07/2013

INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 7 - 2013

BUSINESS CONTINUITY MANAGEMENT

EUROPESE WETGEVING BESCHERMING PERSOONSGEGEVENS

'BREDE' MELDPLICHT DATALEKKEN, PREVENTIE EN PRIVACY

OPEN SOURCE COMPLIANCY VAN BELANG VOOR CONTINUÏTEIT

VOORWOORD

'Burning Man' is een evenement wat jaarlijks gehouden wordt in de woestijn van Nevada. Een week lang wordt Black Rock City bevolkt met meer dan 50 duizend mensen. Aan het eind van het festival wordt een grote houten beeld verbrand. Het wordt een experiment in samenleving, kust, zelfexpressie en onafhankelijkheid. Deelnemers kopen hier kaartjes voor, en brengen alles mee wat ze nodig hebben (water, eten, onderdak, veiligheid) en ruimen naderhand ook weer alles op. Daarnaast nemen ze alles mee voor de expressieve kant. Die kunstuiting krijgt flink de ruimte. Kijk maar naar de vele foto's en video's die te vinden zijn op het internet.
Dat is echter niet waar ik het over wil hebben. Black Rock City is zo groot dat het niet zonder bestuur en regels kan. Er gelden van de organisatie uit 12 principes. De wetten van Nevada en de V.S. gelden er gewoon, en er is ook gewoon politie aanwezig. Ook lopen er groepen hulpverleners rond. Er is een RDW die een beperkt aantal voertuigen registreert om chaos op de weg te voorkomen.
Eigenlijk is Black Rock City een weerspiegeling van de automatisering binnen een hedendaags bedrijf.
Je komt er van alles tegen, het bruist van activiteit, er is minimale afstemming en uiteindelijk gaat toch alles goed. Als iets niet werkt, helpt men elkaar, als iets last bezorgd, wordt in overleg voor een oplossing gezorgd.
Beveiliging is belangrijk. 's Nachts maak je je zichtbaar door te 'gloeien'. Alles wat licht rondstraalt is beter dan een gerichte lamp. Tentpalen worden gemarkeerd en afgedekt.
Je hebt bescherming tegen de zon, een stofafscherming tegen het scherpe zand - er kunnen plotseling gemene zandstormen ontstaan. In de woestijn heb je te maken met grote temperatuurverschillen, meer dan 40 graden. Ook gelden er privacyregels, zo mag je niemand op de foto zetten zonder toestemming.
En hier is het verschil met een bedrijf te zien. Bedreigingen zijn duidelijk, maatregelen ook en eenieder kiest zijn eigen risicobereidheid. Algemene regels zijn tot een minimum beperkt en de regels die er zijn, zijn duidelijk. Toch gaat er maar weinig fout. Komt dat door de gunningsbereidheid en onafhankelijkheid van de deelnemers? Deelnemers worden gewaarschuwd dat een terugkeer naar de 'normale' samenleving nogal wat aandacht vergt... Misschien moet ik maar eens gaan kijken.
Met dank aan Lisa Lorenzin (@llorenzin) en COSAC voor de inspiratie.

Lex Borger, hoofdredacteur

Links

http://www.burningman.com/
http://en.wikipedia.org/wiki/Burning_Man
http://www.huffingtonpost.com/2013/09/17/time-lapse-burning-man-2013_n_3940917.html

INHOUDSOPGAVE

BUSINESS CONTINUITY MANAGEMENT IS MEER DAN ALLEEN HOOFDSTUK 14 - ISO 27001

Gert Kogenhop (1958) is directeur van bcm+, een bedrijf dat is gespecialiseerd in training, consultancy en implementatie van Business Continuity Management Systemen conform de norm ISO 22301. Gert heeft een financieel economische achtergrond en is onder andere werkzaam geweest als Regional Finance Director Northern Europe bij DELL inc. en is tevens een gecertificeerd trainer op het gebied van leidinggeven. Voor meer informatie kunt U terecht op www.bcmplus.nl of per e-mail: gk@bcmplus.nl

We leven in een maatschappij waarvan de complexiteit continu toeneemt. We moeten met steeds meer partijen rekening houden en hebben langere en intensievere afhankelijkheidsketens met een grotere kans op verstoringen op meerdere plaatsen met een steeds grotere hoeveelheid aan verschillende mogelijkheden. Het Nieuwe Werken als oplossing voor flexibiliteit en efficiency lijkt aan belangstelling te verliezen. Het leidt tot flexibilisering van werkplek en woon-werk verkeer. Maar de balans werk-privé en de binding met organisatie, collega en uiteindelijk de klant lijdt hieronder en daardoor het resultaat. Tevens zorgt het voor een groot aantal nieuwe bedreigingen en risico's, zeker op het vlak van Informatiebeveiliging.

In de nabije toekomst komt er duidelijk meer focus op een toename van de verantwoordelijkheid en autonomie van werknemers, inclusief grote aandacht voor de kwaliteit van de samenwerking en daarmee de coördinatie binnen de organisatie - tot en met de klant. ICT is hier de drijvende kracht, de facilitator. Informatiekwaliteit, accuraatheid, veiligheid, betrouwbaarheid, beschikbaarheid en noem alle vereisten maar op, worden in toenemende mate van belang. Uit een recent onderzoek van de Carnegie Mellon University blijkt dat het weerstandsvermogen en de veerkracht van organisaties onder toenemende druk staat door onder andere een toename van het gebruik van technologie (ICT), de globalisering met z'n open grenzen, de versnelde toename van de complexiteit van (operationele) processen en dit alles versterkt door de huidige economische situatie en helaas de van toepassing zijnde wet- en regelgeving. Uit een inventarisatie door onder andere het Business Continuity Institute (BCI) blijkt dat de top drie bedreigingen in Europa op dit moment zijn:

- Unplanned IT and telecom outage
- Data Breach
- Cyber crime

In een artikel in Het Financiële Dagblad eind augustus zegt Dick Schoof (Nationaal Coördinator Terrorisme en Veiligheid - NCTV) over Cybercrime het volgende: 'De risico's die organisaties dagelijks op internet lopen, hebben het kabinet ertoe aangezet de aanpak van digitale kwetsbaarheid tot prioriteit van het veiligheidsbeleid te maken'. Er bestaat inmiddels een Cyber Security raad in samenwerking met het bedrijfsleven en de overheid heeft het National Cyber Security Centrum (NCSC) opgericht. Volgens Schoof nemen de illegale activiteiten in de cyberwereld in rap tempo toe. De weerbaarheid en het herstelvermogen van organisaties groeit gelukkig ook, maar minder snel. De balans is negatief. Wie het nieuws een beetje volgt, wordt hier niet door verrast. Regelmatig zijn er (ver) storingen, zoals in de telecomsector bijna normaal is geworden evenals bij de banken, als het gaat om telebankieren, al dan niet mobiel of met betrekking tot PIN transacties, maar laatst ook in een reserveringssysteem van een grote luchtvaartmaatschappij. Overigens wordt er door de telecomproviders inmiddels gesproken over het overnemen van elkaars sms- en telecomverkeer in geval van een ernstige calamiteit. Een nobel streven, maar het is nog niet zo ver. Ernstiger wellicht zijn de activiteiten van hackers, zoals diverse overheidsinstanties (bijvoorbeeld de belastingdienst) en gemeenten hebben ondervonden. Hoe veilig is onze (klanten)data bij bedrijven en instanties? Of het nu gaat om adres- en eventueel bankgegevens, het hacken van de ontwikkelaars website van Apple, of een ordinair beveiligingslek, iemand is de dupe en niemand wil dat zijn. In

> Het weerstandsvermogen en de veerkracht van organisaties staat onder toenemende druk

de Boardroom Cyber Watch Survey 2013 van IT Governance Ltd staat het volgende te lezen: 'Although businesses tend to focus mainly on the external cyber-threats facing organisations, more than half of respondents say that the greatest threat to their company's data and computer systems in fact comes from their own employees.' En voorts: 'A significant minority – over 40% - of respondents say their company is either making the wrong level of investment in information security or are unsure if their investment is appropriate.' Eén op de vier organisaties heeft het afgelopen jaar te maken gehad met een aanval van buitenaf.

De schade voor de getroffen bedrijven valt zeker niet te onderschatten, of dit nu rechtstreeks toewijsbaar is of dat we spreken over reputatie- en/of merkschade, schade is er vaak direct en is veelal omvangrijk. Bedrijven schade toebrengen door het platleggen van websites of systemen middels bijvoorbeeld een DDoS-aanval leidt al niet meer tot headlines. Het is bijna "business as usual". Gespecialiseerde bedrijven als datacenters doen er vanzelfsprekend van alles aan om de continuïteit van dienstverlening, in dit geval simpelweg toegang tot data, te garanderen (zo optimaal mogelijk waarborgen wellicht). Maar zijn de SLA's die bedrijven afsluiten wel "continuïteits-proof"? Niet zo lang geleden ging een datacenter failliet. Is dan alles wel goed geregeld? Kan iedereen bij zijn of haar data? Van wie is de data - juridisch? Hoe is de transitie geregeld naar een nieuwe oplossing, als de ketting al op het hek zit, het personeel naar huis is en de curator het voor het zeggen heeft? De prestatieverplichting in de SLA helpt dan vaak niet meer, dat mag duidelijk zijn. Voor datacenters in z'n algemeenheid gaat het om vier uitermate kritieke elementen:

- Stroomvoorziening, liefst triple redundant;
- Internettoegang, ook het liefst meerdere opties en uitwijkstrategieën;
- Beveiliging, zowel fysiek als tegen bijvoorbeeld hackers;
- Koeling.

Zij doen hun uiterste best om voor iedereen, de stakeholders, de dienstverlening optimaal te garanderen. Het hoeft geen betoog dat bij menig bedrijf deze processen en elementen niet dezelfde aandacht (en investeringen) krijgen, met alle risico's van dien.

Laten we voor alle duidelijkheid even teruggaan naar de basis. Het begint eigenlijk allemaal met de Missie, Visie en Doelstellingen van de organisaties, leidend tot de uit te voeren activiteiten als gevolg van de gemaakte keuzes en vastgestelde uitgangspunten. Laten we het voorbeeld van het datacenter maar nemen. Wat de Missie en Visie ook zullen zijn, de Doelstellingen zullen liggen in de richting van groei van de activiteiten, gekoppeld aan redelijke doelstellingen met betrekking tot de winstgevendheid (Return On Sales - ROS) en het rendement op het geïnvesteerde vermogen (Return On Investment - ROI). De activiteiten benodigd om deze doelstellingen te bereiken zijn vrij duidelijk in beeld te brengen. Het gevolg hiervan leidt tot de eerste vaststelling. Het datacenter is als het gaat om de eerder genoemde vier kritieke elementen in mindere of meerdere mate kwetsbaar.

We worden toch nog regelmatig verrast door een bedreiging waar niemand rekening mee had gehouden

Het heeft mensen nodig, capaciteit in de vorm van ruimte en machines, energie, internettoegang, een beveiligingssysteem, koelsystemen die te allen tijde functioneren en noem maar op. Deze kunnen allemaal niet zelf worden gecreëerd, in de zin van "self supporting". Technisch gezien is in het kader van risicomanagement en continuïteitsmanagement deze kwetsbaarheid als volgt te omschrijven: *Omstandigheid die ervoor zorgt dat het doel van een object of activiteit mogelijk niet wordt gerealiseerd. Het is een onvervreemdbare eigenschap van een object of activiteit in die specifieke vorm, onafhankelijk van de omgeving. De kwetsbaarheid zelf is een inherente eigenschap, die alleen kan worden weggenomen door het object of de activiteit te veranderen. In het Engels aangeduid als "Vulnerability".* Het is van het grootste belang dat

organisaties een volledig beeld hebben van de kwetsbaarheden, daar dit de Achilleshiel van de organisatie kan bevatten.

Een volgende stap in het proces is vervolgens het kennen van de bedreigingen welke gelden voor de organisatie. In het geval van ons datacenter dus zaken als het uitvallen van de stroomvoorziening, internetverbinding of koeling of het ernstig falen van de beveiliging. De bedreiging wordt in dit kader als volgt omschreven: *Een kwetsbaarheid die daadwerkelijk uitgebuit kan worden in de eigen omgeving is een bedreiging. Het is een eigenschap die afhankelijk is van de omgeving waarin de onderliggende kwetsbaarheid optreedt. Een bedreiging kan worden weggenomen zonder dat de onderliggende kwetsbaarheid is weggenomen. Een kwetsbaarheid kan niet worden weggenomen zonder het object of de activiteit waarin deze optreedt te veranderen. In het Engels aangeduid als "Threat"*. Deze bedreigingen kunnen in kaart worden gebracht. Er bestaat in het algemeen wel voldoende kennis in de organisatie om het merendeel en de belangrijkste bedreigingen boven tafel te krijgen en in beeld te brengen. Bovendien zijn algemene bedreigingen toe te voegen aan de "interne" lijst. Dit gezegd hebbende worden we toch nog regelmatig verrast door een bedreiging waar niemand rekening mee had gehouden (z.g. Black Swans). Een bekend voorbeeld van niet al te lang geleden is de aswolk als gevolg van de vulkanische activiteiten op IJsland die ons land en vooral het vliegverkeer enige tijd danig dwars heeft gezeten. Het woord "aswolk" was sowieso een nieuw fenomeen en wordt bijvoorbeeld niet door MSWord herkend als bestaand woord en als zodanig rood onderstreept als zijnde wellicht niet correct, maar dat terzijde.

Operational Resilience

Als laatste stap in het proces komen we bij het bepalen van de risico's. Hoe groot is de kans dat iets gebeurt, wat zijn dan de gevolgen en hoe lang hebben we last van die gevolgen. Voorts wellicht beoordelen en bepalen hoe wij de risico's kunnen beïnvloeden en wat onze huidige "control levels" zijn. In dit kader kijken we als volgt aan tegen risico's: *Risico is het gevaar op verlies of schade door het manifest worden van een bedreiging. De (geschatte) frequentie waarmee dat gebeurt wordt "kans" genoemd. De nadelige gevolgen in de vorm van verlies of schade worden samengevat onder de noemer "impact". Risico wordt vaak beschreven als - Risico = Kans x Impact. In het Engels aangeduid als "Risk"*. Nu zijn we automatisch aangekomen op de scheidingslijn en/of het raakvlak van risicomanagement en business continuity management.

Het uitvoeren van risicoanalyses gebeurt zowel vanuit een oogpunt van risicomanagement als vanuit bedrijfscontinuïteit

Het uitvoeren van risicoanalyses gebeurt zowel vanuit een oogpunt van risicomanagement als vanuit bedrijfscontinuïteit. Laten we het als volgt stellen. Risicobeoordelingen welke worden uitgevoerd vanuit een Business Continuity Management initiatief zijn over het algemeen gericht op het operationele niveau, daar zij gericht zijn op het voorkomen van en, indien van toepassing, optimaal reageren op een ernstige verstoring (disruption) van activiteiten. Dit is een uitermate waardevolle toevoeging of zelfs essentieel onderdeel van de risicobeoordeling welke wordt uitgevoerd als onderdeel van de risicomanagement inspanning van de organisatie, welke over het algemeen plaatsvindt op ondernemingsniveau, "enterprise", vandaar ook de benaming Enterpise Risk Management (ERM). De overlap tussen BCM en ERM levert de organisatie de ultieme mogelijkheid op om het weerstandsvermogen en de veerkracht (Resilience) te versterken, maar enkel wanneer het integraal wordt uitgevoerd, holistisch, het geheel én de onderlinge samenhang. Resilience wordt in dit kader dan ook gedefinieerd als: *het vermogen van een*

organisatie om een ernstige verstoring (disruption) te verwerken, er effectief op te reageren en hiervan te herstellen op de meest optimale wijze.

De continuïteit van bedrijfsvoering, de levensader van elke organisatie, moet zo optimaal mogelijk worden gewaarborgd. Het gaat aldus veel verder dan alleen ICT en in het geval van ICT bijvoorbeeld hoofdstuk 14, Bedrijfscontinuïteitsbeheer van de ISO 27001 norm. Het gaat om het zo optimaal mogelijk garanderen van de continuïteit van de bedrijfsvoering van elke organisatie, bedrijfsleven en overheid, profit en non-profit, oud en jong, groot en klein. Iedereen heeft belang bij een organisatie die morgen ook nog functioneert. Nu zijn continuïteitsplannen net als vele andere elementen als risicomanagement, communicatiestrategieën, Informatiebeveiliging en crisismanagement allemaal op hun eigen specifieke wijze van belang. Het gaat echter om het realiseren van weerstandsvermogen en veerkracht indien er écht iets gebeurt. 'Voorbereiding is 90% van het resultaat', wordt er wel gezegd en geschreven, maar in dit geval gaat dat zeker op. Het gaat om "Operational Resilience", de organisatie draaiende houden en overleven door een optimale voorbereiding.

Zoals al eerder aangegeven is de toenemende afhankelijkheid van ICT een gegeven, terwijl tevens heden ten dage de grootste bedreigingen ook op dit gebied liggen. Vanuit een holistische gedachte, het geheel (de organisatie) en de onderlinge samenhang van alle activiteiten en de onderlinge afhankelijkheden van de verschillende activiteiten, zowel intern als extern, kan worden gesteld dat ICT het middel is waarop men bouwt, de bron, de voeding en de smeerolie van de organisatie.

Voorbereiding is 90% van het resultaat

Samen met andere activiteiten en met de continuïteitsgedachte als uitgangspunt dienen alle puzzelstukjes op de juiste plaats te worden gelegd om de organisatie te voorzien van bescherming op het juiste niveau. Business Continuity Management is onlosmakelijk verbonden met zaken als Incident Management, Crisis Communication, ICT Disaster Recovery, Risk Management en Emergency Planning.

Zoals gesteld in ISO 27001 dient Informatiebeveiliging opgenomen te worden in het continuïteitsbeheer, dient er te worden beoordeeld welke gevolgen ernstige incidenten kunnen hebben op Informatiebeveiliging en dient er naar gehandeld te worden, moet er aandacht besteed worden aan de beschikbaarheid en hoe lang verstoringen mogen duren (bijv. RPO) en zal dit alles getest en gecontroleerd moeten worden. Laat duidelijk zijn dat niemand deze wensen c.q. eisen betwist, echter ze dienen nooit en te nimmer op zich te staan, als een ICT-ding. Business Continuity Management is van ons allemaal. Iedereen in de organisatie en zelfs daarbuiten, de zogenoemde "Interested Parties", partijen met een belang, een interesse, moeten zich zorgen maken over en zich bezig houden met zowel vandaag als morgen. De fout maken om geen plan te hebben voor wanneer het onverwachte gebeurt, is eigenlijk plannen om een enorme fout te maken wanneer het onverwachte gebeurt. In elke organisatie dienen de bestuurders de afweging te maken of er tijd, geld en aandacht moet worden besteed aan Business Continuity Management. Elke bestuurder zal zijn of haar eigen afweging moeten maken en standpunt bepalen. Is het overbodig, doomdenken en gebeuren "dat soort dingen" bij ons toch niet, of is het een onderdeel van Maatschappelijk Verantwoord Ondernemen en Good Governance. Aan Darwin wordt de volgende quote toegeschreven: 'It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is most adaptable to change.' Hieruit kan worden afgeleid dat zij die de (plotselinge, onverwachte) verandering (gebeurtenis) zo goed mogelijk kunnen opvangen, de grootste kans op overleven hebben. Continuïteitsmanagement, niet alleen binnen ICT en specifiek Informatiebeveiliging, maar voor de gehele organisatie. ●

Business Continuity Management is van ons allemaal

BCM in Context

EUROPESE WETGEVING BESCHERMING PERSOONSGEGEVENS IN DE SCHIJNWERPERS

André J. Biesheuvel is bedrijfseconoom, Register Accountant en Register IT Auditor. Hij is meer dan tien jaar partner bij Duthler Associates (www.duthler.nl). Binnen de praktijk is hij verantwoordelijk voor de dienstverlening op het gebied van gegevensbescherming. Biesheuvel is medeauteur van de NOREA uitgave: "Het Europees privacyrecht in beweging, Overzicht van actuele ontwikkelingen en mogelijke consequenties voor werkzaamheden van IT-auditors".

Guus Bekker is bestuurskundige en heeft een Master in Public Information Management. Hij is consultant bij Duthler Associates (www.duthler.nl) en heeft daarvoor in verschillende functies bij de Rijksoverheid gewerkt. Bekker is binnen de praktijk verantwoordelijke voor de vakinhoudelijke ontwikkeling van gegevensbescherming en in het bijzonder de dienstverlening rond PIA's.

Privacy en de bescherming van persoonsgegevens staan vandaag de dag, onder meer vanwege de recente onthullingen aangaande het PRISM programma, hoog op de agenda. Organisaties krijgen meer en meer het besef dat zij hun verwerkingen van persoonsgegevens op orde moeten hebben. Burgers willen meer controle over hun eigen gegevens en bovendien groeit, zowel nationaal als internationaal, de politieke aandacht voor de bescherming van persoonsgegevens.

Een erg belangrijke positie in dit geheel is weggelegd voor het voorgestelde nieuwe rechtskader voor de bescherming van persoonsgegevens binnen de Europese Unie. In dit artikel wordt dieper ingegaan op dit rechtskader, de achtergronden ervan en de vereisten die uit dit rechtskader voortvloeien. Ook wordt, gezien de overeenkomstige doeleinden, de voorgestelde Richtlijn van het Europees Parlement en de Raad ten aanzien van netwerk- en informatiebeveiliging (NIB) behandeld en wordt de verhouding tot de nu geldende Wet bescherming persoonsgegevens (Wbp) beschreven. De verwachting is dat deze verschillende Europese wetskaders in de zeer nabije toekomst een belangrijke invloed zullen hebben op het verwerken van persoonsgegevens door organisaties.

De introductie van zowel de verordening als de richtlijn vormt het eerste gedeelte van een tweeluik-commentaar. In het vervolgartikel wordt specifieker ingegaan op de potentiële implicaties, die deze regelgeving heeft op het terrein van IT en de op dit speelveld opererende organisaties.

Rechtskader bescherming persoonsgegevens

Op 25 januari 2012 presenteerde de Europese Commissie haar voorstel voor *een verordening van het Europees parlement en de raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (COM (2012) 11 final)*. Wij spreken in dit verband over de Europese privacyverordening. Deze verordening vervangt de bestaande Europese privacyrichtlijn uit 1995 (Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, PB L 281/31 van 23.11.1995).

> Burgers willen meer controle over hun eigen gegevens

Dezelfde dag publiceerde de Europese Commissie ook een voorstel voor *een richtlijn van het Europees parlement en de raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens (COM (2012) 10 final)*. Beide voorstellen dienen met elkaar in samenhang te worden gezien en vormen samen het nieuwe (aankomend) rechtskader voor de bescherming van persoonsgegevens binnen de Europese Unie. Na goedkeuring van het Europees Parlement is de Europese privacyverordening rechtstreeks in alle lidstaten van kracht. In tegenstelling tot een richtlijn, hoeft een verordening niet te worden geïmplementeerd in nationale

> Aan het niet voldoen aan deze vereisten zijn hoge sancties gekoppeld

wetgeving. Vanwege dit verschil in doorwerking, richten wij ons in dit artikel voornamelijk op de voorgestelde verordening.
De Presidency of the Council Justice and Home Affairs of the European Union heeft op 31 mei 2013, na consultatie van de parlementen en de toezichthouders op de effectiviteit van het borgen van de privacy van de lidstaten, aanpassingen op de hoofdstukken 1 tot 4 van de Europese privacyverordening voorgesteld. De voorgestelde aanpassingen hebben vooral betrekking op het plaatsen van de Europese privacyverordening in de context van de bedrijfsvoering van een organisatie en het toepassen van een risk-based benadering bij te treffen en in stand te houden procedures en mechanismen.

- ***Het recht van toegang (artikel15)***
De betrokkene heeft het recht om te allen tijde op verzoek uitsluitsel van de voor de verwerking verantwoordelijke te verkrijgen omtrent het al dan niet plaatsvinden van verwerkingen van hem betreffende gegevens.

- ***Het recht op rectificatie (artikel 16)***
De betrokkene heeft recht op rectificatie van hem betreffende onjuiste persoonsgegevens door de voor de verwerking verantwoordelijke.

- ***Het recht om vergeten te worden en het recht om gegevens te laten wissen (artikel 17)***
De betrokkene heeft er recht op dat de voor de verwerking verantwoordelijke ervoor zorgt dat hem betreffende gegevens worden gewist en de verdere verspreiding van dergelijke gegevens achterwege blijft.

- ***Het recht op dataportabiliteit (artikel 18)***
De betrokkene heeft het recht om van de verantwoordelijke een kopie te krijgen van de gegevens die worden verwerkt in een elektronisch en gestructureerd formaat.

- ***Het recht op bezwaar (artikel 19)***
De betrokkene heeft het recht te allen tijde op gronden die verband houden met zijn bijzondere situatie bezwaar te maken tegen de verwerking.

Kader 1 Artikelen rechten van betrokkene in Europese privacyverordening

Achtergronden
De noodzaak om te komen tot een nieuw rechtskader voor de bescherming van persoonsgegevens kent verschillende achtergronden. Ten eerste wordt bescherming van persoonsgegevens gezien als een grondrecht. Om dit recht te waarborgen is het van belang dat een persoon "in control" wordt gesteld van zijn eigen persoonsgegevens. Niet een bedrijf of een overheidsorganisatie bepaalt wat er met deze gegevens gebeurt, maar de zeggenschap ligt bij de persoon zelf. Dit is een paradigmashift in het denken over en organiseren van de gegevensverwerkingen en informatievoorziening in bestaande processen. In de voorgestelde Europese privacyverordening zijn verschillende rechten van de betrokkene opgenomen. In kader 1 zijn de belangrijkste rechten van betrokkenen opgesomd, waardoor deze ook daadwerkelijk in staat gesteld wordt zeggenschap over zijn gegevens uit te voeren.

Ten tweede bestaat het streven om de huidige verschillen tussen de lidstaten bij de uitvoering van de EU-regels voor gegevensbescherming zoveel mogelijk weg te werken. Dit zorgt voor gelijke voorwaarden voor iedereen binnen de EU en neemt eventuele onduidelijkheden weg over welk regime geldend is.
Een derde drijfveer is gelegen in het zorgen voor een goede bescherming van persoonsgegevens op het moment dat persoonsgegevens naar landen buiten de EU worden doorgegeven. De procedures voor het doorgeven van gegevens moeten worden verbeterd. Het doel is dat bij het samenwerken met landen buiten de EU eenzelfde niveau van bescherming als binnen de EU van kracht is.

> Het wordt verplicht om een functionaris voor de gegevensbescherming (FG) aan te stellen

Tot slot speelt een verdere uitbreiding en harmonisering van de taken, rollen en bevoegdheden van de toezichthouders een belangrijke rol. Voor een daadwerkelijke sterkere positie van de toezichthouders is een EU-breed nieuw rechtskader een belangrijke voorwaarde voor het efficiënter kunnen handhaven van de regels.

Vereisten Europese privacyverordening
De Europese privacyverordening bevat naast de aangeduide rechten voor de betrokkenen nog meer relevante vernieuwingen (zie kader 2).
Zo worden in de Europese privacyverordening eisen gesteld aan het uitvoeren van een Privacy Impact Assessment (PIA), gebruik van privacy by design en privacy by default, het zorgdragen dat een individu zijn rechten ook daadwerkelijk kan effectueren, het aanstellen van een functionaris voor de gegevensbescherming (FG) en het melden van datalekken. Aan het niet voldoen aan deze vereisten zijn hoge sancties gekoppeld.

Deze sancties kunnen oplopen tot een boete van 1 miljoen euro of twee procent van de wereldwijde jaaromzet van de organisatie. Hieronder worden enkele van deze vereisten verder toegelicht.

PIA
Eén van de belangrijkste eisen die de verordening met zich meebrengt, is de in artikel 33 opgenomen verplichting dat gevoelige verwerkingsactiviteiten ten aanzien van persoonsgegevens eerst aan een PIA moeten worden onderworpen. In de verordening is opgenomen dat het effect van de beoogde verwerkingen op de bescherming van persoonsgegevens onderzocht moet worden wanneer verwerkingen gezien hun aard, reikwijdte of doeleinden bijzondere

risico's inhouden voor de rechten en vrijheden van de betrokkenen. Idealiter gebeurt dit in een zo vroeg mogelijk stadium, zodat kostbare en tijdrovende aanpassingen in processen, herontwerp van systemen of stopzetten van een project vermeden worden.

Om organisaties te ondersteunen bij het uitvoeren van een PIA en zo privacyrisico's in een vroeg stadium op een gestructureerde en heldere manier te kunnen identificeren is door de Kennisgroep Privacy Audits van NOREA, de beroepsorganisatie van IT-auditors, een methodische Handreiking voor het effectief en efficiënt uitvoeren van PIA's gepubliceerd. Diverse aanleidingen voor het uitvoeren van een PIA zijn te onderscheiden voor particuliere organisaties:

1. Het opstellen of herijken van intern privacy- en veiligheidsbeleid;
2. Het beoordelen van informatiesystemen en de technische informatie infrastructuur;
3. Het contracteren en uitbesteden van (cloud) diensten;
4. Het voorkomen van datalekken;
5. Het (inter)nationaal overleggen van gegevens;
6. Het voorbereiden op een uit te voeren audit

Voor overheidsorganisaties zijn PIA's ook nodig bij regelgeving met implicaties voor de bescherming van persoonsgegevens. Vanaf 1 september 2013 wordt daarbij het Toetsmodel PIA Rijksdienst standaard toegepast.

Functionaris voor de gegevensbescherming

Voor veel organisaties wordt het met de inwerkingtreding van de Europese privacyverordening verplicht om een functionaris voor de gegevensbescherming (FG) aan te stellen. De Europese privacyverordening zorgt voor een verzwaring van de FG-functie door extra eisen te stellen aan de hoeveelheid en de inhoud van de taken die bij deze functie horen. De taken, die onder de verantwoordelijkheid van de FG vallen, zijn onder meer het informeren en adviseren van de verantwoordelijke voor de verwerking van persoonsgegevens, het toezien op uitvoering en toepassing van het privacybeleid van de verantwoordelijke, het toezien op de (al dan niet light) uitgevoerde PIA's en het toezien op de naleving van de meldplicht datalekken.

De verantwoordelijke is verplicht uiterlijk binnen 24 uur een datalek te melden

Privacy by Design and by Default

Er bestaan uiteenlopende opvattingen over de betekenis van de principes privacy by design en privacy by default. We kunnen zeggen dat in plaats van de wet toe te passen op het systeem, de wet als het ware in het systeem wordt gebouwd.

Enkele vereisten uit Europese privacyverordening

- Rechten van betrokkenen
- Uitvoeren van een PIA
- Privacy by Design en by Default
- Meldplicht datalekken
- Aanstellen van een FG

Kader 2

Deze ingebouwde privacy (by design) en standaardsysteeminstellingen voor maximale privacy (by default) impliceren dat waarborgen voor de bescherming van persoonsgegevens al vanaf de eerste ontwikkelingsfases in systemen, producten en diensten ingebouwd moeten zijn. Te hanteren oplossingen zijn onder meer gegevensminimalisatie, transparantie over het gebruik van persoonsgegevens, het afschermen van de identiteit en het gebruik van privacy-icons en privacy-ontologieën.

Meldplicht datalekken

In de Europese privacyverordening is een vereiste opgenomen dat de verantwoordelijke verplicht is zonder onnodige vertraging en uiterlijk binnen 24 uur nadat hij ervan kennis heeft genomen, een datalek te melden bij de toezichthoudende autoriteit (in Nederland het College bescherming persoonsgegevens (Cbp)).

Parallel aan de voorgestelde Europese privacyverordening ligt momenteel het nationale wetsvoorstel meldplicht datalekken bij de Tweede Kamer. Op 17 juni 2013 is het wetsvoorstel meldplicht datalekken bij de Tweede Kamer ingediend (kamerstuk 33.662). Dit wetsvoorstel bevat wijzigingen van de Wet bescherming persoonsgegevens (Wbp) en Telecommunicatiewet (Tw). Naast het melden aan de toezichthouder houdt de meldplicht in dat de verantwoordelijke aan de betrokkene de inbreuk moet melden indien de inbreuk ongunstige gevolgen zal hebben voor zijn persoonlijke levenssfeer. Het niet voldoen aan deze verplichtingen kan worden gesanctioneerd met een bestuurlijke boete van € 450.000, op te leggen door het Cbp. Verschillende fracties van de Tweede Kamer vinden het een goede zaak dat het maximale boetebedrag, dat door het Cbp kan worden opgelegd bij het niet melden van een datalek, verhoogd wordt naar € 450.000, meerdere fracties vragen zich zelfs af of de sanctie niet op het niveau van de Europese privacyverordening moeten worden gebracht.

Wbp en Europese privacyverordening

In Nederland is nu de Wet bescherming persoonsgegevens (Wbp) van kracht. Hoewel het beoogde doel van de Europese privacyverordening vergelijkbaar is met dat van de Wbp kent de Europese privacyverordening een andere dynamiek. De Europese privacy-verordening vraagt de verantwoordelijke zodanige beheersmaatregelen in de administratieve organisatie en ondersteunende systemen aan te brengen

dat inherent aan de wet wordt voldaan. In de Wbp dient de verantwoordelijke persoonsgegevens en bijbehorende gegevensverwerkingen adequaat te beveiligen met passende technische en organisatorische maatregelen. Dit met het doel om het verlies van gegevens of onrechtmatige verwerking tegen te gaan (Wbp art. 13). Voldoen aan deze eis kan worden beschouwd als een inspanningsverplichting voor de verantwoordelijke.
Nieuw in de Europese privacy-verordening is de eis (in artikel 22 lid 3) dat de verantwoordelijke voor de verwerking van persoonsgegevens mechanismen instelt om ervoor te zorgen dat de doeltreffendheid van de maatregelen wordt getoetst.
Dit betreffen de maatregelen, die zijn ingesteld om te kunnen aantonen dat de verwerkingen van persoonsgegevens compliant aan de verordening plaatsvinden. Deze toetsing wordt uitgevoerd door onafhankelijke interne of externe controleurs, indien die maatregel evenredig is.

Op de naleving van de Wbp wordt toezicht gehouden door het College bescherming persoonsgegevens (Cbp). Om toe te lichten hoe het Cbp bij het onderzoeken en beoordelen van de beveiliging van persoonsgegevens de beveiligingsnormen uit de Wbp heeft toegepast, heeft het Cbp in 2013 de "Richtsnoeren beveiliging van persoonsgegevens' gepubliceerd. Deze Richtsnoeren vormen de verbindende schakel tussen het juridische domein en het domein van de informatiebeveiliging. Op deze manier worden de eisen uit de Wbp verbonden met de benodigde kennis en kunde om aan de gestelde eisen te voldoen. De Richtsnoeren hebben een algemene insteek maar verwijzen naar informatiebeveiligingsnormen die zijn ontwikkeld voor specifieke sectoren. Hierdoor zijn de Richtsnoeren bijvoorbeeld te gebruiken in samenhang met algemeen geaccepteerde beveiligingsstandaarden (NEN ISO/IEC 27002:2007 nl) of de ICT beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum (NCSC).

Tot welke aanpassingen van de Wbp de Europese privacyverordening gaat leiden, is nu nog niet bekend, maar gezien het feit dat een verordening rechtstreeks van toepassing is, is de te verwachten impact van het nieuwe rechtskader op de organisaties groot.

Richtlijn netwerk- en informatiebeveiliging (NIB)
Niet alleen de Europese privacy-verordening richt zich op de bescherming van gegevens.
De Europese Unie wil ook een verbetering van de veiligheid van het internet, particuliere netwerken en informatiesystemen. Voor een nadere uitwerking van deze strategische prioriteit is in februari 2013 een voorstel gedaan voor een *Richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen*. Wij noemen dit hier verder de Richtlijn NIB (zie kader 3).

De primaire doelstelling van de Europese Unie is het verhogen van de bescherming tegen incidenten, risico's en bedreigingen. Doel van de voorgestelde richtlijn is het waarborgen van een hoog gemeenschappelijk niveau van netwerk- en informatie-beveiliging.
Het niveau is momenteel niet in alle lidstaten van een gelijk niveau en dit kan bij het anticiperen op en handelen bij incidenten voor problemen in de afstemming zorgen. Bovendien zijn consumenten en bedrijven in de verschillende lidstaten niet op eenzelfde manier beschermd.

De primaire doelstelling van de Europese Unie is het verhogen van de bescherming tegen incidenten, risico's en bedreigingen

Vereisten richtlijn NIB
- Nationale NIB strategie
- Een voor NIB aangelegenheden bevoegdheden coördinerende autoriteit
- Een voldoende uitgerust CERT

Kader 3

Betere samenwerking is dus benodigd voor een betere beveiliging van gegevens. Bovendien zullen aanbieders van informatiesystemen en-diensten, online platforms en overheden ertoe verplicht moeten worden adequate maatregelen te nemen om beveiligingsrisico's te beheren en ernstige incidenten aan de nationale bevoegde autoriteiten te rapporteren. (Brief inzake netwerk- en informatiebeveiliging richtlijn, Nationaal Coördinator Terrorismebestrijding en Veiligheid, 12 juli 2013). Om dit alles te bewerkstelligen moeten lidstaten volgens de voorgestelde richtlijn gaan beschikken over een nationale NIB-strategie, een voor NIB aangelegenheden bevoegde coördinerende autoriteit en een voldoende uitgerust CERT (Computer Emergency Response Team)
De verschillende lidstaten hebben allen hun positie ten aanzien van de NIB-richtlijn kenbaar kunnen maken. De onderhandelingen over de NIB richtlijn bevinden zich momenteel nog in de beginfase en de verwachting is niet dat de onderhandelingen al in 2013 worden afgerond.

Aantoonbaar zorgvuldig
De in dit artikel uiteengezette aanstaande Europese privacyverordening en de hiermee samenhangende richtlijn NIB, hebben merkbare gevolgen voor organisaties die persoonsgegevens verwerken.
De verantwoordelijke moet er voor zorgdragen dat de privacy en veiligheid van de betrokkenen zorgvuldig en aantoonbaar wordt gewaarborgd. Niet voldoen aan de gestelde eisen houdt hoge sancties in. ●

COLUMN: PRIVACY PEINZINGEN

LATEN WE MEER BEVEILIGINGSFOUTEN MAKEN, HET WORDT ER VEILIGER VAN

Voor burgerrechtenfundamentalisten zoals ik begint het woord Veiligheid inmiddels bijna vies in de mond te smaken. In naam der Veiligheid vindt u het vast niet erg als wij uw e-mails lezen, uw telefoon aftappen, uw lichaam scannen voor u een vliegtuig inloopt of als wij geheime rechtbanken in het leven roepen. In naam der Veiligheid bestrijden wij het terrorisme voor u, vangen wij de boeven en daar wordt het echt allemaal veiliger van voor u. De psychologisering van het woord Veiligheid is tot volle wasdom gekomen. Angst regeert, reguleert en bestraft. Gelukkig bestaat er tegenwicht en laat ook dat nu juist te maken hebben met de psychologie van Veiligheid.
Veiligheid heeft te maken met het creëren van de juiste omgeving. Het stimuleren van een veilige cultuur. Er valt nog een les te leren voor de dames en heren die zich bezig houden met de Veiligheid in de online wereld, de Veiligheid in het kader van terrorisme en de Veiligheid in het kader van cyberwar/criminaliteit. In de luchtvaartindustrie is al jaren geleden gekozen voor het stimuleren van een veilige cultuur. Met zorg worden teams samengesteld, wordt vooraf alles doorgesproken, maar ook erna. Dan wordt gepraat over wat goed ging, maar ook wat fout liep opdat men daarvan kan leren en het de volgende keer niet meer fout gaat. Er wordt niet gedacht in hiërarchie, iedereen – van de stewardess tot de piloot – heeft recht van spreken. Sterker nog, heeft de plicht om het te melden als iets niet goed gegaan is. Veiligheid wordt binnen de luchtvaartindustrie ingezet als middel om een omgeving te creëren waarbinnen het Veilig is om fouten toe te geven en misstanden aan de kaart te brengen zonder dat daarop direct negatieve repercussies gesteld worden.

De Australische professor Sidney Dekker schrijft en spreekt al jaren over juist die luchtvaartindustrie en hoe de veiligheidscultuur daarbinnen gestimuleerd wordt. Er moet volgens hem open gesproken kunnen worden over fouten waarbij 'blame free' leren van die fouten voorop staat. 'The new view of human error' gaat voorbij het kijken naar de fout: "Human error is a symptom of trouble deeper inside a system. To explain failure, do not try to find where people went wrong. Instead, find how people's assessments and actions made sense at the time, given the circumstances that surrounded them." Uiteindelijk gaat het om een evolutie binnen het veiligheidsdenken. Om daarbij technologie en de online wereld als voorbeeld te nemen: we dichten onze systemen technisch gezien zo goed mogelijk af, wij testen, wij auditen, wij controleren of het ook allemaal zo werkt, we monitoren onze veiligheidstechnologie. Een logisch vervolg daarop is het accepteren dat technologie alsook mensen feilbaar zijn. En dat we die feilbaarheid moeten aangrijpen om het Veiliger te maken.

In een systeem waar Veiligheid voorop staat, helpt het niet om het individu te straffen. Dekker: "Punishing is about teaching your people not to get caught the next time. Learning is about countermeasures that remove error producing conditions so there won't be a next time. Punishing is about stifling the flow of safety-related information (because people do not want to get caught). Learning is about increasing that flow." De eerste voorzichtige stapjes naar een cultuuromslag in onze informatiebeveiligingswereld worden door enkelen al gezet. Steeds meer organisaties kennen beleid rondom responsible disclosures waarbij gaten in de beveiliging gemeld kunnen worden. Het is nog slechts een eerste voorzichtige stap, want hoewel gestimuleerd wordt dat de "lekke" organisatie zich zal onthouden van het doen van aangifte tegen de melder, laat het de discretionaire bevoegdheid van het OM onverlet. Het zou ons sieren als wij net dat stapje extra durven te zetten, waarbij we waarlijk afzien van het straffen van het individu en overgaan naar het creëren van die Veilige omgeving, waardoor we leren van de beveiligings-fouten die we maken en we in die derde golf van Veiligheid terechtkomen waarbij feilbaarheid de stimulans is voor een Veiligere online samenleving. Voorzichtig aan zie ik dat het OM dat doet door het RD-beleid te hanteren in haar beslissing al dan niet te vervolgen, maar het blijft 'op zijn Hollands' met een slag om de arm: "Als een hacker direct en veilig communiceert met de eigenaar van het ICT-systeem over een aangetroffen lek in de beveiliging en er geen gegevens zijn verwijderd of gemanipuleerd, kan er sprake zijn van RD en is er geen aanleiding om (verder) strafrechtelijk onderzoek of vervolging in te stellen." Als jurist begrijp ik als geen ander de noodzaak van het woordje "kan", als burgerrechtenfundamentalist en informatie-beveiligingsaficionado zou ik het graag zien verdwijnen. ●

Mr. Rachel Marbus,
@rachelmarbus op Twitter

'BREDE' MELDPLICHT DATALEKKEN, PREVENTIE EN PRIVACY

Mr. dr. M.(Mirjam) H. Elferink is werkzaam als advocaat bij KienhuisHoving in Enschede in de praktijkgroep Intellectuele Eigendom, ICT-recht en Privacy. Zij is sinds jaren gespecialiseerd in Intellectuele Eigendom, ICT-recht en privacy. Mirjam publiceert en doceert regelmatig over deze onderwerpen. Zij is te bereiken via mirjam.elferink@kienhuishoving.nl of @MirjamElferink.

Mr. M.(Martijn) J.M. Kortier is werkzaam als advocaat bij KienhuisHoving in Enschede in de praktijkgroep Intellectuele Eigendom, ICT-recht en Privacy. Hij is gespecialiseerd in Intellectuele Eigendom, ICT-recht en privacy. Martijn is te bereiken via martijn.kortier@kienhuishoving.nl of @MartijnKortier.

Medische gegevens uit personeelsdossiers op straat [1], klantgegevens van Twitteraars uitgelekt via een app [2] en een ziekenhuis dat medische dossiers lekt via een nauwelijks beveiligde computer [3]. Datalekken zijn aan de orde van de dag. De gevolgen voor betrokkenen kunnen aanzienlijk zijn en de maatschappelijke impact hiervan is soms groot. De politiek zit niet stil en heeft wettelijke maatregelen voorgesteld om eventuele schade van datalekken te beperken c.q. te verminderen. Op 21 juni jl. is het langverwachte wetsvoorstel 'meldplicht datalekken' naar de Tweede Kamer gezonden [4]. In dit wetsvoorstel wordt een meldplicht voorgesteld in het geval zich een 'datalek' heeft voorgedaan. Vanwege privacyoverwegingen moeten betrokken personen in zo'n geval snel worden ingelicht. Dit betekent dat organisaties worden verplicht diefstal, verlies of misbruik van persoonsgegevens te melden aan de betrokken personen en aan het College bescherming persoonsgegevens (CBP). Deze meldplicht zal worden opgenomen in de Wet bescherming persoonsgegevens (Wbp).

Wat is men verplicht te doen qua preventie? En welke juridische instrumenten kunnen worden aangewend om de schade van een datalek zoveel mogelijk te beperken? In dit artikel zal worden ingegaan op de vraag welke consequenties dit wetsvoorstel voor organisaties heeft en hoe de verplichtingen daaruit moeten worden geïmplementeerd in protocollen en contracten. Als het wetsvoorstel in de huidige vorm wordt aangenomen en een datalek niet of niet tijdig wordt gemeld, kunnen organisaties namelijk een boete opgelegd krijgen van maximaal € 450.000.

Aanleiding meldplicht

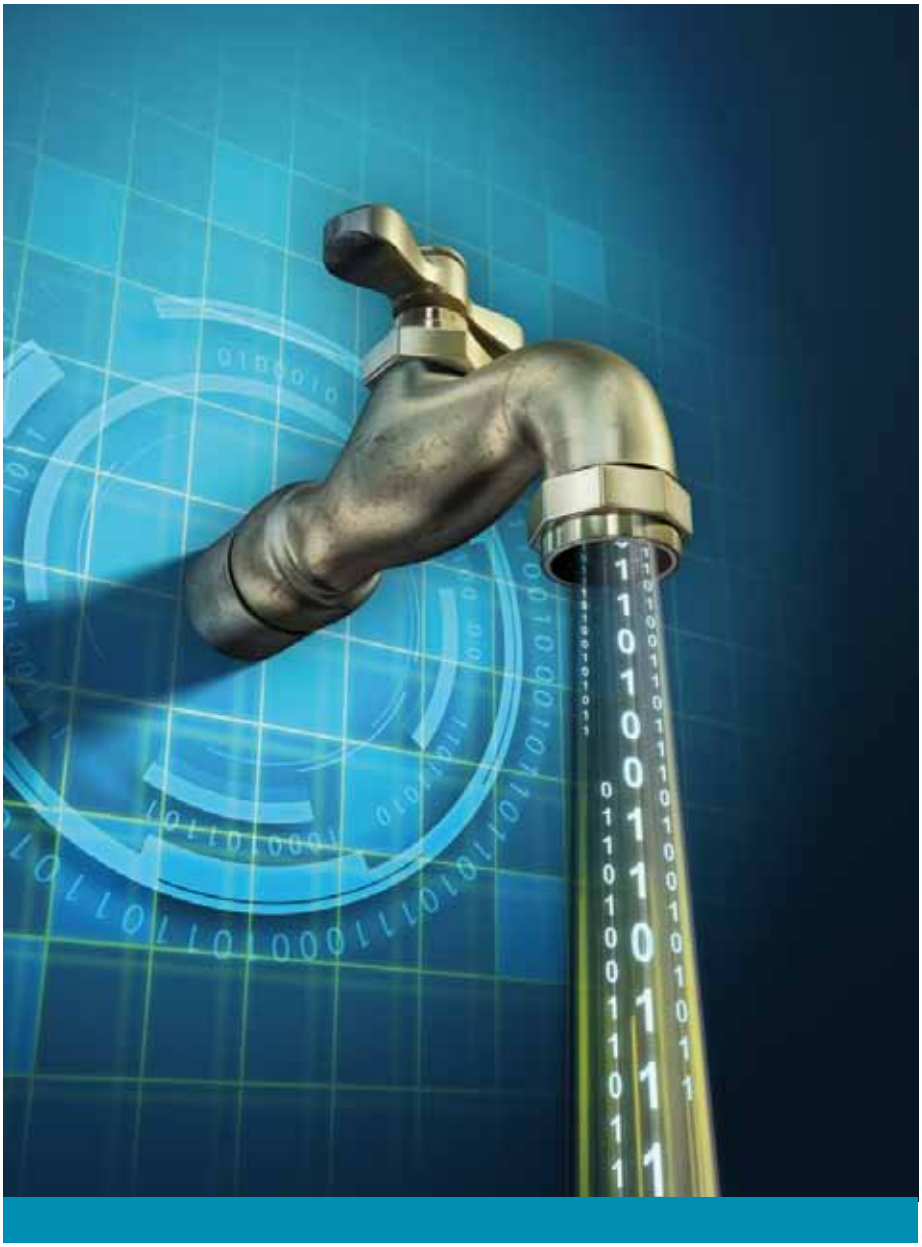
De aanleiding voor het wetsvoorstel is een groot aantal incidenten waarbij sprake is van inbreuken op persoonsgegevens. Sinds juni 2012 geldt al een meldplicht voor telecommunicatiebedrijven en internet servers providers op grond van de Telecommunicatiewet, ook wel de 'smalle' meldplicht genoemd. Deze meldplicht ziet op inbreuken op de beveiliging die nadelige gevolgen hebben voor de bescherming van persoonsgegevens. Daarnaast bestaan al andere meldplichten in verschillende wetten en is er ook nog diverse wetgeving in de maak [5]. Verder is in dit kader van belang dat de Europese Commissie op 25 januari 2012 een voorstel heeft gepresenteerd voor een Algemene verordening gegevensbescherming [6]. Deze ontwerpverordening zal de Wbp op termijn (grotendeels) buiten spel zetten. Ook in deze ontwerpverordening is een meldplicht van datalekken aan de toezichthouder en/of betrokkenen opgenomen. Indien de meldplicht niet wordt nageleefd wordt een boete van 1 miljoen Euro of 2% van de wereldwijde jaaromzet geriskeerd. Vanwege de ontwerpverordening zijn stemmen opgegaan om de aanpassing van de Wbp uit te stellen en volledig op die verordening toe te snijden. Hier is niet voor gekozen, omdat de ontwerpverordening naar de mening van de wetgever nog in een prematuur stadium verkeert en het nog lang niet zeker is of deze in de huidige vorm gehandhaafd zal worden. Naar verwachting treedt de verordening pas in 2016 in werking.

> De meldplicht ziet dus niet op situaties als die rond DigiNotar

De voorgestelde meldplicht is overigens beperkter dan de roepnaam van het wetsvoorstel - 'meldplicht datalekken'- doet vermoeden. Het wetsvoorstel ziet namelijk slechts op 'doorbrekingen van maatregelen voor de beveiliging van persoonsgegevens'. "*De meldplicht ziet dus niet op situaties als die rond DigiNotar waarin fouten*

werden gemaakt in de beveiliging van certificaten waardoor deze onbetrouwbaar waren, of op andere meldplichten met een min of meer verwant karakter (cybersecurity-incidenten)," aldus de memorie van toelichting [7].
Alvorens nader in te gaan op de voorgestelde meldplicht is het van belang enkele aspecten uit de Wbp onder de loep te nemen.

Enkele begrippen uit de Wbp
Verantwoordelijke - bewerker: De meldplicht gaat gelden voor degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In de terminologie van de Wbp de *verantwoordelijke*.



Denk bijvoorbeeld aan een werkgever. Onder het begrip *verwerking* valt elke handeling die betrekking heeft op persoonsgegevens, van het moment van verzameling tot vernietiging. Daaronder valt ook het opslaan van gegevens door een derde. Deze derde 'verwerkt' de gegevens in opdracht van de verantwoordelijke en wordt aangeduid als *bewerker*.

> Nieuw is om de verantwoordelijke op te leggen dat de bewerker de verplichtingen nakomt

Wanneer een onderneming zijn debiteurenadministratie uitbesteedt aan een bureau dat zich volledig onderwerpt aan de instructies van de desbetreffende onderneming en uitsluitend onder diens verantwoordelijkheid gegevens verwerkt, is eveneens sprake van bewerkerschap.

Persoonsgegevens: Wat valt er onder het begrip 'persoonsgegeven'? Volgens de wet gaat het om alle gegevens die informatie kunnen verschaffen over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit kan geschreven informatie zijn, maar ook informatie in beeld en geluid, zoals camerabeelden of stemopnamen. In de praktijk is men zich er vaak niet van bewust dat deze definitie meer behelst dan informatie waarvan alleen al uit de aard blijkt dat het om persoonsgegevens gaat, zoals de combinatie van naam-, adres- en woonplaatsgegevens. Ook gegevens waardoor een persoon indirect kan worden geïdentificeerd vallen hieronder. Denk bijvoorbeeld aan een taxicentrale die ritgegevens bijhoudt. In feite is de verwerking gericht op het registreren van routegegevens, waardoor men in eerste instantie niet snel aan persoonsgegevens zal denken. Dit wordt echter anders indien met behulp van deze routegegevens individuele chauffeurs kunnen worden getraceerd.

Beveiligingsplicht uit hoofde van de Wbp: Wat houdt de meldplicht in? Een verantwoordelijke is gehouden een melding te doen bij het CBP en/of de betrokken persoon, indien zich een inbreuk op getroffen beveiligingsmaatregelen voordoet en wanneer het aannemelijk is dat deze inbreuk een aanmerkelijke kans op nadelige gevolgen voor de bescherming van persoonsgegevens met zich meebrengt, die door de verantwoordelijke worden verwerkt. Kort gezegd: indien sprake is van diefstal, verlies of misbruik van persoonsgegevens moet dit gemeld worden. De voorgestelde

meldplicht staat dus in nauw verband met de beveiligingsverplichting die is neergelegd in artikel 13 van de Wbp. Op grond van deze bepaling is de verantwoordelijke verplicht om passende technische en organisatorische maatregelen ten uitvoer te (laten) leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. De maatregelen moeten bovendien een passend beschermingsniveau garanderen, gelet op de stand van de techniek en de kosten van de tenuitvoerlegging en gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. Het CBP geeft in richtsnoeren aan wanneer er sprake is van een blijvend, passend beveiligingsniveau [8]. Daarin wordt uitgelegd hoe het CBP bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens in individuele gevallen deze open beveiligingsnorm uit de Wbp toepast. Daartoe geeft zij een zogeheten plan-do-check-act-cyclus waarin zij allereerst aanraadt om de risico's goed in kaart te brengen en te beoordelen, en om gebruik te maken van algemeen geaccepteerde beveiligingsstandaarden. Bovendien adviseert het CBP om regelmatig te controleren en te evalueren. Periodiek dient beoordeeld te worden of het beveiligingsniveau nog steeds past bij de risico's die de verwerking en de aard van de te verwerken gegevens met zich meebrengen. Deze richtsnoeren kunnen verder worden toegepast in samenhang met algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van informatiebeveiliging zoals de code voor informatiebeveiliging (NEN-ISO/IEC 27002:2007 NL).

Een datalek valt pas onder de meldplicht indien de technische en organisatorische beveiligingsmaatregelen niet hebben gefunctioneerd en wanneer er sprake is van een aanmerkelijke kans op verlies of onrechtmatige verwerking van persoonsgegevens. Denk aan een hack van een ICT-systeem of een gestolen laptop uit een afgesloten locker, aldus de memorie van toelichting bij het wetsvoorstel. Het is dus niet noodzakelijkerwijs zo dat er sprake moet zijn van tekortschietende beveiligingsmaatregelen. Het gaat er om dat de getroffen beveiligingsmaatregelen teniet worden gedaan of omzeild. Het kan ook gaan om menselijke fouten of een niet adequate beveiliging van bestanden of gegevens, bijvoorbeeld het slordig omgaan met het beheer van wachtwoorden die toegang geven tot informatiebestanden.

Gevolgen brede meldplicht voor organisaties

Organisaties krijgen volgens het huidige wetsvoorstel een aantal nieuwe verplichtingen opgelegd. Dat leidt in ieder geval tot onder meer de volgende veranderingen:

1. Noodzaak tot aanpassen van de bewerkersovereenkomst
2. Protocolplicht verantwoordelijke
3. Opstellen 'datalek'-protocol
   - Aard en inhoud van de melding
   - Kennisgeving aan betrokkenen
   - Kennisgeving aan het CBP
   - Wijze van melden

Noodzaak tot aanpassen van de bewerkersovereenkomst

Wanneer een verantwoordelijke persoonsgegevens te zijnen behoeve laat verwerken door een bewerker, dient hij in een zogenaamde bewerkersovereenkomst een aantal zaken vast te leggen. Dit is een wettelijk vereiste die volgt uit artikel 14 Wbp. Zo moet worden geregeld dat de bewerker de persoonsgegevens slechts in opdracht van en conform de instructies van de verantwoordelijke verwerkt. Verder moet de bewerker de verplichting opgelegd krijgen om de persoonsgegevens adequaat te beveiligen conform de beveiligingsverplichting die voortvloeit uit de Wbp. Op grond van artikel 14, lid 5 van de Wbp is de verantwoordelijke namelijk verplicht om de getroffen beveiligingsmaatregelen ex artikel 13 Wbp schriftelijk vast te leggen. Deze regel is opgesteld in zowel het belang van de betrokkene als de verantwoordelijke. Dit zijn zaken die nu al gelden.
Nieuw is het voorstel om de verantwoordelijke op te leggen er zorg voor te dragen dat de bewerker de verplichtingen nakomt die op de verantwoordelijke rusten ten aanzien van diens meldplicht. Dit betekent dat deze verplichting in de bewerkersovereenkomst zal moeten worden opgenomen. Dit is ook noodzakelijk omdat de verantwoordelijke anders geen weet heeft van een eventueel datalek en hij derhalve eenvoudigweg niet in staat zou zijn om dat te melden.

Protocolplicht verantwoordelijke

De verantwoordelijke zal worden verplicht een overzicht bij te houden van alle inbreuken. Dit betreft niet alleen de meldingsplichtige inbreuken, maar alle geconstateerde inbreuken. Ook als deze niet zijn gemeld. In de memorie van toelichting wordt het belang van dit protocol benadrukt, omdat de toezichthouder achteraf vragen kan stellen aan de verantwoordelijke. Met behulp van dit protocol kan de verantwoordelijke aantonen welke inbreuken hij heeft geconstateerd en welke maatregelen er zijn genomen. Daarnaast moeten de gegevens die aan het CBP zijn verstrekt, alsmede de tekst van de kennisgeving die de verantwoordelijke aan de betrokkene doet, in dit protocol worden opgenomen. Digitale burgerrechtenorganisatie Bits of Freedom heeft ervoor gepleit om

Boete van 1 miljoen Euro of 2% van de wereldwijde jaaromzet wordt geriskeerd

deze protocollen openbaar te (laten) maken. De wetgever gaat daarin echter niet mee, omdat het belang van de vertrouwelijkheid van details met betrekking tot de beveiliging van de gegevensverwerking daaraan in de weg zou staan.

(Opstellen van een 'datalek'-protocol

Aard en inhoud van de melding

Bij de melding moet in ieder geval het volgende worden aangegeven:

- de aard van de inbreuk;
- de instanties waar meer informatie kan worden verkregen over de inbreuk;
- de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken (bijvoorbeeld: het veranderen van gebruikersnamen en wachtwoorden).

Dit laatste punt is iets waar organisaties ons inziens op zouden moeten anticiperen. Omdat de melding onverwijld moet plaatsvinden, is er op het moment dat zich een lek voordoet niet veel tijd om na te denken over eventuele schadebeperkende maatregelen. Wij menen dat organisaties een protocol zouden moeten opstellen met daarin een aantal actiepunten die moeten worden ondernomen op het moment dat er sprake is van een datalek. Daarin zouden ook alvast schadebeperkende maatregelen kunnen worden uitgewerkt voor een aantal mogelijke scenario's. Dit alles maakt dat organisaties sneller kunnen handelen op moment dat zich daadwerkelijk een datalek voordoet en hiermee eventuele schade zoveel mogelijk kunnen beperken. Vanuit het aansprakelijkheidsrecht hebben verantwoordelijken bovendien een schadebeperkingsplicht.

Kennisgeving aan betrokkenen

De aard van de inbreuk kan algemeen worden omschreven. Wanneer een betrokkene wil weten waar hij persoonlijk aan toe is, moet hij contact opnemen met de verantwoordelijke. Dit betekent dat in de kennisgeving contactgegevens moeten worden opgenomen.

Kennisgeving aan het CBP

De kennisgeving aan het CBP is meer omvattend dan de kennisgeving aan betrokkenen. Aan het CBP moeten ook gegevens van technische aard worden gemeld, opdat het CBP in staat is effectief toezicht uit te oefenen. Het kan zijn dat de verantwoordelijke en/of bewerker bij de kennisgeving melding moet maken van technische details die normaliter van vertrouwelijke aard zijn. Desgewenst kunnen bedrijven deze gegevens expliciet als bedrijfsvertrouwelijk in de zin van artikel 10, lid 1 onder c van de Wet openbaarheid van bestuur (WOB) aanmerken. Daarmee wordt voorkomen dat het CBP deze gegevens zal openbaren aan degene die op grond van de WOB daarin inzage zou willen verkrijgen.

> Bits of Freedom pleit om deze protocollen openbaar te maken

Wijze van melden

De wetgever heeft ervoor gekozen de meldingsplicht zo eenvoudig mogelijk te houden. Dit houdt in dat de verantwoordelijke zelf een afweging mag maken aan de hand van een aantal criteria:

- de aard van de inbreuk;
- de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens;
- de kring van betrokkenen;
- de kosten van tenuitvoerlegging.

Deze afweging past volgens de wetgever binnen het systeem van de Wbp. Indien de inbreuk een groot aantal betrokkenen betreft, zou de verantwoordelijke moeten kiezen voor een advertentie in de dagbladen, aldus de memorie van toelichting. Het kan zijn dat in een later stadium nog specifiekere regels aan de kennisgeving worden gesteld bij Algemene Maatregel van Bestuur [9].

Uitzondering meldplicht

Indien de persoonsgegevens zijn beveiligd door bijvoorbeeld encryptie, kan de melding aan betrokkenen wellicht achterwege blijven. Daarvoor is wel vereist dat het redelijkerwijs is uitgesloten dat een datalek kan leiden tot kennisname van persoonsgegevens door onbevoegden.

Aansprakelijkheid verantwoordelijke en/of bewerker?

De verantwoordelijke moet zich goed realiseren dat het voldoen aan de meldplicht nog niet betekent dat hij daarbij is ontheven van eventuele aansprakelijkheid voor schade die voortvloeit uit het toerekenbaar tekortschieten of niet voldoende naleven van de verplichting ex artikel 13 Wbp. Op grond van artikel 49 Wbp is de verantwoordelijke namelijk in beginsel aansprakelijk voor schade die voortvloeit uit het niet naleven van de voorschriften uit de Wbp. De bewerker kan daarnaast zelfstandig aansprakelijk zijn voor schade die voortvloeit uit zijn werkzaamheden. Dit geldt tenzij wordt bewezen dat deze schade niet aan de verantwoordelijke of bewerker kan worden toegewezen. Hieruit volgt het belang van het maken van goede afspraken tussen verantwoordelijke en bewerker.

Preventie: Monitoren werknemers

Hoe kunnen organisaties zich dan weren tegen datalekken? Bedrijven en organisaties zouden bijvoorbeeld kunnen overwegen de werkzaamheden van hun werknemers te monitoren om de kans op datalekken te minimaliseren. Dat zou in veel gevallen opportuun zijn. Recentelijk was te lezen dat werknemers in het Verenigd Koninkrijk steeds vaker worden aangeklaagd voor datadiefstal [10]. De vraag is echter of monitoren van werknemers zomaar mag. Immers, het bijhouden

van wat werknemers doen is een verwerking van persoonsgegevens. Persoonsgegevens mogen alleen worden verwerkt met een legitiem doel. Ook op de werkplek hebben werknemers recht op privacy [11]. Dat geldt in het bijzonder bij privégebruik van aan de werknemers ter beschikking gestelde bedrijfsmiddelen, zoals internettoegang, een e-mailbox of een I-pad. Bedrijfsmiddelen zijn eigendom van de werkgever en daarom mogen werkgevers wel eisen stellen aan het gebruik ervan. De regels omtrent het gebruik van bedrijfsmiddelen, zoals internet- en e-mailgebruik, moeten van tevoren worden vastgelegd in een reglement (ICT-protocol) dat aan de werknemer kenbaar wordt gemaakt. Ook moet in het reglement worden opgenomen wat de sancties zijn bij overtreding hiervan. In de regel gaat het recht op privacy van de werknemer voor op het bedrijfsbelang van de werkgever. De werkgever moet kunnen aantonen dat hij een redelijk vermoeden van wangedrag heeft, alvorens hij mag overgaan tot monitoren.

Aan de hand van een praktijkvoorbeeld zullen wij illustreren hoe de rechter met het monitorenvraagstuk pleegt om te gaan. In een recente rechtszaak deed zich het volgende voor. Een werknemer mailde naar een zakelijke klant de volgende teksten:

"(..) I can tell you it is impossible to work with pigs, and that is what I am facing now!"

en

"(..) Das wissen wir auch nicht was da los ist, es ist hier ein komplett chaos.(..)".

In een ICT-protocol zullen echter vooral verbodsbepalingen staan

De systeembeheerder van zijn werkgever kwam deze e-mails tegen bij een routinecontrole. De vraag die daarop volgde was destijds: "mag dat zomaar en wat kan het bedrijf tegen die werknemer doen?" Tegen de vader van de desbetreffende werknemer, die bij hetzelfde bedrijf werkzaam was, liep op dat moment een ontslagaanvraag. Wellicht is dat één van de redenen waarom de werknemer zich jegens klanten negatief uitliet over het bedrijf. Het bedrijf stelde zich op het standpunt dat zij de zakelijke e-mail zou mogen monitoren daar zij daartoe een gerechtvaardigd doel had en er in casu verdenkingen bestonden dat er meerdere werknemers bij betrokken waren. De werknemer daarentegen stelde zich op het standpunt dat het inkijken in de e-mail een inbreuk op zijn privacy vormde. Volgens hem dienden de e-mails dan ook niet mee te worden genomen in een ontslagprocedure. De kantonrechter was uiteindelijk van mening dat het monitoren van zakelijke e-mail gerechtvaardigd is [12]. Een werknemer mag en kan verwachten dat het bedrijf waarvoor hij werkt, eerder dan bij privé-berichten, de inhoud van de zakelijke e-mailberichten zal bekijken. In dit geval vond de rechter de inbreuk op de privacy van de werknemer dan ook gerechtvaardigd en proportioneel.

In een andere - vergelijkbare - zaak was er sprake van een werknemer die via zijn privé Gmail-account correspondentie voerde over het opzetten van een nieuw concurrerende vennootschap in China. Bovendien bleek uit het privé e-mailadres dat hij producttechnische tekeningen van het bedrijf kopieerde. In dit geval werd zijn privé e-mail soms ook zakelijk gebruikt. Uiteindelijk kreeg het bedrijf inzicht in die e-mails, waarna de werknemer op non-actief werd gezet. Het Gerechtshof stelde vast dat in casu het bedrijf geen toestemming had om de privé e-mail te bekijken [13]. Deze e-mailbox werd bovendien slechts sporadisch zakelijk gebruikt. Het Hof laat de werkgever toe om duidelijkheid te verschaffen hoe en wanneer zij toegang had tot het account en wat de status daarvan was.

Preventie: ICT Protocol

Bovenstaande voorbeelden betreffen het lekken van relatief onschuldige informatie, alhoewel het grote reputatieschade voor het bedrijf met

zich mee kan brengen. Maar stel dat werknemers, al dan niet bewust, veel belangrijkere bedrijfsinformatie lekken. Ze mailen het per ongeluk naar een klant, ze zetten het in de cloud zonder dat daarbij duidelijk is wie de eigendom van de informatie toekomt of ze downloaden software waarmee ze virussen binnenhalen die er uiteindelijk voor zorgen dat informatie beschikbaar wordt voor hackers.
Teneinde het lekken van informatie zoveel mogelijk te beperken, is het raadzaam een zogenaamd ICT-protocol te hanteren. In zo'n protocol kan de wijze waarop werknemers om dienen te gaan met informatie- en communicatietechnologie worden aangegeven. Zo'n protocol kan dan de gedragsregels en richtlijnen bevatten ten aanzien van het verantwoord en onverantwoord gebruik van de ICT-voorzieningen binnen en buiten de muren van het bedrijf.
Bovendien kunnen bedrijven met een ICT-protocol in de hand controles op het 'digitale' gedrag van hun werknemers legitimeren.

Organisaties zouden hun systemen en werkwijzen moeten aanpassen

Veel bedrijven, maar ook scholen, ziekenhuizen en andersoortige organisaties, hanteren al een soort reglement waarin het de gebruikers van hun ICT-voorzieningen verboden wordt bepaalde handelingen op het internet uit te voeren. Zo'n reglement zou echter veel breder moeten zijn. Gebruikers zouden idealiter moeten verklaren dat zij de ICT-voorzieningen en -diensten primair zullen gebruiken in het kader van de uitoefening van hun werkzaamheden en overeenkomstig hun functie. Daarbij zouden bedrijven kunnen overwegen een functionaris aan te stellen die verantwoordelijk is voor de correcte uitvoering en naleving van het bepaalde in het ICT-protocol. Overigens is het maar zeer de vraag of het gebruik van ICT-voorzieningen voor persoonlijke doeleinden volledig kan worden verboden. Dergelijk gebruik kan echter wel beperkt worden.

In een ICT-protocol zullen echter vooral verbodsbepalingen staan. Zo is het raadzaam werknemers te verbieden software te downloaden zonder toestemming van de functionaris. Tevens verdient het aanbeveling werknemers te wijzen op de risico's van het gebruik van sociale media, zowel binnen als buiten werktijd. Tot slot loont het bedrijven de moeite erover na te denken of zij wensen dat hun werknemers gebruik maken van cloudtoepassingen. Men vergeet nogal eens dat daaronder bijvoorbeeld ook Dropbox, Hotmail, Gmail en webmail van providers dienen te worden verstaan. De voorwaarden die die cloudaanbieders hanteren, kunnen in sommige gevallen ernstig nadelig zijn voor het bedrijf, de eigenaar van de gegevens die in die cloudtoepassing worden geüpload. In sommige gevallen is er op grond van die voorwaarden zelfs sprake van overdracht van het (intellectueel) eigendom van die data.

Uiteraard vallen dergelijke ge- en verboden slechts aan werknemers op te leggen indien zij daarmee in (moeten) stemmen en er adequate sanctioneringsmaatregelen zijn overeengekomen. Overigens dient daarbij opgemerkt te worden dat in veel gevallen de ondernemingsraad van het bedrijf toestemming moet verlenen voordat het ICT-protocol kan worden ingevoerd.

Of een ICT-protocol een adequaat middel is om datalekken door menselijke fouten zoveel mogelijk te voorkomen en aldus eventuele schade te beperken, zal de praktijk moeten uitwijzen.
Naast misstappen van personeel zijn er namelijk nog een aantal veel voorkomende oorzaken van dataverlies. Zo wordt er lang niet altijd een effectieve back-up gemaakt, worden data verwijderd die nog steeds in gebruik zijn, wordt het IT-beveiligingsbeleid niet getest of heeft men geen up-to-date antivirussoftware [14]. Een ICT-protocol is in ieder geval een belangrijke eerste stap om ondernemingen en hun werknemers bewust te maken van de gevaren van de omgang met de ICT-voorzieningen van hun bedrijf. Het is een onderdeel van de organisatorische aanpassingen van een onderneming teneinde datalekken te voorkomen. Voorbeelden van werknemers die kwaad willen en daarom doelbewust informatie lekken of zich doelbewust negatief uitlaten over hun werkgever zijn gemakkelijk te bedenken. In de praktijk komt het echter veel meer voor dat er onbewust informatie gelekt wordt. Door werknemers een ICT-protocol te laten tekenen en hen daarbij uitleg te verschaffen, worden zij bewust gemaakt van de risico's die zij,

en niet in de laatste plaats het bedrijf waarvoor zij werkzaam zijn, kunnen lopen. Een datalek ontstaat immers sneller dan men denkt. De eventueel negatieve gevolgen van een datalek kunnen middels een ICT-protocol wellicht (indirect) deels worden afgewenteld op de werknemer die het lek heeft veroorzaakt.

Aanbeveling: richt een adequaat informatiebeveiligingsbeleid in

Zoals besproken brengt het huidige wetsvoorstel een aantal wijzigingen met zich mee die gevolgen hebben voor organisaties. Hoewel de wet nog niet is aangenomen en er in het wetgevingsproces nog het nodige kan worden gewijzigd, is de algemene verwachting dat de meldplicht er komt. Om daarop te anticiperen signaleren wij dat er tenminste op een drietal terreinen het nodige moet veranderen. Ons inziens zouden organisaties hun systemen en werkwijzen moeten aanpassen op zowel technisch, organisatorisch als op juridisch vlak. Door deze driepoot op orde te brengen kunnen bedrijven voldoen aan de op hen rustende beveiligingsplicht op grond van de Wbp, waarmee ze de kans op datalekken en de daaruit voortvloeiende schade kunnen verkleinen.

In technisch opzicht moeten organisaties er voor zorgen dat de beveiliging van hun systemen voldoet aan het passende beveiligingsniveau als bedoeld in artikel 13 Wbp. Wat daaronder dient te worden verstaan verschilt per onderneming en per categorie data. Het is derhalve ondoenlijk om concreet een beveiligingsniveau aan te geven. Het is van bijzonder belang om de gegevens die men verwerkt goed in kaart te brengen en zo mogelijk te classificeren om het beveiligingsniveau in te kunnen schalen.

Op organisatorisch gebied kan worden gedacht aan het opstellen van protocollen waarin de gewenste werkwijzen en processen in een organisatie worden vastgelegd. Vooraf kan men zijn werknemers, al dan niet aan de hand van protocollen, bewust maken van de gevaren die het omgaan met de ICT-voorzieningen en (vertrouwelijke) data met zich mee kunnen brengen en waar men voorzichtigheid dient te betrachten. Dit kan bijvoorbeeld door het hanteren van een ICT-protocol. Indien zich een datalek heeft voorgedaan is het juist weer zaak dat men snel weet hoe te handelen. Dit kan door het hanteren van een 'datalek'-protocol waarin wordt vastgelegd wat er moet gebeuren om te voldoen aan de ophanden zijnde nieuwe verplichtingen uit de Wbp en hoe (verdere) schade zoveel mogelijk kan worden voorkomen of beperkt.

Ook juridisch kunnen organisaties de nodige maatregelen nemen. Voor verantwoordelijken of bewerkers die gehouden zijn een bewerkersovereenkomst te sluiten kan het verstandig zijn daarin al rekening te houden met de aankomende meldplicht. Eveneens kan men vooruitlopen op de eventuele boetes die opgelegd worden als gevolg van het niet naleven van de meldplicht en dan uiteraard met name ten aanzien van de vraag voor wiens rekening die dienen te komen. Contractueel gezien kunnen organisaties hun aansprakelijkheid voor schade uitsluiten en/of beperken.

> Verantwoordelijken of bewerkers kunnen al rekening houden met de aankomende meldplicht

Conclusie

Datalekken lijken, ondanks een ICT-protocol en adequate beveiligingsmaatregelen, niet geheel uit te sluiten. Organisaties kunnen echter veel ondervangen met goede contracten en het creëren van bewustzijn bij werknemers. Daarmee kan de schade die zal ontstaan als gevolg van het datalek zo veel mogelijk worden beperkt en tonen organisaties hun goede wil, wat eventueel bij een aansprakelijkheidstelling mee zal wegen. Wij raden bedrijven dan ook aan om hun processen en werkwijzen zoveel als mogelijk te protocolleren, zowel preventief als repressief, en in hun contracten goede aansprakelijkheids- en boetebepalingen op te nemen.

Links

[1] *Zie o.m. : 'VCD blundert met online verzuimregistratie', 20 april 2012, computable.nl, http://www.computable.nl/artikel/nieuws/security/4492289/1276896/vcd-blundert-met-onlineverzuimregistratie.html.*

[2] *'Twitter ontkent hack van gebruikersaccounts', 22 augustus 2013, informatiebeveiliging.nl, https://informatiebeveiliging.nl/nieuws/twitter-ontkent-hack-van-gebruikers/.*

[3] *'Groene Hart Ziekenhuis lekt medische dossiers', 7 oktober 2012, Nu.nl, http://www.nu.nl/binnenland/2927832/groene-hart-ziekenhuis-lekt-medische-dossiers.html.*

[4] *Kamerstukken II 2012/13, 33 662, nr. 1. Eerder werd al een internetconsultatie over dit onderwerp gehouden, zie: http://internetconsultatie.nl/camerabeelden. Het wetsvoorstel wordt momenteel behandeld door de Tweede Kamer.*

[5] *Zie voor een overzicht de memorie van toelichting bij het wetsvoorstel datalekken: Kamerstukken II 2012/13, 33 662, nr. 3 (MvT), p. 2-3 . Het voert te ver om in het bestek van dit artikel de diverse meldplichten uitvoerig te bespreken. Ik noem slechts de Cyber Security Richtlijn waarin een meldplicht voor een inbreuk op de veiligheid of een verlies van integriteit van elektronische informatiesystemen (hierna ook: ICT-inbreuken) wordt geïntroduceerd.*

[6] *COM (2012), 11 def.*

[7] *Kamerstukken II 2012/13, 33 662, nr. 3 (MvT), p. 2.*

[8] *CBP richtsnoeren: 'Beveiliging van persoonsgegevens', februari 2013,te raadplegen via: http://www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf.*

[9] *Zie: artikel 34a lid 11 wetsvoorstel.*

[10] *'Werknemers vaker aangeklaagd voor datadiefstal', 4 september 2013, webwereld.nl, http://webwereld.nl/beveiliging/79140-werknemers-vaker-aangeklaagd-voor-datadiefstal.*

[11] *EHRM 3 april 2007, nr. 62617/00, NJ 2007, 617 (Copland / Verenigd Koninkrijk).*

[12] *Ktr. Rotterdam, 21 september 2011, ECLI:NL:RBROT:2011:BU4848.*

[13] *Hof 's-Hertogenbosch, 19 maart 2013, ECLI:NL:GHSHE:2013:BZ5206.*

[14] *'De 5 domste oorzaken van dataverlies', 9 augustus 2013, AutomatiseringGids.nl, http://www.automatiseringgids.nl/nieuws/2013/32/de-5-domste-oorzaken-van-dataverlies.*

COLUMN: VERANTWOORDE ONTHULLINGEN

A MAN IN THE MIDDLE OF MONEY AND MEDIA

ING WEIGERT ONTWERPFOUTEN TE ERKENNEN IN DE MOBIEL BANKIEREN APP (2012)

Herinnert u zich de campagne "3x kloppen" nog? Die werd in 2007 gelanceerd door de Nederlandse Vereniging van Banken en is sindsdien onderdeel van het standaardrepertoire om klanten te wapenen tegen internetcriminelen. Stel jezelf bij online betalingen de volgende drie vragen: klopt mijn pc-beveiliging, klopt de website en klopt de betaling?

Hacker @floorter ontdekte begin 2012 dat de bankierenapp van de ING dat zelf onvoldoende deed en kwetsbaar was voor een man-in-the-middle-attack. Dat terwijl al 800.000 mensen de app hadden gedownload en ongeveer 300.000 hem dagelijks gebruikten.

Hij meldde het lek, maar er gebeurde niets. Pas toen hij er een blog over schreef en EenVandaag erbij kwam, luisterde de bank en werd de bug gefixed. Zonder enige erkenning voor Terra's vondst.

Floor Terra is een prototype ethische hacker. Hij is zowel handig in het begrijpen van complexe systemen als betrokken bij het maatschappelijk welzijn. Bij het NIKHEF deed hij data-analyse en onderhield hij de controle- en meet software. Hij was ook een tijdje docent. Op zijn blog floort.net/blog snijdt hij regelmatig actuele veiligheidskwesties aan. Hij heeft ook een blauwdruk gepubliceerd voor verantwoorde onthullingen op responsibledisclosure.nl. Als hij een beveiligingsprobleem vindt, meldt hij het eerst bij de eigenaar van het systeem en niet zoals anderen wel eens doen bij de pers.

De bankierenapp van de ING hoefde hij niet eens te hacken. Hij zag al aan het ontwerp hoe kwetsbaar de app was en belde de ING helpdesk. De medewerker aan de lijn stelde dat de app wel echt veilig was en nam de melding in ontvangst. Terra hoorde weken niets en zette daarom zijn vermoedens 15 januari op zijn blog [1]. Met de vraag: "Mag ik concreet aantonen dat de applicatie slecht beveiligd is om mijn stelling te onderbouwen?" want hij wilde niet de wet overtreden. Toen reageerde de bank wel. Terra werd uitgenodigd om uit te leggen wat hij had gevonden. EenVandaag wilde ook uitleg. Dat kon, maar eerst wilde hij als ethische hacker ING de tijd geven om het lek te dichten. Half maart was de bug eindelijk gefikst. De journalist kon over gaan tot onthulling.

In de uitzending van 21 maart 2012 [2] komt Terra aan het woord: "In eerste instantie dacht ik, ze zullen toch niet *dit* vergeten zijn? Dat heb ik gecontroleerd en binnen een uurtje had ik het zo uitgewerkt dat ik kon afluisteren wat voor verkeer er over ging en mijn eigen server er tussen zetten en te doen alsof ik de ING was." Wat hij ontdekt zou hebben, wordt verbeeld met een animatie van een bank, mobiel en slot dat doorgekruist wordt. Vervolgens komt professor Bart Jacobs in beeld. Na lof voor Terra's werk, legt hij uit dat een man-in-the-middle bedragen en rekeningnummers zou kunnen veranderen. "Dit is een blammage. Hierom wordt ING in security kringen hard uitgelachen." ING zelf reageert alleen schriftelijk, stelt dat de app wel veilig is, zonder melding van Terra's tips. Slechte bank dus.

De avond van de uitzending van EenVandaag twittert @mount_knowledge aan @floorter: "ING app SSL issue is oud nieuws. Ik schreef hier in November al over". En inderdaad, in deze blog [3] van Richard van den Berg werd het probleem al netjes uitgelegd. @floorter: "In dat geval heeft de ING dus keihard tegen mij gelogen toen ze zeiden dat er nooit eerder zoiets gemeld was. Als dit soort security meldingen niet centraal gecoördineerd worden, is dat op zichzelf ook een probleem."

Maar wat was er nu werkelijk mis met de app? ING gebruikte een standaard SSL, die geen controle deed op een reeks attributen van het certificaat. Je zou dus kunnen doen alsof je de server van de ING was met een nep certificaat. Of je dan ook werkelijk kon frauderen, kon Terra echter niet testen, omdat hij daar geen toestemming voor kreeg. Wel kon hij zien aan de update die erop volgde, dat de bank precies dat had aangepakt. Hij had dus gelijk, zonder dat de bank dat wilde erkennen. Dat is jammer, want ING mist hiermee gratis advies en zullen hackers in het vervolg meteen naar de media stappen.

Vlak voor de deadline van deze column krijg ik nog een DM van @floorter. De bank heeft nu ook een meldpunt. Heb mijn tekst direct gemaild naar responsible-disclosure@ing.nl met de vraag of @floorter de aanleiding was. Diezelfde dag antwoordt ING: "De invoering van responsible disclosure is een actie vanuit de verschillende Nederlandse banken in samenwerking met de NVB." Komt het toch nog goed in Nederland. ●

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

Volgende aflevering in *verantwoorde onthullingen*:
"Toen @UID_ de kazerne belde met een fabriekswachtwoord."

Links

[1] Floor's Blog: http://floort.net/blog/verantwoordelijkheid-voor-beveiliging.html
[2] EenVandaag: http://www.eenvandaag.nl/binnenland/40032/mobiel_bankieren_ing_maandenlang_onveilig
[3] Mount Knowledge blog: http://www.mountknowledge.nl/2011/11/09/ing-mobiel-bankieren-authenticatie/
[4] Meldpunt ING: http://www.ing.nl/de-ing/veilig-bankieren/veiligheidsbeleid-van-de-ing/meldpunt-kwetsbaarheden/index.aspx

Reactie ING

ING heeft responsible disclosure ingevoerd, omdat wij het belangrijk vinden dat klanten veilig kunnen bankieren. Wij stellen ons daarom open voor deskundigen om ons hierbij te ondersteunen door een gevonden mogelijke kwetsbaarheid aan ons te melden. De invoering van responsible disclosure is een actie vanuit de verschillende Nederlandse banken in samenwerking met de NVB. Responsible disclosure wordt ook in andere branches toegepast om een kwetsbaarheid in een systeem te kunnen melden. De specifieke zaak van Floor Terra is hiervoor niet de aanleiding geweest.

OPEN SOURCE COMPLIANCY VAN BELANG VOOR CONTINUÏTEIT

J.W. Oordt, IT-jurist bij Software Borg – info@softwareborg.nl

Enkele maanden geleden velde het Landgericht Hamburg een oordeel in de zaak die door softwaremaker Harald Welte was aangespannen tegen hardwareleverancier Fantec [1]. Welte stelde voor de Duitse rechter dat Fantec in strijd handelt met de voorwaarden van de GNU General Public License V2 Open Source licentie. Onder deze voorwaarden was de door Welte ontwikkelde "netfilter/iptables" software beschikbaar. Onderdelen van deze software zitten in de firmware van de mediaplayers die door Fantec worden verhandeld. De broncode van de software van Welte werd door Fantec niet conform de GPLv2-licentie openbaar gemaakt. De rechter constateert schending van de licentievoorwaarden en veroordeelt Fantec onder meer tot het betalen van een boete aan Welte.

Open source software is software die door de maker samen met de daarbij horende broncode voor een ieder beschikbaar is gemaakt. Het gebruik van open source in software neemt flink toe, zo constateert technisch onderzoeksbureau Gartner in 2012 [2]. Het gebruik van open source software heeft namelijk diverse voordelen. Zo zijn er aanmerkelijke kostenbesparingen, omdat voor open broncode niet betaald hoeft te worden. De open broncode kan voorts door een ieder verder worden ontwikkeld, waardoor men niet afhankelijk is van de initiële maker. Een gebruiker kan dus zelf de software voorzien van de door hem gewenste functionaliteit. Ook commerciële softwareleveranciers gebruiken daarom steeds vaker open source in hun producten. In deze bijdrage wordt besproken welke gevolgen het gebruik van open source heeft voor softwareontwikkelaars en hun klanten.

De werking van het open source model

De insteek van open source is het gebruik van het auteursrecht ten behoeve van het vrij beschikbaar maken en vooral houden van een broncode. Het auteursrecht dat op open source rust, stelt de softwaremaker in staat om voor te schrijven onder welke voorwaarden de broncode mag worden gebruikt. De toestemming van de softwaremaker om de broncode te gebruiken (de licentie), wordt slechts verleend en blijft slechts in stand wanneer aan die voorwaarden wordt voldaan. Wanneer dat niet gebeurt, kan de softwaremaker handhavend optreden. Zo kan de softwaremaker van een gebruiker die niet voldoet aan de licentievoorwaarden succesvol een schadevergoeding of zelfs de stopzetting van het gebruik van de broncode vorderen. Dat open source code vrij te gebruiken is, betekent dus niet dat de gebruiker kan doen en laten wat hij wil.

Het verschil met closed source licenties, is dat in open source licenties de licentievoorwaarden gericht zijn op het vrij beschikbaar houden van de broncode. De gebruiker van open source moet bijvoorbeeld in de nieuwe broncodes die hij daarmee ontwikkelt, verwijzen naar de maker van de open source en de vindplaats. Ook kan worden bepaald dat een gebruiker van open source, de bijbehorende licentietekst of de oorspronkelijke broncode beschikbaar moet stellen.

De meest gebruikte open source licentie is de GNU General Public License. De gebruiker wordt in de GPL licentie toegestaan om een verveelvoudiging van de open source broncode te maken of om de code te bewerken. Dit mits de gebruiker ervoor zorgt, dat hij deze verveelvoudiging of bewerking onder de dezelfde licentievoorwaarden openbaar maakt. Deze voorwaarde wordt ook wel een *copyleft bepaling* genoemd.

Gebruik van open source in commerciële software: geen vrijheid, blijheid

Het gebruik van open source gaat eenvoudig, aangezien het niet nodig is om uitdrukkelijk een licentiecontract te tekenen met de softwaremaker. De licentievoorwaarden worden met de open source broncode meegeleverd. Wie vervolgens de broncode verspreidt, bewerkt of verwerkt in eigen software, wordt geacht akkoord te zijn gegaan met de licentievoorwaarden. Dit geldt ook voor commerciële softwareontwikkelaars die open source verwerken in hun (closed source) producten.

Opmerkelijk is dat, gelet op de verstrekkende bepalingen die open source licenties kunnen bevatten, niet alle commerciële softwareontwikkelaars zorgvuldig omgaan met het gebruik van open source. Onterecht wordt bij open source nog gedacht aan "vrijheid, blijheid". Dit terwijl open source licenties vergaande verplichtingen

Open source en broncode-escrow

De Software Borg Stichting levert oplossingen op het gebied van software continuïteit, met broncode-escrow als core business. In het kader van de broncode-escrow onderzoekt Software Borg of de partij die een broncode deponeert bij een IT-notaris (www.it-notaris.nl), tevens houder is van het daarop rustende auteursrecht. Dit wordt het *titelonderzoek* genoemd. Als onderdeel van het titelonderzoek, wordt een *open source compliancy audit* uitgevoerd. In de documentatie van het ontwikkelingsproces en in overleg met de softwareontwikkelaar wordt bekeken of, en zo ja welke open source componenten zijn gebruikt. Ook heeft Software Borg speciale software ontwikkeld, waarmee in de broncode op open source componenten wordt gescand. Wanneer deze in kaart zijn gebracht, wordt vervolgens bekeken aan welke licenties de softwareontwikkelaar zich dient te houden en of hij dat doet. Wanneer de softwareontwikkelaar niet compliant is, dient dat te worden gerepareerd alvorens de broncode wordt gedeponeerd. Dit omdat anders het risico bestaat dat de auteursrechthebbende op de open source componenten, afgifte of het gebruik van de gedeponeerde broncode tegenhoudt.

kunnen bevatten. Wanneer niet aan deze verplichtingen wordt voldaan, kan de auteursrechthebbende softwaremaker het gebruik van de open source componenten tegenhouden. Commerciële softwareontwikkelaars lopen zo het risico dat ze niet meer kunnen voldoen aan hun verplichtingen tegenover hun klanten. Onderhoud op de broncode kan bijvoorbeeld niet worden uitgevoerd, wanneer deze niet meer mag worden gebruikt. Anderzijds kunnen softwareontwikkelaars, wanneer zij wel aan de verplichtingen in de open source-licenties voldoen, verplicht zijn om onderdelen van de broncode van hun eigen (commerciële) softwareproduct vrij beschikbaar te maken. Hiertoe was bijvoorbeeld navigatiebouwer TomTom verplicht, nadat zij open source componenten verwerkte in haar 'GO'-programmatuur. Inmiddels is een aantal van de broncodes van die software gepubliceerd op het internet [3]. De door TomTom gebruikte open source-componenten waren overigens ook ontwikkeld door Harald Welte.

Voor commerciële software-ontwikkelaars betekent dit niet dat zij per definitie moeten afzien van het verwerken van open source componenten in hun product.
Het vermijden van open source kan immers ook extra kosten (want: extra ontwikkelwerk) met zich mee brengen. Allereerst bevatten niet alle open source licenties vergaande copyleftbepalingen. Een voorbeeld van een ruime open source licentie is de Berkeley Software Distribution (BSD) licentie. Deze bevat geen copyleft-bepalingen, maar eist alleen dat de auteursrechthebbende wordt genoemd, de licentietekst beschikbaar is en de naam van de auteursrechthebbende niet wordt gebruikt voor promotiedoeleinden. Voorts is de toepasselijkheid van copyleft-bepalingen afhankelijk van de manier waarop softwaremakers open source in hun eigen product opnemen. De GPL-licentie bijvoorbeeld, leert dat daarvoor het enkele aanroepen van open source componenten niet voldoende is. Daarnaast vallen de onderdelen van de commerciële software die zonder de open source componenten kunnen werken, niet onder de GPL copyleftbepalingen. Dit is evident anders wanneer bij het tot stand brengen van commerciële software de open source-componenten als basis en vertrekpunt worden gebruikt.

Commerciële softwareontwikkelaars kunnen dus probleemloos gebruik maken van open source, mits zij dit op een zorgvuldige manier doen. Voor het gebruik van open source componenten moet duidelijk zijn welke licentievoorwaarden moeten worden nageleefd en op welke manier de componenten technisch gezien worden verwerkt in het commerciële product. Wanneer veel verschillende open source componenten worden gebruikt en ook toeleveranciers van de softwareontwikkelaar met open source werken, kan de inzet van een juridisch expert noodzakelijk worden om de open source-compliancy te bewaken. Zorgvuldig omgaan met open source voorkomt vervelende verrassingen voor de (commerciële) softwareontwikkelaar en zijn gebruikers.

Continuïteit van de gebruiker

Ook voor de continuïteitspositie van organisaties die closed source software gebruiken, is het van belang dat hun softwareleverancier voldoet aan de licentievoorwaarden die horen bij de inzet van open source. Het onderhoud en de doorontwikkeling van het commerciële softwareproduct is immers afhankelijk van de toestemming om de daarin verwerkte open source componenten te mogen gebruiken. Wanneer de softwareleverancier die toestemming niet heeft, kunnen die werkzaamheden stil komen te liggen. Om dezelfde reden is het noodzakelijk, dat ook in het kader van broncode-escrow wordt bekeken of een software leverancier zich conformeert aan de licentievoorwaarden die zijn verbonden aan de open source software die hij gebruikt (zie ook kader 1). ●

Links

[1] *http://www.ifross.org/sites/default/files/130618%20Urteil%20Fantec.pdf*
[2] *http://www.gartner.com/id=2098416*
[3] *http://www.tomtom.com/en_gb/gpl/*

ADVERTORIAL

ONTWIKKEL APPS MET SECURITY ALS UITGANGSPUNT

Bedrijven die 'enterprise mobility' breed hebben omarmd, worden geconfronteerd met een nieuw kwetsbaar punt in de beveiliging: de mobiele applicaties. Met een Mobile Device Management-oplossing kunnen veel security-issues achteraf worden opgelost, maar lang niet altijd is het mogelijk om de mobiele devices van de gebruiker te beheren en controleren. Dan is het beter om de benodigde beveiligingsmaatregelen direct in te bouwen in de mobiele applicaties zelf.

Onderweg nog even snel klantgegevens raadplegen, planningen inkijken of patiëntgegevens inzien; steeds vaker worden mobiele apps ingezet om gevoelige informatie op te halen uit bedrijfssystemen. Deze mobiele apps worden beschikbaar gesteld door de leveranciers van bijvoorbeeld ERP- en CRM-systemen, maar ook steeds vaker gebouwd door de IT-afdeling zelf en aangeboden via een zakelijke 'app store' of de applicatiewinkels van Google, Apple, BlackBerry en Microsoft.

Onvolwassen technologie

Mobiele applicaties zijn daarmee in het zakelijk domein terechtgekomen, een domein waar beveiliging cruciaal is. Het mag immers niet gebeuren dat hackers via de mobiele app meekijken in zakelijke systemen en bedrijfskritische gegevens aanpassen of stelen.
De meeste mobiele apps kunnen zich op het gebied van beveiliging echter nog niet meten met de 'traditionele' bedrijfsapplicaties die vaak al jaren in gebruik zijn. Daarvoor zijn de gebruikte technologie en de beschikbare beveiligingsmaatregelen nog niet volwassen genoeg. Waar het bij de ontwikkeling van webapplicaties gebruikelijk is om de geldende (ISO-) normen en richtlijnen aan te houden, is dat bij de ontwikkeling van mobiele applicaties nog minder gebruikelijk.

Apps veilig gebruiken

Het is daarom van groot belang om een aantal algemene uitgangspunten te formuleren voor een veilig gebruik van mobiele applicaties. Zo is het nooit verstandig om een apparaat te *jailbreaken* om een specifieke mobiele app correct te laten functioneren. Uiteraard moeten ook altijd de actuele updates van het mobiele besturingssysteem worden gedraaid.
Voor het benaderen van bedrijfskritische gegevens zijn platformspecifieke apps, die gebruikmaken van de beveiligingsmaatregelen die in het platform zitten, bovendien te verkiezen boven HTML5-apps.

Om vervolgens de juiste beveiligingsmaatregelen te kunnen nemen, is het belangrijk om de risico's goed af te wegen. Motiv onderscheidt daarbij drie risiconiveaus:

- Public. In dit geval zijn de risico's laag en kan worden volstaan met 'minimale' beveiligingsmaatregelen. Versleuteling van het verkeer is zo'n minimale maatregel die altijd aanwezig moet zijn. Ook moet worden nagedacht over het identificatie- en verificatieproces en op regelmatige basis moet worden gecontroleerd of de app nog correct functioneert.
- Confidential. Als een app bijvoorbeeld wordt gebruikt om transactiesystemen te raadplegen, zijn aanvullende beveiligingsmaatregelen noodzakelijk om de confidentiële informatie te beschermen. Voorbeelden van aanvullende maatregelen zijn het verifiëren van de identiteit van de gebruiker door middel van two-factor authenticatie via een server en het valideren van de applicatie voorafgaand aan iedere sessie. Aan de hand van de 'vingerafdruk' van de applicatie kan worden gekeken of er ongeautoriseerde wijzigingen zijn doorgevoerd in de app.
- High secure. Op dit niveau kan er bijvoorbeeld voor worden gekozen om data-encryptie op het toestel verplicht te stellen voor alle lokaal opgeslagen gegevens, updates van de mobiele applicatie te forceren en een applicatie controleerbaar te maken vanuit een MDM-oplossing.

Kwaliteitscriterium

De beveiligingsmaatregelen die aan de hand van de risicoafweging worden geselecteerd, moeten al in de ontwikkeling van de applicatie worden meegenomen. Op die manier wordt informatiebeveiliging als een onlosmakelijk kwaliteitscriterium meegenomen in het ontwikkeltraject en niet achteraf tegen de applicatie aan geplakt. Ook na de oplevering van een applicatie moet de beveiliging regelmatig worden gecontroleerd. Op die manier wordt voorkomen dat updates of kleine wijzigingen in de applicatie grote gevolgen hebben. ●

> Versleuteling van het verkeer is een minimale maatregel

Rohald Boer (rohald.boer@motiv.nl) is Business line manager Application Development bij ICT Security-specialist Motiv

COLUMN: ATTRIBUTER

TRACEABLE

Traceable is a Business Attribute from the SABSA Business Attributes Taxonomy that is well established in many disciplines but is as yet immature in the field of information security and IT security. We are all familiar with it in our daily lives too.

The Attributer has a wife who is exceptionally quick witted and who can process thoughts at a speed that leaves him (The Attributer) struggling to keep up. So fast in fact that she (The Attributer's Wife) does not always find the time to speak what these thoughts might be, and he, being an ordinary mortal, cannot always see the connection between the new topic of conversation and the previous one, even though such a connection exists. However, the situation is mitigated by the fact that The Attributer's Wife is also a 'SABSA Widow', meaning that she is accustomed to SABSA intruding a great deal into her domestic and social life, and that as a result she has been exposed to a lot of SABSA thinking and is fully conversant with the concept of 'traceability'. Thus when he says: "I need more traceability" she immediately understands how to provide a remedy for his slow-witted brain activity. She fills in the missing links and makes it all traceable.

Consider industries beyond IT and information management. Food production has a health and safety issue associated with it. Should it become necessary to withdraw a food product because it is contaminated, all items from that production batch must be traced. The same applies to the pharmaceutical industry. Batch numbers and dates have been used for this purpose for a long time. Traceability is key to food and drug safety. The motorcar industry is similar in that safety is an issue and from time to time a particular make and model will be found to have a design fault and must be recalled for modification. This requires similar traceability – to be able to find all the cars that fall into that set. The entire mechanical and electrical engineering industry has for a long time used serial numbers to identify individual items and to be able to trace them and their whereabouts for all types of support purposes. So, we see that traceability is not a new concept and is well established as normal practice in many industries.

When we examine IT and information security practice, we find that the otherwise widespread use of traceability is not applied. There is a close parallel to be drawn between 'safety' and 'security' (in French the words are the same). So it seems strange that when we construct security solutions we do so in a way that is not directly traceable to the requirements that the business has for being 'secured'. Looked at from the outside, the IT security controls and practices that are commonly deployed can be seen as little more that anecdotal folklore. The 'best practice' is to take a list of controls compiled by others and to apply these widely in the hope that this will defend the business information and IT systems from the threats that abound in our current business world. The technical and process designs are not traceable to the actual business risks and are not even seen in business terms.

The 'carpet bombing' approach taken by so many organisations is neither effective nor efficient. Some controls are surplus to requirements, other requirements are not adequately met by the control set, because there is no way of tracing and matching business risks with controls. One must question then how can such an approach be regarded as being 'in control' of the business when there is no way to demonstrate that actual business risks have been addressed.

In contrast, SABSA embeds the concept of two-way traceability. If a business identifies a risk, then it should be clear exactly how that risk is to be addressed. It should also be possible to monitor the performance of the specific controls to report back how much risk is actually being experienced and what residual risk is retained. Each control should be business-justified by forward traceability and the successful management of each business risk should be reported by backwards traceability. Controls that do not derive directly from a business requirement are not required. Acceptable risk levels are specified by the business as part of its risk appetite.

SABSA achieves traceability of controls through Business Attributes Profiling. The business requirements are distilled into individual Attributes, each of which is associated with a measurement approach and a performance target. Measurements during the operational lifecycle can be fed back and reported through a risk dashboard or scorecard. For a business that wishes to demonstrate that it is 'in control' how else could this be done? ●

The Attributer

PENETRATIETESTEN UIT HET VERLEDEN BIEDEN GEEN GARANTIE VOOR DE TOEKOMST

Coen Steenbeek is manager bij het Security & Privacy team van Deloitte Risk Services. Hij is meer dan 6 jaar werkzaam bij Deloitte en speelt momenteel een belangrijke rol in de ontwikkeling en lancering van de dienst Hacking as a Service. Coen kan bereikt worden via CSteenbeek@deloitte.nl

Norbert van der Laan is werkzaam als pentester binnen het Security & Privacy team van Deloitte Risk Services. Daarnaast maakt hij deel uit van het Hacking as a Service team waar hij zich voornamelijk bezighoudt met de rapportage vanuit de Deloitte portal. Norbert kan bereikt worden via NvanderLaan@deloitte.nl

Vrijwel dagelijks zien en horen we nieuwsberichten over gehackte systemen en applicaties, de cybercriminaliteit neemt toe. Binnen het cyberdomein wordt een ongelijke strijd gevoerd. Informatiebeveiligers moeten de security binnen een organisatie managen met beperkte middelen, terwijl 'hackers' deze beperking niet hebben. De intelligentie achter hackaanvallen neemt toe en zorgt voor geavanceerde aanvalstechnieken. Eenvoudige tooling maakt hacken ook toegankelijker, het Metasploit framework is slechts een voorbeeld. Het adequaat beveiligen van een online presence lijkt een utopie te worden. Het bedrijfsleven staat voor een uitdaging; nieuwe kwetsbaarheden ontstaan bijna dagelijks, ontdek of je ze hebt voordat anderen het doen.

De toename van het aantal hack-aanvallen is significant te noemen. Het risico om als organisatie gehackt te worden lijkt met de dag te groeien. Het nieuws staat vol met succesvolle hackaanvallen, maar hoe vaak is te lezen dat deze 'hackers' worden gepakt? Een recent voorbeeld zijn de hacks van The New York Times en Twitter. Een hackersgroepering genaamd 'the Syrian Electronic Army (SEA)' zegt hier voor verantwoordelijk te zijn. De groep had een Australische ISP gehackt waar zowel The New York Times als Twitter bij aangesloten waren. Voor beide sites leidde de hack tot problemen met de beschikbaarheid, maar verder leek de schade mee te vallen. Enkele uren daarvoor berichtte de BBC het volgende: *"China hit by 'biggest ever' cyber-attack"*. Deze twee voorbeelden vonden in een tijdspanne van 24 uur plaats. Enkele jaren eerder, in 2011, kwam Sony groot in het nieuws doordat het PlayStation Network (PSN) gehackt was. Als oorzaak werd een 'known vulnerability' aangewezen. Persoonsgegevens tot creditkaartgegevens lekten uit. Het was het grootste security lek tot op dat moment, 77 miljoen accounts werden gecompromitteerd. Niet alleen grote bedrijven werden het slachtoffer van Cyber aanvallen ook diverse Nederlandse webwinkels werden in het afgelopen jaar gehackt waaronder ReplaceDirect [1] en bouwinkoopcentrale.nl [2]. Cyberaanvallen zijn actueel, komen frequenter voor en worden ook steeds gevaarlijker voor organisaties.

> Als gevolg van de stijgende omvang van cybercrime blijven de kosten voor organisaties stijgen

Schade

Als gevolg van de stijgende omvang van cybercrime blijven de kosten voor organisaties stijgen. Inmiddels lijkt het punt te zijn bereikt waar onderzoekers toegeven dat het onmogelijk is om te berekenen wat de exacte kosten van cybercrime zijn. In een recent onderzoek van McAfee [3] werd een schatting gedaan dat de cybercrimeschade, globaal, tussen 300 biljoen en 1 triljoen kan liggen. Daarnaast ondervindt de wereldeconomie ook hinder van cybercrime, omdat het handel tussen landen verstoort en nieuwe innovaties remt.

Oorzaken

De toenemende cyberdreiging is (helaas) niet toe te wijzen aan één factor. We leven in een hyper-connectief land, waar we de grootste mobiele internetdichtheid van de wereld hebben. Steeds vaker worden webpagina's en onderliggende systemen beschikbaar gemaakt voor marketingcampagnes of nieuwe IT-ontwikkelingen, die zaken zoals Bring Your Own Device en thuiswerken mogelijk maken. De online presence van organisaties groeit, meer 'exposure' naar de buitenwereld. Dit geldt niet alleen voor klanten, maar zeker ook voor 'hackers'. Deze toename zorgt voor

een complexe online omgeving, die lastig te managen valt. Het is lastig om digitale informatiestromen binnen een organisatie in kaart te brengen en een uitdaging om de kwetsbaarheid hiervan vast te stellen. Actueel inzicht in deze kwetsbaarheden ontbreekt (nog te) vaak. Naast het ontbreken van actueel inzicht in de kwetsbaarheden die de organisatie loopt, wordt het resultaat van misbruik van deze kwetsbaarheden steeds vaker zichtbaar. Waar vroeger specialistische kennis nodig was om misbruik te maken van een kwetsbaarheid, is het tegenwoordig relatief eenvoudig toegankelijk door bijvoorbeeld het Metasploit framework [4]. De doorloop-tijd tussen het bekend worden van een kwetsbaarheid tot een exploit is verkort naar dagen of soms slechts uren. Het inmiddels bekende 'Armitage' (GUI voor Metasploit) maakt het voor 'hackers' erg eenvoudig, met slechts enkele klikken kan een systeem worden gehackt..

De wereld van cybercrime is inmiddels uitgegroeid tot een miljardenindustrie, vaak wordt het vergelijk gemaakt met de omvang van de globale illegale drugshandel. Complete cybercrime diensten worden aangeboden via ondergrondse forums. Criminelen kunnen voor enkele duizenden euro's een rootkit kopen, een investering die zich terugbetaalt. Het is een lucratieve bezigheid voor cybercriminelen en de pakkans is relatief laag. Tegelijkertijd wordt aan de ontwikkelkant bezuinigd, applicaties moeten tegen concurrerende prijzen worden geprogrammeerd, die extra code review op security aspecten wordt dan vaak 'vergeten'. Dát zijn onder andere de fouten waar cybercriminelen dankbaar misbruik van maken.

Actueel inzicht

Door de toenemende cybercriminaliteit zijn organisaties genoodzaakt actiever te acteren op bekende kwetsbaarheden. Het is niet langer voldoende om te wachten op 'patch Tuesday'. Tegenwoordig is het slechts een kwestie van dagen voordat kwetsbaarheden uitgroeien tot gevaarlijke exploits, die publiekelijk toegankelijk zijn door bijvoorbeeld gebruik te maken van het Metasploit framework (zie ook het Ruby on Rails voorbeeld). Het is noodzaak dat organisaties tijdig weten over het bestaan van een kwetsbaarheid en daar tijdig actie op ondernemen.

> Actueel inzicht in deze kwetsbaarheden ontbreekt nog te vaak

Actueel inzicht in kwetsbaarheden van een online presence zou de norm moeten zijn. Het uitvoeren van een security test geeft eenmalig inzicht in de kwetsbaarheden van de geteste systemen. Maar het is een momentopname. Hoe relevant zijn de bevindingen van een security test over enkele maanden of over een jaar?

Het NCSC zegt hierover: *"Een pentest is een momentopname beperkt naar de laatste stand der techniek. Door ontwikkelingen in deze techniek kunnen er zich nieuwe risico's voordoen of bestaande risico's zwaarder gaan wegen".* Een online presence verandert continu en daarmee ook de kwetsbaarheden.

Online Presence

Webapplicaties en onderliggende infrastructuur, maar ook devices, die vanaf het Internet bereikbaar zijn.

Actueel inzicht is één stap, maar dat lost nog geen kwetsbaarheden op. Wellicht nog belangrijker: wie gaan de kwetsbaarheden oplossen? En wie kan (her)testen of de kwetsbaarheden ook daadwerkelijk zijn opgelost? Deze laatste, belangrijke stap, lijkt vaak te worden overgeslagen. Een actieve houding ten aanzien van de toenemende cyberdreiging is noodzaak. Kwetsbaarheden toebedelen aan IT-specialisten, die systemen voorzien van bijvoorbeeld de laatste security patches. Het beveiligen van een online presence hoort een voortdurend proces te zijn, waar periodieke security testen onderdeel van vormen. Plan-do-check en act, ook voor security testen. Wanneer het online beveiligingsniveau periodiek wordt gecontroleerd en daar actief op wordt geacteerd, is het mogelijk om de toenemende cyberdreiging beter te managen en de kans op succesvolle aanvallen drastisch te verlagen. ●

Van kwetsbaarheid tot exploit

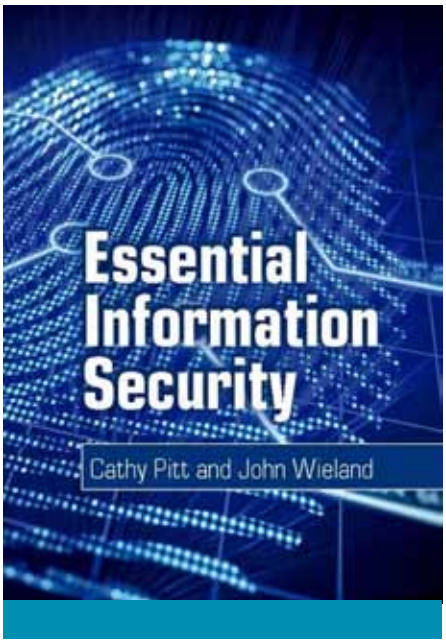
Een bekend voorbeeld van deze dynamiek is een kwetsbaarheid die begin dit jaar bekend werd voor Ruby on Rails (ROR), het websites framework wat o.a. door de Nederlandse overheid bij DigiD wordt gebruikt. Op 8 januari werd een kwetsbaarheid (CVE, 2013-0156 [5]) publiekelijk bekend gemaakt, het ging om een kwetsbaarheid met een hoge CVE score, waar op dat moment nog geen oplossing voor was. Op diezelfde dag is een blogger [6] gaan schrijven over deze kwetsbaarheid en enkele uren later had hij beschreven hoe de toen nog 'theoretische' kwetsbaarheid misbruikt kon worden, zo werd de exploit code vrijgegeven. Daarna was het een kwestie van uren voordat een module werd geschreven voor Metasploit, wat de exploit vrij toegankelijk maakte voor een breed publiek. Kortom, het misbruiken van een kwetsbaarheid wordt steeds eenvoudiger.

Links

[1] *http://www.hpdetijd.nl/2012-05-28/het-onfatsoenlijke-zwijgen-van-replacedirect/*
[2] *https://www.security.nl/posting/36635/*

BOEKBESPREKING

Titel : **Essential Information Security**
Auteur : **Cathy Pitt en John Wieland**
ISBN : **978-90-8753-736-4**
Blz : **239**
Waardering: ★★★☆☆



Information is only as valuable as how it is used. If you create information and never share it, the value is limited to how much you personally care about it.
Dit geeft het beste weer wat de intenties van de auteurs waren bij het schrijven van dit boek. Uit hun schrijfstijl proef je enige gedrevenheid en passie voor het vak informatiebeveiliging en de drang om informatie te delen. Het is een populair geschreven boek dat redelijk snel weg leest. Het allerleukste in dit boek vond ik dat het doorspekt is met populaire uitspraken van bekenden der aarde en de Amerikaanse business wereld en toegepast op informatiebeveiliging. Leuk om over te nemen in presentaties. Een ander aardigheidje is dat elk hoofdstuk, dertien in totaal, wordt afgesloten met een samenvatting en een overzicht met bronvermeldingen. Dat maakt het een aardig naslagwerk. Ik vind dat waardering van drie sterren op zijn plaats is.

Een leuk boek zonder een WOW-factor, maar zoals hierboven vermeld een aardig naslag werk.
Het boek verbindt basis informatie-beveiligingskennis met toepassingen van tegenwoordig als BYOD, social media en cloud computing. Het boek begint met die elementaire kennis en naarmate je het eind van het boek nadert, wordt de theorie omgezet in toepassingen. Dit gaat zover als het beschrijven van netwerkconfiguraties met webservices voor een kantoor aan huis tot en met een blauwdruk(je) van een overheids-instelling met een hoog risicoprofiel. Enige technische affiniteit is wel handig om te hebben bij het lezen van dit boek.
De schrijvers zelf noemen het boek "a tour around the lobby of the Empire State Building". Het geeft een basisniveau informatiebeveiligingskennis, kennis die je mag verwachten van elke informatie-beveiliger of mensen die in dit vak gebied werken. Een korte samenvatting van de hoofdstukken:
Hoofdstuk 1 legt het fundament voor het hele boek en gaat in op definities als Beschikbaarheid, Integriteit, Vertrouwelijkheid, de verschillen tussen identificatie, authenticatie en autorisaties.
Hoofdstuk 2 legt de technieken uit waarop een huidig IT-omgeving is gebouwd. Een technologisch hoofdstuk over tcp/ip, dns, arp, firewalls, client/server communicatie en wat de kritieke punten zijn in dergelijke technologieën.
Hoofdstuk 3 is nog een technologisch hoofdstuk over intruder preventie systemen, VPN, cryptografie en data loss preventie. En waarom deze technologieën onontbeerlijk zijn in een moderne technisch architectuur.

> Over het beveiligen van een website met een gebruikersnaam en wachtwoord door Ned Smtih

Hoofdstuk 4, de schrijvers geven aan dat informatiebeveiliging nooit enkel bestaat uit technologie en dat technologie slechts 10% van het werk is van een security manager. Dit hoofdstuk gaat over het opzetten van de administratieve organisatie van een security omgeving. Beleid, richtlijnen, werkinstructies, een security programma opzetten en daarna dit alles en de technologie in perspectief met elkaar brengen.
Hoofdstuk 5, toch een stuk fysieke beveiliging en fysieke toegangscontrole in relatie tot Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie.
Hoofdstuk 6 en 7 zijn hoofdstukken die gaan over moderne onderwerpen die vandaag de dag spelen, bring your own device, in the cloud en social networking worden besproken wederom in relatie tot Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie.
Hoofdstuk 8, hier worden de eerste 7 hoofdstukken allemaal bij elkaar gebracht in een soort samenvatting en toepassing in een organisatie.
Hoofdstuk 9 behandeld risico management, de nut-en-noodzaak van het houden van een business impact analyse (BIA) en het daadwerkelijk uitvoeren ervan met een registratie.
Hoofdstuk 10 is bedrijfscontinuïteit beheer of management (BCM). Hoe kan BCM een unique selling point worden voor je bedrijfsvoering en de concurrentie.
Hoofdstuk 11 bespreekt het schrijven van een informatiebeveiligingshandboek en waarom je zaken zwart-op-wit moet zetten. Vervolgens wordt er getipt aan een bewustzijn/alertheids programma om het beveiligingshandboek aan de man te brengen.
Hoofdstuk 12 beschrijft hoe je wordt aangevallen, nu je alle maatregelen hebt genomen en iedereen is geïnformeerd en zich bewust is van zijn rol in informatiebeveiliging. Hacked, Cracked en Attacked. Ondanks de genomen maatregelen de "low-hanging-fruits" verwijderen en je hele geïmplementeerde beleid en technologie fine-tunes, meten en continu verbeteren.
Hoofdstuk 13 en de bijlagen gaan over vervolgstappen en geven blauwdrukken voor diverse technologische implementaties. Van een small-office omgeving tot en met een complexe firewall omgeving van een overheidsomgeving. ●

Ronald van Erven

ACHTER HET NIEUWS

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

Waar kunnen we eigenlijk nog wel op vertrouwen? Als het Snowden-nieuws een vraag naar boven haalt, dan is het deze wel. De afgelopen zomer ging er een klein tipje van de sluier die over de inlichtingenwereld hangt omhoog. En hoewel velen wel vermoedden dat er wereldwijd op grote schaal internetverkeer werd afgetapt, laten veel andere nieuwsberichten zien dat het hier zeker niet bij blijft. Zo geven Amerikaanse bedrijven de inlichtingendiensten, naast een kopie van het netwerkverkeer, ook op grote schaal inzage in persoonsgegevens van wereldburgers en lijken ze zelfs mee te werken aan het creëren van specifieke achterdeuren en zwakheden in wereldwijd geaccepteerde encryptiestandaarden. Voor beveiligingsspecialisten biedt deze wetenschap nieuwe uitdagingen. Kunnen we eigenlijk nog wel bouwen op de beveiligingstechnieken en middelen waarvan we dachten dat ze ons een hoge mate van vertrouwelijkheid boden?

Aart Jochem

Het is een beetje raar. Het gevoel van paranoia, dat ons specialistisch vakgebied met zich meebrengt, is opeens mainstream geworden. Meewarig werd geknikt als we over risico's voor meelezen en lekken spraken, nu zijn we de *hipsters* van deze tijd. Jaren aan C-level security awareness heeft niet gebracht wat nu door de onthullingen van Snowden wordt bereikt: er wordt breed nagedacht over de risico's van datalekken. Waar wordt de gevoelige informatie opgeslagen en hoe worden ze beschermd?
Het Cyber Security Beeld van Nederland heeft statelijke actoren al geduid als belangrijkste dreiging voor de vertrouwelijkheid van informatie en offensieve operaties. Met de onthullingen van Snowden komt hier voor een brede groep beeld en geluid bij. Als je voldoende tijd en geld investeert, is het bijna altijd mogelijk binnen te dringen in de systemen van je slachtoffer. Afgelopen jaar zijn hiervan oosterse en westerse voorbeelden aan het licht gekomen. Het is in toenemende mate moeilijk je hiertegen te beschermen.
Wat kun je wel doen? Ik denk dat veel maatregelen die worden genoemd in de beveiligingsplannen met andere ogen bekeken worden en er meer bereidheid is om die door te voeren. Dit maakt de bescherming steviger, maar je bent er niet mee. Goed kijken of je sporen van compromitatie herkent is een andere. Wat je niet kunt voorkomen, kun je misschien wel vroeg detecteren. En als je beter gaat kijken ga je meer zien. Dan wordt je nog meer paranoia en komen we als informatiebeveiligingsprofessionals weer op eenzame hoogte wat dat betreft. Vooral als de rest van de wereld weer overgaat tot de orde van de dag.

Maarten Hartsuijker

Noem mij naïef of te goed van vertrouwen, maar tot voor kort ging ik er oprecht van uit dat grote software bedrijven de veiligheid van hun software niet met opzet in gevaar zouden brengen. Dat inlichtingendiensten en criminelen kwetsbaarheden zoeken en inkopen is al langer algemeen bekend. Maar berichten dat er in software bewust kwetsbaarheden zouden worden gecreëerd (of niet worden verholpen) deed ik af als paranoia. Ik zag de logica er niet van in. Welk bedrijf, dat voor een groot deel afhankelijk is van buitenlandse klanten, zou zo dom zijn om zijn internationale reputatie op het spel te zetten door een specifieke overheid te helpen met een effectieve aanvalsmethode of een achterdeur? Daar zijn de financiële belangen toch veel te groot voor? De regelmatig goed onderbouwde berichtgeving van de afgelopen maanden heeft mij inmiddels een stuk kritischer gemaakt. Ik denk dat we er inmiddels wel van uit mogen gaan dat in elk geval de grote Amerikaanse technologiebedrijven hun overheid actief helpen aan de makkelijkste aanpak om hun technologie te kraken. Niet alleen binnen de Verenigde Staten maar ook (misschien wel: juist) daarbuiten.

Bij het wel of niet exporteren van data zit je gelukkig grotendeels zelf achter het stuur. Maar tegen het in achterkamertjes op intransparante wijze in stand houden van kwetsbaarheden en eenvoudige aanvalsvectoren kun je (als gebruiker, levend in een andere rechtstaat met een andere rechtvaardigheidsmoraal) heel erg weinig doen.

De vraag is hoe we hier als beveiligers mee om moeten gaan. En om heel eerlijk te zijn, heb ik het antwoord er nog niet op. Het is erg ontmoedigend om te lezen dat, terwijl jij bezig bent om de gegevens van je opdrachtgever zo goed mogelijk te beschermen, de middelen waarmee je moet werken op essentiële onderdelen bewust zwak worden gehouden met kwetsbaarheden die ook door kwaadwillenden gevonden kunnen worden. Gelukkig lijkt de drempel om dit soort specifiek gecreëerde zwakheden (want backdoors mogen we het ab-so-luut niet noemen) te gebruiken erg

hoog. Maar tegelijk is het natuurlijk geen goede ontwikkeling dat de kennis over dit soort kwetsbaarheden alleen toegankelijk is voor partijen die door de technologiebedrijven vertrouwd worden. Als dataverantwoordelijke wil ik zelf de controle over de veiligheid van de middelen die mijn data beschermen. En wil ik datavorderingen zelf toetsen tegen de wetten die in mijn land gelden. Hierbij horen de partners waarmee ik mee samenwerk mij te ondersteunen (en niet tegenwerken).

Ik hoop dat de berichtgeving die we de afgelopen maanden zien op termijn tot meer transparantie en controle leidt en niet vooral tot maatregelen die kwetsbaarheden nog onzichtbaarder maken. Maar kan mij voorstellen dat sommigen van mening zullen zijn dat ook dit vertrouwen enige naïviteit in zich draagt.

Ronald van Erven

Ik had een ongeschonden vertrouwen in leveranciers, leveranciers van onder andere crypto producten die vanuit ethiek en hogere moraal-standaarden er alles aan doen om de integriteit en het vertrouwen in hun diensten en producten te beschermen. Nu moeten ze van hun overheid gedwongen achterdeuren inbouwen. Volgens de wet moesten ze wel meewerken anders gaat de CEO het gevang in. Na de lancering van de Apple iPhone 5S met de vingerscanner dacht ik het nog zeker te weten: Een bedrijf als Apple heeft een reputatie van betrouwbaarheid hoog te houden en zal nooit meewerken aan spionage.
Totdat ik op de website van Mashable [1] vernam dat er voor het inbrengen van achterdeuren, in bijvoorbeeld Bitlocker, geld wordt betaald. En daarmee is er een nieuw business model ontwikkeld. Leveranciers verdienen zo aan twee kanten. De bodem viel totaal uit mijn vertrouwen toen Apple in een berichtje aangaf dat de NSA de iPhones kan uitlezen. Dus met de vingerafdrukken uit de nieuwe iPhone 5S [2] kan de NSA haar persoonsdatabase aardig uitbreiden.
Slim ... maar wie kun je dan inderdaad nog vertrouwen? Ik houd mij nu het excuus voor dat dit typisch Amerikaanse toestanden zijn. Onder het mom van technologische vooruitgangen en deze op te dringen aan de wereld bouwen de Verenigde Staten van Amerika aan hun Big Brother Imperium en is overheid van ons kleine, knusse en gezellige Nederland wel te vertrouwen. Voor de zekerheid ontwikkel ik toch maar naar een plan B en C.
Mijn plan B is ... enkel nog met Nederlandse crypto algoritmen en computerchips werken. Dit is ook goed voor onze economie.
En mijn plan C ... stop met elektronische informatie verwerking en ga off-grid, als dat nog kan. Laatst in het ziekenhuis heb ik misschien wel een super dunne GPS-chip geïmplanteerd gekregen. Ik kan mij er in elk geval nog weinig van herinneren. Enfin, die komt bij de bodyscan op Schiphol t.z.t. wel aan het licht.

André Koot

Zo hebben de aluhoedjes dus gelijk gekregen. "Trust noone" blijkt een goed uitgangspunt. De vrienden die we eerder nooit wantrouwden, blijken het uitgangspunt te hanteren dat wij, hun vrienden, wel eens hun vijanden zouden kunnen zijn. Van onze vrienden mochten we ZTE en Huawei niet gebruiken, want daar zouden achterdeurtjes in zitten, nee we moeten ons daar verre van houden. De Cryptografie, Bitlocker, TLS/SSL, NIST standaarden van onze vrieden, daarmee kunnen we ons pas goed beveiligen. Maar voor wie en tegen wie ga je je zo langzamerhand afvragen. Maar wat dan? Je kunt toch moeilijk niets doen? We moeten wel verder.

En als ik even nadenkt, blijk ik daar in ieder geval al even mee bezig te zijn. Soms (lees: vaak) tot leedvermaak van mijn familie en kennissen, als ik, door mijn dogmatische afkeer van het gebruik van gesloten systemen, gesloten standaarden en gesloten netwerken, niet overweg kan met hun bestandjes en uitnodigingen... "nee, ik had je foto's op Facebook niet gezien", "nee, dat docx bestand kan ik niet goed lezen". Gelukkig maar...
Ik had al eerder besloten om zo min mogelijk instrument van de commercie te worden. En laat dat nu juist een gewillige partij blijken om zich te voegen naar de wensen van de Prism-club.

Ik ben zo veel mogelijk overgestapt op vrije standaarden en software.
Het gebruik van onveilig spul is helaas niet te voorkomen, zolang niet iedereen de risico's daarvan inziet. Misschien moeten we in ons land eens vaker kijken naar open source software. Een interessante industrie die niet aan één vriend kostplichtig is.
Ik zal de eerste zijn om te erkennen dat ook open source software niet veilig is, ik zal ook alle broncode niet kunnen beoordelen. Maar de open source communities kunnen dat wel. We moeten wel verder.
Als gemeenschap. En ik denk dat we zo door onze eigen verantwoordelijkheid te nemen ook een voorschot kunnen nemen op betere privacybescherming en beveiliging. En het leuke is dat we meteen onze eigen economie een zetje kunnen geven. ●

Links

[1] http://mashable.com/2013/09/11/fbi-microsoft-bitlocker-backdoor/

[2] http://www.storyleak.com/apple-iphone-5s-big-brother-dream-come-true/

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

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

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: BERRY

Ik zit weer eens met mijn ellebogen op mijn bureau, mijn hoofd rust in mijn handen en ik zit weer met verbazing naar mijn beeldscherm te kijken. Meer en meer verbaas ik mij over de waanzin waarin wij leven en ook dit artikel gaat over deze waanzin. Het artikel beschrijft de situatie van Samsung's smartwatch. Deze is begin september aangekondigd, het bericht dat ik lees is geschreven op 15 september. De Galaxy gear (een prachtige naam voor een horloge) zou op 25 september in de winkels moeten liggen, maar zal binnen een half jaar het stempel "verouderd" op de verpakking krijgen. Een apparaat aanschaffen dat binnen zes maanden vervangen wordt door een verbeterd apparaat met uitgebreidere functionaliteit geeft geen fijne kopersbeleving. Ikzelf was al bijzonder verbolgen dat mijn "verouderde" iPad 1 na twee jaar niet meer geüpdate kon worden met het nieuwste besturingssysteem. Misschien heeft Samsung de smartwatch zo snel uitgebracht om voor te blijven lopen op Apple die binnenkort waarschijnlijk ook met een smartwatch zal komen? Ik kan mijn vrouw niet uitleggen waarom ik mij zo druk maak over dit soort praktijken, maar dat zal ook wel met een stuk beroepsdeformatie te maken hebben waar ik in ernstige mate aan lijd. Van de tientallen miljoenen Android telefoons draait één op de drie op één van de nieuwste besturingssystemen. Twee op de drie apparaten draait dus op een verouderd besturingssysteem en zijn bijna niet te updaten naar een nieuwer en veiliger niveau. Die apparaten lopen dus risico's op het gebied van malware. Met andere woorden, de meeste Android telefoons worden gekocht en verdwijnen uiteindelijk van de markt met dezelfde software als dat ze uit de doos gekomen zijn. Zelf ben ik in mindere mate geïnteresseerd in de hardware, of het toestel nu 4 inch groot is of 4.1 inch vind ik niet spannend. Dat processor X vervangen is door de nog snellere processor Y maakt mij niet uit. Ik wil gewoon een telefoon die het doet en als hij snel genoeg is dan hoef ik niet te vervangen. Wat ik wel heel erg interessant vind is dat de leverancier van mijn telefoon een update van zijn besturingssysteem uitbrengt als er een probleem in de oude versie is gedetecteerd.

Maak het update proces toch eenvoudig en zorg ervoor dat een ieder die een telefoon kan bedienen ook de update kan plaatsen. Mijn leverancier heeft dat goed door en het blijkt ook dat van alle verkochte iPhones 93% op het laatst uitgegeven besturingssysteem draait. De zeven procent die draait op een oudere versie heeft te maken met het feit dat deze telefoons als verouderd worden beschouwd door Apple. De update zelf moet eenvoudig te installeren zijn maar moet natuurlijk ook weer iets extra's bieden. De in september uitgebrachte iOS 7 versie zal eind dit jaar op meer dan 80% van alle iPhones geïnstalleerd zijn, die toestellen hebben dan weer de beschikking over een fris ogend besturingssysteem en gebruikers zullen denken dat ze een nieuwe telefoon hebben. Ik ben benieuwd hoe dat zal gaan met de eerder genoemde Galaxy gear. Mijn verwachting is dat daar nooit een update voor zal worden uitgebracht.

Waarom zit de mens zo in elkaar dat altijd het nieuwste van het nieuwste in huis moet zijn? En waarom weten de fabrikanten, van met name gadgets, daar zo fijn om in te spelen? Psychologen hebben hun hoofd daar al over gebroken en daar komt geen eenduidig beeld uit. De mens wil zich onderscheiden en de fabrikant wil zo goed mogelijk zijn aandeelhouders tevreden stellen. Smartphones van een jaar oud zijn al out-of-date en niet meer hip en worden vervangen door een nieuwer type. De oude gaat naar zus, broer of Marktplaats. Niemand maakt zich zorgen over de verouderde software en de risico's die dat met zich meebrengt. Op een verjaardag kun je zelfs je punt niet maken, een ieder kijkt mij aan met een blik alsof ik niet helemaal fris ben. Om eens een keer heel eerlijk en open te zijn, ik begin daar inmiddels ook aan te twijfelen. Ben ik de enige die zich druk maakt over het feit dat er inloggegevens, mail, foto's en andere persoonlijke informatie van mijn telefoon gehaald kunnen worden omdat deze met verouderde software werkt? Ben ik de enige die risico's ziet op het gebied van veiligheid van verouderde besturingssystemen? Ik denk het wel, ik denk dat heel veel gebruikers denken dat er toch niets spannends op hun telefoon staat en dat hen niets kan gebeuren. Totdat de creditcard wordt geplunderd door criminelen. Bel mij dan niet, ik heb jullie gewaarschuwd! ●

Groetjes, 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