01/2013

INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 1 - 2013

RECHT EN INFORMATIEBEVEILIGING: SAMEN STERK

CYBER RESILIENCE IN DE BESTUURSKAMER

TEK TOK - SECURITY IN SHOWBUSINESS

CLOUD SECURITY ALLIANCE

Kosteloos congres met netwerkplein voor eindgebruikers

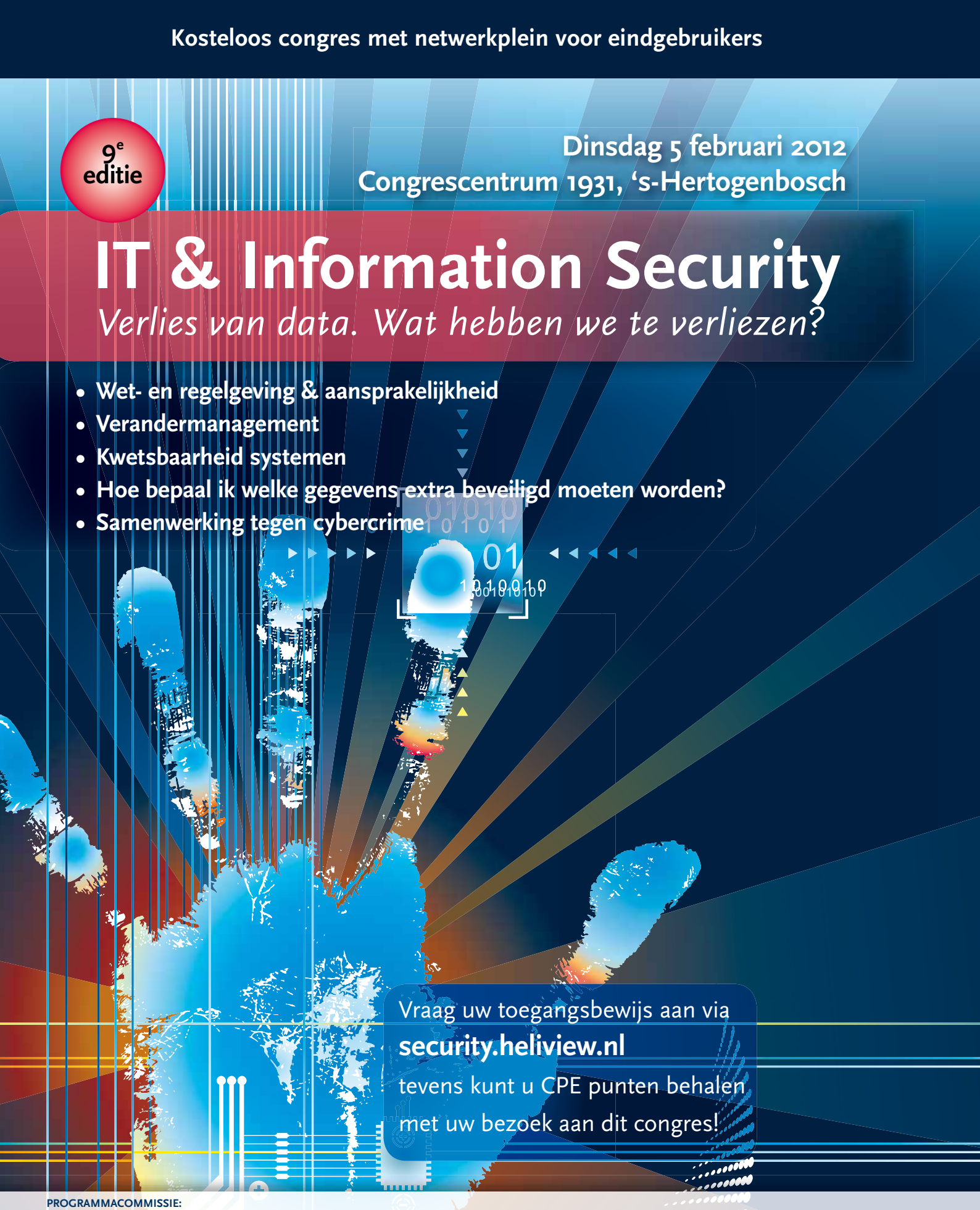
9e editie

Dinsdag 5 februari 2012
Congrescentrum 1931, 's-Hertogenbosch

IT & Information Security

Verlies van data. Wat hebben we te verliezen?

- Wet- en regelgeving & aansprakelijkheid
- Verandermanagement
- Kwetsbaarheid systemen
- Hoe bepaal ik welke gegevens extra beveiligd moeten worden?
- Samenwerking tegen cybercrime



Vraag uw toegangsbewijs aan via
security.heliview.nl
tevens kunt u CPE punten behalen
met uw bezoek aan dit congres!

PROGRAMMACOMMISSIE:

Gilles Ampt,
Enterprise Security Lead,
HP Nederland

Stoffel Bos,
CISO,
ProRail

Jessica Conquet,
Compliance,
KPN Corporate Market &
Bestuurslid, **PvIB**

Beer Franken,
Chief information security & privacy protection officer,
AMC

Ton van Gessel,
Chief Security Advisor,
Microsoft

Paul Oor,
Chief Security Officer,
Atos

VOORWOORD

Cyber security... het houdt velen in een hype-achtige betovering vast. Maar is het oude wijn in nieuwe zakken of is het écht iets nieuws? Het is heel eenvoudig om te zeggen dat cyber security net zo werkt als goede informatiebeveiliging, maar is dat echt zo? Ik vind dat niet. Er zijn vier aspecten waarop het zich duidelijk onderscheidt:

1. Cyberdreigingen komen van buitenaf. Informatiebeveiliging moet nog steeds zowel intern als extern zoeken naar bedreigingen;
2. Cyberdreigingen komen voort uit een kwaadaardige intentie. Informatiebeveiliging moet rekening houden met fouten die medewerkers, partners en klanten maken.
3. Cyberaanvalstechnieken zijn universeel. Informatiebeveiliging moet zich wapenen tegen aanvalstechnieken afhankelijk van de bedrijfssector, cultuur, processen en infrastructuur.
4. Cyberaanvallen kunnen bedrijfs-infrastructuur gebruiken zonder het bedrijf direct schade te veroorzaken.

De eerste drie aspecten geven wel aan dat het lijkt alsof cyber security een subset is van informatiebeveiliging. Dan zou het voldoende moeten zijn om je informatie-beveiliging op orde te hebben om cyberdreigingen aan te kunnen. Juist de groei in het aantal cyberincidenten toont aan dat dit niet het geval is. Collectief falen we om cyber-gerelateerde problemen onder controle te krijgen. Als ik accepteer dat het 'slechts' een subset is van informatie-beveiliging, dan is het een subset die een additionele, specialistische aanpak vergt.

En natuurlijk zien we hier wel dat problemen in de informatiebeveiliging bij cyberaanvallen gebruikt kunnen worden. Kevin Mitnick heeft pijnlijk aangetoond dat wij als mens gemakkelijk te misleiden zijn tot het uitvoering van verkeerd gedrag. We zullen getraind moeten worden om die misleiding te weerstaan. En systemen waarvan de configuratie of toegangsbeveiliging niet goed geregeld is, vallen eerder ten prooi aan cyberaanvallen. Dat verandert niets aan het feit dat de oorsprong van een cyberaanval bij een externe aanvaller ligt en dat deze een bekend arsenaal aan instrumenten hierbij gebruikt. Hoe beter we dit assortiment kennen, hoe beter we weten waar we ons tegen moeten wapenen. De open source aanpak doet het hierbij het best: kijk maar naar Metasploit en Nessus. De kennis is dus universeel en het best vastgelegd als open source. Informatiebeveiliging baseert juist zijn beveiliging op interne organisatiekennis van risico's en specificeert voor de organisatie op maat gesneden maatregelen.

Het laatste aspect legt het fundament voor een bestrijdingsprobleem: waarom zou ik mijzelf beveiligen als ik geen schade heb? In tijden van krappe budgetten moeten we natuurlijk niet onnodig geld besteden. We leven steeds meer in een wereld waarin eenieder alleen zijn eigen hachje redt en geen oog heeft voor de bedreiging van de buurman via eigen ICT. Toch is het goed om jouw deel aan bestrijding te doen, terwijl onbekende anderen ervan zullen profiteren.
Een patroon wat de samenleving hiervoor gebruikt is wet- en regelgeving. Door voor te schrijven hoe een bedrijf bijvoorbeeld om moet gaan met persoonsgegevens komt er voor bedrijven een compliance-risico bij, om direct aan te pakken en profiteert de samenleving van het effect. Of culturele druk kan ook reinigend werken: de ongewild betrokkene krijgt, bij schade elders, zelf te maken met reputatieschade.

Het lijkt er dus op dat we er niet aan ontkomen om cyber security naast of onder informatiebeveiliging specifieke aandacht te geven, of we nou onderdeel zijn van een organisatie, groot of klein, of particulier - met een speciale rol voor de overheid. ●

Lex Borger, hoofdredacteur

INHOUDSOPGAVE

Foto omslag: Official U.S. Navy Imagery

RECHT EN INFORMATIEBEVEILIGING: SAMEN STERK

VOORTDURENDE ONTWIKKELINGEN VERGEN MULTIDISCIPLINAIRE AANPAK

H.J.J. Hensen, directeur van de Software Borg Stichting en J.W. Oordt, IT-jurist bij dezelfde organisatie - info@softwareborg.nl

Voortschrijdend inzicht is bepaald geen onbekend fenomeen in de IT én in de informatiebeveiliging. Het heeft onder andere geleid tot de erkenning van het belang van de continuïteit van informatiesystemen. Zo werd in dit blad in 2004 een artikel gepubliceerd over broncode-escrow [Hoogendoorn, 2004], een belangrijk middel om die continuïteit te realiseren. Nu, acht jaar later, wordt dit middel in een veel breder kader geplaatst. Broncode-escrow is namelijk a. een onderdeel van rechtszekerheid in de informatiemaatschappij en b. de juridische basis onder de informatiebeveiliging van de softwaregebruiker. Het verzorgen van de continuïteit van de softwaregebruiker vergt daarmee kennis vanuit drie vakgebieden: informatietechnologie, informatiebeveiliging en recht.

In 2012 hebben een aantal in informatietechnologie gespecialiseerde notarissen zich verenigd. Zij gaan zich gezamenlijk inzetten voor de bevordering van rechtszekerheid in de informatiemaatschappij. Dit omvat onder andere de waarborging van de continuïteit van de softwaregebruiker. De positie van de notaris in ons rechtsbestel vormt daarvoor een sterke basis. Op grond van de Notariswet kan zijn standplaats niet failliet gaan en zijn akte niet worden aangevochten. Het beperken van risico's en het veiligstellen van bezittingen behoort tot de kerntaken van het notariaat. De nieuwe risico's en bezittingen die ontstaan in de informatiemaatschappij vergen specialisatie van de notaris, onder meer in de van toepassing zijnde wet- en regelgeving. Gedacht kan worden aan de Auteurswet, de Databankenwet en de Wet bescherming persoonsgegevens.
Enkele voorbeelden van de diensten van de IT-notaris zijn: broncode-escrow, juridische beveiliging ASP/SaaS-systemen, bescherming en overdracht van intellectuele eigendommen en het ZZP-IT testament voor het regelen van de nalatenschap van de IT-er. Zie www.it-notaris.nl [1].

Kader 1 - IT-notaris voor rechtszekerheid

Laten dit drie vakgebieden zijn waarbinnen de ontwikkelingen elkaar in hoog tempo opvolgen en elkaar beïnvloeden. Onder deze omstandigheden moet de softwaregebruiker zoeken naar houvast met betrekking tot zijn continuïteit. Vrijwel alle softwaregebruikers krijgen immers slechts een verzameling nullen en enen bij de aanschaf van computerprogrammatuur. Alle materialen en hulpmiddelen die tot die nullen en enen hebben geleid, blijven bij de softwareleverancier.
Welke gevolgen heeft dat voor de gebruiker van bedrijfskritische software?
Software is een goed met een geheel eigen aard, met als belangrijkste eigenschap dat het geen tastbare zaak is. De wetgever heeft daarom voor de bescherming van software bijzondere regelgeving op moeten stellen.
De softwareleverancier krijgt op grond van de Auteurswet een auteursrecht op de computerprogrammatuur die door hem is ontwikkeld. Dit heeft gevolgen voor de wijze waarop de software door de leverancier wordt verhandeld. De gebruiker heeft naast de levering van de software zelf, ook de juridische toestemming van de leverancier nodig om de auteursrechtelijk beschermde software te mogen gebruiken.
Deze toestemming wordt door de leverancier afgegeven in de vorm van het toekennen van een gebruiksrecht (of *licentie*) op de programmatuur aan de softwaregebruiker. Dit wordt geregeld in een daartoe bestemde licentieovereenkomst. Bij de aanschaf van software, ook bij maatwerkprogrammatuur (zie kader 2), wordt dan in beginsel ook betaald voor de verkrijging van het gebruiksrecht. De handel in software betreft kortom voor een belangrijk deel een handel in rechten.

De handel in software betreft een handel in rechten

Hoewel de omvang van het gebruiksrecht van geval tot geval verschilt,

Veel softwaregebruikers zijn zich niet bewust van het feit dat het auteursrecht op de *maatwerk*software die zij hebben laten ontwikkelen, op grond van de Auteurswet, toekomt aan de softwareleverancier. Dit betekent dat de leverancier de broncode van de maatwerksoftware in beginsel niet aan de softwaregebruiker hoeft te verstrekken en ook dat de leverancier de broncode kan gebruiken bij de ontwikkeling van applicaties voor andere klanten. Ook de gebruiker van maatwerksoftware heeft dus met continuïteitsrisico's te maken, waarvoor broncode-escrow een oplossing kan bieden.

Kader 2 - Maatwerksoftware

krijgt de softwaregebruiker in de regel slechts toestemming tot het gebruik van de objectcode van de software, dus van de hierboven genoemde verzameling enen en nullen. De overige onderdelen van het complete software-product, zoals de broncode en bij de ontwikkeling van de programmatuur gebruikte hulpsoftware, worden niet door de leverancier aan hem overgedragen en blijven geheim. Het gevolg hiervan is, dat het sluiten van een licentie-overeenkomst het begin is van een langdurige (rechts)verhouding tussen de softwaregebruiker en zijn leverancier. Alleen de leverancier beschikt immers over het materiaal waarmee de software kan worden onderhouden en doorontwikkeld. Bij de aanschaf van software ontstaat leveranciersafhankelijkheid daarom als vanzelf.

Continuïteit: de verantwoordelijkheid van de softwaregebruiker

Dat een softwaregebruiker voor de continuïteit van het gebruik, het onderhoud en de door-ontwikkeling van zijn bedrijfskritische informatiesystemen volledig afhankelijk is van zijn softwareleverancier, zou voor hem al voldoende reden moeten zijn om tot actie over te gaan. Nochtans dient te worden gewezen op het feit dat hij daartoe op grond van regelgeving ook nog eens verplicht kan zijn. Dit komt allereerst omdat de beschikbaarheid van digitale data afhankelijk is van de beschikbaarheid van de software waarmee deze data worden verwerkt. Stel bijvoorbeeld dat een organisatie software inzet bij het uitvoeren van de administratie. De administratiegegevens moeten op grond van de fiscale bewaarplicht na de vastlegging ervan nog jarenlang voor de Belastingdienst inzichtelijk kunnen worden gemaakt. Op het moment dat de daarvoor benodigde administratie-software niet meer kan worden gebruikt, zal de organisatie niet aan die plicht kunnen voldoen. Een tweede oorzaak is het feit dat regelgeving aan voortdurende verandering onderhevig is. De software waarmee die regelgeving wordt toegepast, dient daarom ook met regelmaat te worden bijgewerkt. Stel dat een overheidsorganisatie bij het uitvoeren van de sociale zekerheidswetgeving gebruik maakt van een daartoe ontwikkeld software-pakket. Wanneer de leverancier stopt met het verzorgen van updates, wordt de software snel onbruikbaar. Dit heeft uiteraard aanzienlijke gevolgen voor de bedrijfsvoering van de overheidsorganisatie.

> De softwaregebruiker is voor de continuïteit van zijn informatiesystemen volledig afhankelijk van zijn leverancier

De softwaregebruiker kan op grond van wetgeving verplicht zijn om de informatie die hij verwerkt te beveiligen. In dit verband kan bijvoorbeeld worden gedacht aan artikel 13 van de Wet bescherming persoonsgegevens. Als onderdeel van dat beveiligingsproces moet hij de beschikbaarheid - naast de integriteit en de vertrouwelijkheid, één van de drie pijlers van informatiebeveiliging - van deze informatie verzorgen. Wanneer de softwaregebruiker de continuïteit van zijn informatiesystemen verzorgt, maakt hij op dit gebied een grote stap. Dit omdat - nogmaals - de beschikbaarheid van digitale gegevens voor een belangrijk deel is verbonden aan de beschikbaarheid van de software waarmee deze gegevens worden verwerkt.

Beperken risico's softwaregebruik: contractuele maatregelen

De wetgever heeft in de Auteurswet ook bepalingen opgenomen die de softwarelicentienemer beschermen. Met die bepalingen worden hem voornamelijk de bevoegdheden toegekend die nodig zijn om de software op een normale manier te kunnen gebruiken. In de regelgeving is verder niet veel vastgelegd over de rechtspositie van de softwaregebruiker, zijn continuïteit wordt nauwelijks wettelijk beschermd. Dat is enerzijds het gevolg van het feit dat wetgeving en jurisprudentie altijd achter de technologische ontwikkelingen aanhobbelen (zie tabel 1). Anderzijds is

Informatietechnologie	Recht
Software (1960)	Bescherming software in Auteurswet(1991)
Internet (1990)	Databankenwet (1999), Wet bescherming persoonsgegevens (2001)
Cloud Computing (2009)	Aankondiging Europese richtlijn Cloud Computing (2012), in Nederland over enkele jaren als wetgeving geïmplementeerd?

Tabel 1 - Ontwikkelingen in de IT en de daarop volgende ontwikkelingen in het recht

het natuurlijk zo dat, van met name de bedrijfsmatige softwaregebruiker, mag worden verwacht dat hij in staat is om zijn zaakjes contractueel te regelen.

Dat dit wordt onderkend, blijkt uit het gegeven dat steeds meer organisaties rond dit thema afspraken maken met hun softwareleverancier. Zo wordt in een onderhoudsovereenkomst vastgelegd met welke frequentie de software van een update moet worden voorzien. In een Service Level Agreement (SLA) kunnen aan de SaaS-leverancier meetbare verplichtingen worden opgelegd ten aanzien van het beschikbaarheidsniveau van de door hem geleverde software. Daarbij kunnen zaken tot in de puntjes worden geregeld: de waarde van het juridisch instrumentarium bij het verzorgen van de kwaliteit en beschikbaarheid van software laat zich zien. Er moet worden samengewerkt tussen technici en juristen. In de contracten die een softwaregebruiker sluit, worden immers eisen aan de techniek gesteld. Ook wordt de wijze waarop die techniek mag worden gebruikt, nader bepaald. In de praktijk komt het niet vaak voor, dat men over de specialistische technische én juridische kennis beschikt om deze zaken uitputtend te regelen (zie tabel 2).

Beperken risico's softwaregebruik: broncode-escrow

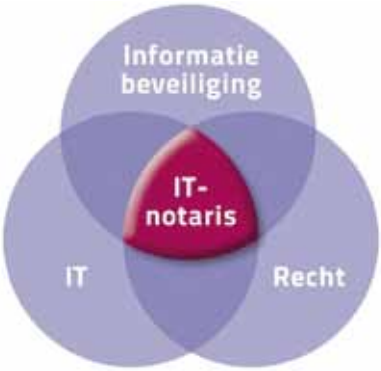
Complicerende factor is dat het contractueel vastleggen van onderhoudstaken en service levels onvoldoende is voor het verzorgen van de continuïteit van de software-gebruiker. Het is namelijk niet zeker dat een softwareleverancier de verplichtingen die hij op zich heeft genomen, gedurende de onbepaalde gebruiksperiode zal (kunnen) vervullen. De contractspartij waarmee de softwaregebruiker in een licentieovereenkomst of SLA afspraken heeft gemaakt, kan met andere woorden wegvallen door bijvoorbeeld een faillissement of blijvende wanprestatie. Wanneer de softwaregebruiker de nakoming van verplichtingen van zijn software-leverancier niet (succesvol) af kan dwingen, staat hij alsnog met lege handen. Hij heeft namelijk niet de beschikking over en de gerechtigdheid tot het broncodemateriaal en de overige faciliteiten die nodig zijn om zelf de continuïteit van zijn informatiesysteem te verzorgen.

De meest gebruikte oplossing waarmee ook na het wegvallen van de softwareleverancier die continuïteit kan worden verzorgd, is broncode-escrow. Hierbij wordt door de leverancier het broncodemateriaal van bedrijfskritische software in bewaring gegeven aan een onafhankelijke derde partij: de escrow agent. De softwareleverancier stemt er vervolgens mee in dat dit broncodemateriaal door de escrow agent aan de gebruikers van de software wordt afgegeven op het moment dat bepaalde *triggering events* zich voordoen. Voorbeelden daarvan zijn de situatie waarin de softwareleverancier niet meer aan zijn onderhoudsverplichtingen voldoet of zijn faillissement.
De softwaregebruiker kan met het broncodemateriaal vervolgens zelf het onderhoud en de doorontwikkeling van de software verzorgen of dit uitbesteden aan een andere partij in de markt.
Inmiddels zijn steeds meer software gebruikende organisaties bekend met de noodzaak van broncode-escrow.
Zo is in de ARBIT-voorwaarden van de rijksoverheid [2], vastgelegd dat een softwareleverancier een broncode-escrowregeling moet kunnen treffen voor de door overheidsorganisaties aangeschafte software.

Specialist	Kennis IT-Juridisch	Kennis Informatietechnologie
Software Engineer	-	+
IT-Auditor	-	+
Informatiebeveiliger	+ / -	+ / -
IT-juristen	+	-
IT-notarissen	+	-

- kennisniveau laag + kennisniveau hoog + / - kennisniveau onbekend

Tabel 2 – Kennisniveau van specialisten die bij het verzorgen van de continuïteit van de softwaregebruiker betrokken zijn. Hoe scoort u?



De juridische basis onder informatie beveiliging

Kwaliteit risico beperkende maatregelen

Hoewel de basisprincipes ervan in een aantal zinnen kenbaar kunnen worden gemaakt, is het opzetten van een kwalitatief hoogwaardige broncode-escrowregeling een proces waaraan veel haken en ogen zitten. In het hierboven aangehaalde artikel van Hoogendoorn zijn deze reeds aangekaart.
Desalniettemin nemen software gebruikende organisaties nog steeds genoegen met een escrowregeling waarvan het onzeker is of deze de nagestreefde continuïteit kan bieden op het uur van de waarheid. Een oorzaak hiervan is, dat uit het oog wordt verloren dat het verzorgen van die continuïteit voor een belangrijk deel een juridische

aangelegenheid is. Softwaregebruikers moeten er namelijk voor zorgen dat zij een zodanige relatie met hun leverancier hebben, dat zij het recht hebben om voor hun eigen continuïteit te zorgen. Dit klinkt vreemd, maar de logica zit hem in het feit dat voor het verzorgen van die continuïteit de softwaregebruiker moet kunnen beschikken over materiaal waarvan de softwareleverancier (auteurs) rechthebbende is. Hiervoor heeft de softwaregebruiker zoals gemeld toestemming nodig, minimaal in de vorm van een gebruiksrecht. Maar wat is die toestemming waard in het geval waarin deze niet kan worden afgedwongen?

De relevantie van deze vraag blijkt onder andere uit het door de Hoge Raad gewezen Nebula-arrest. [3] Hetgeen in dit arrest is bepaald, wordt door juristen beschouwd als een belangrijke graadmeter voor het vaststellen van de kwaliteit van de maatregelen die zijn getroffen om de continuïteit van softwaregebruik te waarborgen [o.a. Neppelenbroek, 2011]. De Hoge Raad oordeelde dat het een curator is toegestaan om de lopende obligatoire overeenkomsten van een gefailleerde niet meer na te komen, zonder dat de wederpartij daarbij recht heeft op schadevergoeding. Gelet op de in dit artikel besproken materie, zou men bij dergelijke overeenkomsten kunnen denken aan onderhoudscontracten en SLA's. In de literatuur wordt echter in het algemeen aangenomen dat een licentieovereenkomst, waarin een gebruiksrecht op auteursrechtelijk beschermd materiaal wordt verstrekt, ook kan worden gewanpresteerd door de curator. De curator zou hierbij bijvoorbeeld baat kunnen hebben op bijvoorbeeld het moment dat hij het auteursrecht, zonder dat het bezwaard is met licenties, wil verkopen aan een derde partij.

Op het moment dat een curator met het Nebula-arrest in de hand besluit een softwarelicentieovereenkomst niet meer na te komen, kan de situatie ontstaan waarin de escrow agent het broncodemateriaal afgeeft, maar waarin het tevens de softwaregebruiker niet meer is toegestaan om de software te gebruiken. Dat voor het treffen van maatregelen ten behoeve van de continuïteit van softwaregebruik de toestemming van de houder van het auteursrecht noodzakelijk is, bedreigt overigens ook op andere manieren het succes van broncode-escrow. Zo komt het voor dat degene die het broncodemateriaal aan de escrow agent in bewaring heeft gegeven daartoe niet bevoegd is, omdat het auteursrecht bij een andere partij ligt.

> Continuïteit is alleen mogelijk wanneer de softwaregebruiker een stevige rechtspositie voor zichzelf creëert

Uit de praktijk blijkt dat softwaregebruikers onvoldoende bewust zijn van de nadelige gevolgen die de auteursrechtelijke bescherming van software heeft voor de mogelijkheden tot het bestrijden van continuïteitsrisico's. Datzelfde geldt helaas ook voor een aantal escrowdienstverleners. Dat is begrijpelijk, want het betreft ingewikkelde juridische materie. Het is echter voor softwaregebruikers essentieel dat de getroffen maatregelen de continuïteit van het gebruik, het onderhoud en de doorontwikkeling van hun bedrijfskritische programmatuur daadwerkelijk waarborgen. Dit niet alleen tijdens de (contract)relatie met hun leverancier, maar juist ook na het wegvallen van laatstgenoemde. Dat kan alleen wanneer de softwaregebruiker een stevige rechtspositie voor zichzelf creëert.

Slotopmerkingen

Hoewel met dit artikel wordt gevraagd om meer aandacht te besteden aan het feit dat voor het verzorgen van de continuïteit van softwaregebruik ook juridisch verantwoord moet worden gehandeld, laat dit onverlet dat ook technici een stevige vinger in de pap moeten hebben. Het is immers voor een softwaregebruiker ook nutteloos wanneer hij gerechtigd is tot het gebruik van een afgegeven broncode, maar hij slechts de beschikking heeft gekregen over een verouderde versie omdat de escrow agent heeft nagelaten een verificatie uit te voeren. Dat is tevens het geval wanneer het broncodemateriaal van een cloudoplossing aan een escrow agent in bewaring wordt gegeven, zonder dat door een informatiebeveiliger is vastgesteld of risico op de onbeschikbaarheid van de met dergelijke programmatuur verwerkte gegevens wel voldoende is afgedekt.

Net als in de vakgebieden van de informatiebeveiliging en informatietechnologie het geval is, volgen de ontwikkelingen in de wereld van het recht zich in een hoog tempo op. Daarnaast is het velen niet gegund om specialist te zijn op al deze drie arbeidsvelden. Het verzorgen van de continuïteit van softwaregebruikers is daarom een doorlopend proces waarbij samenwerking tussen IT-notarissen, informatiebeveiligers, IT-specialisten en IT-juristen is geboden. ●

Literatuur

J.Ph. Hoogendoorn, De effectiviteit van broncode-escrow, *Informatiebeveiliging*, december 2004.
E.D.C. Neppelenbroek, De softwaregebruikslicentie bij de overdracht van het auteursrecht en in het faillissement van de licentiegever, *Tijdschrift voor Insolventierecht* 2011/25.

Referenties

1. *www.it-notaris.nl*
2. *Zie http://www.rijksoverheid.nl/documenten-en-publicaties/besluiten/2010/11/09/algemene-rijksvoorwaarden-bij-it-overeenkomsten-2010-arbit.html .*
3. *HR 3 november 2006, RvdW 2006, 1033 .*

EEN MOBILE DEVICE MANAGEMENT OPLOSSING VOOR ELK WERKPROCES?

Herman Thijssens, Business Consultant bij mITE Systems. mITE is specialist op het gebied van enterprise mobility oplossingen voor bedrijven. mITE biedt advies, consultancy, implementatie en operationeel management van smartphones, tablets, mobiele applicaties en "bring-your-own-device" (BYOD). Herman is bereikbaar via h.thijssens@mite.nl.

Mobile Device Management (MDM) is momenteel een hot topic bij veel bedrijven. Dit wordt mede veroorzaakt door het feit dat bij veel organisaties het management iPads gebruikt of wil gaan gebruiken om gemakkelijk te kunnen vergaderen of om op een eenvoudige manier bij zakelijke informatie te komen. Daarnaast wordt er bij steeds meer organisaties de vraag gesteld door de medewerkers of zij toegang kunnen krijgen tot bedrijfsgegevens zoals e-mail, agenda en contactpersonen op de reeds privé aangeschafte smart devices. In dit artikel bespreken we welke mogelijkheden organisaties hebben om de veiligheid van de zakelijke gegevens te waarborgen als het om smart devices gaat.

Bedrijfsgegevens kunnen worden gecategoriseerd op basis van gevoeligheid van de inhoud. In veel gevallen is dit procesmatig en op papier ingericht, in sommige gevallen wordt het ook al softwarematig opgepakt. Vanwege het feit dat de huidige smart devices de softwarematige kant van het categoriseren nog niet ondersteunen, zal je als organisatie moeten bekijken hoe je met de gevoeligheid van gegevens op een smart device omgaat. Wordt alle informatie, die op een smart device wordt gezet, als vertrouwelijk beschouwd of juist als interne informatie. De verwachting is dat Mobile Device Management oplossingen dit pas goed kunnen oppakken wanneer er een standaard voor dataclassificatie aanwezig zal zijn. Hiermee rijst wel de grote vraag hoe je als organisatie je data kan beschermen op al deze smart devices.
Als organisatie blijf je uiteindelijk verantwoordelijk voor eventueel dataverlies, tenzij er bewezen kan worden dat de werknemer opzettelijk data gelekt heeft. Dat is in veel gevallen zeer moeilijk te bewijzen.

Lagen van beveiliging
Veel organisaties besteden traditioneel vooral aandacht aan het beveiligen van de backend systemen. Dit terwijl ook de overige lagen van beveiliging zeker aandacht kunnen gebruiken. De gebruikers zijn getraind, er is awareness gecreëerd en er zijn goede procedures opgesteld. Daarnaast is de fysieke toegang ook goed geregeld door middel van o.a. toegangspasjes. Ook de firewall en netwerk-segmenten zijn goed ingericht. Op de servers draait up-to-date antivirus software, de allernieuwste patches zijn geïnstalleerd en de servers zijn gehardend. Daarnaast wordt voor verbindingen SSL, TLS, IPSec of aanverwante techniek gebruikt, een gebruikersnaam / wachtwoord voor applicaties en eventueel wordt er data-classificatie toegepast. Hiermee is de beveiligingscirkel redelijk rond.

> Welke mogelijkheden hebben organisaties om de veiligheid van hun gegevens te waarborgen?

Waar veel organisaties echter aan voorbij gaan is hoe dit in te regelen is voor de smart devices die de organisatie binnenkomen. Desktops zijn vaak op een vergelijkbare manier beveiligd zoals hierboven is beschreven, bij smart devices is dat meestal anders. Wat beveiliging betreft zijn deze smart devices niets anders dan kleine, beveiliging-technisch zwakke, werkplekken. Ze kunnen eenvoudig verloren raken of gestolen worden, terwijl er in veel gevallen veel zakelijke informatie op aanwezig is. Er wordt aan veel beveiligings-aspecten vaak voorbij gegaan. Al met al een broeinest voor ongelukken met bedrijfsinformatie. Aan de achterkant wordt alles dichtgetimmerd om vervolgens informatie aan de voorkant de organisatie uit te laten lekken. Wij zien dit in de praktijk erg vaak gebeuren.

Eén van de zaken waar bij het beveiligen van smart devices rekening mee gehouden moet worden zijn de verschillende platformen. Op iOS zijn beveiligings-gerelateerde zaken anders te regelen dan op Android. Daarnaast is er bij elke organisatie ook de discussie tussen veiligheid en gebruiksvriendelijkheid. Deze twee gaan hierin niet samen, dus zal er, afhankelijk van de mate van informatiebeveiliging, een middenweg gekozen worden. Hier kan Mobile Device Management (MDM) bij helpen.

Het beveiligen van zakelijke informatie door middel van MDM
Grofweg genomen zijn er een tweetal

manieren om informatie op smart devices te beveiligen: Alle bedrijfsdata in een afgeschermde zakelijke container plaatsen, of de bedrijfsdata aanbieden aan de eindgebruikers via de native applicaties van de smart devices. Uit de praktijk is gebleken dat in bijna alle gevallen een VDI omgeving niet werkt voor smart devices. Uit beveiligingsoogpunt is een volledige zakelijke container interessant, maar vanuit gebruiksgemak gezien, scoren de native applicaties hoger. Er is dan namelijk geen limitatie met betrekking tot ondersteunde bestandsformaten of e-mailplatformen.
Vanwege deze vraag naar gegevensbescherming is voor veel organisaties een mix van beide beveiligingsimplementaties de betere keus. Er kan dan afhankelijk van functieprofiel of data classificatie gekozen worden voor één van beide opties of voor een hybride vorm.
Momenteel is het voor de meeste MDM oplossingen noodzakelijk om een MDM cliënt / profiel te installeren op smart devices alvorens beveiligingsmaatregelen van kracht kunnen worden. Op deze manier kan de MDM de management API's aanspreken die door de OS leveranciers worden aangeboden. In het geval van Android kunnen ook de API's van hardware fabrikanten aangesproken worden indien de MDM oplossing dat ondersteunt.
Onderdelen van basis MDM functionaliteiten zijn o.a. device inventory, lock, unlock, wipe en password/pincode policy. Dit is voor alle MDM aanbieders hetzelfde, aangezien zij allen gebruik maken van de API's van de smart device OS fabrikanten zoals Apple (iOS) en Google (Android). Het is wat de MDM's daarnaast aanbieden wat het verschil maakt.

De laatste jaren zijn er vele MDM oplossingen bijgekomen, omdat het een interessante markt is en de strijd om de meeste klanten nog niet gestreden is. Daarnaast zijn er een flink aantal MDM partijen overgenomen of gestopt. Er zijn echter een paar MDM oplossingen die momenteel het verschil maken in de markt. Deze MDM partijen bouwen vele extra functionaliteiten bovenop de standaard Exchange ActiveSync mogelijkheden die reeds bij veel organisaties aanwezig zijn.

Huidige processen
In de meeste gevallen is de eerste vraag die bij IT terecht komt de vraag om e-mail te ontsluiten naar iPads / iPhones. Vaak komt deze vraag vanuit het management met daarbij de wens dat het al snel mogelijk moet zijn.
De tweede vraag die hierop redelijk snel volgt, is het kunnen bekijken van interne documenten op de fileserver / sharepoint. Daaruit afgeleid volgt de vraag om deze documenten ook daadwerkelijk te kunnen bewerken en te delen met anderen. Ook komt als tweede of derde vraag naar voren om bedrijfsprocessen te "verAPPen".
Dit alles brengt de security officer bij veel bedrijven in een moeilijk pakket. Hoe kan het management tevreden gehouden worden, maar tegelijkertijd toch de garantie hebben dat het bedrijf niet negatief in het nieuws komt vanwege onbedoeld gegevensverlies.

> Als organisatie blijf je uiteindelijk verantwoordelijk voor eventueel dataverlies

Vanwege het beveiligingsvraagstuk met betrekking tot smart devices en bedrijfsinformatie bieden MDM oplossingen een aantal functionaliteiten om de beveiliging en inzet van smart devices in organisaties te verbeteren.
Dit is niet alleen interessant voor zakelijke smart devices, maar zeker ook voor het BYOD vraagstuk.
De volgende functionaliteiten beschrijven mogelijkheden waar MDM een organisatie kan helpen.

Enterprise AppStore
Met een Enterprise AppStore is het mogelijk om eigen ontwikkelde applicaties aan te bieden aan de eigen medewerkers. Ook is het hiermee mogelijk betaalde applicaties aan te bieden aan de medewerker zonder dat de gebruiker daar zelf voor hoeft te betalen. Dit is in de meeste gevallen volledig controleerbaar via Active Directory groepen, zodat ook het beheer hiervan via de standaard

ingerichte procedures kan blijven lopen. Aangezien zakelijke applicaties een volgende stap voor veel organisaties is, is het raadzaam al wel naar de mogelijkheden te kijken bij het maken van een keuze voor een MDM. Dit voorkomt frustratie op een later tijdstip vanwege een verkeerde keus. Daarnaast zijn er bedrijven op de markt die zich volledig richten op het aanbieden van Enterprise applicaties op smart devices. Deze oplossingen gaan weer een stap verder dan dat de huidige MDM leveranciers aanbieden.

Pincode / Password Policy
De password policy is één van de standaard mogelijkheden van het Exchange ActiveSync Protocol. MDM oplossingen kunnen de configuratie per AD groep laten verschillen en daadwerkelijk geautomatiseerde acties ondernemen indien de gebruiker niet voldoet aan de gestelde eisen. Verschillende beveiligingseisen zijn hiermee te forceren. Afhankelijk van de eis van de organisatie is dit beveiliging op het hele toestel of alleen op de zakelijke container.

Sandboxing / Containerization
Sandboxing is het aanbieden en opslaan van bedrijfsgegevens en -applicaties binnen een afgeschermde en beveiligde zakelijke container. Sommige MDM oplossingen kunnen deze optie aanbieden. Denk hierbij bijvoorbeeld aan Sharepoint informatie of e-mail, eventueel in combinatie met attachments. Vervolgens kan de organisatie bepalen welke informatie uit deze container gehaald mag worden door de gebruiker.
Wat betreft containerization zijn er veel verschillende insteken die MDM aanbieders volgen. Sommigen bieden alle informatie vanuit de sandbox aan (e-mail, kalender, contactpersonen, Sharepoint, applicaties, etc), terwijl anderen hier weer een hybride model voor hanteren, zoals bijvoorbeeld attachments en Sharepoint informatie vanuit de sandbox, maar wel gebruik blijven maken van de native, gebruiksvriendelijke applicaties die reeds aanwezig zijn op de smart devices. Momenteel is er een verschuiving gaande richting dit hybride model door een aantal MDM partijen.

> Qua beveiliging zijn smart devices kleine, technisch zwakke, werkplekken

Encryptie
Encryptie is een heikel punt voor veel bedrijven aangezien dit kan verschillen per toestel. Bij BYOD is het met betrekking tot Android devices goed om te weten dat het merendeel van de huidige smart devices in handen van de consument nog geen encryptie ondersteunt. Om deze smart devices geschikt te maken voor zakelijke informatie dienen aparte applicaties gebruikt te worden. Containerization is voor deze type smart devices ook een mogelijkheid. Indien mogelijk adviseren wij om als basis de meest recente versie van een OS te ondersteunen. In veel gevallen zal dit in de praktijk echter een paar oudere versies bevatten.

> Rekening houden met verschillende platformen

"Zero Footprint"
Controle over bedrijfsinformatie is belangrijk, zeker in het geval van een BYOD.
Indien een medewerker met een eigen toestel zakelijke informatie gebruikt, is het voor bedrijven belangrijk om de mogelijkheid te hebben (gevoelige) bedrijfsinformatie van het toestel te kunnen verwijderen indien de medewerker het bedrijf verlaat.

Dit zonder daadwerkelijk het hele privé toestel volledig leeg te gooien. Hierover zullen goede afspraken gemaakt moeten worden met de eindgebruiker in geval van een BYOD.

Certificaten
Sommige MDM's hebben de mogelijkheid automatisch certificaten aan te vragen bij de interne Certificate Authority en deze uit te rollen naar de toestellen. Hierdoor kunnen smart devices user-based certificaten gebruiken voor VPN, WiFi en Exchange authenticatie. Indien dit volledig automatisch wordt uitgerold naar de smart devices heeft de gebruiker geen last meer van het wijzigen van het wachtwoord in geval van een AD wachtwoord change. (Kerberos). De uitrol van deze certificaten kan bepaald worden door het lidmaatschap van een AD groep waardoor het beheer hiervan vereenvoudigd wordt. We zien steeds meer organisaties die op deze manier een extra laag van beveiliging aanbrengen op Exchange ActiveSync.

Kiosk Modus
Organisaties kunnen er belang bij hebben om een smartdevice volledig af te sluiten voor persoonlijke applicaties. Field Service smart devices zij hier een goed voorbeeld van. IT kan vervolgens volledig bepalen welke applicaties en instellingen benaderd kunnen worden door de medewerker, waardoor het voor een servicedesk eenvoudiger is deze smart devices te beheren en problemen op te lossen.

Geautomatiseerde Events
Door middel van een geautomatiseerd event is er de mogelijkheid de gebruiker of beheerder op de hoogte te stellen indien een smartdevice buiten beleid valt. Op basis hiervan kunnen automatische acties worden gestart zoals het in quarantaine zetten van de zakelijke informatie totdat de gebruiker weer voldoet aan het gestelde beleid.

Verschil maken tussen zakelijke en privé smart devices
Met MDM is het mogelijk onderscheid te maken tussen zakelijke en privé smart devices. In geval van een gebruiker met zowel een zakelijk als privé toestel kan er onderscheid gemaakt worden welke zakelijke informatie bekeken kan worden. Zo kan bijvoorbeeld een privé smartdevice geen toegang hebben tot Sharepoint data en een zakelijk device wel.

Cisco ISE
Cisco ISE koppelt met MDM om real time informatie van het netwerk, de gebruikers en smart devices te verkrijgen en op basis hiervan te handelen. Op deze manier is het mogelijk om op basis van policies controle uit te oefenen of smart devices bij de opgevraagde bedrijfsinformatie mogen komen.

Conclusie
Veel organisaties kunnen, wat betreft de hele mobility shift, nog grote slagen maken op het gebied van het beveiligen van bedrijfsgevoelige informatie op smart devices. Organisaties hebben vaak niet in de gaten welke beveiligingsrisico's er momenteel gelopen worden door enkel ActiveSync toegang te activeren. De vraag naar e-mail ontsluiting is in de meeste gevallen de eerste stap om zakelijke informatie op een smart device beschikbaar te maken. De stappen daarna, zoals het aanbieden van zakelijke documenten op applicaties, zullen vroeg of laat een keer gaan volgen. Om toch duidelijk te houden waar zakelijke informatie zich bevindt en om hier controle over te hebben is het inzetten van een MDM oplossing vanzelfsprekend.

> MDM oplossingen zijn nog lang niet uitontwikkeld

MDM oplossingen zijn nog lang niet uitontwikkeld. Daarnaast ontwikkelen MDM oplossingen ook vaak verschillende richtingen op. Hierdoor is het ook belangrijk een goede keuze te maken en in alle gevallen ook naar de mobility roadmap van de eigen organisatie te kijken. Aan de hand hiervan kan vaak een juiste MDM oplossing gekozen worden.

Wij verwachten dat er een shift zal gaan plaatsvinden van het beheren van het toestel naar het beheren van de data. Dit gaat echter pas goed doorgang vinden zodra er een duidelijk standaard is op basis waarvan de MDM's hun ontwikkelingen kunnen vervolgen. MDM zal dan veranderen van Mobile Device Management naar Mobile Data Management. ●

COLUMN

TIEN ZAKEN DIE U MOET WETEN OVER UW GRONDRECHT OP PRIVACY

Opdat u in het nieuwe jaar goed beslagen ten ijs kan komen en zonder al te veel geglibber kan voorkomen dat u onderuitgaat, start ik 2013 met een lijstje van tien wetenswaardige zaken over het grondrecht op privacy.

1. Het grondrecht op privacy is vastgelegd in art. 10 Nederlandse Grondwet, art. 7 European Charter of Fundamental Rights, art. 8 Europees Verdrag voor de Rechten van de Mens, art. 17 Internationaal Verdrag van Burger en Politieke Rechten.
2. De tekst van de Nederlandse Grondwet luidt als volgt: "Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer".
3. Het grondrecht op privacy voorziet in beginsel alleen op verticale verhoudingen. De grondrechten zijn geformuleerd als rechten voor burgers ten opzichte van haar overheid. Het is de overheid niet toegestaan in die fundamentele rechten te treden, tenzij daarin bij wet is voorzien en de rechten van burgers worden gewogen tegen de ernst van de inbreuk. In beginsel kunt u daarom het grondrecht niet inzetten in horizontale verhoudingen (private partij vs. private partij). Echter, van het EVRM is wel horizontale werking aangenomen, in juridische geschillen tussen private partijen wordt daarom doorgaans een beroep gedaan op het EVRM en niet op de Nederlandse Grondwet.
4. Het Europese Hof voor de Rechten van de Mens heeft in bepaalde gevallen geoordeeld dat bescherming van de identiteit van personen ook onder het EVRM valt. Vaak gaat het daarbij over geschillen met betrekking tot de naam van personen of over familierecht. Een recht op bescherming van de identiteit als zodanig is echter nooit erkend.
5. Juridisch gezien omvat het recht op privacy drie elementen: het huis, het gezinsleven en de correspondentie. In combinatie met de lichamelijke integriteit vormen deze de kernelementen van het recht op privacy. Het grondrecht op privacy is dus breder dan alleen de bescherming van informatie van personen. Het dataprotectie recht is daarmee dan ook slechts een klein onderdeel van privacy in de juridische zin van het woord.
6. De Amerikanen kennen binnen de Constitution geen recht op privacy. Zij leiden echter wel een recht op privacy af uit het first en fourth ammendment. Dit afgeleide recht ziet alleen op verticale verhoudingen (de overheid vs. burgers). Als Europeaan heeft u hier echter niets aan, het afgeleide privacyrecht geldt alleen voor Amerikaanse staatsburgers.
7. Indien de overheid een privacy invasieve maatregel wil uitvoeren dan dient zij dit naar voorbeeld van het EVRM volgens drie stappen te toetsen om te bezien of het toegestaan is. A) er dient een wettelijke grondslag te zijn. B) de gewenste maatregel moet maatschappelijk gezien noodzakelijk zijn. C) de maatregel dient proportioneel (is de maatregel niet te zwaar voor het doel dat men wil bereiken?) en subsidiair (kan het doel op een minder invasieve manier bereikt worden?) te zijn.
8. Naar algemeen aangenomen in wetenschappelijke kringen zijn Warren en Brandeis (twee Amerikaanse rechters) de eersten die een recht op privacy omschreven. In 1890 publiceerden zij een artikel waarin zij het recht op privacy omschreven als 'het recht om met rust gelaten te worden' ('the right to be let alone').
9. Vooralsnog valt een emailbericht niet onder de bescherming van correspondentie. In artikel 13 van de Nederlandse Grondwet staat momenteel nog het zogenaamde 'brief, telefoon en telegraafgeheim'. Dat moet zeer letterlijk worden genomen, een brief betekent dus de enveloppe met het papier erin. Een wijziging is echter op komst, het kabinet heeft aangegeven het artikel meer in overeenstemming met de huidige communicatievormen te willen brengen. Overigens, dit terzijde, het briefgeheim strekt zelfs zover dat het echtgenoten niet toegestaan is elkaars post open te maken…
10. Als laatste geef ik u een vraag mee om te overdenken. De bescherming van het huis moet juridisch gezien even letterlijk genomen worden als het briefgeheim. Het is niet toegestaan uw bakstenen huis binnen te treden. Gezien de ontwikkelingen in het digitale tijdperk waarin steeds meer mensen de online wereld als een woonkamer gaan gebruiken (soms zelfs achter digitale sloten); is het dan niet eens tijd voor een digitaal huisrecht?

Dat 2013 voor u allen maar een mooi jaar mag worden met weinig inbreuken op uw privacy, en mocht het dan toch nog gebeuren… dan hoop ik dat u met het bovenstaande een beetje munitie erbij heeft gekregen in het arsenaal om te ageren tegen de erosie van het grondrecht op privacy. ●

Mr. Rachel Marbus, @RachelMarbus op Twitter

CYBER RESILIENCE IN DE BESTUURSKAMER

THE GRAND CONFERENCE IN AMSTERDAM

Marieke Klaver is R&D programmamanager Cyber Security bij TNO.
Zij is te bereiken via marieke.klaver@tno.nl

Op 16 oktober 2012 vond in Amsterdam The Grand Conference plaats. Deze conferentie werd georganiseerd door het Centre for the Protection of National Infrastructure (CPNI.NL) in nauwe samenwerking met de Europese Commissie, de Europese Network and Information Security Agency (ENISA), het Amerikaanse Department of Homeland Security (DHS) en het World Economic Forum (WEF). Het thema was 'Building a Resilient Digital Society'. De internationale conferentie was gericht op de top van het bedrijfsleven, overheden en andere organisaties en trok ruim tweehonderd deelnemers uit tweeëntwintig landen.

The Grand Conference was een activiteit van de gezamenlijke EU - VS werkgroep op het gebied van cyber security en cybercrime. Deze werkgroep richt zich onder andere op informatie-uitwisseling, kennisdeling en samenwerking op het gebied van veiligheid van Industrial Control Systems (ICS), procescontrolesystemen, en Smart Grids. Deze procescontrole-systemen spelen in het functioneren van een groot deel van onze vitale infrastructuur, zoals bijvoorbeeld elektriciteitsnetwerken, drinkwater- en waterbeheersystemen en tunnelveiligheid, een belangrijke rol. Daarom is het van groot belang dat de procescontrolesystemen voldoende robuust zijn tegen verstoringen.
De afhankelijkheden tussen (vitale) infrastructuren en de onderlinge connecties en afhankelijkheid tussen organisaties maken dit een gedeelde verantwoordelijkheid, die vraagt om samenwerking tussen landen, tussen overheden en private partijen en tussen leveranciers en gebruikers van deze systemen.
De conferentie was er op gericht om de verschillende aspecten van het creëren van een veilige en robuuste digitale samenleving te belichten. Beginnend bij de kansen die de toenemende connectiviteit biedt, via mogelijke bedreigingen naar oplossingsrichtingen op het gebied van risicomanagement, organisatorische strategieën en het inzetten van economische prikkels om het doel te bereiken.

> De conferentie was gericht op de top van het bedrijfsleven en trok deelnemers uit 22 landen

Na de opening door organisator Annemarie Zielstra, director van CPNI.NL, schetste Harry van Dorenmalen, voorzitter van IBM Europa, een positieve toekomstvisie rond de rol van ICT in 2030 en de mogelijkheden die dit de maatschappij gaat bieden. Mikko Hypponen, Chief Research Officer van F-Secure, schetste juist de duistere kant van cyberspace en ging in op de vele spelers die misbruik proberen te maken van de toegenomen connectiviteit van organisaties. Het grootste gevaar ziet hij komen van door staten gesponsorde aanvallen; hij acht het voor organisaties heel moeilijk om zich te verdedigen tegen "James Bond" gewapend met USB-stick. Mike Maddison (Deloitte), Rod Beckstrom (voormalig CEO van ICANN) en prof. Michel van Eeten (TU Delft) belichtten de eerdere geschetste oplossingsrichtingen. 's Middags vonden er masterclasses plaats op het gebied van risicomanagement voor ICS en Smart Grids, crisiscommunicatie/ reputatiemanagement en ICS Security voor managers. Met name de live hack demo door het gouden CyberLympics-team van Deloitte maakte veel indruk op de aanwezigen.

> Het grootste gevaar komt van door staten gesponsorde aanvallen

Cyber Resilience manifest
Vanwege het grote economische belang van cyber security was het World Economic Forum (WEF) één van de partners van de conferentie. Vanuit het WEF wordt fors ingezet om het onderwerp cyber resilience op de agenda van iedere bestuurskamer te krijgen, aangezien zij zien dat in een "hyperconnected world" een weerbaar cyberdomein van cruciaal belang is voor het functioneren van organisaties. Hiertoe heeft het WEF een manifest ontwikkeld met de titel "Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World - Principles and Guidelines"[1]. Dit manifest bevat richtlijnen en principes voor de inbedding van cyber resilience tot op het hoogste niveau binnen organisaties. De principes die de WEF heeft gedefinieerd, luiden:

- De organisatie erkent de onderlinge afhankelijkheden in deze hyper-connected wereld en zijn eigen rol

Ondertekening Cyber Resilience manifest

om bij te dragen aan een veilige digitale omgeving.

- Het managementteam van de organisatie is zich bewust van haar leidende rol bij het uitdragen en organiseren van cyber resilience.
- De organisatie erkent het belang van het integreren van cyber risicomanagement binnen de algemene risico afwegingen en volgt hierbij de beschreven richtlijnen en principes.
- De organisatie stimuleert zijn afnemers om deze richtlijnen en principes ook te volgen.

Het WEF promoot dit manifest als middel om de dialoog rond cyber resilience binnen organisaties op gang te brengen en om het commitment op bestuurskamer niveau te bestendigen. Tijdens de conferentie toonden bestuurders van Alliander, KPN en TNO dit commitment door publiekelijk het WEF-manifest te ondertekenen.

In het slotgedeelte van The Grand Conference onderstreepte Mark Dierikx, directeur-generaal van het Ministerie van Economische Zaken, Landbouw en Innovatie, het belang dat zijn ministerie hecht aan een goede en betrouwbare cyberinfrastructuur. De conferentie werd afgesloten met een speech van Eurocommissaris mevrouw Kroes.

Zij constateerde dat er een toename is in zowel aantal als ernst van cyberincidenten. De EU is daarom bezig haar inspanningen op het gebied van digitale veiligheid te versterken door het uitbrengen van een Europese Cyber Security Strategie. De strategie beschrijft de noodzaak van internationale samenwerking tussen de EU landen. De ICT infrastructuur en de aanvallen daarop houden zich immers niet aan landsgrenzen. De Europese Commissie streeft daarom naar een versterking van het niveau van digitale bescherming in alle EU landen. Daarnaast ziet zij samenwerking met de verschillende partijen uit de vitale infrastructuur als essentieel. Het gaat hierbij bijvoorbeeld over transport, energievoorziening, gezondheidszorg en de financiële sectoren. Publieke en private partijen binnen deze sectoren moeten gezamenlijk optrekken, waarbij ieder zijn verantwoordelijkheid neemt.

Een weerbaar cyberdomein is cruciaal voor het functioneren van organisaties

Publieke en private partijen moeten gezamenlijk optrekken

Eurocommissaris mevrouw Kroes

De verantwoordelijkheid voor cyber security ligt volgens de Eurocommissaris niet alleen bij bedrijven en overheden, maar ook bij iedere ICT gebruiker. Er zijn simpele maatregelen die iedereen afzonderlijk zelf kan nemen. Europa heeft daarom oktober als European Cyber Security Month ingesteld om de thuisgebruikers in de veiligheidsdiscussie te betrekken. Tenslotte noemde mevrouw Kroes internationale samenwerking met landen buiten de EU als essentieel onderdeel: "It's time to give cyber-security the attention it deserves. Let's be strategic, let's work together, and let's ensure we protect our infrastructure, and our citizens, in the digital age".

Als invulling van deze oproep tot samenwerking vond één van de hoofdbestanddelen van de conferentie 's avonds plaats. Een select gezelschap van rond de veertig topbestuurders ging tijdens een walking dinner aan de hand van een drietal toekomstscenario's concreet met elkaar aan de slag, om ook op bestuurskamer niveau het cyber security netwerk te bouwen en input te leveren voor de WEF-bijeenkomsten in december (Dublin en Washington) en januari (jaarlijkse conferentie wereldleiders in Davos). Duidelijk werd dat het tonen van leiderschap in de top van de organisaties cruciaal is om de digitale weerbaarheid van onze maatschappij verder te verhogen. De overheid moet daarbij de private sector faciliteren, stimuleren en belemmeringen wegnemen. Deze conferentie is een eerste opstap naar structurele discussies tussen publieke en private partijen over cyber resilience en de weg om dat te bereiken.

De conferentie kan met recht een succes genoemd worden wanneer deze vervolgacties concreet worden opgepakt en leiden tot meer commitment voor cyber resilience in de bestuurskamer. Eén succes is al binnen: namens de Europese Commissie gaf mevrouw Kroes haar steun aan de organisatie van een vervolg conferentie in 2013, The Grand Conference 2013.

U en uw organisatie zijn aan zet

Ook u en uw organisatie kunnen nu al aan de slag. Op de Cyber Resilience website van CPNI.NL [2] kunt u meer informatie vinden over cyber resilience. Daar vindt u onder andere een verzameling met bewustwordingsmateriaal, een database met verschillende incidenten en een C-suite executive checklist op basis van de WEF-principes. Door het invullen van de vragenlijst krijgt u een overzicht van het cyber resilience volwassenheidsniveau van uw organisatie en hoe dit zich verhoudt tot andere organisaties. Bij een interactieve sessie met de deelnemers aan de conferentie, bleken de aanwezige organisaties bovengemiddeld te scoren daar waar het gaat om hun eigen volwassenheid. Daar waar het ging om zicht op de hele toeleveringsketen bleek dit beduidend minder goed geregeld. Gebruik de tools om te bepalen waar uw organisatie staat en (indien nodig) uw eigen digitale weerbaarheid te vergroten. ●

(Dit artikel is eerder verschenen in het managementblad Beveiliging)

Referenties

1. *World Economic Forum, Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World - Principles and Guidelines, on-line: http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf.*
2. *Meer over cyber resilience: www.cyber-resilience.org*

TEK TOK - SECURITY IN SHOWBUSINESS

Lex Borger is principal consultant bij Domus Technica.
Hij is te bereiken via lex.borger@domustechnica.com.

Voor wie de 'droge' professionele security bijeenkomsten niet meer zo aantrekkelijk vindt: er is nu Tek Tok. Néé, niet Tech Talk, maar gewoon Tek Tok. Volgens de organisatie gaat het over informatietechnologie, maar het gehalte informatiebeveiliging is hoog en het niveau is laagdrempelig. De toegang is gratis. Op 4 December werd Tek Tok voor de 3e keer gehouden, in het Paard van Troje in Den Haag. De security bijeenkomst is een uitje geworden...

Christian van 't Hof presenteert Tek Tok en doet dat op een manier alsof hij al jaren "The Price is Right" presenteert. Ook de ambiance in het theater en de professionele opname crew doen denken aan de televisiestudio's. Maar het is geen televisie, het is YouTube. En het publiek zit er niet om op commando te reageren met gelach of applaus, maar wordt door Christian betrokken. En dát kom je nou juist niet tegen bij andere security bijeenkomsten. Er is een prettig showbusiness sausje overheen gegoten.

> Er is een prettig showbusiness sausje overheen gegoten

Oplettende lezers kennen Christian van 't Hof van een artikel in dit blad uit 2011, "Tagology, één taal voor alles". Dit artikel behandelt een onderwerp dat niet direct security mainstream is, maar wat wel security raakt. Maar vergis je niet: Tek Tok zit veel dichter tegen de informatiebeveiliging aan. In ieder geval tot zover.

Hacking

De betrokkenheid van het publiek was er tijdens de eerste twee bijeenkomsten al geweest op een gevoelige manier: Onderzoeksjournalist Brenno de Winter had een Wifi hotspot opgesteld met een SSID "KPN" en "T-Mobile", twee favorieten van de meeste Nederlandse smartphones. Op deze avond geeft Brenno aan maar niet gekozen te hebben een Vodafone hotspot na te doen. Daarvoor in de plaats haalt Christian een geintje uit, waarvan de uitleg wat complexer is. Wie daar meer van wil weten moet maar de videobeelden van die avond bekijken. Gasten komen aan de lopende band het podium op. Ik noemde Brenno de Winter al - eigenlijk geen gast als je er elke keer bij bent. Hij stipt het actuele nieuws aan, in dit geval veel aandacht voor Henk Krol, die gearresteerd was voor het "hacken" van medische dossiers. Michael van der Vaart van Spicy Lemon stuurt een laptop het publiek in en laat aan het eind van de avond zien wat de besmettingsgevolgen waren - een dozijn of twee.

> Wel gedurfd, zo net nadat een politieman en officier op het podium hadden gestaan

Politie

Er zijn ook gasten vanuit de overheid: Michel Savelkoul, de ketencoördinator Meldpunt Identiteitsfraude, die vertelde over identiteitsfraude, vechtscheidingen en sterke en niet-zo-sterke wachtwoorden. En later op de avond betrekken Pim Takkenberg (teamleider High Tech crime, KLPD) en Lodewijk van Zwieten (landelijk Officier van Justitie

Fotografie: Dick Aalders

Vragen aan Brenno

Fotografie: Dick Aalders

Chris tussen Lodewijk van Zwieten (L) en Pim Takkenberg (R)

Fotografie: Dick Aalders

Jam op het podium

Cybercrime) het podium. Ze worden vakkundig ondervraagd door Christian, onder andere over de grenzen van ethisch hacken en responsible disclosure.

Als laatste kan Bart de Koning over zijn boeken vertellen, "De veiligheids-mythe" en "Operatie Blauw". Hij schetst hoe moeilijk het is om de politie te reorganiseren. Wel gedurfd, zo net nadat een politieman en officier op het podium hadden gestaan.

Muziek

Het geheel wordt opgeluisterd door de funk-band "Power to the Pipo". De muziek is aanwezig, maar niet overheersend en daarmee een prettige toevoeging aan de show. ●

Links

Homepage Tek Tok:
http://tektok.nl/index.php/tek-tok-late-night

Christian's Tagology artikel:
https://www.pvib.nl/download/?id=17678161

Centraal Meldpunt Identiteitsfraude:
http://www.overheid.nl/identiteitsfraude

Homepage Power to the Pipo:
http://www.myspace.com/powertothepipo

KENNISMAKING MET: ERWIN BOSMA

In 2001 ben ik de informatiebeveiliging ingerold, nadat ik eerst jarenlang betrokken was bij het technisch onderhoud van de Boeing 747. Als information risk manager ben ik begonnen bij het Corporate Information Security Office van de KLM. Om me te oriënteren op dit vakgebied werd ik destijds naar de Algemene Leden Vergadering van het Platform Informatiebeveiliging (PI) gestuurd, één van de voorgangers van het PvIB. Slechts een kleine groep oudere grijze mannen was aanwezig en de ALV was in mijn beleving niet dan meer een formaliteit.

Gelukkig was de daarop volgende activiteit bij en met de gemeente Delft wel inspirerend. Daarna heb ik nog veel bijeenkomsten meegemaakt, bijna altijd weer motiverend en georganiseerd door gedreven vrijwilligers. Dit samen met alle andere gemotiveerde vrijwilligers, die van het huidige PvIB een succes-volle vereniging maken, hebben mij aangestoken om hier een steentje aan bij te dragen. En nu ben ik zelf een van de ouderen die in het bestuur zitten. Gelukkig bestaat het bestuur nu niet meer alleen uit oudere grijze mannen, maar hebben we nu ook vrouwen en jongeren in het bestuur.

Na de KLM heb ik een aantal posities bij verschillende organisaties bekleed, waar ik de informatiebeveiliging op

Erwin Bosma

een hoger plan heb mogen brengen. Mijn belangrijkste doel hierbij is om informatiebeveiliging als toegevoegde waarde voor het bedrijf in te zetten en niet als doel op zich. Daarbij zoek ik naar pragmatische oplossingen en dat hoeft niet altijd te liggen in het implementeren van een tool.
In mijn huidige baan bij Holland Casino houd ik mij op corporate niveau ook weer bezig met informatiebeveiliging. Hierbij gaat mijn aandacht hoofdzakelijk uit naar het strategische en tactische deel van de beveiliging en dat strekt zich uit van kantoorautomatisering tot aan de slotmachines… ●

CLOUD SECURITY ALLIANCE

André Koot is board member van de Nederlandse afdeling van de CSA.
Daarnaast is hij zelfstandig gevestigd security consultant en redacteur van dit blad.

Als er één hype is die maar niet ophoudt om hype te zijn, dan is het wel cloud computing en met name cloud security. Welk congres je ook bijwoont, of welk vakblad je ook openslaat, cloud security is misschien wel het meest genoemde onderwerp. En dan met name omdat security volgens veel onderzoeken als grootste belemmering wordt gezien voor het op grote schaal outsourcen van diensten naar de cloud. En ook opvallend dat bijvoorbeeld een begrip als 'Patriot Act' als het gaat om security het meest genoemd wordt. Dat bleek onlangs ook bij het eerste EMEA congres van de Cloud Security Alliance in Amsterdam. De eerste vraag uit de zaal bij de eerste presentatie ging over de Patriot Act. Los van het feit dat dat natuurlijk een heel belangwekkend onderwerp is, is er wel meer te zeggen over cloud security. Maar laten we even bij het begin beginnen.

De Cloud Security Alliance is een non-profit organisatie die erop gericht is kennis te ontwikkelen op het gebied van beveiliging van en binnen de cloud.

> To promote the use of best practices for providing security assurance within cloud computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.
>
> *Missie-statement CSA*

Lekker breed, maar wel met enkele belangrijke aandachtspunten:

- Best practices
- Security Assurance
- Education

De leden van de CSA zijn allemaal professionals op het vakgebied die pogen om op een effectieve en efficiënte manier cloud security inzichtelijk en beheersbaar te maken. En iedereen kan gewoon lid worden. Lid worden van de LinkedIn groep van de CSA is voldoende. Vorig jaar is de Netherlands Chapter opgericht.

Doel van een Chapter is om de CSA dichter bij de leden te brengen, maar ook om specifieke kennis te (helpen) ontwikkelen. Doel van de Nederlandse afdeling is dan ook om te trachten de CSA kennis te verrijken vanuit de specifieke Nederlandse situatie, zoals daar zijn wet- en regelgeving. Als je lid bent van de LinkedIn groep van het Netherlands Chapter, dan ben je dus ook aangesloten bij het chapter.

Iedereen kan lid worden van CSA

Naast de individuele leden kent de CSA ook sponsors. De CSA heeft enkele full-time professionals in dienst en die kosten worden feitelijk opgebracht door de sponsors.

Risico's

Voordat je start met het ontwikkelen van hulpmiddelen is het verstandig om te analyseren wat nou precies het probleem is. In 2010 heeft CSA zelf een rapport opgesteld waarin de volgende dreigingen werden geïdentificeerd:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Interfaces and APIs
- Malicious Insiders
- Shared Technology Issues
- Data Loss or Leakage
- Account or Service Hijacking
- Unknown Risk Profile

Voor elk van deze dreigingen heeft CSA geanalyseerd waar het speelt (bijv. SAAS, PAAS of IAAS) en welke maatregelen getroffen zouden kunnen worden om de dreiging tegen te gaan. Maar zoals vaker voorkomt, zijn er meer instanties die dergelijke rapportages opstellen. Het goede nieuws is dat de CSA heeft besloten om te gaan samenwerken. Er zal vermoedelijk dan ook geen nieuwe eigen CSA dreigingenanalyse worden opgesteld, maar worden samengewerkt met bijvoorbeeld ENISA, dat zelf ook een cloud-risicoanalyse heeft opgesteld.

Best Practices

De CSA propageert het gebruik van Best Practices. Maar die moeten er dan dus wel zijn. Een belangrijke bestaansgrond van de CSA is dan ook het verzamelen en integreren van bestaande Best Practices tot een heel beveiligingsraamwerk. En natuurlijk levert dat ook wel een risico op: als de CSA zelf weer best practices beschrijft, staan die dan niet haaks op andere best practices, iedereen weet toch zelf wat het best is? We zijn

toch gewend het wiel steeds opnieuw uit te vinden en 'not invented here' is misschien wel de grootste oorzaak van kostenoverschrijdingen.

Binnen de CSA bestaat veel aandacht voor juist dat aspect. Hergebruik van bestaande best practices is een basis bij het ontwikkelen van eigen standaarden. Zo is elke best practice in beginsel te projecteren op bestaande andere best practices.

Werkgroepen

Dat werk wordt binnen de CSA uitgevoerd in de verschillende werkgroepen. Het volgende overzicht is verre van compleet, maar geeft ongeveer aan hoe divers het werkveld binnen cloud security is.

Cloud Controls Matrix

De belangrijkste best practice is misschien wel de Cloud Controls Matrix (CCM). Deze matrix lijkt natuurlijk heel veel op andere frameworks, met name op CobiT (4.1). De opbouw is ook vergelijkbaar: per beheersdoelstelling worden beheersmaatregelen opgesomd die passen bij een gedefinieerd volwassenheidsniveau. In de CCM zijn natuurlijk specifieke beheersmaatregelen voor cloud security opgenomen.

> De belangrijkste best practice is misschien wel de Cloud Controls Matrix (CCM)

Mobile Working Group
De CSA Mobile working group is verantwoordelijk voor onderzoek naar veilige mobiele gebruik van cloud.

Big Data Working Group
Big Data is de CSA werkgroep die best practices voor security en privacy in big data moet identificeren.

Privacy Level Agreement Working Group
Deze werkgroep ontwikkelt PLA sjablonen voor zelfregulering bij onder meer cloud providers op het gebied van privacybescherming.

Cloud Controls Matrix (CCM)
Security controls raamwerk voor cloud service providers en cloud gebruikers.

CloudTrust Protocol
Het CloudTrust Protocol (CTP) is een mechanisme waarmee cloudgebruikers inzicht krijgen in transparantie bij de cloud service providers.

Cloud Data Governance
Verantwoordelijk voor het ontwikkelen van Data Governance instrumenten binnen de cloud.

Trusted Cloud Initiative
Veilige identiteiten in de cloud.

Security as a Service
Deze werkgroep onderzoekt hoe security oplossingen in cloud service-modellen kunnen worden ingebed.

Telecom Working Group
Werkgroep die zich buigt over de securityaspecten van cloud en telecom.

Health Information Management
Deze werkgroep is gericht op het onderzoek naar security binnen de Health sector in de Cloud.

Niet alleen staan de beheersmaatregelen en de aspecten waarop deze van toepassing (infrastructuur, soort dienst) zijn vermeld, maar ook de mapping op externe baselines en benchmarks.
Een voorbeeld van een deel van de uitwerking van de CCM voor HR-01, HRM security – Background Screening:

"Pursuant to local laws, regulations, ethics and contractual constraints all employment candidates, contractors and third parties will be subject to background verification proportional to the data classification to be accessed, the business requirements and acceptable risk."
Deze beheersmaatregel is relevant voor het aspect: Data (dus niet voor bijv. fysiek of storage)
Relevant voor: Corporate Governance
Betreft zowel SAAS, PAAS als IAAS leveranciers en geldt voor zowel leveranciers als afnemers ('tenants')
Verwijzingen (niet uitputtend!)

- Cobit 4.1: PO 7.6
- Er is hiervoor geen specifieke verwijzing in HIPAA / HITECH act
- ISO 27001: A.8.1.2
- Nist800-53 R3: PS-2 en PS-3
- Ook verwijzing naar Jericho Commandment #2, #3, #6, #9

Security Assurance

Op het gebied van Security Assurance heeft de CSA onlangs misschien wel het meest innovatieve product gelanceerd, namelijk CSA Security, Trust & Assurance Registry, Star.
De Open Certification Framework werkgroep van CSA is verantwoordelijk voor ontwikkeling van het het CSA OCF raamwerk op basis waarvan cloud providers kunnen worden

Domain	Control Group	CID	Consensus Assessment Questions	AWS Response
Compliance	Audit Planning	CO-01.1	Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	AWS obtains certain industry certifications and independent third party attestations and provides certain certifications, reports and other relevant documentation directly to AWS customers under NDA.
Compliance	Independent Audits	CO-02.1	Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports?	AWS provides third party attestations, certifications, Service Organization Controls 1 (SOC 1) Type II report and other relevant compliance reports directly to our customers under NDA. AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership.
Compliance		CO-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	
Compliance		CO-02.3	Do you conduct regular application penetration tests of your cloud infrastructure as prescribed by industry best practices and guidance?	
Compliance		CO-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	

Tabel 1 - Amazon AWS questionnaire voor STAR

gecertificeerd en opgenomen in Star. De registratie houdt dus feitelijk in dat de provider voldoet aan de beheersmaatregelen conform de CCM. Om te kunnen worden opgenomen in Star, kunnen providers zelf de CSA Consensus Assessments Initiative Questionnaire invullen. Deze vragenlijst en de antwoorden van de betreffende provider worden gepubliceerd op de site van CSA en op de site van de provider zelf. Hierboven een voorbeeld van een deel van de ingevulde vragenlijst door Amazon voor de EC2 webdienst.

Audit

Natuurlijk is een self-assessment waardevol, maar controle is vaak nog beter. Maar zoals we wel weten staat niet elke provider erom te springen dat elke klant even binnenloopt om een audit uit te voeren. Mede om die reden is de CSA ook bezig met een audit framework. CSA CloudAudit wordt op dit moment ontwikkeld om Audit, Assertion, Assessment en Assurance (A6) van hun IaaS, PaaS en SaaSdiensten geautomatiseerd te kunnen laten uitvoeren door hun klanten. Dat zal gaan gebeuren via een veilige, open en uitbreidbare methode met een bijbehorende set van API's. Het product is nog niet beschikbaar, maar het wordt een nuttige aanvulling op het huidige instrumentarium.

> STAR registratie betekent dat de provider voldoet aan CCM

Opleiden

CSA is natuurlijk geen opleidingsinstituut, maar wat is een Amerikaans instituut zonder eigen certificering? Ook de CSA heeft dus een certificering, namelijk de 'Certificate of Cloud Security Knowledge', CCSK. Dit is een certificaat waarmee de kandidaat aantoont te beschikken over de kennis omtrent Cloud Security en met name de onderwerpen waarvoor de CSA best practices heeft geformuleerd. Inmiddels wordt de certificering al twee jaar aangeboden en is het ook mogelijk in Nederland trainingen te volgen.

EMEA Congres

Dit jaar vond het eerste CSA congres buiten Amerika plaats en wel in Amsterdam. Los van het feit dat het congres zeer professioneel was georganiseerd, zat het ook wel goed met de inhoud. Laat ik niet te veel uitweiden, maar het was opvallend hoeveel aandacht er was vanuit de juridische disciplines. Veel juristen in de zaal en op het podium. Veel aandacht voor privacywetgeving, contracten en natuurlijk de Patriot Act. Dat bleek uiteindelijk niet het spannendste onderwerp. Met name de onbekendheid met de oude Fisa-regulering in de VS was opvallend: een recente aanpassing van die wet maakt het Amerikaanse toezichthouders mogelijk om buiten de VS niet-burgers van de VS te bespionneren. Opmerkelijk, niemand die dat wist. Via Twitter hebben enkele deelnemers melding gemaakt van de lezing van Caspar Bowden (voorheen privacy goeroe bij Microsoft). Dat FISA-muisje zal nog wel een staartje krijgen.

Veel aandacht voor cloud vanuit de juridische disciplines

Netherlands Chapter

Het Netherlands Chapter bestaat inmiddels ongeveer een jaar en het leidt, helaas, een betrekkelijk stil leven. Elk chapter moet een research onderwerp hebben. Wij hebben gekozen voor het onderwerp cloudrisico's, met name continuïteit. We hebben in het afgelopen jaar acte de presence gegeven bij diverse evenementen en we hebben een enkele malen een webinar over het onderwerp gehouden, maar het is verder vrij stil. De reden is vooral dat het 'bestuur' (met mij) bestaat uit nog maar drie leden en dat is niet genoeg. Twee van de oprichtende leden hebben om verschillende redenen moeten besluiten hun taken te laten vallen. We zoeken dus nog aanvulling, zodat we de plannen (o.a. vergevorderde plannen voor een eendaags cloudseminar) verder uit kunnen voeren.

Besluit

De CSA is zeer actief en beschikt over een groot aantal instrumenten om organisaties te helpen bij het beveiligen van cloudomgevingen. Door initiatieven als CCM en STAR wordt het voor zowel providers als klanten mogelijk om zelf na te denken over beveiliging van de cloud en beveiliging in de cloud en kan een organisatie zelf al grote stappen zetten, zonder het wiel zelf te moeten uitvinden. Hoewel we in Nederland niet heel actief zijn, denken we toch dat er goede mogelijkheden zijn om ook in Nederland een bijdrage te leveren.

Referenties

CSA:
http://www.cloudsecurityalliance.org

CSA_NL:
http://chapters.cloudsecurityalliance.org/netherlands

CSA dreigingenrapport:
https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

COLUMN

SERVICE ORIENTED

It's the New Year and we take another look at Business Attributes from the SABSA Business Attributes Taxonomy, looking at what these might mean in the coming year. This time we examine what might be meant by 'service oriented', since it seems that this might be changing in its nature as we move forward into 'everything-as-a-service'.

Service Oriented Architecture (SOA) is a business-centric IT architectural approach that supports integrating your business as linked, repeatable business tasks, or services (Source: IBM). One of the goals is to reduce the number of business applications and hence save costs, but the main focus is on creating an IT environment that has the flexibility to move and develop at the speed of business. The chief drivers for this are global competition and time-to-market. Business leaders are riding the wave of mobile technologies and trying to harness the skills of Generation Y – those who have grown up with information technology from the cradle to the workplace and who's expectations are very different from those of previous generations. The way forward to achieve this 'New Way of Working' is to provide cloud services for maximum flexibility in connectivity and functionality.

For a long time we have talked about the enterprise service bus (ESB) as the core infrastructure concept of a SOA. The ESB provides logical connections between service providers and service consumers using well-defined interfaces. In the 1990's this was first developed using middleware – a layer that sits between the hardware and the application software. At first this was little more than a messaging bus to provide a virtual connection between clients and servers – the first steps towards virtualization. By 2002 The Gartner Group was using the term Enterprise Service Bus. By this they meant a concept that had become much more than a simple message queuing layer. It now embraced a multi-layered 'stack' that supported business process automation. By 2008 Gartner was using the term 'cloud computing' to describe the relationship between consumers of IT services and their suppliers, many of which were by this time third parties, following on from the trend of outsourcing the ownership of hardware and the hosting of applications.

Now it is 2013 and things have moved on further. Now we divide the rather complex stack into main categories of 'infrastructure as a service' (IaaS –meaning the hardware and networks), 'platform as a service' (PaaS – meaning a completely virtualized computing platform including operating system functionality) and 'software as a service' (SaaS – meaning the development of business applications using tools and functionality provided by the PaaS). Each of these layers has many sub-layers and the complete stack is a highly refined multi-layered architectural approach that provides for agile software development and the ability to move at what people are calling 'the speed of business'. This latter characteristic is exactly what business has been complaining has been lacking in previous generations of IT architecture, and the expectation of meeting this requirement is what will be challenging corporate IT departments in the coming year. With the emergence of third party cloud services providers the very future of the corporate IT department is itself in question: who needs them and what will be their new role?

So how shall we as architects meet this new challenge? If speed of change and maximum flexibility are to be achieved, then having an infrastructure and platform base that is managed by a formal change request process is not going to work. We need to provide a rich tool-kit of functions and services that are 'ready for use' by those agile application development teams. This means that we can no longer think in pure technology terms and have IT strategies that are driven by technical knowledge alone. Instead we need to be engaging with the business on a constant basis and providing a PaaS that is business-ready. Previous architectural approaches have failed to do this and will continue to fail unless we change our strategy. This is where the whole method of SABSA Business Attributes Profiling comes into play.

It is no coincidence that during this new year of 2013 the next generation of TOGAF will be published. In that publication SABSA Business Attributes Profiling will be introduced as the central method for requirements management for all architectural work conducted under the TOGAF umbrella. This then will show the way forward for those who are challenged with providing a private PaaS and other private and hybrid cloud services. It will be by engaging with business stakeholders and knowing their business strategies that architects will succeed in meeting demands for new services. So what does the 'service oriented' attribute mean? It means the entire concept of Business Attribute Profiling as the future of business solution development. We wish you all a Happy New Year. ●

The Attributer

3e EDITIE IDENTITY.NEXT

Robert L. Garskamp is organisator van IDentity.Next.

Op 20-21 november 2012 vond alweer de 3e editie van IDentity.Next event plaats, deze keer in het New Babylon Center in Den Haag. In tegenstelling tot de voorgaande edities was het programma deze keer verspreid over twee dagen. Er kwamen meer dan 150 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.

IDentity.Next hanteert naast het congres ook sinds de eerste editie het bekende Open Space format. De kracht van dit format is dat er ruimte is voor ontmoetingen met kennis-experts, 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. Met het Open Space format, wordt de agenda - in relatie met de thema's – op de dag zelf vastgesteld. Ook werden de deelnemers van het congres uitgenodigd om hun mening/visie te delen via o.a. twitter (met hashtag #idn12) waarbij de tweets veelvuldig in diverse discussies werden gebruikt.

Missie: Een onafhankelijk platform te bieden voor ondersteuning en facilitering van innovatieve benaderingen in de wereld van de digitale identiteit.

Doel: 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.

Missie en doel van IDentity.Next

Esther Makaay introduceert de unconference sessie

IDentity.Next werd geopend door Robert Garskamp, de organisator van dit event. Na een korte introductie werd Gabor Bartha als openingsspreker voorgesteld. Gabor is jurist binnen de Europese Commissie task force legislation team (eIDAS). Deze taskforce is verantwoordelijk voor het leveren van een voorspelbare regelgeving voor elektronische identificatie en vertrouwen in diensten voor elektronische transactie in de interne markt voor het gemak van de gebruiker en om het vertrouwen in de digitale wereld te vergroten. Gabor gaf een update van de bereikte doelen van de taskforce. Na deze highlights werd het congresdeel met de parallel tracks voortgezet.

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

- Social Consumer (How will social identity turn around the new value chain?)
- MobileMe (How is it possible to control your mobile Identity?)
- Private Eye (Who owns and controls online privacy and should we really care?)
- E-Citizen (Next generation eGovernment and its identity issues)
- 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?
- Up in the air (identity information is part of the crown jewels of many organisations. How can you govern, what's far away?

Daarnaast waren er op dag 2 ook nog twee paralleltracks:

- OpenID (ingevuld door de OpenID foundation)
- eHerkenning (eRecognition) met inhoud over de opzet en vorderingen rondom eHerkenning

Elke track bestond uit presentaties door (vooral) bekende sprekers uit binnen- of buitenland, die werkzaam zijn binnen de wereld van de digitale identiteit, zoals Mariette Lokin (Ministerie van Financiën), Jaap Henk Hoepman (TNO, Radboud), Debby Kraaijeveld (Ministerie BZK), Alessandro Festa (Quest), Henk Marsman (Deloitte), Travis Spencer (Twobo) en nog vele anderen. Dat het een internationaal congres is, blijkt uit de aanwezigheid van sprekers uit onder andere Rusland, Australië, Sri Lanka.

Deze dag werd afgesloten met een keynote presentatie van David Birch van Hyperion. David deelde zijn visie over de ontwikkeling van de digitale identiteit in de huidige maatschappij en zijn frustratie dat het niet met de snelheid gepaard gaat die hij zou graag zien. David deelde ook zijn toekomst verwachtingen met de aanwezigen, waaronder:

1. Mobile will drive innovation. Mobile will drive everything. Remote control for identity in cloud? i.e. don't' need to store identities in handset...
2. Identity battle. Commerce will drive the next stage of evolution of electronic id, which id? Banks, telcos, retailers? Government wants private sector to deliver digital identities in marketplace. E.g. retailers drive customer transactions. Identity in mass wallet – whose identity? Api based competition into retailer wallets as intermediaries.
3. Shouldn't underestimate conservatism of people. Change is slow. Is there something psychological about identity that we don't understand? Even if private sector solution with anonymity etc, do people still want something to look like a passport?

Op dag 2 was er wederom een vol programma met een diversiteit van onderwerpen. Naast de tracks die door IDentity.Next werden gefaciliteerd, was er ook de mogelijkheid om sessies over eHerkenning en OpenID te kunnen bijwonen. De dag begon met een keynote presentatie van Frans van der Reep (sr. Strategist van KPN). Frans had een interessante lezing over de context van het begrip digitale identiteit. Waarbij door Frans werd gesteld dat identiteit in de term van credentials en operatie steeds belangrijker wordt voor bedrijven om met elkaar verbonden te zijn voor samenwerking e.d.. De digitale identiteit gaat volgens Frans niet om technologie, maar juist om mensen. De lezing van Frans bracht veel discussie teweeg vanuit het publiek. Aansluitend was er een paneldiscussie met Frans, Poppe Wijnsma (PKIpartners) en Ronald Prins (Fox-IT). De panelleden (en ook het publiek) werd hun mening gevraagd over verschillende stellingen zoals 'Moet er ook een nationale digitale brandweer komen (na het echec van Diginotar) en willen we het DNA van alle Nederlanders in een database plaatsen om zodoende mensen sneller te kunnen opsporen'. De meningen waren flink verdeeld en brachten een goede discussie teweeg.

De tweede dag werd uiteindelijk afgesloten met een presentatie van John Bradley. John is technisch architect van Ping identity maar ook boardmember van de OpenID foundation. In zijn presentatie gaf John o.a. een update over het gebruik van een aantal protocollen zoals OpenId.connect oAuth. Deze protocollen worden vooral toegepast voor autorisatie bij transacties op een eenvoudige en standaard methode in web, mobiele en desktop applicaties. John maakte de aanwezigen duidelijk dat we dit – in ons leven - dagelijks gebruiken, maar dat we er ons eigenlijk niet bewust van zijn. Een beetje jammer dat deze lezing inhoudelijk inging op OpenID, goed verhaal, maar een meer ontspannen reflectie op digitale identiteiten zou ook wel leuk zijn geweest.

Access Governance

Door een IDentity.Next werkgroep is gewerkt aan een raamwerk voor Access Governance. Hierin worden de missie, visie, strategie, principes en maatregelen beschreven voor het beheersen van de toegang tot informatie binnen een organisatie. Tijdens de paneldiscussie onder leiding van werkgroeplid Jacoba Sieders werden de bevindingen uit dit rapport met de aanwezigen gedeeld. Het rapport zal januari 2013 beschikbaar zijn voor publicatie.

Open Space

Esther Makaay (SIDN) 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

David Birch presenteert zijn visie op de identity toekomst

Twee voormalig IB hoofdredacteuren bespreken digitale dood

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. De notulen van al deze sessies staan ook on-line op de website van IDentity.Next.

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. Onder leiding van Hermen van der Lugt (directeur Novay) was een jury samengesteld: Kevin Cox (eDentiti, winnaar Novay Digital Identity award 2012), Leendert Bottleberghs (Head of Business Development -Marktplaats, eBay Classifieds Group), John Hermans (managing partner KPMG Risk consulting). Uit de open inschrijving waren drie genomineerden door de jury geselecteerd:

- Evolok is een Engels product dat een identity & access management system met een micro-payment paywall-systeem voor online-uitgevers.
- eHerkenning
- IDchecker. Het Nederlandse IDchecker biedt een Software-as-a-Service oplossing om fysieke identificatiemiddelen zoals rijbewijs of paspoort te verifiëren.

Uiteindelijk werd eHerkenning door de jury als winnaar gekozen. Hermen van der Lugt, directeur van Novay en voorzitter van de jury vermeldt hierover het volgende: *"Wat de jury met name innovatief vindt is dat eHerkenning een open e-identity trust framework is, waarin private ondernemingen concurreren om identiteitsdiensten aan te bieden. eHerkenning loopt hierin voor op bijvoorbeeld de Verenigde Staten en het Verenigd Koninkrijk. Deze landen kennen vergelijkbare initiatieven, maar die zijn beduidend minder ver". De jury is positief over het feit dat het gebruik van eHerkenning groeit en dat online zakendoen met de overheid makkelijker en betrouwbaarder wordt. Wat ook meetelt is dat eHerkenning bezig is om hergebruik van dezelfde identiteiten voor online zaken tussen bedrijven onderling mogelijk te maken.*

Wat nemen we mee?

Bij IDentity.Next zijn verschillende thema's regelmatig aan de orde geweest. Verschillende van deze thema's zullen de komende tijd vaker de revue passeren:

- Outsourcing van user management naar de cloud, Social login gaat het helemaal worden!
- Geld verdienen met Identity Management... door overheden!
- User provisioning in de cloud door middel van Secure Cross-domain Identity Management (SCIM) en Just-in-Time user provisioning d.m.v. SAML.
- Federatie en volmachten via onder meer eHerkenning (voor B2G en B2B)
- BYOD en Bring Your Own Identity, OAuth en OAuth wrap
- Trust levels voor digitale identity providers en digitale identiteiten
- SAML wordt vervangen door OpenIDConnect (zie artikel van Kick Willemse in dit blad)

De volgende editie van IDentity.Next is op 19-20 november 2013, ook weer in Den Haag.

Links

http://www.identitynext.nl

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

DNA DATABASE

Het mooie van deze rubriek is dat we snel in kunnen spelen op het nieuws. Maar soms gebeurt er zoveel dat we tijdens de keuze voor een onderwerp al weer door de actualiteit worden achterhaald. Bultrug Johannes en de schietpartij in Newtown waren de laatste dagen belangrijker dan al het andere. Dus tijd om even terug te grijpen naar wat voor ons actueel was. De discussie over de landelijke DNA databank. Dankzij die databank werd de moordenaar van Marianne Vaatstra gevonden. Het doel heiligt de middelen geldt hier overduidelijk. Maar zijn er misschien grenzen aan zo'n opstelling? Of gaan we in de toekomst nog meer doelen nastreven met die middelen? Moeten we misschien nog wel meer gaan vastleggen om opsporing te vergemakkelijken en onschuldigen eerder vrij te pleiten van onterechte verdachtmakingen? Een interessante vraag voor onze redacteuren.

Lex Dunn

Een probeersel mijnerzijds (overigens is de potentiële moordenaar van Marianne Vaatstra NIET door de landelijke DNA databank gevonden, want die is er nog niet, maar door het matchen van de vrijwillig afgestane samples van de ongeveer 8000 onderzochte mannen uit de regio).

Landelijke DNA-bank: vloek of zegen? Naar aanleiding van de affaire Marianne Vaatstra gaan nu stemmen op om een landelijke DNA databank, waarin iedereen verplicht zijn/haar DNA moet aanleveren, aan te leggen. Hiermee zou in een handomdraai elk misdrijf, waarbij DNA sporen worden aangetroffen, op te lossen zijn. Is zo'n landelijke DNA databank een goed idee of niet? Volgens mij niet. Er zijn al talloze scenario's gepasseerd, waarin een onschuldige, door het laten slingeren van zijn DNA, als verdachte in bijvoorbeeld een moordzaak wordt aangemerkt, puur en alleen op basis van het DNA spoor. En dat Justitie er soms naast zit, is net weer gebleken met de Zes van Breda. Bovendien: wat zou je met deze DNA samples in de toekomst kunnen gaan doen? De wetenschappelijke ontwikkelingen gaan snel, misschien dat bedrijven straks deze DNA samples kunnen gaan raadplegen om te bezien of sollicitanten wel een goede gezondheid hebben, of (nog erger) dat vóórdat je gaat trouwen en kindjes mag maken, je eerst toestemming van de overheid moet hebben op basis van het matchen van de DNA profielen van jou en je aanstaande huwelijkspartner (dat dan in het ongetwijfeld goed bedoelde kader om de kosten voor de gezondheid in toom te houden, maar toch ....). Ik ben van mening dat DNA samples een prima "tool" zijn in het koffertje van de forensisch onderzoeker, maar om nu maar alvast iedereen een sample te laten inleveren gaat me te ver (en dat geldt ook voor vingerafdrukken).

Lex Borger

De stelling is dat met zo'n databank de moordenaar van Marianne Vaatstra meteen gevonden zou zijn. Een snel en stellig middel om waarheid te ontdekken en ons

rechtsgevoel te dienen. Maar zijn er misschien grenzen aan zo'n opstelling? En gaan we in de toekomst nog meer doelen nastreven met die middelen? Moeten we misschien nog verder gaan met vastleggen om opsporing te vergemakkelijken, schuldigen op te pakken en onschuldigen eerder vrij te pleiten? Een interessante vraag voor onze redacteuren.

Activistisch bekeken kun je alleen maar tegen een nationale DNA databank zijn. Laten we eens verder kijken. Net als bij een onderwerp als het EPD vind ik dat je de discussie alleen kunt aangaan als je vertrekt vanuit het standpunt dat er een goed gedefinieerd doel is. Omdat de databank er niet is en er ook geen opdracht voor gegeven is, wordt het meteen al moeilijk om het te beoordelen.

André positioneert het als opsporingsmiddel in een zaak à la de moord op Marianne Vaatstra. Peter R. de Vries benoemde de mogelijkheid tot identificatie van slachtoffers bij grote rampen. Beide argumenten kampen in de uitvoering met een probleem: het middel dient zeldzame gebeurtenissen, die psychologisch door ons helemaal verkeerd beoordeeld worden. Bruce Schneier heeft hier al veel over geschreven: Ze worden belangrijker ingeschat dan de optelsom van gewone gebeurtenissen. We hebben niet stapels onopgeloste moorden liggen met wachtend DNA bewijs. Als we de Puttense moordzaak toevoegen is de kans op deze incidenten eens in de vijf jaar. Vergelijk dit met het EPD, wat een effect heeft op de dagelijkse communicatieprocessen tussen zorgverleners.

Zijn er gewone voordelen te vinden voor een DNA databank? Ik denk het wel, maar dan moeten we het zoeken in de gezondheidszorg, als onderdeel van diagnose. En dan doen we iets heel anders dan DNA gebruiken als identificatie, we willen weten hoe de genetische opmaak in elkaar steekt.

Veel hiervan kan in gedeeltelijke of volledige anonimiteit gedaan worden.

Zonder een realistisch doel is de DNA databank niet wenselijk. Dan is de discussie over het effect op privacy niet eens te voeren. Dan is het alleen maar een bijdrage aan big data, voor big brother. Terug naar 1984.

André Koot
De laatste jaren zijn er verschillende aansprekende voorbeelden uit de rechtspraak waaruit blijkt, dat menselijke herinneringen en meningen niet overeenkomen met de werkelijkheid en ook dat tunnelvisie bij overheden het zicht op de werkelijkheid vertroebelt. Dus op naar de echte feiten. En dan zijn DNA sporen misschien wel de meest objectieve van allemaal.
Een DNA spoor is immers uniek. Andere biometrische identificatoren zijn al gekraakt of gekopieerd, waardoor ze niet echt als uniek eenduidig bewijsstuk gehanteerd kunnen worden. Een DNA spoor is dus een mooi bewijsstuk. Maar, er komt een maar. Een identificator is alleen maar zo sterk als betrouwbaarheid van de informatie en de contra-informatie.
En daar begin ik me wat zorgen te maken. Als een sleutel gekraakt wordt, dan moet je zorgen voor een nieuwe.
Als een biometrisch gegeven gehackt of gelekt wordt, dan moet je ook zorgen voor een alternatief. Als een vingerafdruk gekraakt is, nou, dan heb je er nog 9 over die als bewijs of contra-informatie zouden kunnen dienen.
Maar je DNA? Daar is maar één unieke versie van. Dat betekent twee dingen: als iemand mijn DNA op een plaats delict achterlaat, dan heb ik een probleem. Als iemand in de centrale database mijn DNA spoor wijzigt, dan heb ik ook een probleem. Dat eerste is niet goed te voorkomen, dat bepaalt feitelijk de waarde van het instrument als bewijsmiddel op zichzelf.
Het tweede is een fors risico, dat groter wordt naarmate er meer dreigingen en kwetsbaarheden bestaan. Dus hoe groter de database en hoe meer mensen erbij kunnen, hoe groter het risico dat iemand gaat knutselen met mijn gegevens. We hebben deze discussie al eens gevoerd over het landelijke EPD en daarbij ging het alleen maar over privacy. In dit geval gaat het om meer, namelijk mijn vrijheid. Ik weet het wel... ●

REGISTER INFORMATIEBEVEILIGING 2012

● Artikel ▼ Verslag ■ Interview

Artikelen

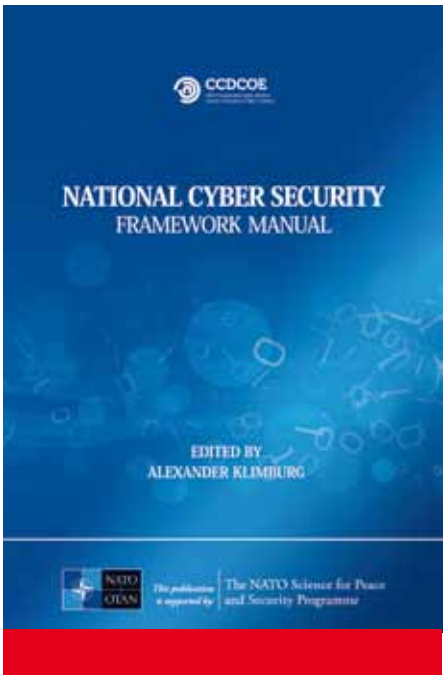
NATIONAL CYBER SECURITY FRAMEWORK MANUAL

De steeds grotere verwevenheid van cyberspace met alle facetten van de samenleving verhevigt ook de discussie over de gerelateerde nationale veiligheidsaspecten: wat is nationale cyber security en hoe verhoudt zich dat tot de nationale en internationale veiligheid? Een vraagstuk dat voor het NATO Cooperative Cyber Defence - Centre of Excellence (CCD-CoE) in Tallinn, Estland uitgewerkt is in het National Cyber Security Framework Manual (NCSFM).

Op 6 december 2012 werd de pdf van het boek beschikbaar gesteld op internet. De e-book en hard copy versies volgen later in december resp. januari 2013.

Het National Cyber Security Framework Manual (NCSFM) is geschreven door een groep van internationale experts die hun ideeën gevalideerd hebben in drie internationale workshops. Het NCSFM geeft een gedetailleerde theoretisch kader en leidraad voor het ontwikkelen van nationaal cyber security beleid, wet- en regelgeving, besluitvormingsprocessen, etc., waarbij rekening wordt gehouden met nationale aspecten als ICT-volwassenheidsniveau, rechtskader, overheidsstructuur en cultuur.

Tegelijkertijd wordt het grens-overschrijdende karakter van cyber-dreigingen onderkend. Het NCSFM beslaat de politieke, strategische, operationele en tactische/technische niveaus. Het NCSFM bouwt voort op het NAVO cyber defensiebeleid dat de nadruk legt op preventie en veerkracht van de NAVO en nationale vitale (informatie-gebaseerde) infrastructuren in plaats van op een (militaire) reactie. NAVO verwacht overigens wel een bepaalde mate van cyberverdediging van de NAVO kerntaken door de bondgenoten. Het gebruik van het NCSFM door de NAVO-lidstaten en door partnerlanden ondersteunt



de strategische doelstelling van de NAVO om de cyberverdediging van het bondgenootschap en de partnerlanden te verbeteren. De doelgroep van het NCSFM omvat alle belanghebbenden van de nationale cyberverdediging van een NAVO-lidstaat of partnerland, waaronder beleidsmakers, wetgevers, toezichthouders en dienstverleners.

Auteurs van het NCSFM zijn Dave Clemente (Royal Institute of International Affairs), Victoria Ekstedt (Zweedse krijgsmacht - computer network operations unit), Melissa Heathaway (voormalig Cyber Security adviseur van de presidenten Bush en Obama), Jason Healey (Atlantic Council's " Cyber Statecraft Initiative), Alexander Klimburg (Austrian Institute for International Affairs), Gustav Lindstrom (Geneva Centre for Security Policy), Eric Luiijf (TNO) en Tom Parkhouse (Atlantic Council's " Cyber Statecraft Initiative). ●

Het NCSFM is te downloaden van http://www.ccdcoe.org/369.html

Bron:
TNO, Ir. Eric Luiijf

COLOFON

Informatiebeveiliging is het huisorgaan van het Platform voor InformatieBeveiliging (PvIB) en bevat ontwikkelingen en achtergronden over onderwerpen op het gebied van informatiebeveiliging.

Redactie
Lex Borger (hoofdredacteur),
e-mail: hr@pvib.nl
Motivation Office Support bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

Redactieraad
Tom Bakker (Allianz)
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
Maarten Hartsuijker (ANWB)
Aart Jochem (NCSC)
André Koot (i3advies)
Rachel Marbus (KPMG, IT Advisory)
Gerrit Post (G & I Beheer BV)
Bart van Staveren (UWV)

Advertentieacquisitie
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 2013
De abonnementsprijs bedraagt 115 euro per jaar (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

COLUMN

TERUGKIJKEN IS MOOI!

Gelukkig hebben we het allemaal weer achter de rug, Sinterklaas zit weer in zijn uppie in het (w)arme Spanje, de Kerstdagen zijn we allemaal weer goed doorheen gerold en Oud en Nieuw was ook weer een mooie ervaring, maar het ergste van de genoemde periode is wel de onuitputtelijke reeks van jaaroverzichten die op allerlei gebied over je heen worden gestort. Griekenland, Spanje, het Nederlands elftal, de krediet crisis. Het komt eerlijk gezegd mijn neus uit en daarom maar een eigen jaaroverzicht gemaakt (die overigens echt niet compleet is) met wat hoogte- en/of dieptepuntjes uit 2012.

2012 was voor onze beroepsgroep weer een mooi jaar waarin incident na incident zich opstapelden om uiteindelijk het beeld te schetsen dat we het echt niet onder controle hebben. Diverse data zijn gekopieerd (grappig dat je data niet kunt stelen) om op andere plaatsen misbruikt te worden. Veel data wordt gekopieerd zonder dat wij als gebruiker er van op de hoogte worden gebracht. Bedrijven die het zat zijn zich scheel te betalen aan het laten uitvoeren van penetratietesten doen het maar gewoon niet meer. Mijn klanten voeren hun gegevens toch wel in als ze iets van mij nodig hebben. Ik vraag ze ook even om hun e-mailadres om de bevestiging van de bestelling te sturen en vervolgens misbruik ik dat e-mailadres tot vervelens toe voor allerlei aanbiedingen. Op mijn website plaats ik altijd dat het product uit voorraad leverbaar is, als ik er namelijk op zet dat mijn klanten een aantal dagen moeten wachten dan gaan ze gauw naar een ander toe. Ik laat ze betalen en dan doe ik gewoon mijn best om het product zo snel mogelijk toe te zenden. De telefoon beman ik wel maar ik ga niet teveel helpdeskmedewerkers inzetten, de klant kan beter wachten dan dat onze helpdeskmedewerkers met elkaar zitten te kaarten. Vervolgens train ik mijn medewerkers in het aan het lijntje houden van mijn klanten.

Prijsafspraken worden gemaakt over de beeldbuis TV's (die grote diepe dingen die we vroeger allemaal hadden) om de inkomsten maar op niveau te houden. Prijsafspraken over de benzineprijzen zijn nooit aangetoond, maar (laat ik mij voorzichtig uitdrukken) het zou niet onmogelijk zijn. Och, zo worden we door iedereen om de tuin geleid.

En dan nog het opvallende cijfer dat er momenteel meer smartphones worden verkocht dan de conservatieve telefoon, nog sterker, momenteel zijn er in Nederland meer smartphones dan de ouderwetse telefoon. Dit jaar is het nog niet gehaald, maar volgend jaar worden er meer dan 1 miljard (1.000.000.000) smartphones en tablets verkocht. Het merendeel van Samsung en Apple die rollebollend door iedere rechtbank rollen om nog meer winsten te kunnen genereren. Model 1 is nog niet door een Chinees geassembleerd of er wordt al geadverteerd met een telefoon die nog spectaculairder is dan de vorige. Een iPad van de eerste lichting is binnen 2,5 jaar zo sterk verouderd dat deze niet meer in aanmerking komt voor een update van het operating system. Om de groei van Samsung bij te kunnen houden, heeft Apple besloten om niet ieder jaar de machines te upgraden maar dit een keer in de 6 maanden te doen. En geloof het of niet, er zijn heel veel mensen die echt het nieuwste van het nieuwste willen. Zo maken we elkaar allemaal gek en we kijken er niet eens meer van op. We nemen andere clubs over om onze aandeelhouders gelukkig te houden. We fuseren, versoberen de arbeidsvoorwaarden en halveren het aantal medewerkers om maar meer winst te maken. We sturen een lid van de Raad van Bestuur naar het NOS journaal om met het meest droevige gezicht wat hij kan maken aan te kondigen dat het allemaal helaas niet door natuurlijk verloop kan geschieden.

De banken zijn er flauw van om alle geleden schade van skimmers aan klanten uit te betalen, maar zijn niet in staat om het probleem op te lossen. Weet je wat, blokkeren we toch alle passen in het buitenland en als je dan toch in het buitenland wil pinnen, kan je dat op de site aangeven. Ik ben benieuwd of de algemene voorwaarden ook zo zijn aangepast dat de geleden schade dan voor eigen rekening is. Ik denk het niet, ik denk dat de banken toch wel het fatsoen hebben om de verantwoordelijkheid te nemen voor het door hen veroorzaakte probleem? Toch?

Een diepe zucht ontsnapt bij mij. Ben ik nu zo ouderwets of maken we er met zijn allen een zootje van? ●

Berry

Data Leakage

Bring Your Own Device

Security As A Service

Compliance & Auditing

SECURITY

geen keuze, maar noodzaak!

De toepassingsmogelijkheden van Bring Your Own Device, Security As A Service, Data Leakage en Compliance & Auditing ontwikkelen zich in hoog tempo. Daarmee nemen ook bedreigingen toe in de vorm van Cybercrime, Hacking en Identiteitsfraude. Ook worden deze bedreigingen steeds geavanceerder. Adequate beveiliging van werkomgevingen, data en identiteitsgevens zijn inmiddels geen keuze, maar noodzaak geworden. Security vereist nu ervaren, betrouwbare en loyale partners. CRYPSYS is toonaangevend op het gebied van security analyse, advies en installatie bij overheden, semi-overheden, gemeenten, grote bedrijven en organisaties.

CRYPSYS
secure computing

CRYPSYS Data Security BV Edisonweg 4 4207 HG Gorinchem **tel** +31 (0)183 62 44 44 **fax** +31 (0)183 62 28 48 **mail** sales@crypsys.nl **web** www.crypsys.nl

CRYPSYS is officieel distributeur van: Sophos. Lumension. Norman. Cryptzone. Cryptshare. Adyton. Tenable. Kanguru