node/5

Risk Management

[RM.1] ISF IRAM2 :https://www.securityforum.org/uploads/2015/03/ISF-IRAM2-ES.pdf & http://www.infosecurity-magazine.com/news/isf-launches-inforisk-assessment/

[RM.2] ISO/IEC 31000 Series: http://www.iso.org/iso/home/standards/iso31000.htm

Security Management

[SM.1] IEC/ISO 27000 Series: http://www.iso.org/iso/iso27001

[SM.2] NEN 7510: https://www.nen.nl/NEN-Shop-2/Standard/NEN-75102011-nl.htm

[SM.3] BIR: https://www.communicatierijk.nl/vakkennis/r/rijkswebsites-verplichte-richtlijnen/inhoud/baseline-informatiebeveiliging-rijksdienst-bir--nen-iso-iec-27001-en-27002

[SM.4] BIG: https://www.ibdgemeenten.nl/producten/strategische-en-tactische-big/

[SM.5] ISF Standard of Good Practice:https://www.securityforum.org/tool/the-isf-standardrmation-security/

[SM.6] NIST Cybersecurity Framework: http://www.nist.gov/cyberframework/

[SM.7] IETF RFC 2196 Site Security Handbook: https://www.ietf.org/rfc/rfc2196.txt

[SM.8] AICPA SSAE 16: http://ssae16.com/SSAE16_overview.html

[SM.9] CSA Cloud Controls Matrix: https://cloudsecurityalliance.org/group/cloud-controls-matrix/

Security Technologie

[ST.1] NCSC Whitepapers: https://www.ncsc.nl/actueel/whitepapers

[ST.2] NIST SP-800 Series: http://csrc.nist.gov/publications/PubsSPs.html

[ST.3] IETF RFCs: https://www.ietf.org/rfc.html

[ST.4] IETF RFC 3631 Security Mechanisms for the Internet: https://tools.ietf.org/html/rfc3631

[ST.5] ETSI Digital Signature: http://www.etsi.org/technologies-clusters/technologies/security/digital-signature

Veilige Software

[SW.1] OWASP Application Security Verification Standard: https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

[SW.2] OWASP Top Ten: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[SW.3] SANS top 25 Most dangerous software errors: https://www.sans.org/top25-software-errors/

[SW.4] CIP Grip op SSD: https://www.cip-overheid.nl/downloads/grip-op-ssd/

Cloud Security

[CS.1] CSA Security Guidance: https://cloudsecurityalliance.org/group/security-guidance/

[CS.2] CSA SecaaS Implementation Guidances (10!): https://kevinfielder.wordpress.com/2012/11/01/security-as-a-service-implementation-guidance-documents-published/

[CS.3] CSCC Cloud Security Standards: http://www.cloud-council.org/deliverables/CSCC-Cloud-Security-Standards-What-to-Expect-and-What-to-Negotiate.pdf

Privacy

[P.1] AP Richtsnoeren beveiliging persoonsgegevens: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

[P.2] AP Beleidsregels melkplicht datalekken: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken.pdf

Security Documentatie en Audit

[DA.1] Boek SIVA: http://vuuniversitypress.com/15-nederlands/overige-content/99-siva

[DA.2] Twee bronnen over SIVA: https://www.deitauditor.nl/beroepsontwikkeling-reglementering/siva-methodiek-voor-de-ontwikkeling-van-auditreferentiekaders/ & http://www.norea.nl/readfile.aspx?ContentID=68278&ObjectID=940136&Type=1&File=0000036004_Referentiekaders.pdf

Security Certificaties

[SC.1] Beroepsprofielen Informatiebeveiliging: https://www.pvib.nl/download/?id=17696376

[SC.2] ISC2 CISSP: https://www.isc2.org/cissp/

[SC.3] ISACA CISM: http://www.isaca.org/certification/cism-certified-information-security-manager/pages/default.aspx

[SC.4] SABSA Chartered Security Architect: http://www.sabsa.org/certification

[SC.5] Cloud Security - CSA CCSK & ISC2 CCSP: https://cloudsecurityalliance.org/education/ccsk/ en https://isc2.org/ccsp-how-to-certify/default.aspx

WOENSDAG 12 OKTOBER SECURITY-CONGRES 2016

DATA IN THE FUTURE

Amsterdam Arena
ArenA Boulevard 1
1101 Amsterdam
www.amsterdamarena.nl

Het congres zonder files,
georganiseerd door ISACA, NOREA en PvIB

Al ingeschreven op het succesvol terugkerend congres?
Mis het niet en schrijf u nu in!

Een mooi en afwisselend programma is voor u samengesteld.

Dagvoorzitter: André Beerten

Onderwerpen:	**Keynotes:**
Privacy	Actualiteiten op privacy-gebied met bijzondere aandacht voor de meldplicht datalekken en de EU-verordening over gegevensbescherming ***door Wilbert Tomesen, vicevoorzitter Autoriteit Persoonsgegevens***
Identity	ID Ergo sum ***door Marcel van der Velde***
Het jaar 2022	Wat staat de CIO komende vijf jaar te wachten in de exponentieel ontwikkelende wapenwedloop van security? ***door Aart van der Vlist, CTO/CIO (UWV) en trendwatcher***

De onderwerpen passeren zowel plenair als in parallelle sessies de revue. Een vast onderdeel van het programma is de uitreiking van de Joop Bautz Information Security Award.

Het volledige programma vindt u op www.security-congres.nl

Dit congres wordt mede mogelijk gemaakt door:

Capgemini
CONSULTING. TECHNOLOGY. OUTSOURCING

motiv
ICT SECURITY

ONSIGHT
IT Security Experts

WatchGuard

Wij ontmoeten u graag op 12 oktober 2016!

Meer informatie:
www.security-congres.nl

Organisatie:

ISACA
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

PvIB
Platform voor InformatieBeveiliging

EN, WANNEER HOUDEN WE OP MET KENTEKENS SCANNEN?

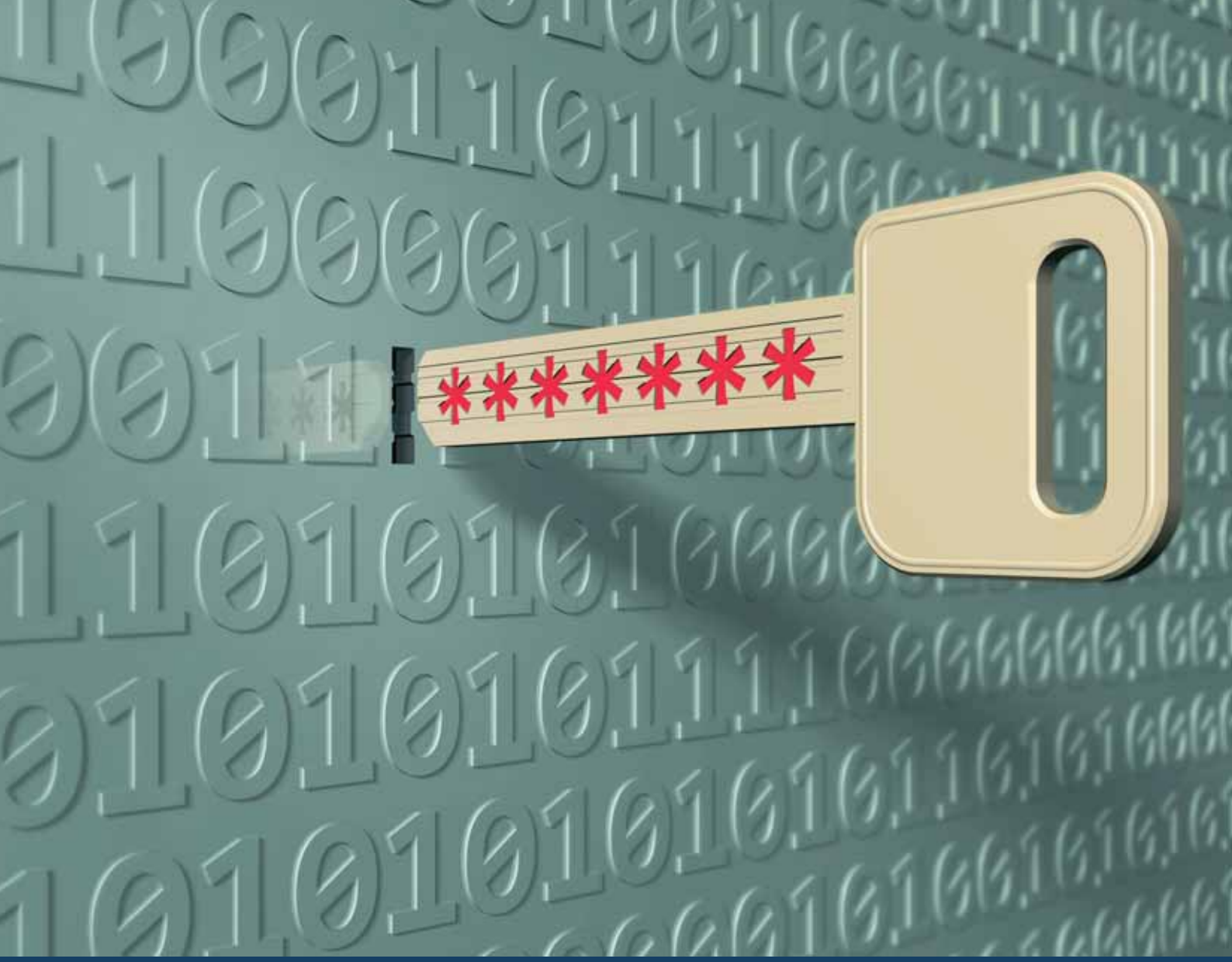
Ze hangen er inmiddels al verschillende jaren: de camera's die langs de weg automatisch de kentekens van alle automobilisten scannen. Die prachtige vergaarbak aan gegevens werd de afgelopen jaren dan ook heerlijk gekoppeld met andere vergaarbakken. Bijna altijd met als doel "het vangen van boefjes" (lees: voor het innen van belasting en boetes). Ik noemde het jaren geleden al eens een van de grootste privacyschendende plannen ooit, want iedereen is bij voorbaat al overal van verdacht. Maar, wellicht is een indamming van het ongebreidelde gebruik van die gegevens een stuk dichterbij gekomen dan ikzelf gedacht had.

In de derde week van augustus bracht de Advocaat-Generaal een negatief advies uit aan de Hoge Raad over het gebruik wat – met name – door de Belastingdienst gemaakt wordt van de zogenaamde ANPR (automatic number plate recognition). De AG oordeelt dat dit in strijd is met het grondrecht op privacy (art. 8 EVRM) en dan met name omdat het gaat om ongericht en ongebreideld gebruik van de gegevens waarvoor niet eens een wettelijke grondslag te vinden is.

Het hele zaakje stinkt al een tijdje. Wettelijk is bepaald dat bij het scannen door de politie alleen de zogenaamde "hits" (een bekend "boefje") bewaard mogen blijven en dat de overige kentekens gewist moeten worden. Na een WOB-verzoek bleek in 2013 dat alle gegevens werden bewaard en dat deze ook nog eens allemaal aan de Belastingdienst werden doorgegeven. Er was zelfs een heus convenant afgesloten tussen politie en de Belastingdienst. We werden en worden dus bedonderd waar we bij staan. Het NRC schreef daarover indertijd: "Het bewaren van de kentekens is ook opmerkelijk omdat het kabinet-Balkenende IV de Tweede Kamer in 2010 beloofde dat dat niet meer zou gebeuren. Dat was nadat twee politiekorpsen daarvoor door het CBP (Nu AP, red.) op de vingers waren getikt. Een onrechtmatige inbreuk op de persoonlijke levenssfeer, zo oordeelde de privacywaakhond destijds."

Nu is het natuurlijk niet gezegd dat de Hoge Raad het advies van de AG ook zal volgen (alhoewel zij dat wel vaak doet). Laat mij dan nog een duit in het zakje doen. Het hele gebruik, ongeacht of het om de Belastingdienst gaat of niet, is buitenproportioneel en niet subsidiair. De Nederlandse overheid gebruikt luchtafweergeschut om een mug neer te schieten. De middelen die zij inzet om het doel te bereiken, namelijk "wie moet er nog een beetje belasting betalen of wie krijgt een boete", zijn dermate exorbitant dat zij geen rechtvaardiging kunnen vormen om op deze manier het doel te behalen. Een klein voorbeeldje. Op 19 augustus 2016 bericht PZC (Provinciale Zeeuwse Courant) dat er wel 113 bekeuringen zijn uitgeschreven bij een controle op de Eerste Deltaweg (N256). Van 4564 voertuigen werd het kenteken gescand. En dan nu waarvoor er boetes vielen: 5 x voor het niet dragen van een gordel, 1 x voor niet handsfree bellen, 5 x voor te hard rijden. Er was ook nog iemand met een openstaande boete. En bij de radarcontrole (die er dus ook was) reden 101 mensen te hard. GEEN ENKEL VAN DEZE FEITEN VEREIST HET SCANNEN VAN KENTEKENS. Al deze 113 boefjes konden gewoon "normaal" gepakt worden. Nou, vooruit, wellicht kon die ene persoon met een nog openstaande boete makkelijker gepakt worden door het scannen. Dan is dus voor die boete van maar liefst 117 euro (!) de privacy geschonden van 4563 personen. Hoog tijd om al die camera's te demonteren.

Mr. Rachel Marbus
@rachelmarbus op Twitter



VERSLEUTELEN EN BEHEER VAN DE SLEUTELS

Versleutelen van data is niet meer weg te denken in de huidige digitale wereld. Cloud, BYOx, Mobile en IoT bieden veel mogelijkheden en privacy is steeds vaker een delicaat onderwerp. Met het versleutelen (cryptografisch beveiligen) van deze data kan er meer privacy worden gewaarborgd en kan er voldaan worden aan nieuwe regelgeving op dat gebied.

Het versleutelen van data wordt aangeraden mede uit oogpunt van de nieuwe Privacywetgevingen, EU-richtlijnen, etcetera. Lekken van versleutelde date kan minder ernstige gevolgen hebben dat data dan het lekken van data die niet versleuteld is. Teneinde versleuteling van data in de systemen mogelijk te maken zijn cryptografische sleutels nodig. Het gebruik van deze sleutels bepaalt voor een deel het vertrouwen van de consument voor de opslag van gegevens. Zonder een gedegen sleutelmanagement, ook wel te noemen key management, kunnen sleutels verloren gaan, gestolen worden of worden misbruikt met alle gevolgen die hieruit kunnen voortvloeien.

Sleutelbeheer

De (cryptografische) sleutels die worden gebruikt voor de beveiliging van de data worden op verschillende niveaus gebruikt en opgeslagen. Er bestaan diverse soorten sleutels die in de systemen worden gebruikt voor verschillende toepassingen namelijk: voor netwerkbeveiliging (TLS, SSL), voor de authenticatie, voor de applicatie om data te versleutelen alsmede versleuteling op databaseniveau. Elk systeem heeft hierbij één of meer cryptografische sleutels, die gebruikt kunnen worden voor encryptie en authenticatie. Bij het verlies van deze cryptografische sleutels verlies je tevens de toegang tot de applicatie of zelfs de mogelijkheid om de data te ontsleutelen. Het beheren van deze cryptografische sleutels is voor veel bedrijven een moeizaam onderwerp. Dat komt vaak doordat er weinig tijd voor beschikbaar gemaakt wordt en key management vaak als extra taak bij één of twee medewerkers belegd wordt. Veel bedrijven zijn klein en kunnen niet een hele afdeling opzetten om de sleutels te beheren.

Sleutelbeheer

Sleutelbeheer kun je opsplitsen in een aantal afzonderlijke onderdelen, te weten:

- Sleutelgeneratie
- Sleuteldistributie
- Levensduur van sleutels
- Sleutelgebruik
- Sleutelopslag
- Intrekken en vernietigen van sleutels

Hieronder vallen ook de standaard sleutelbeheerprincipes die men ook voor andere cryptografische toepassingen kan gebruiken, bijvoorbeeld Blockchain, TLS of S/MIME. Hierna een kleine uitleg van de belangrijkste onderdelen van key management die hierboven zijn benoemd.

1. Sleutelgeneratie

Het genereren van een sleutel is een fase in het proces waar je goed de aandacht aan moet besteden. Indien je dit niet goed doet, is de sleutel wellicht minder veilig dan je denkt. Een Random-Key-Generator waarbij het gebruik van zogenaamde "zwakke sleutels" is uitgesloten kan de basis zijn voor het genereren van een goede sleutel. Hiervoor zijn diverse programma's geschreven of beschikbaar.
Het genereren kan met softwaretoepassingen worden gedaan maar het is ook mogelijk om hiervoor speciale hardware te gebruiken. Het genereren van sleutels kan ook met een speciale Hardware Security Module (HSM) uitgevoerd worden. De door goedgekeurde en gecertificeerde hardware gegenereerde sleutels zijn van hogere kwaliteit dan die door software zijn gegenereerd. Een sleutel in een HSM wordt als veilig gezien omdat deze hardware dermate beveiligd is dat de sleutel er niet uit te halen is.

Softwareapplicaties (toepassingen) waarmee sleutels gegenereerd kunnen worden zijn bijvoorbeeld:

- OpenSSL
- PuTTYGen
- PGP-software

Voorbeelden van hardwareoplossingen zijn:

- Thales nShield
- Thales P-shield HSM Boxen
- Safenet Luna
- Utimaco CryptoServer

Nadeel is dat dit soort hardware erg duur is en strikter onderhoud vereist. Het voordeel is dat je deze hardware ook kunt gebruiken om de sleutels veilig op te slaan. Beheer van dit soort speciale hardware is zeer belangrijk en zal gedegen ingeregeld moeten worden.

Harld Röling is werkzaam bij de afdeling CISO van een Nederlandse bank en heeft zich vanaf 1999 gespecialiseerd in de technische en organisatorische aspecten van asymmetrisch Key Management en PKI. Daarnaast is Harld vrijwilliger bij Bits of Freedom, Privacy Cafe's en de Toolbox. Harld is bereikbaar via harld.roling@hroling.nl.

2. Sleuteldistributie

Als een sleutel gegenereerd is wil je deze op de meest veilige manier op de plaats krijgen waar je de sleutel gaat gebruiken. Dit is eveneens een onderdeel van het uitvoeren van een key management-taak.

Het op de juiste plaats installeren van de gegenereerde sleutel is een proces dat veilig moet verlopen, dat meestal nogal moeizaam verloopt. Het handmatig invoeren van een sleutel is hierbij een mogelijkheid die procedures vergt om de sleutel op een goede manier naar de plaats van bestemming te krijgen. Voor Cloud-toepassingen is dat zeer omslachtig en niet haalbaar in de praktijk.

Teneinde het proces via het netwerk uit te voeren zijn speciale algoritmes bedacht. De oudste en nog steeds gebruikte manier is het sleutel-uitwisselingsprotocol Diffie-Helman. Hiermee wordt de sleutel waarmee de verbinding versleuteld wordt op een veilige manier verstuurd en vindt versleuteling plaats op basis van Public Key-protocol. Een ander protocol is het RSA-encryptie-algoritme. Dat is het bekendste en kan ook gebruikt worden voor sleuteluitwisseling.

Public Key-protocollen zijn gebaseerd op twee sleutels, een geheime die op één plek beschikbaar is en een publieke die door iedereen gebruikt kan worden. Met de publieke sleutel versleutel je de gegevens en alleen met de geheime sleutel kan deze weer leesbaar gemaakt worden.

3. Levensduur van sleutels

Elke sleutel heeft een levensduur. Nadat de sleutel is verlopen moet er een nieuwe gegenereerd worden. Voor een TLS-certificaat kun je een korte sleutel, bijvoorbeeld 2048 bits (RSA-algoritme), gebruiken en deze dan twee jaar geldig laten zijn. Een levensduur van twee jaar is tegenwoordig redelijk standaard en na die twee jaar dien je een nieuwe sleutel te genereren. Wil je de sleutel langer gebruiken, maak dan een sleutel van 4096 bit, deze kun je dan bijvoorbeeld vijf jaar of nog langer gebruiken.

Een andere vorm van cryptografie is Elliptic Curve Cryptography (ECC). Deze sleutels zijn korter en daardoor beter te gebruiken als je een website hebt waarop veel gebruikers gelijktijdig actief zijn. Sleutels van 256 bit zijn hier een vervanger voor de 2048 bit RSA-sleutel met als voordeel dat versleutelen met ECC sneller uitgevoerd wordt. Hoe langer de sleutel is, hoe meer tijd het kost om gegevens te versleutelen.

4. Sleutelgebruik

Bij het op een goede manier toepassen van key management gebruik je een gegenereerde sleutel in principe maar voor één toepassing of functie. Als je meer functies of toepassingen hebt op één server, maak je een nieuwe sleutel aan. Hierdoor kun je meerdere sleutels krijgen op één server. Voorbeeld is dat de web-applicatie een eigen sleutel heeft en de beheer-applicatie een andere.

Het resultaat is dat bijvoorbeeld een gestolen of gecompromitteerde sleutel van het S/MIME-certificaat geen gevolgen heeft voor bijvoorbeeld de versleutelde gegevens die op de harddisk opgeslagen zijn.

5. Sleutelopslag

Een ander zeer belangrijk onderwerp is een antwoord te vinden op de vraag waar je een sleutel gaat opslaan. Dit dient de nodige aandacht te krijgen. Je kunt kiezen voor de volgende methodieken: opslag in software, opslag in speciale hardware zoals de HSM, de TPM-chip in laptops of in een kluis. Het belangrijkste is om sleutels zodanig te bewaren, opslaan dat zo min mogelijk personen erbij kunnen. HSM en andere speciale hardware zijn tamper proof (sleutels kunnen er niet uitgehaald worden) en hebben een gehardend OS.

Een ander vraagstuk dat beantwoord moet worden is waar je deze sleutel bewaard en gebruikt. Doe je dat op dezelfde locatie als waar de data is opgeslagen, of ga je de sleutels gebruiken op een andere locatie? Bijvoorbeeld: versleutelde gegevens in de public Cloud en de sleutels in je eigen

datacenter. Belangrijk is dat de sleutels op een andere locatie zijn dan waar de versleutelde data is opgeslagen. Hierdoor zijn bij het stelen van de data alleen de versleutelde gegevens beschikbaar en hiermee kan niet veel gedaan worden.

6. Intrekken en vernietigen van sleutels

Intrekken van sleutels kun je uitvoeren als de sleutels zijn gestolen of niet meer nodig zijn. Dit is een optie die niet voor alle sleutels mogelijk is, dit kan alleen als een Certificate Authority (CA) de sleutel heeft ondertekend, dit geldt voor asymmetrische sleutels. Intrekken van sleutels (revocation) kun je alleen uitvoeren als deze door een CA getekend zijn en in vorm van Certificaat gebruikt worden. Deze CA zal de ingetrokken sleutels publiceren om validatie mogelijk te maken. Technieken die daarvoor gebruikt worden zijn validatie door middel van CRL (Certificate Revocation List) en OCSP (Online Certificate Status Protocol). Aan het einde van de levensduur van de sleutel, is vernietigen een mogelijkheid. Als je deze sleutel hebt gebruikt voor versleutelen van gegevens, moet je wel iets moeten regelen om de gegevens toch ooit weer te kunnen ontcijferen. Indien je tijdelijke sleutels gebruikt, of de data opnieuw versleuteld met de nieuwe sleutel, kun je de ouder sleutel vernietigen.

Conclusie

Opslag en gebruik van data in Cloud, BYOx, Mobile en IoT, en het versleutelen van deze data wordt steeds belangrijker en gaat breder ingezet worden. Vooral privacygevoelige data moet straks versleuteld worden, gebruikte sleutels gaan hierbij steeds belangrijker worden.

Wettelijk is het nu geregeld dat datalekken gemeld moet worden. Indien je de data versleuteld, en op een andere plek opslaat en gebruikt dan waar de versleutelde data staat, is het lekken van deze data minder ernstig. Derden kunnen het niet lezen want ze hebben niet de beschikking over de sleutels om de gegevens weer leesbaar te maken.

Het invoeren van gedegen key management in bedrijven is duur, waardoor er bedrijven deze als dienst (gaan) aanbieden. Dit is een positieve ontwikkeling waardoor de sleutels beter beheerd worden. Er is wel een maar dat het uitbesteden want er zijn sleutels die je wettelijk niet mag uitbesteden aan derden. Als je het key management op bovenstaande punten gedegen inregelt en goed nadenkt over additionele mogelijkheden van beveiliging, kun je alle soorten gegevens in public cloud opslaan. Want na het versleutelen van de data is het eigenlijk geen informatie meer. Je bent dan klaar om voor in toekomst de data overal op te kunnen slaan.

VERSLAG

CALLING ALL CRAZY (CYBERSECURITY) ONES!

VIER LEERPUNTEN VAN TNW EUROPE 2016

TNW organiseert jaarlijks technologie- en innovatie-conferenties in Amsterdam en New York. Snelgroeiende startups, bewezen innovatieve bedrijven en leiders in de industrie vertellen hier hun verhaal. Dit jaar werd een recordaantal van zo'n twintigduizend bezoekers gedurende twee dagen bereikt.

Onder anderen Koning Willem-Alexander en Neelie Kroes, toenmalig eurocommissaris voor de digitale agenda, verzorgden al eerder de opening-keynotes. Dit jaar gaf Josephine, een Britse 11-jarige, een keynote die vele deelnemers koude rillingen bezorgde, toen ze begon met: "Ik ben de toekomst…". En vervolgde dat wij, als technologie- en innovatiebedrijven, beïnvloeden hoe haar toekomst gevormd wordt en hoe wij deze planeet een betere plek kunnen maken door de toepassing van technologie.

Van de vele presentaties en workshops die ik heb bijgewoond, volgen hier vier belangrijke leerpunten:

1- Het bouwen van nieuwe producten start niet met de oplossing, maar met het 'people-problem' dat we proberen op te lossen

Julie Zhou, VP, Director of Product Design bij Facebook, gaf precies aan waar het om draait toen ze zei: "Het is niet zo makkelijk om het mens-probleem te beschrijven, we moeten het kunnen uitleggen aan niet-techneuten. Een goed uitgangspunt voor een nieuw product begint met het WAAROM. Als je niet kunt uitleggen waarom, dan zul je niet de juiste set van oplossingen kunnen verkennen."
Om te voorkomen dat je je niet te veel focust op de oplossing, zijn dit vragen die je jezelf kunt stellen:

- Wat voor een soort 'people problem' zijn we aan het oplossen, wat zal uiteindelijk daadwerkelijk waarde toevoegen aan jouw leven?
- Is het een probleem dat het waard is om opgelost te worden (bijvoorbeeld raakt het genoeg mensen, is het betekenisvol, kwantitatieve/kwalitatieve analyse)? Valideer het probleem.
- Wanneer weten we dat het probleem opgelost is? Wees eenduidig over hoe een succesvol product eruitziet.

De opname van haar presentatie is te vinden op YouTube onder 'TNW Europe 2016' en 'Julie Zhou' [1].

2- Pas TrendWatch-gedreven innovatie toe

Een geweldige manier om genoemde problemen in een vroeg stadium te identificeren, is om de laatste innovatietrends te volgen. David Mattin, van TrendWatching.com, gaf vier inzichten om een trendgedreven innovator te worden:

1. Focus op wat jouw cliënten de volgende keer willen – ze weten dit vaak niet totdat je dit hen vertelt
2. Stop met het kijken naar je cliënten, start met het kijken naar innovaties en de verwachtingen die deze innovaties creëren!
3. Innovaties die een basale menselijke behoefte dienen op een andere manier, zijn de verwachtingen van de cliënt aan het veranderen en aanpassen. Bijvoorbeeld, de Blackphone, welke de boodschap verkondigt van een veilige smartphone, of Google's project Ara betreft modulaire smartphones. Deze producten hoeven niet per sé een groot succes te worden, maar het idee erachter zal onze verwachtingen veranderen. Bijvoorbeeld in het geval van veilige telefoons en data encryptie, neem het voorbeeld van de iPhone versus FBI-rechtszaak over privacy en encryptie; het is de standaardverwachting geworden.
4. En als we écht innovatief zijn, dan spotten we niet alleen de trends, maar worden we zelf de nieuwe trend!

De opname van zijn presentatie is te vinden op YouTube onder 'TNW Europe 2016' en 'David Mattin' [2].

3- Product experience: de formule om het goed te doen

Is de trend eenmaal geïdentificeerd, dan moet de nieuwe productervaring worden geoptimaliseerd.
Aparna Chennapragada, Director of Product bij Google, legde uit hoe de best doordachte productervaringen, lijken te komen van een simpele, maar effectieve formule: AI + UI + I. AI (Artificial Intelligence) + UI (User Interface naar die intelligentie) + I (hoe te personaliseren naar elke individu die er gebruik van maakt in verschillende situaties).

Zij vertelt dat mobiliteit (op dit moment meer dan drie miljard mensen die overal een smartphone met zich mee dragen) ons ongekende toegang tot informatie, apps en services biedt welke we nooit tevoren hebben gehad. Deze combinatie geeft ons de kans om elk echt wereldprobleem, in een softwareprobleem of nog belangrijker, in een AI-probleem te

Hong Gie Ong is Managing Consultant Cybersecurity bij Capgemini en bereikbaar via hong-gie.ong@capgemini.com.
Peter Maarten Westerhout is co-founder van TimeLabz.com.
Hij is bereikbaar via petermaarten@timelabz.com. Beiden zijn gastdocent bij de Technische Universiteit Delft voor het vak 'Impact of Technological Developments on Business and Society'.

Uiteindelijk heb ik vele krachtige twintigminuten-presentaties gezien en een 'abundance' aan nieuwe technologie- en innovatie-inspiratie opgedaan!

veranderen. Bijvoorbeeld, transport en het sturen van auto's door het verkeer – een informatieprobleem, gezondheidsmonitoring en fitness – wederom een informatieprobleem.

Zodra een product gebruikt wordt, moeten de voordelen direct duidelijk gemaakt worden aan de gebruiker (e.g. Google Waze laat direct betere routes zijn door bijvoorbeeld verkeersopstoppingen), aldus de User Interface (UI). En de I (Individu) geeft de gebruikers de mogelijkheid om ons te leren, vraag gebruikers om feedback.

De opname van haar presentatie is te vinden op YouTube onder 'TNW Europe 2016' en 'Aparna Chennapragada' [3].

4- Pas technologieën op een veilige manier toe of wordt gehackt

Als laatste, mocht je een reminder nodig hebben, waarom onze technologieproducten en -services veilig moeten worden gebouwd, check dan deze praktische hack voorbeelden in de videoplaylist van Samy Kamkar, YouTube's favoriete hacker en inspirerende technologie-enthousiast. Zijn presentie (op YouTube onder 'TNW Europe 2016' en 'Samy Kamkar' [4]) ging over allerlei fascinerende technologie-hacks die hij bedacht had door trial-en-error, gedreven door nieuwsgierigheid of dat überhaupt mogelijk was. Zie Samy's creativiteit aan het werk en abonneer je op zijn YouTube-kanaal voor waanzinnige applied hacking-videos. Bijvoorbeeld die ene over het hacken van drones (hij werd getriggerd door een mededeling van Amazon dat ze binnen 5 jaar pakketten zouden gaan bezorgen via drones). Dus ontwikkelde hij SkyJack, een drone, geconstrueerd om autonoom andere drones binnen wifibereik op te sporen, te hacken en draadloos over te nemen, om zo een leger van zombie-drones onder zijn controle te creëren. Zijn playlist is te vinden op YouTube [5] onder 'Applied Hacking'.

Uiteindelijk heb ik vele krachtige twintigminutenpresentaties gezien en een 'abundance' aan nieuwe technologie- en innovatie-inspiratie opgedaan!

Het woord Abundance is hier een knipoog en referentie naar een term bekend gemaakt door één van de bekende 'visionairs' uit Silicon Valley, Peter Diamandis [6][7], en verwijst naar een toekomst welke dankzij technologische innovatie zorgt voor een betere wereld voor de samenleving over de hele wereld.

Andere sprekers in het fascinerende programma [8] waren onder andere: de CEO van Uber, de medeoprichter van The Pirate Bay, de CEO van Periscope, de CEO van Booking.com, de CEO van TomTom, de CEO van WeMakeVR en de CEO van Hyperloop.

Om alle presentaties te zien, zie het YouTube-kanaal 'The Next Web' [9]. Volgend jaar iemand van ons op het podium? Are we crazy enough?

Links

[1] Julie Zhou: https://www.youtube.com/watch?v=IIm289_YMIE
[2] David Mattin: https://www.youtube.com/watch?v=U-Lsdgsa7IQ
[3] Aparna Chennapragada: https://www.youtube.com/watch?v=-rahR7cIBXo
[4] Samy Kamkar: https://www.youtube.com/watch?v=kJyGZDXCbmA
[5] Samy Kamkar's YouTube-kanaal: https://www.youtube.com/user/s4myk
[6] Boek Peter Diamandis: https://en.wikipedia.org/wiki/Abundance:_The_Future_Is_Better_Than_You_Think
[7] Website Peter Diamandis: http://www.diamandis.com/abundance/
[8] TNW Sprekers: http://thenextweb.com/conference/europe/speakers
[9] The Next Web YouTube-kanaal: https://www.youtube.com/user/thenextweb

REGRESSION PLANNED

First reported in the Telegraph on 21st April 2016, and later by Channel Four News on 24th May 2016, was an incident affecting UK National Security that occurred during the previous year, on 13th June 2015.

"Semaphore, the computer system that checks passengers on their way to the UK against watch lists of suspect individuals, had faltered after being flooded by tens of thousands of messages. The malfunction, believed to have originated on British Airways' systems, had been spotted on Saturday 13 June last year but snowballed over the weekend. Between 7pm and 8pm on Sunday some 175,000 error messages swarmed the system as BA officials scrambled to contain the meltdown."

"The backdrop could not have been more serious, with the country on heightened alert after jihadists had gunned down 12 people in Paris after storming the offices of satirical magazine Charlie Hebdo. At the time England football fans who had gone to Slovenia for their team's 3-2 victory that day would likely have been on their way home."

Given that business context, it is clear that both the UK Home Office and British Airways were far too cavalier about allowing a contractor to make changes to such a critical system without peer review and without a way to anticipate and fix a possible failure. At one point 1.8 million messages were queued at the Home Office Semaphore system, which crashed completely, and it left all airlines flying to Britain off-line to Semaphore and with no access to the 'no-fly list' for 48 hours, an unacceptable business interruption.

It is a well-known experience, often widely reported in the news media (as in this case, after a year of secrecy), that software upgrades and changes can go wrong, and when they do, critical business services suffer an outage. The way to manage this risk is to have a regression plan

The process begins with peer-reviewing and testing new code to make sure there are no identifiable bugs within it. It is quite common for old faults to re-emerge during the evolving life cycle of software. Sometimes this happens because a previous fix gets lost through poor revision control, either by faulty processes being applied or by human error in applying a good process. In other cases a previous fix may be 'fragile', in that it fixes a bug in a very local context where it was first observed, whereas it actually exists in the global context of the software and will re-emerge later in the life-cycle when other changes are implemented. Then there is the possibility that when a feature or function is redesigned and replaced with a new version, the same mistakes will be made in that redesign that were made in the original design, removing any fixes that may have been made to correct that problem.

Regression testing is the process of going back over the entire history of bug fixes and retesting them to ensure that they still work and have not re-emerged in the latest version. It requires that a complete history of previous releases, bugs, the fixes for them and the test procedures that expose them be maintained. There are tools on the market that can automate this regression-testing plan.

Finally, there should be the capacity to regress back to a previous known release of the software, known to work, but not with the new or redesigned features, so that business as usual can be maintained while the problem is investigated.

It seems that so many organisations still do not join the dots between business critical services and the ICT that underpins them. Technologists are in charge of the shop, with apparently no notion of what their actions can mean to the business. An IT department that did understand this principle would never allow a critical software release without a full-scale regression plan. It seems that much more SABSA thinking is needed to make the world a better, safer place.

The Attributer

CYBERSECURITY-AWARENESS HOGER OP DE AGENDA VAN BESTUURDERS?

In de Verenigde Staten is cybersecurity meerdere keren in het nieuws geweest als onderdeel van de verkiezingsstrijd. De republikeinse kandidaat deed zelfs openlijke oproepen om de mail van de democratische kandidaat te hacken. Hiermee heeft de noodzaak van informatiebeveiliging weer een nieuwe dimensie gekregen. Berichten over beveiligingsincidenten halen ook in Nederland regelmatig de voorpagina's. Niemand, ook bestuurders niet, zal nu nog stellen dan informatiebeveiliging voor zijn of haar organisatie niet belangrijk is. Maar dat houdt nog niet in dat de betreffende bestuurder zich ook realiseert wat er in de organisatie moet gebeuren. Kennis op dit gebied laten ze veelal ophalen door medewerkers naar specialistische seminars, beurzen en symposia te laten gaan. In incidentele gevallen gaan bestuurders zelf naar symposia als ze weten dat daar ook collega's aanwezig zijn of wanneer ze als keynote-spreker worden gevraagd. Er zijn nu tekenen dat bestuurders zich nu ook zelf in de materie van Cybersecurity gaan verdiepen. In de NRC van zaterdag 13 augustus is een paginagrote advertentie opgenomen voor een door die krant georganiseerd seminar (Cyber(in)security) dat belooft de kennis van bestuurders in een dag up-to-date brengen.

Gaan deze ontwikkelingen er voor zorgen dat we als informatiebeveiligers niet meer hoeven uit te leggen waarom ons vakgebied belangrijk is?


Tom Bakker


Kas Clark


Lex Dunn


Maarten Hartsuijker

Tom Bakker

Bestuurders worden inderdaad meer geconfronteerd met cybersecurity of eigenlijk gewoon informatiebeveiliging. Cyber is een buzz-word, maar goed, als het maar helpt aandacht te krijgen. Dat bewustzijn is er ergens wel zo langzamerhand maar ik zie toch ook nog wel dat cybersecurity als een 'audit dingetje' wordt gezien. Daar toezichthouders en certificerende instanties ook wat vinden van cybersecurity en daarop audits uitvoeren, is het bij bestuurders toch nog wel van 'het oplossen van audit findings want ik wil geen gezeur'. De in de inleiding geschetste ontwikkelingen stemmen hoopvol maar niet meer hoeven uitleggen waarom ons vakgebied belangrijk is? Het belang zal nooit ontkend worden maar de daden (geld, middelen) blijven toch wel achter. En waar is de CISO als bestuurder als het zo belangrijk wordt gevonden? Op die poging van de NRC moet ik nog zien of daar veel bestuurders op afkomen. Of gaan daar de CISO's naar toe?

Kas Clark

Het verhogen van awareness rondom cybersecurity, iets waar informatiebeveiligers al jaren mee bezig zijn, is van toepassing op zowel de eindgebruikers alsook de bestuurders. Wellicht in meerdere mate de laatste groep, want het zijn de bestuurders die nu na het zien van de voorpagina van de krant of het avondjournaal zelf het initiatief nemen om naar een seminar te gaan. Zo'n media "schrik" moment maakt meer indruk op bestuurders dan welke awareness-campagne dan ook. Maar toch is dat volgens mij niet voldoende; mensen, ook bestuurders, zijn geneigd om zich niet te identificeren met slachtoffers. Hierdoor ebt de noodzaak om er concrete maatregelen voor te treffen langzaam weer weg na zo'n media-moment. Het gevoel blijft bestaan dat een ernstig cyberincident bij een buitenlandse organisatie nooit bij hun eigen organisatie zou kunnen gebeuren: ander land, andere sector, andere situatie. Het is aan ons als informatiebeveiligers om te helpen met het maken van deze vertaalslag, zodat bestuurders zich niet alleen realiseren dat er een dreiging is, maar ook dat hun organisatie doelwit kan worden, met grote gevolgen. Onze taak is om de noodzaak van dit onderwerp te vertalen naar een specifiek risicoprofiel. Vervolgens moeten we de bijbehorende maatregelen op een begrijpelijke en toepasbare manier kunnen presenteren aan iedere sector. Dan pas zal het besef doordringen en zullen er concrete acties worden ondernomen, waarbij terugval naar het "oude" denken niet meer aan de orde is. We hoeven na vandaag misschien niet meer te zeggen dat ons vakgebied belangrijk is, maar wel waarom het voor alle organisaties belangrijk is.

Lex Dunn

Met alle publicaties rondom cyber-incidenten zal het C-level zich ondertussen wel bewust zijn, dat ze in dat domein een uitdaging hebben. Echter, in de dagelijkse praktijk zie ik nog weinig verschuiving van de Security Officer richting de Boardroom. Meestal zit de security-functie nog bij de IT-afdeling, en rapporteert deze aan het Hoofd IT. Gezien de verstrekkende impact van cybersecurity-incidenten, en de steeds verder gaande wetgeving op privacy gebied, zou de Security Officer een vaste plek tussen de CxO's moeten hebben. Dat houdt ook in dat de rol van de Security Officer verandert: een tiental jaren geleden was het nog voldoende om (diep) inzicht in de techniek te hebben, vandaag de dag moet de Security Officer zich als volwaardige gesprekspartner van de CxO's opstellen, en dus in businesstermen praten. En nog steeds die techniek op zijn minst begrijpen. Wordt het makkelijker, nu de CxO's vergast worden hun eigen "Security Awarness"-seminars? Dat moet ik nog zien, in de praktijk zal het er vermoedelijk op neerkomen dat de Security Officers naar dat seminar gestuurd worden. Pas als er in de management opleidingen (MBA's en dergelijke) meer aandacht aan cyber, en de security implicaties daarvan, gegeven gaat worden, zal de Security Officer wellicht direct tot zaken kunnen komen bij de CxO, in plaats van eerst te moeten uitleggen waar het nou eigenlijk over gaat.

Maarten Hartsuijker

Beveiligingsincidenten zijn tegenwoordig zo overduidelijk aanwezig dat de meeste bestuurders zich zeer bewust zijn van het belang van informatiebeveiliging. Een CEO die met CEO-fraude te maken heeft gehad hoef je niets meer over het belang van een goede awareness-campagne uit te leggen. Maar aan de overvloed aan incidenten kleeft ook een risico. Daar waar je je vroeger moest schamen als je bedrijf gehackt werd, ben je nu één van de velen geworden. Ernstige beveiligingskwetsbaarheden worden een steeds "normaler" risico. Je kunt je eigenlijk niet meer op een feestje vertonen als je organisatie nog géén datalek heeft gehad. En doordat inlichtingendiensten met zeer veel kennis, geld en gehamsterde zero days iedereen laten zien dat er tegen hackers eigenlijk niet op te beveiligen valt, lopen we steeds meer het risico dat er, wat vertrouwelijkheid betreft, een soort van "beveiligingsmoeheid" gaat ontstaan. Want als je toch continu kwetsbaar bent, waarom zou je dan nog zoveel in blijkbaar niet doeltreffende beveiligingsmaatregelen investeren?

Ons vakgebied wordt dan wel voor ons verkocht, maar daarbinnen bevindt zich voor ons een belangrijke rol om het nieuws dat het C-level bereikt te duiden en binnen de context van ons eigen bedrijf te plaatsen. Om eerlijk uit te leggen dat je niet altijd dure oplossingen hoeft aan te schaffen om 95% van de ellende buiten je deur te houden. En om te bevestigen dat we inderdaad nooit bulletproof zullen worden. Onze rol verandert en dat houdt het vakgebied interessant.

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 (Capgemini)
Maarten Hartsuijker (Classity)
Rachel Marbus (NS)
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 2016
De abonnementsprijs in 2016 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

ECHTE NAMAAK

Een tijd geleden was ik op een verjaardag waar ik een ontwerper van een groot bedrijf tegenkwam. Ik noem geen namen, maar als je denkt aan de oud-sponsor van PSV dan ben je behoorlijk warm. Hij werkt op de afdeling waar scheerapparaten worden ontwikkeld. Nu heb ik geen enkel verstand van scheerapparaten omdat ik me altijd met een mesje scheer.

Ik vroeg hem waarom zo'n ding zo duur is. Dat was de verkeerde vraag, want nadat hij een diepe zucht had geslaakt begon hij met een monoloog. Ik bespaar jullie de eerste drie uur, maar aan het eind werd het leuk. De firma heeft erg veel last van namaakapparaten. Ieder nieuw model dat ze op de markt brengen is binnen drie maanden leverbaar in China. Hij heeft er eens een gekocht daar en uit elkaar gehaald. Tot zijn verbijstering zag hij dat ieder onderdeel minutieus was nagemaakt, of nog sterker: hij kon dit apparaat niet onderscheiden van zijn eigen ontwerp. Het enige verschil was de prijs, het Chinese model was slechts een kwart van de prijs die zij vroegen. Ik wilde er nog een grapje over maken, maar een plotselinge pijn in mijn been na een onopvallende maar kordate correctieve handeling van mijn vrouw deed mij beslissen meewarig met het hoofd te schudden.

Later vertelde ik het verhaal aan een van mijn kinderen, die mij aankeek alsof ik een grap maakte. Papa, kijk toch eens op DealeXtreme, Alibaba of andere Chinese sites. Ik lachte wat schamper en ging gauw over op een ander onderwerp. Toen ze weg waren ging ik eens zoeken op 'Chinese namaak' en was verbijsterd over de hoeveelheid namaakartikelen die er te krijgen zijn.

Ik vond al snel een iPhone 6 (zoek maar eens op Goophone) die niet op iOS draait maar op een aangepaste versie van Android met de look & feel van de iPhone. Het toestel is alleen erg slecht gebouwd. Zoek eens op 'Chinese Rolls Royce' en je staat verbaasd. Kijk eens op Alibaba.com en je ontdekt dat er werkelijk geen product is dat niet is gekopieerd of (slecht) is nagemaakt. Je vindt cd's, dvd's, computerspelletjes, sieraden, kleding, parfum en dat allemaal te bestellen tegen een fractie van de prijs. Het wordt redelijk snel bezorgd. Invoerrechten heb ik nog nooit betaald.

Toch heb ik er wel een beetje een naar gevoel over, ik denk terug aan de zeurende ontwerper die veel energie steekt in een nieuw model, dat zomaar zonder pardon wordt nagemaakt. Mag dat allemaal? Je mag officieel drie producten meenemen maar het is eigenlijk niet te controleren. Als ik een bandje voor mijn smartwatch koop dat maar één-twintigste van de officiële prijs is, dan weet ik dat het namaak is.

Toch is er een keerzijde: leg ze naast elkaar en ze lijken identiek. Nergens beweert de namaker dat het om een origineel product gaat van de originele leverancier. Voor het horlogebandje van de originele leverancier betaal ik 59 euro, voor de namaak 3 euro. Het bandje is nagemaakt en dat is niet correct. Maar 59 euro vragen voor een siliconen bandje is ook een soort diefstal.

En hoe zit het met de kwaliteit? Mocht je je horloge kwijtraken omdat het Chinese bandje toch iets minder stevig was dan verwacht, dan is dat niet goed.

Berry

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

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

Stappenplan ISO 27001/NEN 7510

Download kosteloos de whitepaper 'Stappenplan naar informatiebeveiliging'

www.dnvgl.nl/whitepapers