iB
INFORMATIEBEVEILIGING
jaargang 14 - 2014
#1

COMPLEXE SAMENLEVING

Wat betekent het voor internetbedrijven 'vitale infrastructuur' te zijn?

De CBP-Richtsnoeren nader beschouwd

Tethering Enterprise Interest

COLUMN: De wedergeboorte van privacy

SECURITY Academy

Al 6 jaar uw vertrouwde opleidingspartner

Inhouse- en maatwerkopleidingen

Beste PVIB-lezer,

Als eerste wil ik u een heel goed en leerzaam 2014 wensen.
Wij hopen u in 2014 weer te mogen verwelkomen op één van onze Academy's (Security Academy, Business Continuity Academy, Security Management Academy).

In 2013 zagen wij een grote toename in de vraag naar inhouse- en maatwerkopleidingen. Wij hebben naar aanleiding hiervan een unieke propositie in de markt gezet.

Onze opleidingsadviseur inventariseert met u de opleidingsbehoeften, het kennisniveau van de potentiële cursisten en de gewenste opleidingsduur, waarna de opleiding wordt samengesteld uit de meer dan 100 beschikbare modules. De maatwerkopleidingen laten wij zoveel mogelijk aansluiten op uw organisatie (uw beleid, procedures en IT-omgeving). Uw security (beleid) wordt zo een onderdeel van de opleiding waardoor de overgebrachte kennis direct in de dagelijkse praktijk toegepast kan worden. Na de opleiding kan de docent eventueel worden ingezet als coach om het geleerde in de praktijk verder te ondersteunen.

Voor meer informatie over inhouse opleidingen en maatwerk kunt u contact opnemen met een van onze opleidingsadviseurs via info@securityacademy.nl

Open inschrijvingen

CISSP Preparation Course

- Startdatum: 10 maart
- Duur: 11 dagen
- Prijs: € 5.950,- excl. BTW
- € 100,- korting voor PVIB-leden

CISM Preparation Course

- Startdatum: 6 mei
- Duur: 5 dagen
- Prijs: € 3.250,- excl. BTW
- € 100,- korting voor PVIB-leden

Post-HBO Security Management

- Startdatum: 7 maart
- Duur: 15 dagen
- Prijs: € 9.870,- excl. BTW
- € 100,- korting voor PVIB-leden

Post-HBO Netwerk Security

- Startdatum: 12 maart
- Duur: 15 dagen
- Prijs: € 9.870,- excl. BTW
- € 100,- korting voor PVIB-leden

COMPLEXE SAMENLEVING

Het duizelt mij soms als ik me besef wat allemaal deel uitmaakt van onze kritieke infrastructuur. Een helder overzicht van de sectoren in deze infrastructuur is te vinden op de website van infracritical [1]. We hebben een complexe samenleving gebouwd in de afgelopen paar duizend jaar! Een aantal van deze sectoren bestaan al sinds de oudheid, al waren ze toen wellicht nog eenvoudig in te vullen: de voedselketen, financiën, transport, gezondheidszorg, watervoorziening. De urbanisatie hebben daar overheidsdiensten en nooddiensten aan toegevoegd, gevolgd door de industriële revolutie, die er industrie, energievoorziening en communicatie aan toevoegden. Alle bestaande diensten werden trouwens flink complexer. De enige nieuwe sector die erbij gekomen is in de laatste 100 jaar, is de IT-sector. Of beter gezegd, deze is bijgevoegd in de communicatiesector. En dat een kritiek falen mogelijk is, hebben we inmiddels ook gemerkt, ik noem alleen even het woord 'Diginotar' [2]. Als je vervolgens inhoudelijk kijkt naar de invulling van alle sectoren, dan moet je wel constateren dat alle andere kritieke infrastructuur afhankelijk is geworden van ICT, met alle gevolgen van dien. Denk maar bijvoorbeeld aan de pompen in Veere [3]. In het hippie-tijdperk was IT niet kritiek. Alles in de samenleving kon doorgaan zonder IT. Gaandeweg is dit in de tussenliggende jaren veranderd. Mainframes krompen van zaalvullende, hitteproducerende monsters naar kleine zoemende kabinetten in de hoek van een kantoorgebouw of een paar centimeter in een serverrack. De 'PC' is uitgegroeid van een hobbydoos tot een rekenwonder met onvoorstelbare opslag- en verwerkingscapaciteit.
Ik heb leren programmeren op de Intel 4004 [4]. Het is deze processor geweest die mij het inzicht gaf dat, met zulk een veelzijdige hardware, met software alles mogelijk was wat je maar kon verzinnen. Vervolgens heb ik de luxe gekend om te werken op Burroughs mainframes [5] en aan een gepartitioneerd Unix systeem, 'THE KUNix' [6], die beiden dit gevoel alleen maar verstevigden. Alles wat ik me toen kon voorstellen, en nog veel meer, is nu mogelijk op een PC of een mobiel apparaat. Het is geen wonder dat we onszelf toegestaan hebben dat deze apparaten en de software die er op draait tot een kritiek deel zijn geworden van de infrastructuur die we als samenleving neergezet hebben. We hebben dit echter te gemakkelijk laten gebeuren. Het wordt nu wel zaak dat we er verantwoordelijk mee leren omgaan. Dit zal wat tijd vergen, maar het is kritiek dat wij de beveiligingsvraagstukken en de privacyvraagstukken die ontstaan zijn en nog gaan komen voor de samenleving goed oplossen. Snowden heeft de knuppel in het hoenderhok gegooid. Nu zijn wij aan zet.

Lex Borger, hoofdredacteur

Links

[1] Critical Infrastructure Sector Map: http://www.infracritical.com/images/cip-sectors5.jpg1
[2] 5 beveiligingsflaters van DigiNotar: http://webwereld.nl/beveiliging/1051-5-beveiligingsflaters-van-diginotar---update
[3] Zeeuwse gemalen te hacken via SCADA-lek: http://webwereld.nl/beveiliging/56064-zeeuwse-gemalen-te-hacken-via-scada-lek---update
[4] Intel 4004: http://en.wikipedia.org/wiki/Intel_4004
[5] The Burroughs B5900 and E-Mode: http://jack.hoa.org/hoajaa/Burr126b.html
[6] Het "THE KUNix" systeem: Disk software en Multi processor opzet: http://repository.tue.nl/296104

In dit nummer

Wat betekent het voor internetbedrijven 'vitale infrastructuur' te zijn? - 4

Column Privacy: De wedergeboorte van privacy - 7

De CBP-Richtsnoeren nader beschouwd - 8

Column Attributer: Integrity Protected - 15

Tethering Enterprise Interests - 16

Beveiliging is niet alleen een zaak van de IT-afdeling - 20

Security Café - 24

Verantwoorde onthullingen #4: "I Hacked KPN, and all i got was this lousy t-shirt." - 27

IDentity.Next 2013 - 28

Achter het nieuws - 30

Jaaroverzicht 2013 - 32

Column: Berry - 35

WAT BETEKENT HET VOOR INTERNETBEDRIJVEN VITALE INFRASTRUCTUUR TE ZIJN?

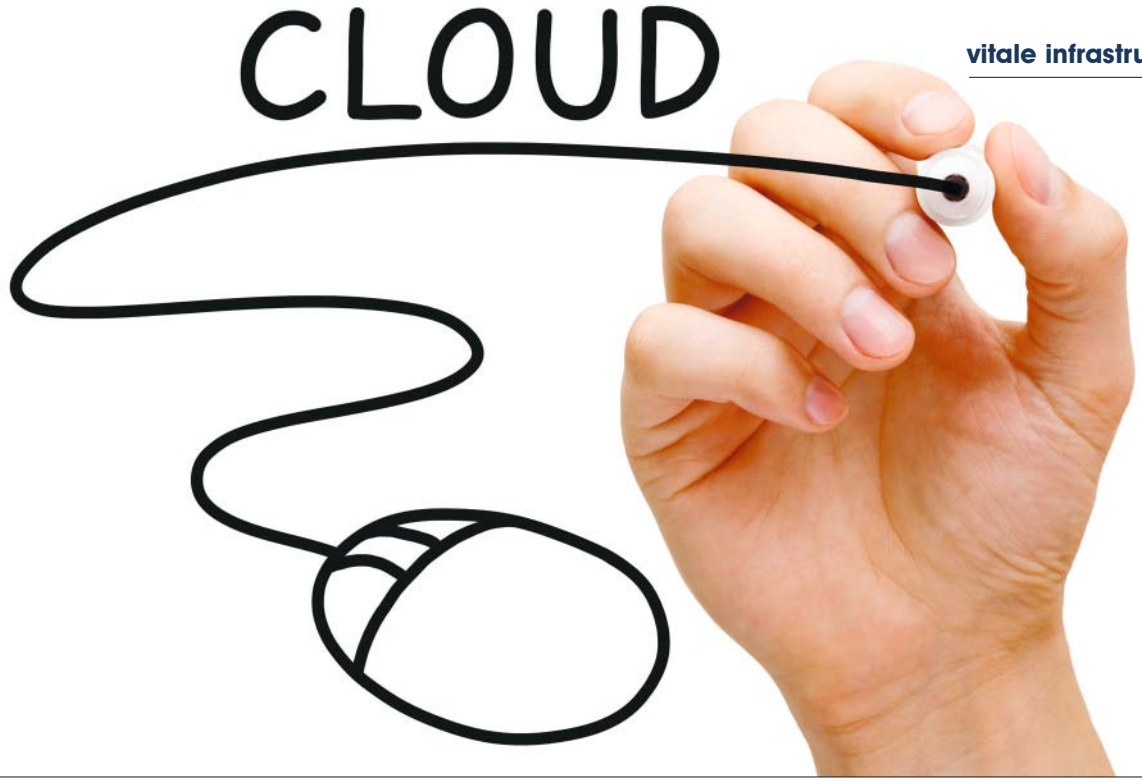
Op de lijst van sectoren en bedrijven die de vitale infrastructuur [1] van het land vormen, is weinig kritiek. Het overzicht is duidelijk en roept geen vragen op bij de pers of het grote publiek. Maar wat betekent het voor bedrijven uit de sectoren die hier worden genoemd? Weten ze dat wel, vinden ze het terecht en wat is de impact?

Om antwoord op die vragen te krijgen zijn, voor een sector, vijf internetbedrijven benaderd. De keuze voor internetbedrijven is gemaakt om twee redenen. Ten eerste omdat de definitie van vitale infrastructuur aansluit bij een inmiddels 12 jaar oud rapport, opgesteld door Stratix en TNO in opdracht van het Ministerie van Verkeer en Waterstaat [2]. De vragen die daarbij centraal stonden: is internet kwetsbaar en een vitale infrastructuur en is toezicht van de overheid op die sector nodig. Dit rapport kan worden beschouwd als de aftrap voor de discussie over vitale infrastructuur in relatie tot internet.

De conclusie van het rapport uit 2001 was dat de sector op dat moment te divers en diffuus was voor overheidstoezicht. De mogelijkheden van de overheid zouden op praktische gronden beperkt zijn, niet in de laatste plaats door het grote aantal aanbieders en het feit dat het om zowel nationale als internationale partijen ging. Anno 2013 is de markt voor internet niet overzichtelijker dan in 2001. Volgens de KvK zijn er tenminste 1.200 bedrijven die internetdiensten leveren, gevestigd in Nederland. Daarbij moeten nog worden opgeteld de bedrijven die op de Nederlandse markt actief zijn, maar hier geen fysieke vestiging hebben. Het aanbod is uiterst divers en omvat alles van grote internationaal georiënteerde netwerkbeheerders, via nationaal opererende datacenters tot hostingbedrijven die een regionale footprint nastreven. Een ding hebben al deze partijen gemeen: ze zijn onderdeel van een dynamische keten die inmiddels onmisbaar is voor de samenleving en daarom vitale infrastructuur heet te zijn.

Rashid Niamat is journalist en werkzaam bij ISPam.
Rashid is te bereiken via rashid@niamatmediagroup.nl

Dat is de tweede reden voor het benaderen van deze sector. Als er een sector van de vitale infrastructuurlijst is die het laatste decennium een gestage opmars maakte en inmiddels alle facetten van de samenleving raakt dan is het wel de op internet gebaseerde dienstverlening. Hoezeer die afhankelijkheid is toegenomen, blijkt op het moment dat er sprake is van verstoringen van de dienstverlening. Het begrip domino effect behoeft hier verder geen toelichting. Het grote publiek weet inmiddels: zonder internet komt (een groot deel van) het land tot stilstand.



Meer dan 90% van de huishoudens zijn online en meer dan 55% koopt online

Een andere manier om die toegenomen afhankelijkheid te illustreren is te kijken naar de groei van internetgebruik en e-commerce tussen 2001 en 2013. Ultimo 2001 maakte 55% van de huishoudens voor privé doeleinden gebruik van internet [3] en minder dan 15% had de voorgaande periode van 3 maanden iets online besteld [4]. Eind 2012 was meer dan 90% van de huishoudens online en meer dan 55% had recente e-commerce ervaring. Cijfers die aantonen dat de status vitale infrastructuur wel ergens op is gebaseerd, maar hoe zien de aanbieders van internetdiensten dat zelf?

Reacties

De vragen zijn voorgelegd aan vijf bedrijven [5]. Het dienstenaanbod verschilt per bedrijf, maar omvat het hele scala van toegang tot het internet voor consumenten en bedrijven, hosting, storage tot datacenterdiensten. In een opzicht deden de bedrijven niet voor elkaar onder: de animo de eigen visie over dit onderwerp met het PvIB magazine te delen was groot. De bedrijven reageerden snel en vooral uitgebreid.

Alle partijen gaven aan bekend te zijn met de begrippen vitale- en kritische infrastructuur en konden daar ook invulling aan geven. Dit werd onder andere geïllustreerd door de antwoorden op de vraag: is het terecht dat internet als vitale infrastructuur geldt? Iedereen was het hier mee eens, sommigen lieten weten dat men zich maar al te goed bewust was van de eigen rol in de keten, terwijl dat begrip niet in de vraagstelling voorkwam.

Op de vervolgvraag: "wat betekent dat voor je bedrijfsvoering en je klanten" volgde meer uiteenlopende antwoorden. WideXS reageerde met: "Veel en in een groot aantal gevallen heel veel zo niet alles". Men gaf verder aan dat uit eigen onderzoek blijkt dat het onderwerp top of mind is voor veel klanten. Oxilion verlegde in het antwoord het accent naar de bedrijfsvoering: "Het begint wat mij betreft bij het besef dat het vitale infrastructuur is. Bij alle mensen die erbij betrokken zijn en dat begint dus bij jezelf en je eigen medewerkers". Een van de benaderde partijen exploiteert datacentra. Deze focus op een beperkt deel van de keten maakt dat het weer een andere kijk heeft op het begrip vitale infrastructuur: "Voor ITB2 betekent het dat we bij het inrichten van onze datacenters en het beheer ervan nauw moeten aansluiten bij de voorwaarden die door de meest veeleisende klanten worden gesteld". Drie antwoorden die elk een andere invalshoek laten zien.

‘Het is onze plicht de Cloud infrastructuur optimaal aan te bieden’

Op de concrete vraag “lust of last?” antwoordden de meeste ondernemers dat ze het zien als een lust. De vertaling naar een commerciële propositie lag bij de meesten ook voor de hand. Fundaments was hiervan een goed voorbeeld: “We zien het als onze plicht de Cloud infrastructuur optimaal aan te bieden aan onze klanten.[...] Deze uitdaging vertalen we graag naar een lust”.

Link met certificeringen

De aanbieders weten wat vitale infrastructuur is, maar gaat dat ook op voor de klanten of leveranciers, stellen zij hier vragen over? Hier lopen de reacties uiteen: “Wij krijgen er geen vragen over” (WideXS); “Ja, onze klanten vragen er concreet om, het is vaak een voorwaarde” (Solcon) en “De lange lijst met wensen en hoge eisen die verschillende klanten op tafel leggen, maakt duidelijk dat zij onze datacenters als vitale infrastructuur zien” (ITB2). Oxilion merkte op dat leveranciers er vaker op inspelen door te komen met aanbod dat nog meer gericht is op stabiliteit en beschikbaarheid.

De wijze waarop de bedrijven omgaan met dit soort vragen loopt minder uiteen. Ook al is er geen directe link tussen vitale infrastructuur en (bijvoorbeeld) ISO27001 zoals WideXS terecht opmerkt, feit is dat voor veel bedrijven in de sector audits en certificeringen de manier zijn om te laten zien dat men zich bewust is van de eigen rol. Dat blijkt ook uit het feit dat het aantal bedrijven in deze sector dat 2013 bekend maakte voor het eerst naar ISO27001 gecertificeerd te zijn groter is dan voorgaande jaren.

Naast de aandacht voor audits en procedures komt een ander aspect zo mogelijk nog sterker naar voren: het streven naar optimale dienstverlening - het begrip zorgplicht is in de antwoorden meermaals genoemd - te combineren met de realiteit dat niet iedere klant daadwerkelijk 24/7/365 service wenst of een 100% up-time. Daar zit een tegenstelling: men voelt zich een vitale infrastructuur, maar weet ook dat lang niet alle klanten dat verwachten (lees: daar wil men niet voor betalen).

Conclusie

Als de reacties van deze vijf bedrijven representatief zijn voor de sector kan worden geconcludeerd dat het label vitale infrastructuur geen negatieve lading heeft. Veel meer is er sprake van acceptatie van iets dat de sector al lang wist: internetbedrijven hebben een belangrijke functie in de economie. Tegelijkertijd ziet men het als een mogelijkheid meer invulling te geven aan begrippen als kwaliteit, invulling van de zorgplicht en verdere professionalisering van de sector. De vraag is of een dergelijke houding eveneens bij de andere vitale infrastructuursectoren en bedrijven geldt of dat internetbedrijven een buitenbeentje zijn.

Referenties

[1]
nctv.nl/onderwerpen/nv/voorkomen-voorbereiden/bescherming-vitale-infrastructuur/

[2]
zoek.officielebekendmakingen.nl/dossier/26643/kst-26643-30?resultIndex=293

[3]
Bron: TNS NIPO publicaties

[4]
Bron: eurostat.ec.europa.eu definitie voor e-commerce: Individuals having ordered/bought goods or services for private use over the Internet in the last three months)

[5]
Deelnemende bedrijven op alfabetische volgorde:
Fundaments.nl
ITB2.nl
Oxilion.nl
Solcon.nl
WideXS.nl

"Education is the most powerful weapon which you can use to change the world."

- Nelson Mandela -

DE WEDERGEBOORTE VAN PRIVACY

Defaitisme heeft geen plaats. Ik heb gemerkt dat 2013 het jaar is geweest waarin mijn leken-omgeving geschokt is geraakt van alle privacyschendingen die het nieuws hebben gehaald. Ik durf ze bijna niet te vertellen van alle zaken die het nieuws niet haalden. Dat waren er meer dan genoeg. Liever spreek ik van die andere beweging die in 2013 is ingezet en waarvan ik hoop dat die in 2014 tot volle wasdom kan komen.

Mr. Rachel Marbus, @rachelmarbus op Twitter

We zijn namelijk met steeds meer. De voorvechters van privacy en burgerrechten. En we zitten niet stil, we vertellen, we onderwijzen, we vermeerderen en verspreiden kennis. Ik zag de groeiende aandacht voor cryptoparties. Workshops aangeboden door hackerspaces waar burgers kunnen leren om zichzelf te beschermen tegen een al te nieuwsgierige overheid of opdringerige bedrijven. Mensen leren er om anoniem te browsen en versleuteld e-mail te versturen. Hackerspaces vragen daar geen geld voor, zij geven de cryptoparties omdat zij kennis willen delen en mensen weerbaar willen maken.

De NOS plaatste eind vorig jaar een artikel met daarin vijf tips hoe mensen het best hun privacy kunnen beschermen. Daarbij onder meer wijzend op het gebruik van TOR en het belang van het beveiligen van draadloze internetverbindingen. In het kader van defember wijst GeenStijl nog eens op de Privacy Inzage Machine van Bits of Freedom. Met de PIM kun je geautomatiseerd brieven genereren om gebruik te maken van het recht op inzage onder de Wet bescherming persoonsgegevens. De Piratenpartij voegt daar nog geautomatiseerde WOB-brieven aan toe waarmee bij de AIVD persoonlijke dossiers opgevraagd kunnen worden.

Kohnstamm, voorzitter van het College Bescherming Persoonsgegevens, sloeg met de vuist op tafel. Wij, Nederland, zijn te klein om het in ons eentje op te nemen tegen NSA en de USA en daarom moeten we samen optreden, zo riep hij de andere lidstaten in de EU op in een interview. Ik had het genoegen Kohnstamm onlangs nog te horen spreken waarbij hij vertelde dat steeds meer bedrijven in een spagaat komen te zitten, omdat zij zich graag aan EU privacywetgeving willen houden, maar door de Amerikaanse overheid onder druk worden gezet om juist die privacy terzijde te schuiven. Het CBP heeft met haar 70 werknemers te weinig slagkracht om de privacy van burgers in deze gevallen te beschermen, zo gaf Kohnstamm toe. Desalniettemin wordt er wel op de barricades geklommen.

De algemene vergadering van de VN liet ook publiekelijk van zich horen. Duitsland en Brazilië stelden een resolutie op die door de 193 landen unaniem is aangenomen. Privacy is een grondrecht en een dergelijk recht hoort te beschermen tegen wereldwijd afluisteren van burgers. Hoewel een dergelijke resolutie niet bindend is, heeft het wel degelijk grote politieke betekenis.

Ook jongeren laten zien dat zij steeds bewuster met hun privacy omgaan. Ja, iedereen stuurt weleens zeer privaat materiaal naar anderen. Laten we niet onze kop in het zand steken en zeggen dat jongeren dat niet zouden moeten doen, het gebeurt namelijk toch wel. Leer ze hoe het beter kan. Snapchat, een app waarmee je foto's kunt versturen die zichzelf in korte tijd vernietigen, wordt inmiddels zeer veel gebruikt en dan vooral door jongeren.

Neemt u als goed voornemen vooral ook eens een kijkje op https://bespied-ons-niet.nl waar Bits of Freedom vijf maatregelen poneert om de massale spionage van burgers een halt toe te roepen. Vooral punt 4 zal u informatiebeveiligingshelden moeten aanspreken. Oh… En mocht u het gemist hebben… Vergeet die 'selfie' die u nu zojuist met snapchat aan uw lief gestuurd heeft, want volgens dictionary.com is de selfie helemaal niet het woord van 2013, maar is die eer gegund aan Privacy.

Van mij mag privacy een nog grotere opmars gaan maken. Ik zal er in ieder geval regelmatig over blijven publiceren, onderwijzen en spreken. En met mij een heel leger andere privacyvoorvechters. Ik wens u een mooi en privacyvriendelijk 2014.

Frans Kersten RE RA. Frans is zijn hele werkzame leven vanuit verschillende rollen (accountant, IT-auditor, consultant) betrokken bij de betrouwbaarheid van de informatievoorziening. Bij zijn vorige werkgever heeft hij te maken gehad met het aantoonbaar moeten voldoen aan AV-23 en een privacy audit. Thans is hij werkzaam voor het Admiraal de Ruyter Ziekenhuis. Hij is bereikbaar via kersten210@msn.com.

DE CBP-RICHTSNOEREN NADER BESCHOUWD

Op 19 februari 2013 heeft het College Bescherming Persoonsgegevens (CBP) het document "Richtsnoeren" uitgebracht. Dit document vervangt het document "Achtergrondstudies en Verkenningen nummer 23, Beveiliging van persoonsgegevens", in de wandelgangen bekend als AV-23. In Informatiebeveiliging, nummer 6 – 2013, is al kort op de inhoud van deze nieuwe Richtsnoeren ingegaan. Dit artikel gaat nader in op de inhoud en sluit af met een conclusie of het document voldoet aan de door het CBP aangegeven doelstellingen. Het start bij de wettelijke eisen tot beveiliging van persoonsgegevens. Vervolgens volgt een terugblik op AV-23. Daarna wordt nader ingegaan op de nieuwe Richtsnoeren.

AV-23 had onvoldoende aansluiting op verschillende ontwikkelingen op het gebied van informatiebeveiliging

De wettelijke regels voor de bescherming van persoonsgegevens voor zover deze niet voortvloeien uit de Grondwet, zijn voor het eerst nader uitgewerkt in de Wet Persoonsregistratie (Wpr) van 1 juli 1989. In 2001 is deze wet vervangen door de huidige Wet Bescherming Persoonsgegevens (Wbp). In de Wpr was de noodzaak tot beveiliging opgenomen in artikel 8. In de Wbp is dit vervangen door artikel 13 met de volgende inhoud:

De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Deze tekst bevat een aantal formuleringen die krachtig samenvatten waar het in beveiliging eigenlijk onder alle omstandigheden om gaat: een passend niveau van beveiliging, rekening houdend met de risico's en belangen, de kosten en stand der techniek. Dit laatste is van belang, omdat dit de mogelijkheid volledig openhoudt om rekening te houden met technologische ontwikkelingen. Als we terugzien naar het begin van de Wbp dan vergde bescherming van persoonsgegevens door inzet van encryptie rond 1980 nog kostbare maatregelen, nu zijn deze standaard geworden en tegen lage kosten beschikbaar via toepassingen zoals https, SSL, Truecrypt, e.d.. Al in de Wpr was voorzien in toezicht op de naleving van de wet door de toenmalige Registratiekamer. Deze is opgevolgd door het huidige College Bescherming Persoonsgegevens (CBP). Dit orgaan heeft een belangrijke rol gespeeld bij de nadere invulling van deze beveiligingsbepaling.

Korte terugblik op AV-23

De Registratiekamer en later het CBP heeft naast een toezichthoudende ook een adviserende taak. Onder de Wpr is op deze wijze de publicatie "Beveiliging van persoonsregistraties" uitgebracht. In deze publicatie wordt de link gelegd naar de noodzaak tot beveiliging zoals vastgelegd in het toenmalige artikel 8 van de Wpr. Aangegeven wordt dat beveiliging doorgaans afgemeten wordt aan drie criteria: beschikbaarheid, integriteit en exclusiviteit. In de publicatie ligt het accent op exclusiviteit. Er wordt gewezen op het belang van risicoanalyse. Er wordt al melding gemaakt van 'state of the art' beveiliging, in de Wbp verankerd via 'stand van de techniek. De basis is echter de indeling in drie exclusiviteitsniveaus (basis, 2 en 3) en de bijbehorende normen. De normen zijn geformuleerd in termen van de te treffen maatregelen.

Met de wijziging van Wpr naar Wbp is in de geactualiseerde opvolger de titel veranderd in "Beveiliging van persoonsgegevens". Later is deze publicatie met nummer 23 ondergebracht in de reeks "Achtergrondstudies en verkenningen".

AV-23 kent samengevat de volgende inhoud. Eerst volgt een introductie hoe de inhoud aansluit bij de bepalingen van de Wbp. Naar analogie van de voorganger is voorts sprake van een indeling in wat nu, in plaats van exclusiviteitsniveaus, risicoklassen wordt genoemd. Deze risicoklassen geven een indeling van persoonsgegevens naar oplopend belang van bescherming. Er is sprake van drie klassen, waarbij klasse 3 de hoogste mate van bescherming behoeft. In het vervolg van AV-23 wordt dit vertaald in de bij die klasse behorende eisen.

Als zodanig was AV-23 te beschouwen als een normenkader hoe persoonsgegevens te beveiligen. Daarmee vormde AV-23 de basis voor de systematiek van privacy audits en assessments

zoals dat later door het CBP in samenwerking met het koninklijk NIvRA (thans NBA) en de NOREA is ontwikkeld. Tevens is AV-23 gebruikt als normenkader bij de uitbesteding van ICT, met name vanuit de overheid. Dit liep uiteen van de ontwikkeling van informatiesystemen tot outsourcing van de technische infrastructuur.

Waarom AV-23 vervangen moest worden

Er is een aantal bezwaren aan te wijzen tegen de inrichting van AV-23 en daarin is ook de argumentatie opgenomen waarom AV-23 nodig vervangen moest worden:

1. Formulering van normen in termen van maatregelen in plaats van formulering in termen van doelstellingen;
2. Mede hierdoor inmiddels te beschouwen als op onderdelen strijdig met de Wbp zelf;
3. Onvoldoende aansluiting op verschillende ontwikkelingen op het gebied van informatiebeveiliging en in (de organisatie) van ICT.

Achter AV-23 ging echter een manco schuil dat veel normenkaders treft: de eisen waaraan men zich moet houden zijn niet verwoord als doelstellingen (objectives) maar in de vorm van te treffen maatregelen. Vaak zijn er meer mogelijkheden om tot een passende beveiligingsoplossing te komen voor een bepaald probleem. Zie de verschillende oplossingen op het gebied van logische toegangsbeveiliging. Formulering in termen van maatregelen kan dan een bepaalde oplossing propageren en aanvaardbare alternatieven negeren. Aan de andere kant is een ervaringsgegeven dat in de situatie dat met doelstellingen gewerkt wordt, zeker de minder deskundigen graag willen weten welke maatregelen voldoende zijn om aan de doelstelling te voldoen. Het bekende dilemma van 'principle based' versus 'rules based'.

In het geval van AV-23 heeft de 'rules based' benadering uiteindelijk negatief uitgewerkt. Artikel 13 Wbp is zodanig geformuleerd dat technologische ontwikkelingen geen belemmering mogen vormen. Tijdens een privacy audit mocht ik echter meemaken dat een non-compliancy werd geconstateerd tegen de norm dat het aantal keren kunnen ingeven van een foutief wachtwoord beperkt moest zijn tot drie. De werkelijke instelling op een server had de waarde vijf. Er was echter sprake van een uit meer lagen opgebouwde beveiliging waarbij op de eerste schil sprake was van een op tokens gebaseerde toegangsbeveiliging. In een objectieve beschouwing wordt zonder meer voldaan aan de door de wet verlangde toereikende logische toegangsbeveiliging. Je zou derhalve kunnen concluderen dat AV-23 op onderdelen strijdig was geworden met de Wbp zelf: achterlopend bij de technologische ontwikkelingen.

Tot slot is AV-23 ook achterhaald door verschillende andere ontwikkelingen. Op het gebied van informatiebeveiliging hebben ISO-27001 en ISO-27002 zich ontwikkeld tot de meest gevolgde standaarden. Ten tijde van het "Advies beveiliging van persoonsgegevens" was een "kruisverwijzingslijst" opgesteld waarin de relatie werd gelegd met de toenmalige versie van de Code voor Informatiebeveiliging en het Voorschrift Informatiebeveiliging Rijksdienst (eerste versie uit 1994). Deze lijst is (helaas) niet onderhouden. Wie geprobeerd heeft de aansluiting te maken tussen AV-23 en ISO-27001/2 zal gemerkt hebben dat die niet volledig te maken was. Daarnaast heeft outsourcing, al dan niet via cloud computing, een belangrijke vlucht genomen. Daarbij kun je te maken krijgen met verschillende partijen, zoals de eindverantwoordelijke voor de gegevensverwerking, een systems integrator, de leverancier van de applicatie en de leverancier van de IT-infrastructuur. De maatregelen uit AV-23 moet je dan verdelen over meer partijen, waarbij één maatregel bij meer partijen (of zelfs alle) terecht kan komen. AV-23 ging niet nader in op deze verdeelproblematiek.

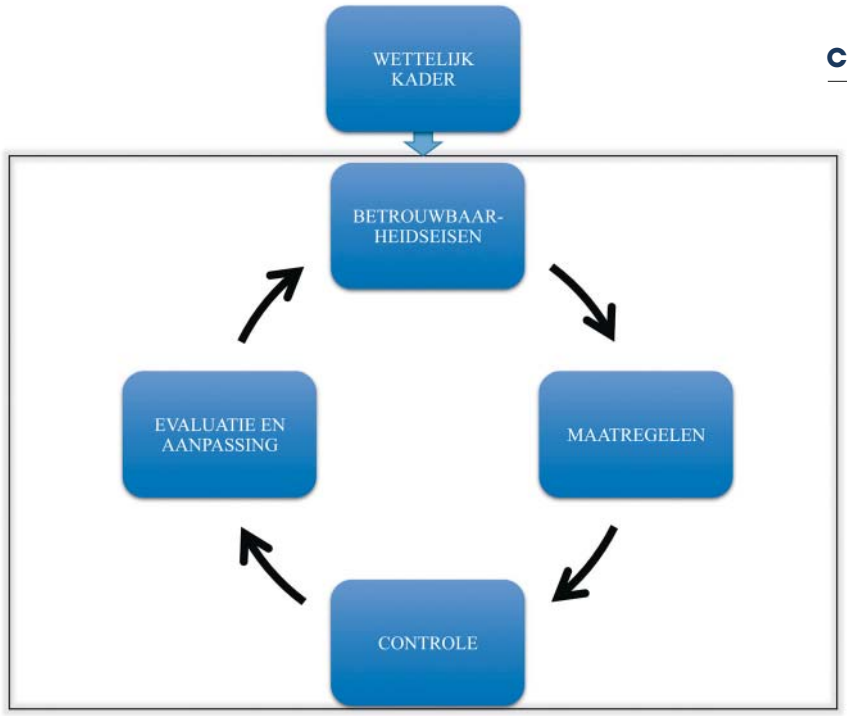
De nieuwe Richtsnoeren

De Richtsnoeren kennen na de inleiding en de samenvatting de volgende hoofdstukken:

1. **Beveiliging in de Wbp**
2. **Het vakgebied informatiebeveiliging**
3. **Beveiliging in de praktijk**
4. **Beveiliging bij verwerking door een bewerker**
5. **Handhaving en de rol van het CBP**

Tussen de samenvatting en de hoofstukken is nog een schema "beveiliging van persoonsgegevens" opgenomen dat de samenhang tussen de verschillende hoofdstukken en paragrafen toelicht. In een bijlage zijn de meest relevante bepalingen uit de wetgeving overgenomen. Via voetnoten zijn verwijzingen naar andere, mogelijk relevante publicaties opgenomen.

In de samenvatting geeft het CBP aan dat beveiliging van persoonsgegevens een van de speerpunten is in het handhavingsbeleid van het CBP. Belangrijk hierbij is de vraag wanneer beveiligingsmaatregelen 'passend' zijn zoals de Wbp eist? Het CBP geeft aan "dat de richtsnoeren uitleggen hoe het CBP bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens in individuele gevallen de beveiligingsnormen uit de Wbp toepast. De richtsnoeren vormen de verbindende schakel tussen enerzijds het juridisch domein, met daarbinnen de eisen uit de Wbp, en anderzijds het domein van de informatiebeveiliging, waarin de noodzakelijke kennis en kunde aanwezig is om daadwerkelijk aan die eisen te voldoen. Dat betekent dat de richtsnoeren in samenhang moeten worden gebruikt met algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van de informatiebeveiliging, zoals de Code voor



Figuur 1 - Plan-Do-Check-Act cyclus in de richtsnoeren

Informatiebeveiliging of de ICT-beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum."

Het CBP start vanuit de wettelijk basis voor beveiliging zoals die vastligt in de artikelen 12 (verwerking in opdracht; geheimhoudingsplicht), 13 (beveiliging) en 14 (beveiliging bij verwerking door een bewerker). De beveiligingsmaatrelen moeten vervolgens getroffen en beheerst worden op basis van een plan-do-check-act-cyclus is opgebouwd, zie figuur 1.

Hierbij geldt dat de maatregelen (moeten) worden getroffen op basis van risicoanalyse met inachtneming van de gestelde betrouwbaarheidseisen en met toepassing van vigerende beveiligingsstandaarden. Voorts zie je nadrukkelijk aandacht voor de situatie waarin een of meer onderdelen van de gegevensverwerking zijn uitbesteed en dus sprake is van een bewerker. Deze wordt geacht ook zelf een risicoanalyse uit te voeren. Vervolgens komen de maatregelen dan terug in de vorm van afspraken in de bewerkingsovereenkomst. Daarna komt de bewerker ook terug in de stappen: controle, evaluatie en aanpassing. Dit in de vorm van toezicht op de naleving van de afspraken en evaluatie en aanpassing van verwerking door de bewerker.

Vraag is of de Richtsnoeren toegevoegde waarde hebben. Hierbij is gekeken naar enerzijds de doelstelling om nadere invulling te geven aan de beveiligingseisen uit de Wbp, anderzijds het hanteren als toetsingskader voor het CBP in het kader van handhaving. Onderstaand komt eerst aan bod wat er positief is aan de nieuwe Richtsnoeren. Helaas zitten hier ook een aantal negatieve kanten aan. Deze blijken vooral te maken te hebben met toepassing als een normenkader. Deze problematiek komt in de daaropvolgende paragraaf aan bod.

Wat is er positief aan de Richtsnoeren

1. Aansluiting op de Wbp zelf
   De teksten zijn zodanig opgebouwd dat telkens wordt uitgelegd waarom een bepaalde keuze in aanpak, zoals beschreven in de Richtsnoeren goed, aansluit op de wetteksten.

2. Risicoanalyse
   In aansluiting op de tekst van artikel 13 Wbp staat risicoanalyse nadrukkelijk centraal. Het proces van risicoanalyse zorgt er immers voor dat de juiste afwegingen kunnen worden gemaakt om te komen tot een passende beveiliging in overeenstemming met de risico's. Een goede risicoanalyse zorgt ook voor een juiste combinatie van technische en organisatorische maatregelen.

3. Aansluiting op beveiligingsstandaarden
   Door aan te geven dat bij de inrichting van de beveiliging gebruik moet worden gemaakt van beveiligings-standaarden is aansluiting mogelijk op de dagelijkse praktijk en ontwikkelingen op het gebied van beveiliging. Dit voorkomt dat, zoals bij AV-23, maatregelen voorgesteld worden die feitelijk niet meer passend zijn. De breedte aan standaarden maakt het mogelijk om op allerlei deelgebieden passende oplossingen te vinden, zonder de beperking van AV-23. Vanuit de praktijk is het logisch dat daarbij ISO-27001/2 genoemd worden: deze worden immers het meest toegepast. De frequentie van

aanpassing van deze standaarden is echter relatief laag. Gelukkig worden ook andere standaarden genoemd die frequenter onderhouden worden.

4. [Hiermee ook] Aansluiting op de plan-do-check-act cyclus
   Deze cyclus is kern van kwaliteitssystemen en -standaarden in brede zin en ook van beveiligingsstandaarden. Hiermee wordt onderkend dat beveiliging geen statisch, maar een dynamisch geheel moet zijn. Dit draagt bij aan blijvende passendheid in de tijd gezien. Indirect volgt hier ook uit dat eenmalig een risicoanalyse uitvoeren en beveiligings-maatregelen selecteren en implementeren niet voldoende is.

5. Juiste accenten
   Op diverse plaatsen wordt gewezen op het belang van 'security by design' c.q. 'privacy by design' en de toepassing van Privacy Enhancing Technologies (PET). Dit is niet alleen van belang voor het realiseren van een passend beveiligingsniveau, maar draagt ook bij tot verlaging van de kosten zodat deze realisatie beter haalbaar wordt.

6. Onderkennen ketenproblematiek
   Nadrukkelijk wordt onderkend dat informatieverwerking dikwijls niet beperkt blijft tot de organisatie van de eigenaar van de persoonsgegevens. Niet alleen komt de problematiek van gebruik van een 'bewerker' aan bod. Ook wordt onderkend dat deze bewerker weer gebruik kan maken van één of meer 'subbewerkers'.
   In het kader van het verkrijgen van zekerheid of de bewerker zich houdt aan de gemaakte afspraken wordt de mogelijke rol van een Third Party Mededeling (TPM) of certificering benoemd. Er wordt terecht opgemerkt dat de verantwoordelijke zelf moet nagaan of deze voor hem voldoende zekerheid verschaffen.

7. Praktijkvoorbeelden / nadere toelichtingen
   Er zijn voorbeelden uit de praktijk en aanvullende toelichtingen ("nader bekeken") opgenomen als illustratie van de meer theoretische beschrijvingen. Niet alle voorbeelden vind ik even gelukkig gekozen. Ik denk dat het maken van een back-up en deze terugzetten na een calamiteit met verlies van gegevens nog altijd aansprekender is dan je verzekeren om benadeelde klanten een schadevergoeding te kunnen betalen na een geslaagde hack.

Wat had beter gekund

Onderstaand komen de punten aan bod die mijns inziens beter uitgewerkt hadden kunnen worden c.q. waarom de Richtsnoeren niet geheel voldoen aan de (zelfopgelegde) doelstellingen van het CBP.

1. Conceptueel/theoretisch minder goed doordacht
   In de aanpak is er afzonderlijk aandacht voor het onderkennen van betrouwbaarheidseisen en risicoanalyse. Daarnaast onderkent het CBP het belang van de Privacy Impact Assessment (PIA) als een belangrijk hulpmiddel. "Een PIA helpt de verantwoordelijke om de risico's te beoordelen die een verwerking van persoonsgegevens met zich meebrengt voor de rechten en vrijheden van de betrokkenen en om maatregelen te treffen die deze risico's beperken." Het CBP stelt echter dat de PIA valt buiten de reikwijdte van art. 13 Wpb en de Richtsnoeren. Er wordt niet toegelicht waarom het CBP dit vindt. Wellicht omdat de PIA zich richt op meer dan alleen beveiliging.

   Er zijn echter methoden voor risicoanalyse, zoals IRAM van het ISF, die nadrukkelijk een eerste fase Business Impact Analyse (BIA) kennen. Tijdens de BIA worden de betrouw-baarheidseisen bepaald. BIA is dus onderdeel van de risicoanalyse en staat daar niet los van. BIA richt zich op de drie bekende, ook in de Richtsnoeren aangehaalde criteria, beschikbaarheid, integriteit en vertrouwelijkheid. Mijns inziens is er een duidelijke overlap tussen PIA en BIA/Risicoanalyse. Waar het gaat om het voorkomen van dubbel werk, steeds belangrijker in 'lean and mean' ingerichte organisaties, een gemiste kans.

   Voorts ontbreekt in de beschrijving van de risicoanalyse in par. 2.4. aandacht voor kwetsbaarheden c.q. de kwetsbaarheidsanalyse zoals die in veel methoden (IRAM, maar ook CRAMM, A&K-analyse, e.d.) voorkomt. Hierdoor is de analyse niet volledig en kunnen maatregelen gemist worden. Overigens komt de aandacht voor technische kwetsbaarheden wel terug onder de maatregelen (blz. 23 bovenaan).

2. Niet meer hanteerbaar als normenkader
   In Studierapport 3 van de NOREA is een voorzet gedaan van de eisen die worden gesteld aan normenkaders die hanteerbaar zijn in een audit. Eén van de onderkende (meta)normen is eenduidigheid: de mate van precisering en eenduidigheid van formulering. In de richtsnoeren ontbreken normen die aan deze eis voldoen. Zie ook het aparte kader over "normenkaders". Dit wordt niet opgelost door de verwijzing naar beveiligingsstandaarden. De benadering in ISO-27001/2 is daarvoor te grof c.q. biedt teveel keuzemogelijkheden.

3. Loslaten classificatie (rubricering / labelling)
   Classificatie is mijns inziens één van de oudste maatregelen van informatiebeveiliging. Informatie was geheim of was dat niet. Al vanuit de klassieke oudheid zijn maatregelen bekend (zie de historie van versleuteling / encryptie) hoe geheime informatie te beschermen. Aan de classificatie

De Richtsnoeren vormen geen toetsbaar normenkader

hing dan een manier van omgang met de informatie van de klasse vast. Er was dus een nauwe samenhang tussen de classificatie en de te hanteren beveiligingsmaatregelen. De classificatie was dus het gevolg van een (al dan niet verkorte) risicoanalyse. In eerdere versies, zoals AV-23, was classificatie een essentieel onderdeel via de risicoklassen. Het CBP laat de verantwoordelijke nu deze risicoanalyse volledig zelf maken waarbij hij zelf inschattingen moet maken van het belang op basis van zaken als de aard van de gegevens, de hoeveelheid en de context waarbinnen het gebruik plaatsvindt. Hoewel de koppeling aan maatregelen een risico op toepassing van verouderde maatregelen inhoudt, gaf de indeling in risicoklassen duidelijk richting aan de te onderkennen betrouwbaarheidseisen en de indeling daarvan. Deze is nu helaas weggevallen. Dit was ook vooral van belang in situaties van uitbesteding (outsourcing). De aanbestedende partij hoefde enkel AV-23 op te nemen in het programma van eisen en daarbij de risicoklasse aan te geven. De leverancier wist waar hij aan toe was. Nu moet de aanbestedende partij meer moeite doen om de eisen te formuleren. Vervolgens is er een groter risico dat de leverancier daar zijn eigen invulling aan geeft die (door meer focus op de kosten) een lager beveiligingsniveau oplevert, dan de aanbestedende partij voor ogen had.

4. Wederom veroudering
   Het gebruik van standaarden suggereert een grote keuzevrijheid. De maatregelen(doelstellingen) die het CBP noemt, zijn echter ontleend aan de ISO-27002 en wel de 2007 versie. Een zo harde verwijzing naar de 2007 versie kan zorgen voor snelle veroudering: voor ISO-27001 is immers recent de 2013 versie aangebracht met de nodige aanpassingen. Dan mag worden verwacht dat snel een nieuwe versie van ISO-27002 zal uitkomen

5. Ongelukkige verwoording van maatregelen
   Het CBP geeft aan welke maatregelen(doelstellingen) belangrijk worden geacht. Deels gebeurt dit door maatregel(doelstelling)en uit ISO-27002 te verwoorden in eigen termen. Dit is passend waar het gaat om de aandacht te leggen bij persoonsgegevens. Dit kan echter aanleiding geven tot interpretatieverschillen tussen de verschillende bewoordingen en is als zodanig niet handig. In omgevingen met een lager beveiligingsbewustzijn of bij minimalistisch gedrag kan dit leiden tot het selectief toepassen van maatregelen uit ISO-27002 (alleen die maatregelen die men herkent vanuit de Richtsnoeren). Daarnaast zijn bepaalde eigen bewoordingen ongelukkig gekozen. Zo wekt de beschrijving van social engineering tests de indruk dat dit alleen per e-mail of telefoon gebeurt, terwijl ook het verkrijgen van fysieke toegang tot deze tests kan behoren.

Tot slot ontbreekt een eenduidig begrippenkader zodat verschillende termen worden gebruikt zonder dat in alle gevallen duidelijk is of daar hetzelfde of iets anders onder wordt verstaan (zoals software, systemen, toepassingssysteem, informatiesysteem, informatiedienst, subsysteem).

Conclusie

De huidige Richtsnoeren beveiliging van persoonsgegevens doen hun naam recht aan waar het gaat om het leggen van de verbinding tussen de verplichtingen in de Wbp en het vakgebied (informatie)beveiliging. De praktijkvoorbeelden en nadere toelichtingen kunnen zeker voor niet-deskundigen verhelderend werken. De koppeling met de praktijk is voorts gewaarborgd door toepassing van risicoanalyse, de PDCA-cyclus en gebruik van beveiligingsstandaarden.

Ten opzichte van de voorloper AV-23 zijn de Richtsnoeren niet meer te gebruiken als normenkader. Hiervoor ontbreken voldoende eenduidig geformuleerde normen of doelstellingen. Zoals is aangegeven lag hierin echter de valkuil van normen die te zeer gekoppeld zijn aan een bepaalde stand van de techniek en daarmee zorgen dat het normenkader veroudert raakt en zelfs strijdig wordt met de wet. Door zo hard te verwijzen naar de 2007 versie van ISO-27002 zijn de Richtsnoeren al snel achterhaald. Voorts is het mijns inziens jammer dat de indeling in risicoklassen is losgelaten. Deze maakte het mogelijk praktisch aan te sluiten op enerzijds het vastleggen van de betrouwbaarheidseisen (of BIA) als onderdeel van de risicoanalyse, anderzijds gaf deze handreiking voor de invulling van de maatregel classificatie (rubricering). Dit maakte het eenvoudiger om bij uitbesteding afspraken te maken tussen de verantwoordelijke en de bewerker.

Het ontbreken van een eenduidig normenkader betekent dat audits op een andere wijze aangepakt moeten worden. Tot slot laten de Richtsnoeren in conceptueel / theoretisch opzicht een aantal steekjes vallen.

Alternatieve aanpak

Dit artikel brengt nog eens de problematiek naar voren die samenhangt met het hebben van goede normenkaders. Ook in de Diginotar-affaire is deze problematiek nadrukkelijk aan de orde geweest in relatie tot de gehanteerde ETSI-normen. Voorgeschreven toepassing bleek niet garant te staan voor een inhoudelijk valide normenkader. Het is een problematiek die vergelijkbaar is met de (eeuwige) discussie over "principles versus rules based".

In essentie zou je normen willen hebben die geformuleerd zijn als doelstellingen. Op het moment dat je dat doet, ontstaat er behoefte aan verduidelijking. In beveiligingsland betekent dat het concretiseren aan de hand van mogelijke maatregelen. Deze maatregelen zijn echter aan veroudering onderhevig. Voorts kan normering in termen van maatregelen, zoals beschreven in het artikel, ten onrechte non-compliance met de wet- en regelgeving veroorzaken. Dit indien toepassing 'naar de letter' en niet 'naar de geest' plaatsvindt.

De enige mij bekende studie naar eisen aan normenkaders is die zoals uitgevoerd door de NOREA en verwoord in Studierapport nr. 3. Daarin staan ook metanormen verwoord. Een daarvan is de aangehaalde eis van "eenduidigheid". Kijkend naar hoe deze metanormen uit zijn gewerkt in het Studierapport, dan zie je weer rijen van als maatregelen verwoorde normen. De hiervoor aangehaalde problemen blijven dan bestaan.

Beoordeeld tegen deze metanormen vormen de Richtsnoeren zeker geen toetsbaar normenkader. Wel staat een aanpak beschreven die in eerste instantie als proces geaudit kan worden. Grofweg: zijn de betrouwbaarheidseisen vastgesteld op het juiste niveau, zijn deze adequaat meegenomen in de uitvoering van de risicoanalyse, was deze uitvoering ook overigens adequaat zodat een juiste, volledige en consistente set aan beveiligingsmaatregelen is geselecteerd en is deze ook geïmplementeerd. Bij de beoordeling van deze maatregelenset kan men te rade gaan bij de beveiligingsstandaarden. Dan zal men zich moeten realiseren dat deze standaarden een verschillend niveau van detaillering kennen. Het niveau van de Code voor informatiebeveiliging is dan niet voldoende. De Richtlijnen voor de beveiliging van webapplicaties gaan dan een slag dieper. In voorkomend geval zul je uitkomen op de richtlijnen van de leverancier. Het privacy assessment of de privacy audit zal dan moeten vaststellen dat deze slag gemaakt is. Ieder assessment c.q. iedere audit blijft daarmee maatwerk.

In dit verband wijs ik nog graag op een beperking die al bij het uitbrengen van NIvRA-geschrift 58 naar voren werd gebracht. Dit geschrift verscheen naar aanleiding van de komst van de Wet persoonsregistraties en behandelt de problematiek van privacy bescherming en de rol van de accountant. De beperking zit in het volgende. (Financial) audits zijn er op gericht om vast te stellen dat binnen zekere grenzen (betrouwbaarheid, nauwkeurigheid) wordt voldaan aan de normen. Daarbij worden een of enkele fouten geaccepteerd. Probleem met de privacywetgeving is dat fouten een overtreding vormen van de wet. Deze fouten wil en kun je eigenlijk niet toestaan. Geconcludeerd werd dan ook dat onderzoeken naar de permanente werking van de beveiliging van individuele persoonsgegevens niet mogelijk is...

Literatuurlijst

- Wet Bescherming Persoonsgegevens (www.wetten.nl)
- G.W. van Blarkom en drs. J.J. Borking, 'Beveiliging van persoonsgegevens', Achtergrondstudies en Verkenningen nr. 23, Registratiekamer, april 2001 (http://www.cbpweb.nl/downloads_av/av23.pdf)
- CBP, 'Richtsnoeren beveiliging van persoonsgegevens', februari 2013 (http://www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf)
- Rina Steenkamp, Risico's voor betrokkenen centraal in de CBP-Richtsnoeren beveiliging, Informatiebeveiliging – nummer 6, 2013
- NOREA, Studierapport 3 "Raamwerk voor de ontwikkeling normenstelsels en standaarden", december 2002, ISBN-nr. 90-74409-08-3
- Information Security Foundation (ISF), The Information Risk Analysis Methodology (IRAM)
- ACIB, Handboek A&K-analyse
- NIVRA-Geschrift nummer 58, Deel VIII. Privacybescherming; de gevolgen voor organisaties en de rol van de accountant, Kluwer Bedrijfswetenschappen, Deventer, ISBN 90 267 1550 1, januari 1991

INTEGRITY PROTECTED

Integrity is one of the long-standing attributes within the discipline of information security. In this article we take a look at this from a SABSA Business Attributes perspective to discover some of the complexities that lie behind this attribute when applied to data and information. That immediately raises the question of what might be the relationship between 'data' and 'information', since the concept of 'integrity' might mean different things in these two cases. The following table provides the SABSA view of a data / information architecture mapped onto the SABSA layered architecture stack.

Architecture Layer	Type	Explanation
Contextual	Wisdom	Ultimately humans use information to support decision-making. This requires both good knowledge and good judgement. Decisions can be operational (Is it safe to cross the road now?) or tactical (When and where shall I take a holiday?) or strategic (Shall I marry this person?). Good knowledge implies high integrity protection of the information, and also the data on which the information is based.
Conceptual	Knowledge	In order for information to become human knowledge, the human must first understand the language in which the information is written or encoded. Knowledge is information with human interpretation, which may vary from one human to another depending upon their fluency in the language and their semantic understanding.
Logical	Information	Information exhibits high levels of structure in the form of records or sentences. The structure comprises complex combinations of data that now carry human meaning because of the structure. This structure is some form of human readable language.
Physical	Data	Data is pretty raw stuff. In its most raw state it is merely a sequence of binary digits. Even with minimal structure, such as alphanumeric characters, or even words or field syntax definitions in a dictionary, it conveys little meaning to a human.
Component	ICT	Data is generated, captured, processed, used, stored and transported (and perhaps ultimately destroyed) by systems that include people, processes and technology. The 'data lifecycle' is managed by these systems.

The Attributer was recently reviewing a paper that is intended to be a set of policy guidelines for general applicability on the protection of data throughout its entire lifecycle. He encountered the following statement: Data integrity protection must be consistent throughout the data lifecycle, regardless of its location or environment.

To which the Attributer's comment was: Nonsense! Data that begins life as highly secret can later be published. There are numerous examples of such life-cycles: market sensitive data during preparation of company financial results will be published a few weeks later, at which point the data security requirements will change utterly from confidentiality to integrity – what you publish had better be correct – before publication it's work in progress and may contain errors.

Then there was another related statement: The integrity of data must be maintained over its entire lifecycle.

Which received the following comment: This defies the laws of physics. The second law of thermodynamics tells us that entropy tends to increase and that you have to do work to maintain order. That's an awful lot of work that needs to be justified by business case – and not all business cases will need this, so mandating it as a principle is silly. Additionally, the value of data can degrade over time and thus the value of data integrity should not be maintained unless there is a specific business case – the 'old news' has little value, so who cares if it's accurate – unless you're a historical researcher.

Here we have explored only a small fraction of the issues that surround integrity protection, but it already becomes clear that these issues are very complex and require some considerable work effort to define some broadly applicable principles for integrity protection. This demonstrates the value of the SABSA Business Attributes approach, in which the very specific business requirements and business cases can be explored and articulated. One size does not fit all requirements, and so statements of high-level principles must make this clear.

The Attributer

TETHERING ENTERPRISE INTERESTS

Op strategisch niveau is het doel van de informatiebeveiliging en enterprise risk management in het algemeen, volgens dit artikel, het beschermen van de belangen van key stakeholders in de organisatie en de belangen van de organisatie als geheel. Wij als vakgenoten willen derhalve, gezamenlijk aan key stakeholders inzichtelijk maken dat informatiebeveiliging een instrument is waarmee hun strategische belangen te verzekeren zijn. Dit artikel zal een aantal stellingen en definities presenteren met als doel de lezer te ondersteunen bij het strategisch positioneren van de informatiebeveiliging in organisaties.

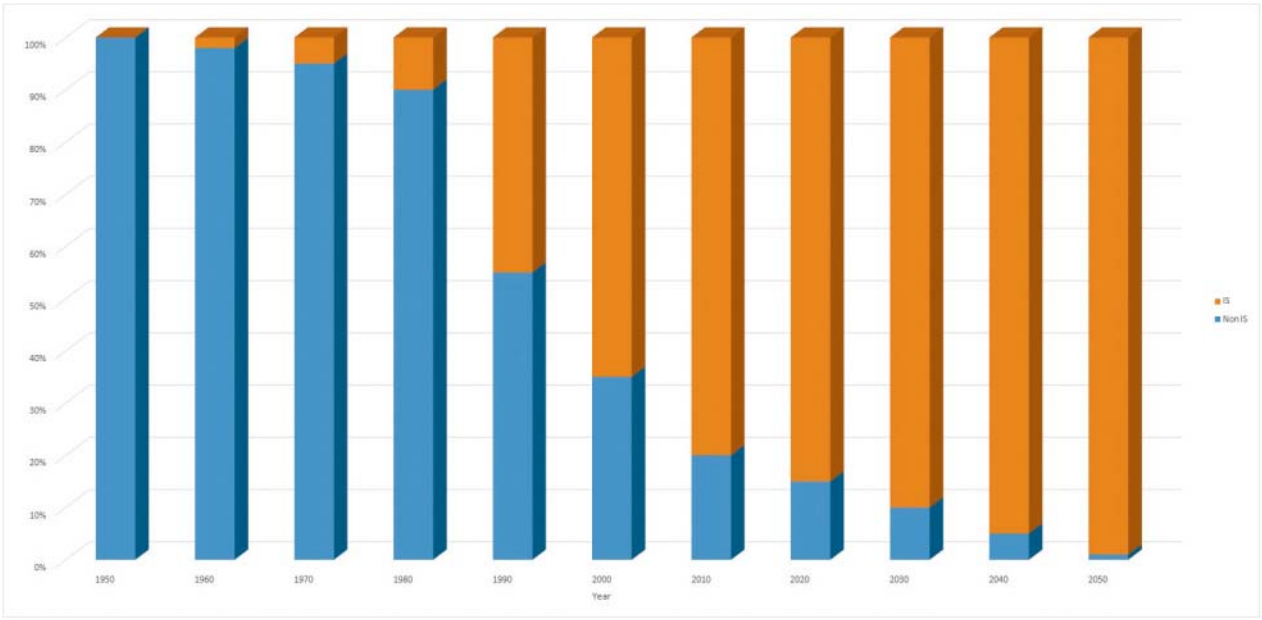
Stelling 1: Know your organisation

Met iedere organisatie gaat in impliciete of expliciete zin een operating model gepaard dat de beoogde samenhang tussen processen, mensen, organisatiestructuren en technologie definieert. Misvattingen over de werking van organisaties vormen een belangrijke obstakel voor het effectief ondersteunen van belangen van organisaties in het algemeen. Het komt nog te vaak voor dat wij als vakgenoten (informatiebeveiligers en operationele risk managers) een vaktechnische blik op organisaties hebben. Regelmatig wordt hierdoor het belang van de organisatie uit het oog verloren, waardoor we partijen in de organisatie met gemeenschappelijke belangen niet altijd herkennen. Onze eerste stelling luidt: **Kennis van de organisatie is een kritische succesfactor.**

Stelling 2: Information security controls are key controls

Als vakgenoten mogen wij getuige zijn van een bijzondere ontwikkeling. Zeventig jaar geleden bestonden er in een organisatie geen IT-controls. Door de steeds verdere

Maurice Gittens CISA werkt als consultant met informatiemodelleren, informatieverwerking, informatiearchitecturen en informatiebeveiliging. Hij is momenteel Business Account Manager bij een Nederlandse Bank. Hij is te bereiken via maurice@gittens.nl



Figuur 1 - Verhouding controls

Op strategisch niveau is een investering in informatiebeveiliging niet anders dan een willekeurige andere investering.

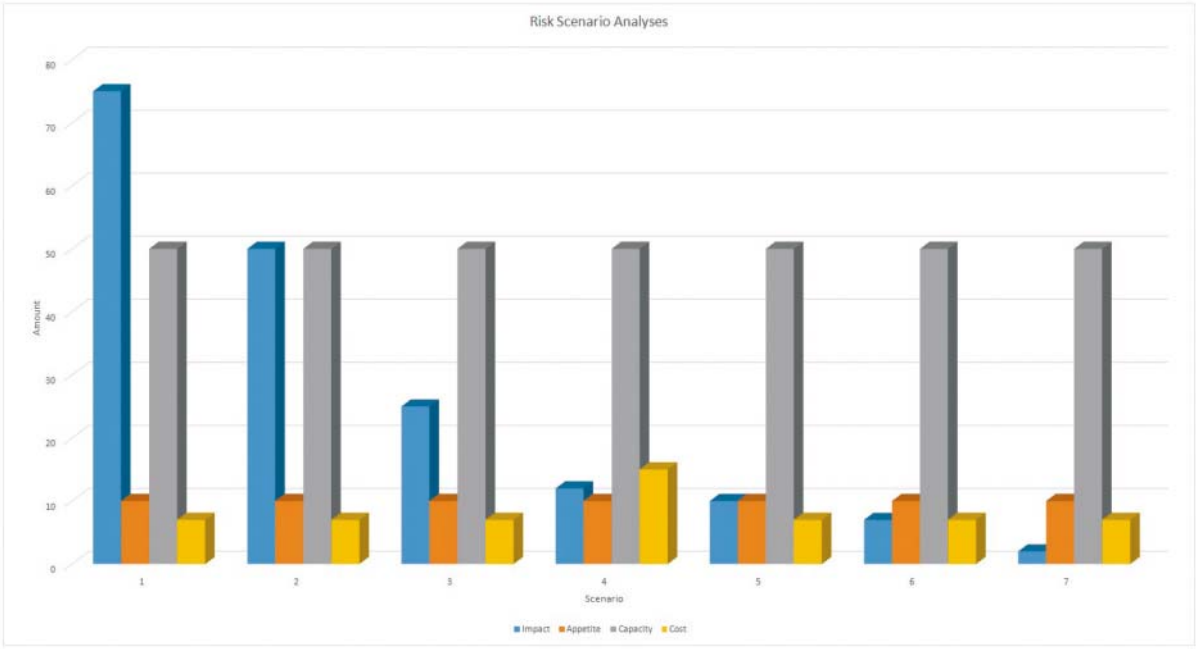
automatisering van de bedrijfsvoering in de afgelopen decenia zijn steeds meer controls in IT-systemen ondergebracht. Qua opzet zijn vele controls niet wezenlijk veranderd, maar qua bestaan, inrichting en werking des te meer. Ik stel: vrijwel alle effectieve controls die een IT afhankelijkheid hebben, zijn direct of indirect afhankelijk van de effectiviteit van de informatiebeveiliging. Figuur 1 toont op basis van fictieve cijfers een trend aan die eenvoudig te herkennen is. Het zet de verhouding tussen controls met een (indirecte) information security afhankelijkheid en controls zonder een information security afhankelijkheid in de tijd tegen elkaar uit.

Laten we stil staan bij de vraag:
Welke controls in een enterprise risk control framework zijn niet direct of indirect afhankelijk van information security controls? Het antwoord op deze vraag lijkt me duidelijk, zeker als we denken aan enabling security capabilities zoals:

- Identity management
- Toegangsbeveiliging op platform- en applicatieniveau
- Integriteitscontrols in financiële administraties en risicomodellen
- Et cetera

Een kernstelling in dit artikel is op basis van het bovenstaande te formuleren als: Information security controls are key controls
Deze stelling zal wat mij betreft steeds vaker gelden, zeker bij financiële instellingen en gelijkaardige organisaties, juist omdat de integriteit, volledigheid en juistheid van bancaire risico-modellen en administraties in hoge mate en in essentiële zin afhankelijk zijn van de effectiviteit van information security controls.

Stelling 3: ITs about the business case
Op strategisch niveau is een investering in informatiebeveiliging niet anders dan een willekeurige andere investering. We zullen met kosten/baten analyses, ROI modellen, et cetera aan beslissers inzichtelijk willen en moeten maken dat een investering zakelijk gezien de moeite waard is. Mijn aanbeveling is om minder de focus te leggen op horror verhalen en juist meer de nadruk te leggen op het feit dat informatiebeveiliging een instrument is waarmee de belangen van het concern, in strategische zin, beschermd en bestendigd kunnen worden. Beschouw eens figuur 2, deze zet in een aantal (fictieve) scenario's impact, appetite, capacity en treatment cost uit tegen een maat voor de jaarlijkse impact op een organisatie.



Figuur 2 - Fictieve scenario's

Een korte omschrijving van de scenario parameters langs de horizontale as:

Concept	Omschrijving.
Impact	De reële schade potentieel.
Appetite	De maximale schade die in de ogen van key stakeholders hoort bij de cost of doing business.
Capacity	De schade die maximaal geleden kan worden zonder dat er onherstelbare schade aan bedrijfsbelangen geschiedt.
Treatment Cost	De kosten van het in place zetten van een risico management regime.

Wie op basis van soortgelijke diagrammen bijvoorbeeld de huidige en gewenste situatie met key stakeholders bespreekt zal in staat zijn om een win-win voor concernbelangen en de belangen van de informatiebeveiliging te verwezenlijken. Dit onderwerp zou samen met ondersteunende diagrammen zelf onderwerp van een volledige artikel kunnen zijn. Voor onze huidige doelstellingen laten we het hierbij.

Stelling 4: Inflexibility is a vulnerability

Een van mijn favoriete aforismen is: Nothing persists like change. De inrichting van een effectief risk control framework zal flexibel moeten zijn. Deze flexibiliteit is strategisch gezien een belangrijke eigenschap. Het is namelijk een gegeven dat alles, inclusief onze eigen inzichten en opvattingen, aan verandering onderhevig is. Evidente voorbeelden zijn:

- de opzet van de organisatie
- de mensen
- de processen
- de technologie
- et cetera.

Dus een belangrijke requirement voor een risk control framework is dat het resulterende risk control regime met relatief weinig kosten aan een veranderende omgeving kan worden aangepast. De controls die het risk control framework belichamen zullen zich aan veranderde capabilities moeten kunnen aanpassen zonder aan effectiviteit in te boeten. Niemand zit namelijk te wachten op controls die afdoen aan de agility van primaire business functies. Inflexibiliteit van een risk control framework draagt, in het algemeen, niet bij aan de doelstellingen van key stakeholders en vormt vanuit de invalshoek die we in dit artikel kiezen een kwetsbaarheid. Het streven is naar effectiviteit en verbeterde flexibiliteit.

Stelling 5: Iedereen beschermt zijn belangen

Ik herhaal: wie draagvlak voor informatiebeveiliging op bestemde niveaus in een organisatie wil creëren en bevorderen, zal zich willen verdiepen in de belangen van verschillende stakeholders in de organisatie. Zij zal zich telkens

willen afvragen: hoe helpt informatiebeveiliging het belang van specifieke stakeholders te verwezenlijken en te bestendigen? Door telkens vanuit het antwoord op deze vraag te denken, is het mogelijk om verschillende stakeholders te bedienen met de capabilities die aansluiten op hun strategische belangen. In het Engels: Stakeholders protect their interests; we need to enable them to do so effectively!

Stelling 6: Via belangen identificeer je kwetsbaarheden
Inzicht krijgen in de kwetsbaarheden die afbreuk doen aan de belangen van key stakeholders geeft inzicht in de assets die in de ogen van een stakeholder bescherming verdienen. Als informatiebeveiligers zetten we informatiebeveiligingscontrols in om deze assets, en hun afgeleiden, te beschermen. Het afstemmen van onze controls op de kwetsbaarheden van key stakeholders is mijn inziens wezenlijk voor de mate waarin deze stakeholders bereid zullen blijken om in deze controls te investeren. Vanuit de informatiebeveiliging, op strategisch niveau gezien, definiëren we de exposure van een stakeholder als de verzameling kwetsbaarheden die afbreuk doen aan de belangen van de betreffende stakeholder. Als beroepsgroep beperken we ons hierbij tot die kwetsbaarheden waarvoor effectieve informatiebeveiligingscontrols bestaan of kunnen bestaan.

Stelling 7: Via belangen identificeer je opportunities
Wie de belangen van key stakeholders in het oog houdt, zal in staat zijn om opportunities te identificeren die stakeholder-belangen ondersteunen. Analoog aan de exposure definiëren we de opportunity palette als de verzameling opportunities die de belangen van een stakeholder avanceren. Er bestaan geen opportunities zonder exposure. In het extreme getrokken zou je kunnen stellen dat opportunity en exposure onderdeel van dezelfde entiteit zijn; elkaars Jing en Jang als het ware.

Het Identificeren van belangen

Stakeholderbelangen hebben in dit artikel een centrale plaats ingenomen. Wat zijn, vanuit informatiebeveiliging of operational risk management gezien, de belangen van key stakeholders en hoe zouden we deze kunnen identificeren? Het is mijn opinie dat naast inzicht in de organisatie, de balans van een bedrijf een instrument is dat goed bruikbaar is. Per slot van rekening geeft het inzicht in de financiële positie van een bedrijf op een gegeven tijdstip en bovendien geeft het inzicht in de stakeholders die achter de rekeningen schuil gaan. Dit is een toepassing van het credo: Follow the Money!

Wat is een Tether?

Ik hoorde voor het eerst het woord tether toen ik op een data governance project in London een collega de uitdrukking "I'm at the end of my tether" hoorde gebruiken. Op mijn vraag naar verduidelijking volgde een interessante discussie die ook inbreng van andere collega's genoot. Met verschillende idiomen hielpen mijn collega's mij aan een beter begrip van het woord. De link met operational risk management was snel gemaakt toen een collega deelde dat hij de term kende in de context van een tethered vs een untethered jailbreak. Volgens het woordenboek is een letterlijke vertaling voor het woord tether een touw. Niet alleen een touw in de letterlijke zin, maar juist ook in overdrachtelijke zin. Het is in deze zin dat het woord in de titel van dit artikel gebruikt is. Naast het gebruik van het woord als zelfstandig naamwoord wordt het ook als bijvoeglijk naamwoord gebruikt, bijvoorbeeld "a tethered jailbreak". Het gerundium van het woord is tethering. Voor de doelstellingen van dit artikel definiëren we tether als: een instrument waarmee we de belangen van een stakeholder kunnen verzekeren. Of u het van mij wilt aannemen of niet; terwijl ik de bovenstaande definitie noteer, ontdek ik dat een nederlandse vertaling voor een tether een (ver)zekering zou kunnen zijn. Een verzekering in de zin van het tijdens een storm op zee spullen zekeren om te voorkomen dat ze wegwaaien. Concepten die we met tethers kunnen verzekeren zijn bijvoorbeeld: interests, exposures, risks & opportunities. We kunnen, bijvoorbeeld, ook spreken over untethered interests en tethered opportunities.

Samenvatting

In dit artikel zijn via 7 stellingen stakeholderbelangen centraal gesteld als ingang tot key stakeholders in een organisatie. De boodschap is eenvoudig: Informatiebeveiliging is, in strategische zin, een instrument waarmee we stakeholder belangen kunnen verzekeren. Onze uitdaging is om bij de key stakeholder over te brengen dat we over de kennis en kunde beschikken die passend hun belangen zou kunnen beschermen en avanceren. **It is all about tethering enterprise interests.**

Hans Kompanje. Hans is Technical Consultant bij KPN Consulting. Hij is te bereiken via hans.kompanje@kpn.com

BEVEILIGING IS NIET ALLEEN EEN ZAAK VAN DE IT-AFDELING

Hoe als organisatie hiermee om te gaan

Beveiliging is een hot issue voor organisaties wereldwijd. Traditioneel had een organisatie een eigen netwerk, dat afgescheiden was van de rest van de wereld. Alleen door fysiek op de omgeving in te loggen was het mogelijk om de data die hier beschikbaar was te benaderen. Tegenwoordig is alles met elkaar verbonden. Door Het Nieuwe Werken, bijvoorbeeld, benaderen medewerkers hun data vanaf een willekeurige locatie vanaf een willekeurig device. Natuurlijk is het geweldig als je met je smartphone, tablet of laptop altijd overal kunt werken en je documenten kunt printen op elke beschikbare printer. Het management moet bewust gemaakt worden van de risico's die dit alles met zich meebrengt.

Een aantal risico's zijn verlies of diefstal van bedrijfsdata - die op verschillende devices staan en daardoor toegankelijk zijn, datalekken via ongeautoriseerde draadloze verbindingen met het bedrijfsnetwerk en inbraak op het bedrijfsnetwerk door misbruik van kwetsbaarheden in dat netwerk. Dit betekent dat er veel aandacht voor beveiliging moet zijn. Er komen steeds meer mogelijkheden om devices te beveiligen en scantools die kwetsbaarheden ontdekken en hier oplossingen voor bieden. Dit brengt ook steeds meer werk met zich mee. Doordat tegenwoordig alles met elkaar verbonden wordt en via internet bijna alles te benaderen is, wordt beveiliging van de omgeving steeds belangrijker. Wat en wie laat je binnen en wat en wie niet? Welke beveiligingsmethode gebruik je en hoe bepaal je waar een medewerker wel en waar een medewerker niet bij mag? En is dit nu een taak van de beheerder of zijn er meer mensen verantwoordelijk voor de beveiliging van de organisatie? Wat komt kijken bij het beveiligen van de bedrijfsdata en devices?

Waarom beveiligen?

Organisaties maken gebruik van diverse componenten in de IT-infrastructuur zoals servers, werkplekken en netwerkcomponenten om de dagelijkse werkzaamheden uit te kunnen voeren. Iedere organisatie heeft deze componenten. Men denkt vaak dat de gaten zitten in de desktops en servers, maar alle componenten bevatten helaas fouten, zogenaamde bugs of veiligheidsrisico's. Managers zijn zich hier vaak niet van

bewust. Door deze kwetsbaarheden is het mogelijk om in te breken op een systeem en hier misbruik van te maken. Bij een grote organisatie waar ik een project heb uitgevoerd is dit ook daadwerkelijk gebeurd. Er heeft een hack plaatsgevonden. Naar aanleiding van deze hack is besloten om de beveiliging aan te scherpen en maatregelen te nemen om te zorgen dat dit niet meer voorkomt. Er is een groot project gedefinieerd, dat alle componenten gaat scannen op mogelijke beveiligingslekken. Deze lekken worden gerapporteerd aan de verantwoordelijke managers en de beheerders die dit gaan oplossen.

Wat is nodig om de beveiligingsstatus te controleren?

Om te detecteren welke beveiligingslekken aanwezig zijn op de verschillende systemen is er speciale software die omgevingen scant en lekken rapporteert. Tevens maakt deze software aanbevelingen hoe dit voorkomen kan worden. Dit kan een patch zijn, maar ook een softwareinstelling of een verwijzing naar een beleidsrichtlijn binnen de organisatie. Het project voerde deze scans uit en maakte werkpakketten die worden uitgezet naar de beheerders van de verschillende systemen. Theoretisch klinkt dit plausibel om werkpakketten bij beheer uit te zetten en hun de lekken te laten dichten, echter er komt veel meer bij kijken dan alleen rapportages naar beheerders te sturen en vervolgens verwachten dat dit op korte termijn is opgelost. Een belangrijke voorwaarde voor succesvolle uitvoering is goed inzichtelijk te hebben hoe de omgeving is opgebouwd en gedocumenteerd. Vragen die in ieder geval beantwoord moeten worden:

- Welke systemen zijn binnen de organisatie aanwezig?
- Wie is hiervoor verantwoordelijk?
- Wie is de beheerder van dit systeem?
- Staan de systemen in een (centrale) CMDB?
- Is er een proces afgesproken voor Patch Management?
- Is er een proces afgesproken voor Change Management?
- Is er een proces afgesproken voor Lifecycle Management?

Alle techniek komt bij elkaar in Lifecycle Management. Het is de totale levenscyclus van een device, van ontwikkeling, testen, productie tot uitfaseren. In elk van deze stadia is beveiliging een belangrijk onderdeel. Wat gebeurt er bij elke fase, wordt hier rekening gehouden met beveiliging? Is dit beschreven, onderdeel van het proces? Bijvoorbeeld bij het invoeren of uitfaseren, wordt dit doorgegeven in de CMDB, Patch Management en rapportages? In een kleine organisatie is dit meestal gemakkelijk, hier is een persoon of afdeling verantwoordelijk. Bij grotere bedrijven is dit complexer, want dan zijn er meerdere datacenters, locaties en samengevoegde organisatieonderdelen betrokken. Wat staat er in een datacenter, wat voor type devices zijn dit en is dit alles? Wie is de beheerder van het systeem, wat zijn de IP-ranges van deze VLAN's en welke componenten bevat dit VLAN? Daarnaast wil je graag weten waar de grootste risico's zitten. Een systeem dat rechtstreeks aan het internet hangt, heeft een hogere prioriteit dan een systeem dat op een afgescheiden segment achter meerdere firewalls staat. Een goede CMDB, waarin actuele gegevens van alle systemen staan én wijzigingen worden bijgewerkt in de Change Management en Lifcycle Management systemen, is essentieel. Daarnaast moet gekeken worden naar de opbouw van een omgeving. Is deze virtueel, dan wordt gebruik gemaakt van zogenaamde server templates. Het is gemakkelijk om snel een nieuwe server uit te rollen met behulp van zo'n template. Dit betekent dat als er een beveiligingslek in de template zit, dit lek ook bij elke nieuwe instantie van dat template in de virtuele machine aanwezig is.

Wat is er nodig om deze problemen op te lossen?
Als eerste moet worden bepaald wat het gewenste beveiligingsniveau moet zijn. Dit kan een beheerder niet beslissen. Hij kan hierin hooguit adviseren. Installeer ook de laatste patches en updates. Maar veel van deze updates of instellingen verwijzen naar organisatiebreed beleid. Vanuit het management zal moeten worden aangegeven hoe de omgeving beveiligd moet worden.

Dilemma voor het management

Gaat men voor gebruiksgemak of voor optimale beveiliging? Zijn er richtlijnen of beleid binnen de organisatie die beschrijven waaraan voldaan moet worden? Denk hierbij aan bijvoorbeeld certificaten, gebruik van bring your own device (BYOD), (secure) printing, tokens en websites.

- Moet een gebruiker automatisch overal ingelogd worden, of wordt er voor elke applicatie een eigen authenticatie gebruikt?
- Staat het management toe dat er met zelf meegebrachte apparatuur verbinding wordt gemaakt met het (draadloze) netwerk?
- Mogen personen verbinding maken met een (draadloos) netwerk en gebruik maken van printerfunctionaliteit?

Zeker met BYOD is het wenselijk dat alle gebruikte devices beveiligd worden. Natuurlijk kan de beheerafdeling hier beveiliging voor inrichten, bijvoorbeeld een met een MDM (mobile device management) oplossing zoals MobileIron, of centrale beveiliging van de devices. Dit is niet alleen een beheerbeslissing, maar tevens een managementbeslissing. Om dit goed te regelen is op alle lagen van de organisatie commitment wenselijk. De directie maakt het beleid en bepaalt wat er wel en niet toegestaan wordt. De beheerafdeling zorgt

voor de inrichting hiervan. Op die manier maken medewerkers op een verantwoorde manier gebruik van de geboden functionaliteit. Het management zou hier richtlijnen of een gedragscode voor kunnen opstellen die medewerkers bij indiensttreding moeten ondertekenen en doornemen.

Uitvoeren van beheerwerkzaamheden

Beheerders voeren hun dagelijkse werkzaamheden uit en worden volgepland met werkzaamheden. De scans die moeten worden uitgevoerd houden in dat zij extra werkzaamheden krijgen. Nu kun je zeggen dat deze werkzaamheden hier ook bij horen, maar nog niet zijn uitgevoerd. Achterstallig onderhoud dus. Zolang er vanuit het management geen druk wordt uitgevoerd op de voortgang zal een beheerder hier weinig prioriteit aan geven. Vanuit de organisatie worden veel verzoeken neergelegd bij beheer. Het patchen houdt in dat er goed gekeken moet worden of en wanneer dit mogelijk is en of dit impact heeft op business applicaties. Vaak wordt door business applicaties bepaald of patchen wel of geen prioriteit heeft. Het draait, dus laten draaien. Het management heeft vaak geen idee van de status van de beveiliging. Men gaat ervan uit dat dit op orde is. Hoewel ze niet geïnteresseerd zijn in details, is het zaak om vanuit het management hier gericht op te sturen. Dit is te realiseren door het management bewust te maken van de risico's die het niet goed beveiligen van de omgeving inhoudt. Er zijn tegenwoordig veel mogelijkheden om dit inzichtelijk te maken. Een voorbeeld is om een veiligheidsscan uit te laten voeren door een externe partij en de risico's inzichtelijk te maken. Wat kan iemand van buitenaf en wat voor business impact heeft dat? Is het mogelijk om de omgeving down te brengen, data te wijzigen of bedrijfsdata te stelen?

Wat valt er allemaal te beveiligen?

Een aanname is dat als we een firewall hebben, we beschermd zijn tegen de boze buitenwereld. Maar lang niet altijd wordt een beveiligingslek via een externe locatie uitgevoerd. Tegenwoordig is een wifi-netwerk in een kantoorpand heel normaal. De beheerafdeling kan alles helemaal dichtzetten, maar dit komt de gewenste laagdrempeligheid niet ten goede. Vanuit het management is dus een visie gewenst. Waar kiest men voor, gemak of beveiliging en hoever ga je hier in? Medewerkers worden echter steeds flexibeler, Het Nieuwe Werken wordt geïntroduceerd, men werkt vanaf een willekeurig device en maakt verbinding met het bedrijfsnetwerk via een (beveiligde) verbinding. De tijd dat een beheerder bepaalde wat er werd gebruikt, is voorbij.

Niet alleen beheerders, maar ook management en medewerkers

Er moet beleid gemaakt worden met betrekking tot security. Men moet aangeven waar prioriteit aan gegeven wordt en wat wenselijk is binnen het organisatie. Is men bewust van de risico's om bepaalde zaken open te zetten of beschikbaar te maken voor medewerkers? Hiervoor is overleg nodig tussen de directie die het uiteindelijke beleid bepaalt en goedkeurt en de technische achterban. Afhankelijk van de grootte van een organisatie kan dit door een persoon worden uitgevoerd of door een hele afdeling. Stel een security officer aan die verantwoordelijk is voor de beveiliging van het bedrijf of bij

grotere bedrijven een security afdeling die namens het bedrijf de beveiliging en het beleid hieromtrent vastlegt en controleert. Het is dan echter wel zaak om dit binnen het bedrijf kenbaar te maken. Men moet weten dat er een afdeling is die het beleid en de richtlijnen met betrekking tot beveiliging maakt én het moet duidelijk zijn wat deze inhouden. Het beleid en de richtlijnen dienen op regelmatige basis te worden bijgesteld en getoetst op haalbaarheid. Veel bedrijven hebben wel beleid, maar naleving of toetsing van dat beleid blijft vaak achterwege.

Beveiligingsstandaarden en -richtlijnen

Er zijn veel (internationale) standaarden beschikbaar zoals bijvoorbeeld de CIS standaarden die beschrijven hoe de beveiliging van de verschillende systemen moeten worden ingericht. Het is wenselijk om zoveel mogelijk te voldoen aan deze standaarden. Alleen roepen heeft echter geen zin. Je kunt vertellen dat de bedrijfsvoering compliant moet zijn aan ISO 27002 of dat de software een CIS (Center for Internet Security) certificatie moet hebben. Deze standaarden zijn echter geen harde checklists. Het zijn richtlijnen en niet regels die één op één door te voeren zijn. Elk bedrijf is anders en heeft andere wensen. De bepalingen uit de standaard moeten worden aangepast naar werkbare oplossingen binnen een bedrijf. Een security afdeling zou dit moeten oppakken en aan de hand van deze standaarden richtlijnen moeten uitzetten binnen de organisatie. Deze richtlijnen moeten door het hogere management worden vertaald naar beleid en door de beheerders worden uitgevoerd met behulp van security policies en templates. De security afdeling bewaakt of er wordt voldaan aan het beleid en controleert de implementatie door beheer. De richtlijnen moeten vanuit het hogere management worden gedefinieerd. Zij bepalen het beleid, de overige afdelingen voeren dit uit. Indien er geen beleid is gedefinieerd, zal elke beheerder of afdeling zijn eigen standaard gaan bepalen. Dit brengt risico's met zich mee, aangezien niet iedereen op dezelfde manier over beveiliging denkt en niet iedereen dagelijks hiermee bezig is. Als het van bovenaf wordt opgelegd en wordt gecontroleerd door de security afdeling, zal dit leiden tot een verhoogd beveiligingsniveau.

Uitvoeren van richtlijnen

Het management geeft de richting aan, die via beleid wordt verspreidt binnen de organisatie. De beheerders voeren deze richtlijnen uit en de security afdeling controleert dit.
Tenslotte de medewerkers. Ook zij zijn verantwoordelijk. Zij moeten op de hoogte worden gebracht van het aanwezig zijn van security beleid, zodat ze weten dat veiligheid een belangrijke zaak is. Bewustwording helpt hierbij. Het management en directie moeten hierop gaan sturen. Medewerkers gebruiken verschillende apparatuur en zij maken en bewerken de bedrijfsdata. Zij maken met hun laptops, smartphones en tablets gebruik van deze functionaliteit. Ook hier ligt een verantwoordelijkheid. Ze dienen te zorgen dat deze devices geen bedrijfsdata bevatten, tenzij deze ge-encrypt zijn. Indien zij hier niet verantwoordelijk mee omgaan, kan dit grote impact hebben op de veiligheid. Dit kan duidelijk gemaakt worden door de medewerkers een bewustwordingstraining te geven met betrekking tot veiligheid en de risico's die zij en de organisatie lopen. De apparatuur die ze gebruiken moet beveiligd zijn. Indien dit desktops of laptops zijn die door de werkgever worden verstrekt, kan dit centraal worden geregeld. Maar wanneer ze niet op een werkplek werken die beheerd wordt door de IT-afdeling, is een medewerker zelf verantwoordelijk. Zeker bij het toelaten van BYOD is het wenselijk dat deze apparaten veilig zijn. Zorg voor een up-to-date versie van het systeem, installeer mogelijke updates en zorg voor een ge-encrypte data-opslag indien gebruik wordt gemaakt van lokale opslag. Daarnaast is het wenselijk om medewerkers te attenderen op de fysieke veiligheid binnen een kantoorpand. Wordt er gewerkt met toegangscontrole, kan iedereen zomaar naar binnen of buiten lopen met hardware? Is er een pasje waaraan je een medewerker of bezoeker herkent?

Allemaal veilig

Natuurlijk is de beheerder zich bewust van de noodzakelijkheid van het beveiligen van de omgeving en wordt hij hierop aangesproken, maar dit is zinloos als hij dit alleen moet doen. Iedereen van hoog tot laag moet zich bewust zijn van de noodzaak tot het veilig omgaan met de apparatuur en het maken én volgen van het beveiligingsbeleid van de organisatie. Bij het organisatiebreed doorvoeren van dit beleid zal de omgeving een stuk veiliger zijn.

Wat kun je doen?

Het beveiligen van de omgeving is een zaak van iedereen. Het is een onderdeel dat vaak wordt vergeten maar essentieel is in de huidige tijd van het internet. Maak ook iedereen hiervan bewust. Wat zijn de risico's en consequenties als er data door onbevoegden worden benaderd en wat kunnen ze ermee? Wat kosten deze risico's de organisatie? Als er geen richtlijnen zijn, vraag hier dan om bij het management en maak beveiliging een basisingrediënt van de IT-infrastructuur. Dit geldt zowel technisch als functioneel. Denk niet dat het voor je wordt geregeld, uiteindelijk is iedereen verantwoordelijk voor de beveiliging.

VERSLAG

SECURITY CAFÉ

INLICHTINGEN EN ONZE PRIVACY

Nederland wil opheldering over het mogelijk verzamelen van internetgegevens door Amerikaanse veiligheidsdiensten. Het zusterbedrijf van Belgacom blijkt twee jaar lang bespioneerd te zijn door de Britse geheime dienst (GCHQ) en de mobiele telefoon van Angela Merkel blijkt afgeluisterd te worden door de Amerikanen in Duitsland.

Vier maal per jaar organiseert Trust in People het Security Café. De editie van 19 november 2013, werd bij Schuberg Philis te Schiphol-Rijk georganiseerd. In het expertpanel Alexander Blom, CEO van Budget Phone Company en bestuurslid Internet Society Nederland. Ronald Huijgens van Unisys. Erik de Jong als cybercrime lead van FOX-IT en Ricky Gevers als IT-forensic specialist van Digital Investigation. Hier volgt een impressie van de discussie aangevuld met onthullingen in het NRC over het NSA-Dossier.

Om maar met de deur in huis te vallen met de eerste vraag: Hoe kan een inlichtingendienst twee jaar lang spioneren zonder dat een telecomprovider dat door heeft en er ook geen andere alarmbellen afgaan? En als ze dan toch ontdekt worden, hoe komt het dan dat het te traceren is naar de Britse geheime dienst? Allereerst moet je van goeden huize komen om zo'n lek te ontdekken, omdat top-hackers aan de andere kant echt wel weten wat ze doen. Echter, soms worden er kleine 'foutjes' gemaakt die de identiteit van de aanvaller toch blootleggen, alsdus IT-forensic specialist Ricky Gevers. Niettemin hebben de documenten van Snowden geholpen bij het vaststellen wie de ongenode gast was, alsdus Erik de Jong.

Hoezo kan de Britse GCHQ zomaar een commercieel Belgisch bedrijf bespioneren? Er zijn toch wel wettelijke regels voor? De wereld van 'Intel' en 'diplomatie/politiek' zijn ver van elkaar verwijderd, aldus Erik de Jong. Dat is wat de huidige situatie zo gênant maakt voor veel partijen (en niet alleen de daders). Spionage is een 'geaccepteerd' middel van alle tijden, het grote verschil is hier wel de mate waarin dat wordt gedaan in deze gevallen. Het is een interessant vraagstuk, in welke mate spionage acceptabel is. Hoeveel kost het en wat levert het eigenlijk op? Aangezien elk land op dit vlak zijn eigen spelregels kan maken. Je moet jezelf afvragen of overheden boven de wet staan en de 'privacy' mogen ontnemen zonder gegronde reden.

Het lijkt alsof buitenlandse overheden gegevens opvragen/vastleggen over Nederlanders, aldus Alexander Blom. Niemand lijkt verantwoordelijk te zijn of inzicht te kunnen geven in wat er precies gebeurt. Hier moet de rechter kritisch naar kijken. Daarom steunt o.a. Internet Society Nederland het initiatief om minister Plasterk aan de klagen voor witwassen van informatie over Nederlanders. De honger naar data is niet te stillen bij inlichtingendiensten.

Gerco Kanbier is directeur van Trust in People – the information protection company.

Hij is te bereiken via gerco.kanbier@trustinpeople.com

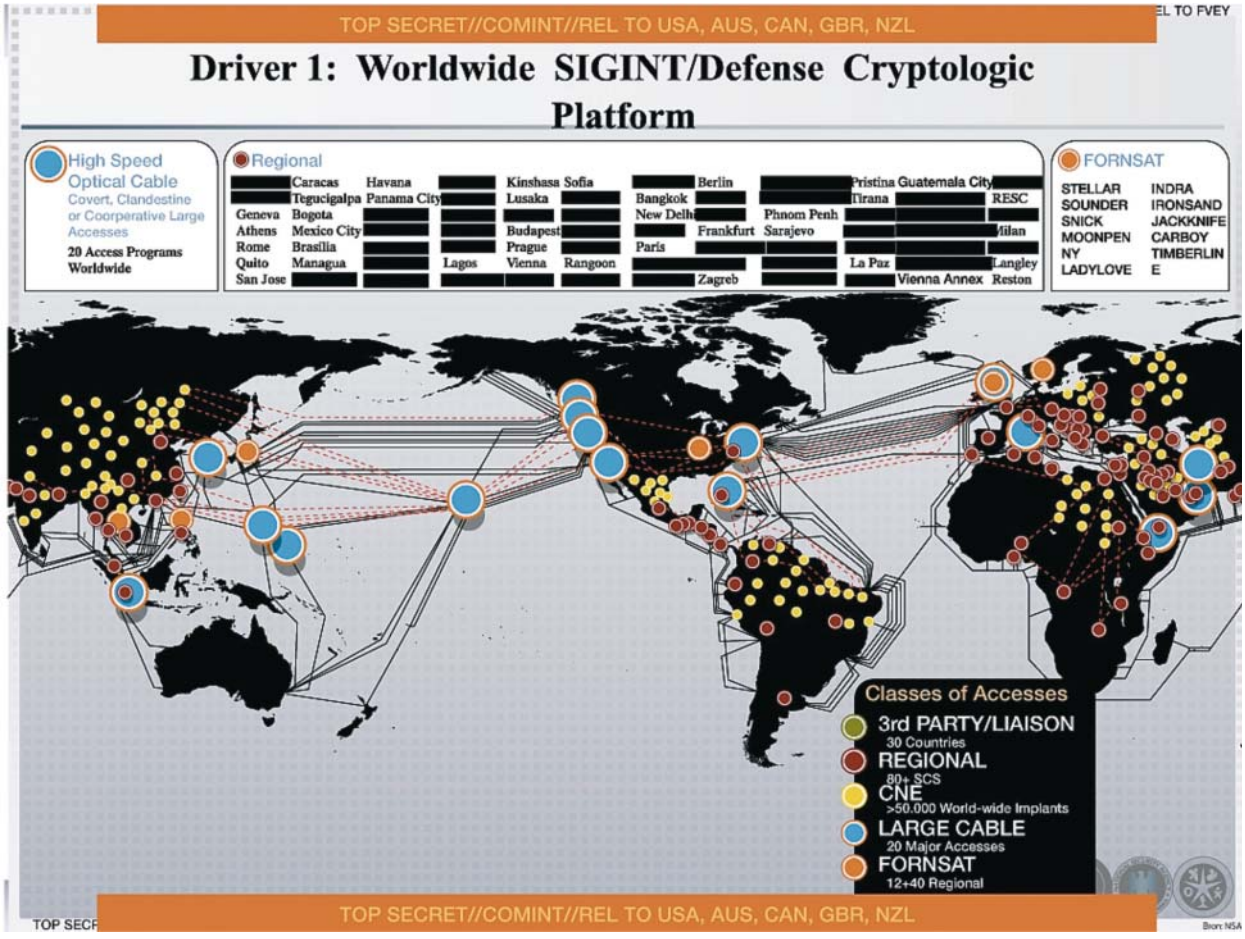
"Opinie over NRC onthullingen"

Dit Security Cafe viel nog net vóór de onthullingen van de NRC over het NSA Dossier, dat gebaseerd is op de documenten van Snowden. De 'opheldering' die minister Plasterk heeft gekregen van de Amerikaanse overheid, is dat er meta-gegevens zijn vastgelegd van 1,8 miljoen telefoongesprekken per maand. Er is in de media heel weinig over bekend of dit Nederlanders zijn die naar Amerika hebben gebeld, of dat dit de top van het Nederlandse bedrijfsleven is, of alleen mogelijke terroristen. Ik heb zelf even gekeken hoeveel ik bel per maand. Dat komt neer op grofweg 300-500 gesprekken en zou impliceren dat metagegevens van zo'n 4 tot 10.000 Nederlanders zijn vastgelegd door de NSA. Op zeer beperke schaal dus en dan alleen nog maar de metagegevens. Dan is vervolgens de vraag: Geeft Nederland deze informatie over telefoongesprekken of opereren de Amerikanen op eigen houtje? Gezien de vraag over opheldering van minister Plasterk, vermoed ik dat laatste. Danwel is het een slechte poging om de samenwerking tussen inlichtingendiensten te verhullen. Op zaterdag 23 november 2013 stond in het NRC dat de Amerikaanse inlichtingendienst NSA meer dan 50.000 computernetwerken heeft gehackt en sinds 1948 Nederland bespioneert.

In dezelfde krant staat de oprichting van het Joint Sigint Cyber Unit in 2014, een samenwerkingsverband tussen de MIVD en AIVD om actief te monitoren in cyberspace. Nu is het volgens de Wet op de Inlichten- en Veiligheidsdiensten verboden om data ongericht te analyseren van kabelgebonden-informatie. Let op, analyseren is volgens de wet iets anders dan verzamelen. Het project met de naam Argo II is bedoeld om vanaf 2014 'informatie uit communicatiemiddelen te verwerken tot inlichtingen', schreef minister Plasterk van Binnenlandse Zaken deze zomer aan de Tweede Kamer. Het systeem zal waarschijnlijk worden gebouwd door het Israëlische Nice Systems, gespecialiseerd in surveillance- en afluistersoftware, aldus een artikel in de Volkskrant. Volgens de technologiewebsite Tweakers kan dit systeem landelijk data onderscheppen, monitoren, analyseren en opslaan, en automatisch waarschuwen bij verdachte patronen. Wij Nederlanders zijn verontwaardigd dat we bespioneerd worden door onze bondgenoten, maar toch gaat Nederland nu de wet aanpassen om de burgers beter te beschermen door ongericht informatie over medelanders vast te leggen. Met welk doel? Gaat de JSCU (AIVD+MIVD) de NSA, GHCQ en de Mossad een koekje van eigen deeg geven door alle wereldburgers te bespioneren?

Wat mij ook opvalt aan deze kaart is het ontbrekende gedeelte: namelijk de 30 landen die als liaison samenwerken, waaronder Nederland. Hoe werkt Nederland dan samen met de NSA? Is dat, net zoals bij dat zusterbedrijf van Belagcom in Belgie, specifiek met één bedrijf die 'stiekem' informatie levert en daarom uit de NRC-publicatie is weggelaten? Dat kabeltje voor een aftakking naar een inlichtingendienst ga je niet vinden met een parlementair onderzoek. Hier heb je voorkennis van een 'insider' nodig, zoals Snowden. Met alle huidige publicaties rond dit onderwerp, wordt het onwaarschijnlijk dat er officieel gebruik wordt gemaakt van de aftapverplichting die alle telefonie- en internet bedrijven hebben.

Nu werden in het NRC Google, LinkedIn en Facebook ook genoemd als bronnen waar de NSA onbeperkt toegang toe zou hebben. Deze bedrijven zijn aangesloten bij het Safe Harbour convenant, waarin de verschillen in wetgeving tussen EU en de VS op gebied van Privacy en de Data Protection Act worden 'gerepareerd'. Dit houdt in dat Google, Facebook of LinkedIn jou als klant netjes horen te melden wanneer de NSA jouw gegevens heeft opgevraagd. Voor zover ik uit diverse media begreep, wordt er op zeer beperkte schaal klantdata opgevraagd o.b.v. een officiële verdenking. Echter, ik heb het vermoeden dat de NSA zich niet aan stoort officiële verdenkingen. Vanwege het staatsbelang kan de NSA gewoon meta-gegevens verzamelen op andere toegangspunten tot het internet (op tier 1 niveau). Op deze punten worden metagegevens van telefoon, e-mail, locaties en bankoverschrijvingen ontsleuteld en verzameld. Dit alles met als doel terrorismebestrijding. Of is kennis toch macht, die we ook mogen gebruiken voor politieke en commerciele doeleinden? Dit laatste is een glijdende schaal en ligt in dezelfde categorie als voorkennis van koersgevoelige informatie. Doelbinding en streng toezicht zijn een eerste vereiste. Ik verwacht dat de toezichthouders ook in deze branche de honger naar kennis nog moeten gaan beteugelen.



Hoe kan een inlichtingendienst spioneren zonder dat een telecomprovider dat door heeft?

Tot slot hadden we het in het Security Café over die politieke rel rond het afluisteren van de mobiele telefoon van Angela Merkel. Ronald Prins van Fox-IT had in Pauw en Witteman een cryptotelefoon meegebracht naar de uitzending. Zo'n telefoon is natuurlijk een oplossing, maar dan kun je niet voorkomen dat je privé-telefoontjes onderschept worden, daar beide partijen zo'n telefoon nodig hebben. Volgens Ronald Huijgens is dit ook anders op te lossen. Unisys heeft namelijk voor het ministerie van Defensie in Amerika (Department of Defence) technologie ontwikkeld die onzichtbaar is in alle communicatiekanalen (internet, WAN, wireless, 3G, 4G en satelliet) zolang het maar 'packet- switched' is. VoIP verkeer via Skype is dus prima te beveiligen. Deze beveiliging werkt echter niet zodra het circuit-switched is, zoals het geval is bij traditionele telefonie. Daarom blijft het mogelijk dat met de juiste apparatuur (zoals een mobiele zendmast op naburige ambassade) makkelijk een man-in-de-middle attack op te zetten. Alle telefoontjes in een bepaalde straal zoeken namelijk het sterkste signaal van de dichtstbijzijnde mast. Als die mast van een derde partij is, kun je alle gesprekken in een bepaalde straal opvangen en meeluisteren zonder dat men het doorheeft.

Aan het einde van de panelsessie, werd ik door een oud-MIVD-er aangesproken opdat wij wel erg naïef zijn als security professionals. Nu zijn inlichtingendiensten een wereld waar informatiebeveiliging professionals zich niet dagelijks begeven. Maar voor de maatschappelijk discussie was dit café wel een wake-up call.

Links
Security Cafe: http://www.trustinpeople.com/security-cafe

Verantwoorde onthullingen #4

"I HACKED KPN, AND ALL I GOT WAS THIS LOUSY T-SHIRT."

@stevenketelaar, @bl4sty en de 10 miljoen modems (2013)

Het jaar is net gewisseld als KPN een voorzichtig e-mailtje binnenkrijgt: "We hebben iets gevonden, maar zijn bang dat jullie ons oppakken". Het is versleuteld en verzonden vanaf een generiek e-mail adres. Menig helpdesk zou hier wellicht niet op reageren, maar wel het KPN Cert Team. De melding komt terecht bij Security Officer Martijn van de Heide. Hij stelt de hackers gerust dat ze niet direct worden opgepakt, garandeert hun anonimiteit en nodigt hen uit bij KPN hun verhaal te doen.

In een besloten setting laten ze zien hoe ze het modem van KPN kunnen hacken en al het verkeer afluisteren. Maar ook hoe het lek gedicht kan worden. Het blijkt te gaan om de Zyxel, die wereldwijd door tientallen miljoenen mensen wordt gebruikt. KPN neemt diezelfde dag contact op met de fabrikant en geeft hun een termijn, want de jongens willen begin april hun bevindingen presenteren op Hack in the Box. KPN kan gelukkig de modems op afstand updaten via hun management interface en zorgt ervoor dat ze allemaal voor eind maart gereset zijn. De gebruikers hebben als het goed is niets gemerkt.

Als ik Martijn spreek op het KPN kantoor in Den Haag is er taart voor iedereen. Zijn team is derde geworden bij de Cyberlympics, een jaarlijkse hack competitie in Las Vegas, waar Nederland altijd goed is vertegenwoordigd. Hier dus een groep mensen die begrijpen hoe hackers denken. Van de Heide spreekt dan ook met veel respect over de hackers. Hij begrijpt hun voorzichtigheid ook wel. Toen hij 6 jaar geleden voor het eerst een dergelijke melding binnenkreeg, kwam direct de juridische afdeling in actie. Die wilde de identiteit van de hackers weten en een zaak beginnen. Zijn afdeling heeft toen hard moeten strijden om de melders te beschermen. Gaandeweg ontwikkelden ze een Responsible Disclosure beleid en krijgen ze gemiddeld een melding per week die binnen een dag wordt afgehandeld. En de twee modem hackers, die hebben nu een leuke video namens het KPN Guest Hacker Program [1].

Het blijkt te gaan om @stevenketelaar en @bl4sty – ook wel Peter Geissler. Als ik Peter spreek hoor ik een bekend verhaal: school niet interessant, maar uitermate nieuwsgierig, autodidact en probeert van alles uit om te kijken hoe iets werkt. En zo kwamen hij en Steven er bij toeval achter dat ze bij hun modem een hulppagina konden opvragen en daar tekst konden invoeren. Bij meer dan 58 tekens crashte die. Uit de crashes konden ze afleiden wat er gebeurde. Ze schreven een script om de crash te besturen en vervolgens poort 7676 over te nemen. Dat is de management interface waarmee KPN het modem op afstand voorziet van updates. Na vijf dagen werk konden ze hun eigen software installeren tussen de gebruiker en het internet. De mogelijkheden zijn legio. Voor hun demo bij Hack in the box kozen ze ervoor een VoIP gesprek af te tappen.

Op 10 april staan beide heren bij Hack in the Box in een soort Star Trek-achtig overhemd op het podium met een geïmproviseerd LAN voor zich. De titel van hun presentatie "How I met your Modem. De ZyXEL P-260IHN-FI"[1]. Na een technische verhandeling die ik jullie hier zal besparen, belt Steven iemand via de VoIP en vraagt diegene een vooraf gegeven code te noemen. Peter rommelt wat aan zijn laptop en jawel, hij tovert het gesprek tevoorschijn. Applaus. En als ze vertellen hoe KPN omging met de melding roept Peter ze erbij. Op het podium verschijn de CISO Jaya Baloo: "On behalf of KPN I would like to thank you for hacking our network". Ze overhandigt beide heren een T-shirt met daarop de tekst "I hacked KPN, and all I got was this lousy T-shirt". Nog meer applaus. Jaya: "It shows Responsible Disclosure works!". Peter: "Yes, some times it does…"

Toch zit iets me nog niet helemaal lekker. De modems worden beheerd vanaf de providerkant via de beruchte poort 7676. Dus als je voor deze onthulling al gehackt was, kon KPN het niet meer patchen. Dat klopt volgens Peter, maar volgens hem zijn zij de eersten die dit hebben ontdekt. Maar zelfs dan nog. Hoe zou het nu vergaan met die 10 miljoen andere modems die niet van KPN zijn? Zou Zyxel alle providers en individuele gebruikers hebben geïnformeerd? Daar zullen we dan vanzelf wel achter komen…

Volgende aflevering in verantwoorde onthullingen #5:
"Toen @lilaselmatani een studieboek kocht, kreeg hij er 1600."

Links:
[1] http://www.youtube.com/watch?v=eK8VbFmb0gE

[2] http://www.youtube.com/watch?v=9rBB_Ng7EZA

Chris van 't Hof (www.cvth.nl)

De belangrijkste missie van IDentity.Next is om een onafhankelijk platform te bieden voor ondersteuning en facilitering van innovatieve benaderingen in de wereld van de digitale identiteit. Het voornaamste doel is het dissemineren van kennis, expertise en ervaring door het organiseren van evenementen en workshops etc. op een verscheidenheid aan thema's, gemaakt van en door expertises binnen de wereld van IT en Business en Marketeers.

VERSLAG

IDentity.Next 2013

Op 20-21 november 2013 vond voor alweer de 4e editie van IDentity.Next'13 event. Net als de vorige keer vond het deze keer ook weer plaats in New Babylon Center in Den Haag, verspreid over twee dagen. Er kwamen meer dan 100 deelnemers uit binnen- en buitenland bijeen om zich te laten inspireren, te netwerken en de ontwikkelingen rondom het onderwerp 'de digitale identiteit' met elkaar te kunnen delen. Al sinds de 1e editie wordt IDentity.Next ondersteund door PvIB waardoor PVIB leden met korting toegang krijgen.

Het un-conference principe werd ook weer tijdens deze IDentity.Next gehanteerd. De kracht van dit Open Space format is dat er ruimte is om de agenda te beïnvloeden tijdens het event. Daarnaast zijn de onderlinge ontmoetingen tussen kennisexperts, is er samenwerking, interactie, discussie en creativiteit. Daarbij ontstaat vanzelf de mogelijkheid om te luisteren en spreken met deskundigen en professionals en zelf deel te nemen aan debatten en discussies.

IDentity.Next werd geopend door Robert Garskamp, de organisator van dit event. Na een korte introductie ging het event van start met keynote presentaties van Michael Schwartz (founder van Gluu) en een voorstander van gebruik van open standaarden als SAML en oAUTh2 en Steve Pannifer (Consult Hyperion) over de 'value van digital identity'. Na deze highlights werd het congresdeel met de parallel tracks voortgezet.

Het congresdeel van IDentity.Next was verdeeld over zes tracks:

- E-Citizen (Next generation eGovernment and its identity issues)
- Social Consumer (How will social identity turn around the new value chain?)
- Up in the air (identity information is part of the crown jewels of many organisations. How can you govern, what's far away?
- Own (y)our data (Who's data is it anyway? Our daily lives result in a lot of digital footprints. Do we have any say in who can access?
- MobileMe (How is it possible to control your mobile Identity?)
- Private Eye (Who owns and controls online privacy and should we really care?)

Elke track bestond uit presentaties door (vooral) bekende

sprekers uit binnen- of buitenland, die werkzaam zijn binnen de wereld van de digitale identiteit, zoals Nils Fjelkegard (Swedish eIdentification board), Mike Chung (KPMG), Steve Pannifer (Consult Hyperion), Frank Leyman (Fedict), Peter van Buijtene (PostNL), Paulan Korenhof (TiIT), Hans van der Burght (Ministerie EZ), Menno Stigter (Gemeente Den Haag), Maarten Everts (TNO) en vele anderen. Dat het een internationaal congres was, bleek uit de aanwezigheid van sprekers uit Australië, Duitsland, Spanje, USA, Denemarken en andere landen.

Open Space

Jacoba Sieders (Rabobank) was de facilitator van de Open Space sessies in de middag van dag 1. Open Space betekent in het kort dat een discussie- en netwerkvergadering zonder agenda wordt gehouden. Allereerst moet er wel een agenda worden vastgesteld. Om dit te kunnen doen konden alle aanwezigen een onderwerp voorstellen en uitleggen wat hun belang is om dat onderwerp te bespreken, welke problemen/ontwikkelingen men op tafel wil leggen, gerelateerd aan de thema's binnen IDentity.Next. Deze onderwerpen worden in een tijdschema op een muur geprikt. De muur wordt dan uiteindelijk de agenda van die middag. Hierop komen alle onderwerpen te staan, sessies en de duur ervan. Wanneer iedereen (die zich geroepen voelde) dit heeft gedaan kan de agenda als definitief worden beschouwd. Elk van de aanwezigen mag dan besluiten aan welke sessie wordt deelgenomen. Er is verder geen limiet aan het (minimaal en maximaal) aantal mensen per sessie. Wel heeft elke sessie een gespreksleider en wordt een kort verslag van de sessie gemaakt. Dat wordt vervolgens plenair weer gedeeld.

Award

Aan het eind van de 1e dag vond ook dit jaar weer de uitreiking plaats van de Novay Identity Award. De award dient als ondersteuning voor het beste nieuwe concept of product op het gebied van digitale identiteit. Met deze prijs ondersteunen IDentity.Next en het ICT-onderzoeksinstituut Novay innovaties die de toekomst van onze digitale identiteiten vormgeven. Er was een jury samengesteld onder leiding van Maarten Wegdam (managing consultant Novay). De overige juryleden waren: Sander Swienink (eHerkenning, winnaar Novay Digital Identity award 2013), Leendert Bottleberghs (Head of Business Development - Marktplaats, eBay Classifieds Group), Marko van der Zwam (managing partner Deloitte), Pernille Tranberg (journalist, auteur en spreker bij Digital-Identitet.dk). Uit de open inschrijving waren drie genomineerden door de jury geselecteerd:

- IMPRINTS is een multidisciplinair onderzoeksproject, uitgevoerd door Loughborough University, dat zich richt op acceptatie van innovaties op het gebied van digitale identiteiten door te kijken naar wat gebruikers doorgaans doen en welke gevoelens de innovatie oproept.
- NXP: SmartTouch is een technologie die het mogelijk maakt om een gebied op het oppervlak van een smartcard te configureren als PIN-toetsenbord of een zogenaamde gesture area, waarmee veilig een pincode, bankrekeningnummer of over te schrijven bedrag kan worden ingegeven.
- idBCN is een Identity & Access Management (IAM) dienst die door de stad Barcelona als gratis publieke dienst wordt aangeboden. Houders van idBCN identiteiten kunnen deze gebruiken om toegang te krijgen tot allerlei digitale diensten; op dit moment zijn dat de diensten van de stad Barcelona zelf, maar binnenkort wordt het mogelijk om andere digitale diensten te gebruiken van zowel overheden als private bedrijven

Uiteindelijk werd idBCN door de jury als winnaar gekozen. Het juryrapport meldt: "Wat de jury met name interessant vindt, is de combinatie van verschillende innovaties zoals het gebruik van mobiel en het combineren van fysieke en digitale identiteit. De jury vindt het bijzonder dat het om een lokaal initiatief gaat, waarbij verschillende publieke en private partijen betrokken zijn, dat op korte termijn een significante impact op gebruikers zal hebben." Deze eerste dag werd afgesloten met een keynote presentatie van Pernille Pravat. Zij is een Deense privacy expert en aciviste. Met veel voorbeelden gaf zij aan welke dreigingen er bestaan en hoe we ons daartegen kunnen verweren.

Op dag 2 was er wederom een vol programma met een diversiteit van onderwerpen. De dag begon met een keynote presentatie van Mike Chung. In een niet alledaagse presentatie over 'predictions' gaf Mike aan op hoeveel gebieden voorspellingen niet zijn uitgekomen. Hij was niet te benauwd om aan te geven dat ook zijn eigen organisaties ontwikkelingen te zonnig voorspelde of zelfs ontwikkelingen in het geheel niet zag aankomen.

De tweede dag werd uiteindelijk afgesloten met een presentatie van Liesbet van Zoonen over het genomineerde onderzoeksproject van Loughborough (en andere Engelse universiteiten) over hoe de jeugd omgaat met identiteiten.

Net als vorig jaar was er ook dit jaar een sidetrack over overheididentiteiten, dit keer over internationale eID-initiatieven en -samenwerking. Die samenwerking is er momenteel te weinig en gebruik over en weer van nationale eID's is niet mogelijk. De resultaten zullen in vervolgbijeenkomsten worden uitgewerkt en we zullen proberen ook in dit blad daarover terug te koppelen.

Meer informatie: http://www.idnext.eu

Robert L. Garskamp is founder of IDentity.Next.

Achter het nieuws

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

EEN NIEUW JAAR, NIEUWE BEDREIGINGEN?

Namens de redactie van uw lijfblad wensen wij u allen een voorspoedig, maar vooral veilig 2014 toe. We hopen natuurlijk allemaal dat het veilig en zonder al te veel grote verstoringen zal verlopen. Maar wat voor cyber malheur verwachten de redactieleden in dit nieuwe jaar? Nog meer onthullingen over de afluisterpraktijken van onze nationale veiligheidsdiensten? Grootschalige cyberverstoringen? Gaan we iets zien wat we nog nooit hebben meegemaakt? Of hebben we alles ondertussen "onder controle"? Een ding is zeker: het zal weer een interessant jaar worden.

Tom Bakker – DESIGN

Een aantal zaken spelen nu al en zullen in 2014 ook gaan spelen. De nieuwe Europese privacy wetgeving zal een behoorlijke impact hebben op organisaties. Denk maar aan Privacy Impact Analyses (PIA), Privacy-by-design en de meldplicht van lekken (en de eventuele boetes!). Daar zijn in het afgelopen jaar een aantal artikelen over verschenen in o.m. ons blad. Ik verwacht dat vanuit het Privacy-by-Design vanzelf ook het Security-by-Design de nodige aandacht zal krijgen. De vraag is of de wetgeving meteen in 2014 al van kracht wordt. De EU-top heeft zaken wat vertraagd. Maar je kunt er beter nu alvast mee beginnen.
Ook de afluisterschandalen zullen gevolgen hebben. Men is zich meer bewust van beveiliging en ik zie een grote vlucht voor digitale identiteiten en encryptie van gegevens. Zeker omdat we steeds meer gegevens in de cloud zijn gaan opslaan. Misschien ook grote kansen voor het Jericho Forum om hierop in te haken. Een ander punt is dat men meer aandacht zal gaan besteden aan 'detectie en respons' in plaats van de focus op 'preventie'. Het blijkt toch maar weer dat men uiteindelijk toch wel een keer gehackt wordt en/of slachtoffer wordt van een DDOS aanval. Dus adequaat reageren is van groot belang.En dan als laatste zie ik nog meer aandacht voor security- of beter risk awareness. Het is al vaak gezegd, maar de mens blijft de zwakste schakel. Hopelijk hebben de afluisterpraktijken mensen aan het denken gezet. Beveiligingsmaatregelen zullen wat mij betreft dan ook eenvoudiger in het gebruik moeten worden. Anders haakt men af en zijn we nog niets opgeschoten.
Al met al genoeg werk en kansen voor ons informatiebeveiligers in 2014!

Maarten Hartsuijker – CONNECTED CAR

Afgelopen zomer zagen we hoe de Amerikaanse onderzoekers Charly Miller en Chris Valasek de aanval opende op een Toyota Prius. Vanaf de achterbank namen ze de controle over van de bestuurder en konden daarmee invloed uitoefenen op de besturing van het voertuig. Misschien is 2014 nog wat vroeg, maar ik verwacht dat IT-veiligheid in auto's de komende tijd een steeds belangrijkere rol zal gaan spelen. We zien industrie breed dat fabrikanten steeds vaker "af fabriek" een connected car leveren. En diverse partijen onderzoeken mogelijkheden om connected car dienstverlening te leveren voor bestaande auto's. Met meer dan een miljard auto's (devices, volgsystemen) op de weg moet dit de aandacht van hackers en inlichtingendiensten gaan trekken.

Ronald van Erven – TOP 5

Nieuwe bedreigingen, neen een jaar van uitdagingen die wij met een "can do attitude" tegemoet zien. Awareness is geen issue meer, omdat er een nieuwe generatie professionals van de opleidingen komt. Een basisniveau IB is hen bijgebracht op deze opleidingen. Voor de nieuwe IB-professionals is IB gesneden koek. Gelet op de stand van de techniek in de tijd, gelet op de aandacht voor het onderwerp in de media helpt dit bij het verhogen van ons aller bewustzijn en alertheid. Niets bedreigingen, in de toekomst alles valt onder beheerste risico's en die worden gemanaged. 2014 brengt een aantal nieuwe uitdagingen die wij als IB-professionals moeten beheersen. Hierbij mijn top 5.

(1) De nieuwe privacy wet - met aandacht voor datalekken. Door deze aankomende wet komen naast ICT-beheer en incident management ook security architecturen goed op de radar. Security & Privacy by design.

(2) De term IT-security officer of IT-security manager zal ophouden te bestaan. De nieuwe term is information risk officer (IRO). Iemand die het interne informatie beveiligingsprogramma coördineert en die informatie risico's, i.s.m. met de business en ICT-afdelingen, managed. Dit in een tijd waar ICT-afdelingen worden uitbesteed, cloud diensten hot zijn en waar de eerste bedrijven toch al weer terugkomen van uitbesteding van hun beheerafdelingen. De IRO moet met deze golfbeweging mee kunnen deinen.

(3) De IRO heeft veel gemeenschappelijk met de nieuwe functionaris gegevensbescherming, uit de aankomende privacy wet, maar ook met het coördineren van een bedrijfscontinuiteitsprogramma. Een leuke en uitdagende combinatie, die de IRO uit het ICT-domein haalt en in de business en bestuurskamer zet.

(4) En dat brengt ons bij het vierde punt voor 2014. Regievoering over je leveranciers. Natuurlijk beschikbaarheid. Maar vooral in SLA's de term informatiegevoeligheid in brengen. Gevoeligheid is een container begrip voor betrouwbare informatie en vertrouwelijke informatie. En daarmee brengt uitbesteding en cloud computing dataclassificatie goed op de radar. Dataclassificatie een moeizaam, grijs, bureaucratisch onderwerp dat toch heel belangrijk is, omdat je als business moet weten waar je waardevolle informatie uithangt.

(5) Een jaar van BYO en verdere consumerization van ICT met als gevolg dat vaste security patronen niet meer werken. Informatie moet vrij stromen. Mensen kennen hun taken en verantwoordelijkheden in relatie tot de omgang met informatie en dan blijft voornamelijk cryptografie over als laatste informatiebeveiligingsmaatregel.

Kortom, 2014 een jaar om naar uit te kijken. Ik wens u een veilig 2014.

André Koot - DOE HET ZELF

De trend voor volgend jaar heeft natuurlijk alles te maken met de onthullingen van Edward Snowden over de NSA cs. Het ongelimiteerd stofzuigen en het ongericht surveilleren heeft voor heel veel onrust gezorgd. Mensen die zich nooit druk hebben gemaakt over het beschermen van hun online privacy, vragen zich nu af of ze inderdaad niets te verbergen hebben, of beter gezegd, ze vragen zich af waarom geheime diensten hun informatie nou eigenlijk nodig hebben. Wij, de security professionals, vroegen ons dat al veel langer af en wij hebben ons dan ook gewapend tegen dat rondsnuffelen, wij gebruiken allemaal natuurlijk al lang PGP en veilige Europese dropbox alternatieven. Maar niet heus... ik was onlangs mijn PGP-secret phrase kwijt. Nee, crypto is ook voor ons niet altijd handig. Vandaar mijn trend: gebruikersvriendelijke crypto oplossingen worden werkelijkheid. En ze gaan ook gebruikt worden. Een paar voorlopers zijn Mailpile en Darkmail. Mailpile is een IJslands initiatief, dat via crowdfunding gefinancierd werd en dat als open source gepubliceerd zal worden. Dat kun je dus op een eigen server installeren, maar er zullen vast ook services komen. Darkmail is het initiatief van de eigenaren van Lavabit, de mailprovider waar Edward Snowden zelf gebruik van maakte. Ook Darkmail is een open source oplossing en ook via crowdfunding gefinancierd. Deze beide mailservices gaan ervan uit dat niet ervaren eindgebruikers op een veilige manier willen communiceren. En dat geldt dan ook voor ons soort mensen. Eindgebruikers gaan dus zelf veilig communiceren, 2014 wordt eindelijk het PGP-jaar.

De links naar de projectpagina's: http://www.indiegogo.com/projects/mailpile-taking-e-mail-back
http://www.kickstarter.com/projects/ladar/lavabits-dark-mail-initiative

Artikelen

[V] Arts, T. e.a., **Security naar de boardroom**, IB5:20
[A] Baaten, D., **Met patchen kun je niet winnen, wel verliezen**, IB6:4
[A] Bekker, G. e.a., **Europese wetgeving bescherming persoonsgegevens in de schijnwerpers**, IB7:8
[A] Bekker, G. e.a., **Europese privacywetgeving: de route naar compliance**, IB8:16
[O] Berg, J. van den e.a., **Wat gaan we doen tegen de cyberaanvallen?**, IB4:10
[A] Biesheuvel, A. e.a., **Europese wetgeving bescherming persoonsgegevens in de schijnwerpers**, IB7:8
[A] Biesheuvel, A. e.a., **Europese privacywetgeving: de route naar compliance**, IB8:16
[V] Borger, L., Tektok - **Security in showbusiness**, IB1:16
[I] Borger, L., **Interview met Juuso Pesola - Encryption with a twist**, IB2:20
[V] Borger, L., **Expertgesprek I&AM Volwassenheid**, IB2:9
[A] Borger, L., **BYOD & privacy in 1995**, IB4:24
[V] Borger, L., **"BCM is leuk"**, IB4:18
[A] Demarteau, A., **IPv6, niet alleen een langer adres!**, IB3:17
[A] Egan, G, **Veilig informatieverkeer in een BYOD-wereld**, IB3:13
[A] Elferink, M. e.a., **'Brede' meldplicht datalekken, preventie en privacy**, IB7:13
[V] Elsinga, B. e.a., **Security naar de boardroom**, IB5:20
[A] Eygendaal, R., **Op weg naar Internet of everything**, IB8:4
[V] Garskamp, R., **3e editie identity.next**, IB1:23
[A] Graaf, P. de e.a., **Geen digitalisering zonder digitale veiligheid**, IB3:7
[A] Haas, J. de, **Onbekende certificeringen voor IB professionals**, IB8:25
[V] Hanekamp, W., **Privacy en security over glasfiber**, IB4:22
[O] Hartel, P. e.a., **Wat gaan we doen tegen de cyberaanvallen?**, IB4:10
[A] Hensen, H.J.J. e.a., **Recht en informatiebeveiliging: samen sterk**, IB1:4
[A] Hoorweg, E. e.a., **Geen digitalisering zonder digitale veiligheid**, IB3:7
[A] Joosten, R, **Van risicomanagement naar succes governance**, IB2:4
[O] Junger, M. e.a., **Wat gaan we doen tegen de cyberaanvallen?**, IB4:10
[V] Kagie, S., **Aanstormend talent verdient een podium**, IB8:7
[A] Kamphuis, A., **Cybercrime, mag een beetje preventie ook?**, IB5:25
[V] Kanbier, G., **Security café - Mobile App security**, IB4:26
[A] Kanbier, G., **Login, logout, waar gaat het fout?**, IB5:17
[V] Kanbier, G., **Security café - Big data & security**, IB8:22
[V] Kerkdijk, R. e.a., **Hands-on innovatie in het nieuwe Cyber Security Lab van TNO**, IB5:22
[V] Klaver, M., **Cyber resilience in de bestuurskamer**, IB1:13
[A] Kleiberg, **De valkuilen van security monitoring**, IB8:10
[V] Koelmans, M., **Twee dagen onder hackers bij Hack in the Box Amsterdam**, IB6:18
[A] Kogenhop, G., **Business Continuity Management is meer dan alleen hoofdstuk 14 - ISO 27001**, IB7:4
[A] Koning, R. de e.a., **Geen digitalisering zonder digitale veiligheid**, IB3:7
[A] Koot, A., **Cloud Security Alliance**, IB1:18
[I] Koot, A., **Interview met Kalle Palomäki**, IB3:20
[A] Koot, A., **Diagnostiek voor U**, IB4:4
[A] Koot, A. e.a., **Starreveld komt weer uit de kast**, IB2:15
[V] Koot, M., **Bob Lord over security bij Twitter**, IB6:11
[V] Koppen, L., **Artikel van het jaar 2012**, IB4:8
[A] Kortier, M. e.a., **'Brede' meldplicht datalekken, preventie en privacy**, IB7:13
[A] Laan, N. van der e.a., **Penetratietesten uit het verleden bieden geen garantie voor de toekomst**, IB7:25
[A] Lent, R. van, **De evolutie van het nieuwe 'mobiele' werken (HNmW)**, IB3:4
[V] Menter, R. e.a., **Hands-on innovatie in het nieuwe Cyber Security Lab van TNO**, IB5:22
[O] Meulen, N. van der, **Baseer de aanpak van cyberaanvallen op een realistisch scenario**, IB4:14
[A] Niamat, R., **Noodzaak landelijke campagne tegen identiteitsfraude**, IB6:14
[V] Noord, F. van e.a., **Informatiebeveiligers maken werk van professionalisering**, IB5:26

Jaarregister 2013

[A] Ogórkiewicz, M., DDoS - Smashing the business for fun and Profit, IB5:8
[A] Oordt, J.W., Waarborgen continuïteit SaaS-informatiesystemen, IB5:4
[A] Oordt, J.W., Open source compliancy van belang voor continuïteit, IB7:21
[A] Oordt, J.W. e.a., Recht en informatiebeveiliging: samen sterk, IB1:4
[V] Pater, J., Themasessie incident response, IB4:17
[V] Redactie, Nominaties voor Artikel van het Jaar 2012, IB2:27
[V] Redactie, Artikelen schrijven in dit PvIB blad, IB4:16
[V] Redactie, Data breach investigation report 2013, IB4:20
[V] Spruit, M. e.a., Informatiebeveiligers maken werk van professionalisering, IB5:26
[A] Steenbeek, C. e.a., Penetratietesten uit het verleden bieden geen garantie voor de toekomst, IB7:25
[A] Steenkamp, R., Risico's voor betrokkenen centraal in de CBP-richtsnoeren beveiliging, IB6:12
[A] Stuljens, M. e.a., Starreveld komt weer uit de kast, IB2:15
[A] Thijssens, H., Een mobile device management oplossing voor elk werkproces?, IB1:8
[A] Velde, M. van de, Women in Cyber Security: nut of noodzaak?, IB5:15
[V] Verkoelen, C., Man in the Browser, IB2:25
[A] Vonken, C., File-collaboration op de zaak, IB3:22
[A] Vooren, T. van, Agile in informatie- beveiligingsprojecten, IB8:13
[O] Wesselingh, E., No function creep by design, IB6:8

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

Achter het Nieuws

DNA Database, Dunn, L., Borger, L & Koot, A., IB1:26
Responsible Disclosure, Jochem, A., Koot, A. & Hartsuijker, M., IB2:28
APT1 - Klopt het of is het opgeklopt?, Koot, A., Erven, R. van, Hartsuijker, M. & Borger, L., IB3:28
Media reacties door de banken op DDoS aanvallen, een gemiste kans?, Hartsuijker, M., Koot, A., Erven, R. van, IB4:28
PRISM, Koot, A., Dunn, L., Hartsuijker, M., Borger, L. & Erven, R. van, IB5:28
CISO versus white hats: een haat-liefde verhouding?, Borger, L., Hartsuijker, M., Bakker, T. & Dunn, L., IB6:28
Waar kunnen we nog op vertrouwen?, Jochem, A., Hartsuijker, M., Erven, R. van & Koot, A., IB7:28
Adobe werd gehackt, Dunn, L., Bakker, T. & Hartsuijker, M., IB8:28

Column – Privacy peinzingen – Rachel Marbus

Tien zaken die u moet weten over uw grondrecht op privacy, IB1:12
Zullen we gewoon eens opnieuw beginnen?, IB2:14
De inval, IB3:16
Privacyschending door de overheid een theoretische discussie?, IB4:13
Wat je niet hebt, kan je niet ontnomen worden, IB5:14
Sterft je privacy na je dood?, IB6:10
Laten we meer beveiligingsfouten maken, het wordt er veiliger van, IB7:12
Tien zaken die u moet weten over privacy voor 2014, IB8:12

Column – Verantwoorde onthullingen – Chris van 't Hof

Hoe @legosteentje een witte hoed verdiende, IB6:16
A man in the middle of money and media, IB7:20
Toen @UID_ de kazerne belde met een fabriekswachtwoord, IB8:20

Column – Attributer

Service Oriented, IB1:22
Future Ready, IB2:26
Adaptive, IB3:27
Valuable, IB4:21
Supportable, IB5:24
Traceable, IB7:24
Identified, IB8:24

Column – Berry

Terugkijken is mooi!, IB1:31
Snoep verstandig, gebruik een Apple, IB2:31
Wie doet er mee met 4G?, IB3:31
Liever een leren bank, IB4:31
Internetjes wel of internetjes niet, IB5:31
Hoge bergen vangen veel wind?, IB6:31
Bij de tijd, IB7:31
Onder de bovenwereld, IB8:31

Boekbespreking

Luiijf, E., National Cyber Security Framework Manual, IB1:30
Erven, R. van., Cyberoorlog, "O ja, dat was waar ook", IB6:26
Erven, R. van, Essential Information Security, IB7:27
Erven, R. van, De zwakste schakel in de informatiebeveiliging, IB8:27

Kennismaking

Erwin Bosma, IB1:17
Martijn Veken, IB8:21

Voorwoord

Cyber Security, IB1:3
Goedkope expertise, IB2:3
Monitoring, IB3:3
Privacy, IB4:3
Big Data en privacy, IB5:3
Versleutelde email, IB6:3
Burning Man, IB7:3
De malware strijd, IB8:3

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 Ideas to Interconnect) e-mail: hr@pvib.nl
Motivation Office Support bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

REDACTIERAAD
Tom Bakker (Digidentity BV)
Lex Dunn (Capgemini)
Ronald van Erven (Timeos Pensioendiensten)
Maarten Hartsuijker (ANWB)
Aart Jochem (NCSC)
André Koot (Strict)
Rachel Marbus (NS, IT Advisory)
Bart van Staveren (UWV)
Martijn Veken (SNS REAAL)

ADVERTENTIE ACQUISITIE
e-mail: adverteren@pvib.nl;
of neem contact op met MOS (Motivation Office Support)
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 2014
De abonnementsprijs in 2014 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

"ALLES ZELF OP HET INTERNET DOEN"

Het zonnetje schijnt buiten en toch heeft Berry weer eens zijn zorgen. Ik lees een aantal berichten over de zorgverzekeraars die veel te veel winst zouden maken en daardoor de premies omhoog zouden helpen. Ik lees echter niet dat de toezichthouder de zorgverzekeraars verplicht om vereiste reserves op te bouwen. Ik lees ook een bericht over een grote zorgverzekeraar die 20% van zijn personeel gaat ontslaan omdat "de klant zelf alles op internet wil doen". Ik herlees de laatste zin een aantal keren en denk terug aan de sector die met dit alles is begonnen, namelijk de banken. De met marmer en andere hoogwaardige materialen aangeklede gebouwen die ze onderhouden hebben volgens mij geen enkele functie meer, want (los)geld storten gaat niet meer en grote bedragen afhalen doen ze ook niet meer. Wat al die broekpakken dan in die gebouwen doen is mij volstrekt onduidelijk.
Het zou ongeveer hetzelfde zijn wanneer mijn bakker op een bepaalde dag zou stoppen met het verkopen van brood. Mocht je verstrikt raken in het zakendoen met je bank via je app of internetbrowser, dan kun je altijd een betaalnummer bellen, die jou ook niet verder kan helpen. Telefoonnummers van je 'eigen' filiaal zijn niet meer te vinden. Het heeft uiteindelijk 25.000 banen gekost en dat de dienstverlening nu beter is geworden kan ik niet echt zeggen. Inmiddels zijn de zorgverzekeraars met een vergelijkbare actie begonnen, want de klant wil toch alles zelf via internet doen. Die wil geen declaraties opsturen die willen ze toch zelf kunnen uploaden? Een zorgverzekering uitzoeken is natuurlijk geen sinecure, maar gelukkig hebben we de hulp van vergelijkingssites. Ze zijn misschien niet allemaal even onafhankelijk, maar gelukkig zijn er meer vergelijkingssites. Het wachten is nog op een site die de vergelijkingssites gaat vergelijken…
Even terug naar onze zorgverzekeraars die eigenlijk allemaal met hetzelfde bezig zijn als de banken een paar jaar geleden. Iedere verzekerde moet zo snel mogelijk achter de knoppen. Zelf je mutaties invoeren en zelf een fotootje maken met je telefoon van je declaratie, deze uploaden naar de verzekeraar die deze zal uitbetalen als je ervoor verzekerd bent.
Dat deze ontwikkeling heel veel banen gaat kosten is evident. Wat mijzelf een beetje beangstigt, is dat we allemaal eenzelfde fragiele sleutel gebruiken, namelijk het DigiD. Het DigiD wordt vaak alleen gebruikt met een gebruikersnaam en password die jaren bij iemand in gebruik kan zijn. De gebruiker hoopt dat hij de enige is die deze combinatie kent, zo niet dan worden zijn gegevens gedeeld met een onbekende. Salarisgegevens, pensioengegevens, gemeentelijke gegevens en zo kan ik wel even doorgaan. Al die gegevens worden afgeschermd met een combinatie van twee woorden waarvan het wachtwoord in 15% van de gevallen 123456 is.
Het lijkt verbazingwekkend dat zo'n hoog percentage zo'n eenvoudig wachtwoord heeft, maar op zich is dit wel te verklaren. Tegenwoordig moet je je (bijna) overal registreren en een gebruikersnaam (veelal je e-mailadres) en een wachtwoord kiezen voordat je je boek kunt bestellen, je waterstanden kunt doorgeven en dergelijke. Voor al die websites een eigen gebruikersnaam en wachtwoord? Natuurlijk hebben u en ik altijd verschillende wachtwoorden die allemaal lastig te onthouden zijn zodat wij gevrijwaard blijven van identiteitsdiefstal. Wij doen dat soort domme dingen niet, wij horen niet bij die 15% van de gebruikers want wij hebben een enorm geheugen en kunnen alle combinaties wel onthouden. Wij schrijven onze combinaties ook niet op in een Word bestandje om ze zo nu en dan te kunnen raadplegen.
Vroeg of laat zal dit een enorm probleem gaan worden, want hoe bewijs je dat je geen wasmachine hebt besteld bij die ene webshop. Hoe kun je je vrienden uitleggen dat die vreemde berichten op Facebook echt niet van jou zijn, maar van iemand die doet als hij jou is. Zoals ik in één van mijn eerdere columns aangaf, is internet nooit bedacht voor dit soort toepassingen. Het is niet bedacht om wasmachines te bestellen en declaraties in te dienen. Het is niet bedacht om allerlei financiële transacties uit te voeren, maar we doen het allemaal wel. Mochten jullie nu online iemand tegenkomen die zich als Berry voordoet, onthoudt dan dat ik nooit iets via internet regel. Ik zoek altijd de instantie op of ik probeer ze te bellen, al moet ik toegeven dat dat allemaal wel erg lastig is geworden de laatste jaren.

Groetjes Berry

Rijksoverheid

Bouw jij mee aan een digitaal veilig Nederland?

Werken bij de Rijksoverheid betekent een bijdrage leveren aan een beter Nederland. Dus ook aan een veilige en rechtvaardige samenleving voor iedereen. Veiligheid en Justitie verdedigt en beschermt de rechtsorde. Het Nationaal Cyber Security Centrum (NCSC) staat voor een digitaal veilig Nederland. Wij bouwen 24 uur per dag aan een veilig Nederland en aan een organisatie die het hoofd kan bieden aan de digitale uitdagingen die ons te wachten staan.

Het NCSC, onderdeel van de Nationaal Coördinator Terrorismebestrijding en Veiligheid bij het ministerie van Veiligheid en Justitie in Den Haag zoekt:

Onderzoeker/analist cybersecurity m/v

Je maakt tactische maar ook technische analyses van cybersecurity ontwikkelingen en dreigingen. Daarbij maak je een vertaling naar de mogelijke impact op de digitale veiligheid van Nederlandse bedrijven en overheden. Ook onderhoud je relaties met cyberonderzoekers en -analisten bij onze samenwerkingspartners, de cybersecurity-community en internationale partners.

Je hebt een universitaire opleiding, bij voorkeur op het gebied van cybersecurity, informatiebeveiliging of ICT met een securitycomponent. Je hebt enkele jaren ervaring als adviseur, auditor of analist op het gebied van cybersecurity of informatiebeveiliging. Je maximale salaris is € 4.380,- bij 36 uur per week.

Security specialist en security specialist proces control m/v

Je creëert inzicht en overzicht in actuele ICT-dreigingen en kwetsbaarheden, pakt incidenten aan en levert een bijdrage aan de (door)ontwikkeling van CERT (Computer Emergency Response Team) systemen en het NCSC. Ook onderzoek je zelfstandig of in teamverband de security-impact van nieuwe ICT-ontwikkelingen en beschrijf je de lessons learned van ICT-veiligheidsincidenten.

Je hebt een afgeronde technische hbo- of universitaire opleiding. Je hebt uitgebreide ervaring met ICT-veiligheid en kennis van actuele dreigingen. Je hebt kennis van internettechnieken, de structuur van webapplicaties, UNIX-/Linux-systemen en Windows-omgevingen. Als security specialist proces control ben je daarnaast ook bekend met DNP3, Modbus, PROFIBUS of PROFINET. Je maximale salaris is € 4.380,- bij 36 uur per week.

Meer weten of reageren? Kijk op www.werkenvoornederland.nl/NCSC