05/2012

INFORMATIE BEVEILIGING

PvIB Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 5 - 2012

VERGETEN GEGEVENSRISICO'S

ISO 22301 MAATSCHAPPELIJKE VEILIGHEID

GOED HUISVADERSCHAP IN DE STRIJD TEGEN CYBERCRIME

PINCODE VOOR JE PACEMAKER

ONSIGHT IT SECURITY CONGRES 2012

VOORWOORD

Het is weer zomer, tijd om een hit te maken met simpele, voor de hand liggende ingrediënten. Enige diepgang is uit den boze. De topper van vorig jaar - Trust - doet deze keer een duet met een hele oude bekende: MD5. En de single die ze uitbrengen is er een met een dubbele A-kant.

Even een intermezzo voor wie niet weet wat een single is en een A- & B-kant... Vroegûh - vóór de CD - werd geluid analoog in krassen op een schijf vinyl opgeslagen. Deze schijf had zo weinig opslagruimte, dat beide zijden gebruikt moesten worden. De verwachte hit stond op de A-kant en meestal stond op de B-kant iets onbetekenends. Als op de B-kant ook een potentiële hit stond, was er in de volksmond sprake van een dubbele A-kant.

Terug naar mijn verhaal: Op de ene zijde van deze zomersingle de "Password Hash". MD5 gebruikt zijn oude vertrouwde techniek om iets herkenbaars te maken. De raps van Trust in de achtergrond zijn nog net te horen. MD5 weerstond de druk om een nieuwe mix te laten maken door DJ Salt. Dat zou zijn publiek niet herkend hebben. En de hash klinkt al zo snel vertrouwd... MD5 scoort al jaren goed met deze hit op de besloten bedrijfsfeestjes van LinkedIn, eHarmony en Last.fm.

In ieder geval - dat weten we nu, want de video's van de feestjes zijn op Facebook gezet. Hoeveel andere bedrijven dit soort feestjes hadden achter gesloten deuren, weten we niet. In ieder geval weer goed als meeswinger!

Op de andere zijde de "Certificate Clash". Hier komt Trust beter tot zijn recht, maar hij heeft zich laten verlokken tot een simpel duet met MD5, wat heel lekker en makkelijk klinkt, maar zonder het zomersfeertje eigenlijk niet genoeg diepgang heeft. Hier weten we - weer van Facebook - dat Trust een regelmatig geziene artiest is op de bedrijfsfeestjes van Microsoft, maar ook dat hij daar ook al behoorlijk kon doorzakken met MD5 tot in de late uurtjes. Samen signeerden ze de software van ontwikkelaars op die feestjes. Deze opname klinkt helemaal niet als de Trust die wij kennen, MD5 maakt het meer tot een algemene, lekker in het oor liggende hit, maar MD5 zou deze hit ook makkelijk met een andere artiest hebben kunnen maken. In de tabloids wordt zelfs beweerd dat Trust niet zelf de opnames heeft ingezongen. Dit is moeilijk om achteraf te verifiëren. Zelf mis ik met de gevoelige teksten van Trust die je diep van binnen zo'n veilig en zeker gevoel geven.

De zomerhit-combi scoort lekker. Beter dan het Nederlands elftal. Toch zou ik graag zien dat Trust zijn duet-keuzes wat zorgvuldiger kiest. Als hij blijft gaan voor de oppervlakkige, snelle hits zoals MD5 brengt, denk ik dat zijn carrière toch een vroegtijdig einde zal kennen. Trust is een gevoelige artiest, hij heeft de diepgang nodig die een artiest als SHA256 in hem los kan maken. MD5 zal dat niveau nooit kunnen halen.

INHOUDSOPGAVE

VERGETEN GEGEVENSRISICO'S

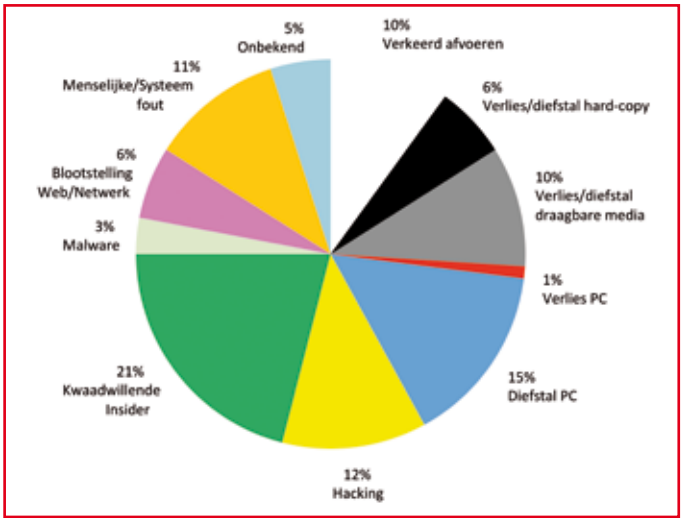
BEVEILIGINGSBEWUSTZIJN OVER GEVAREN HARDWAREVERPLAATSINGEN NODIG

Drs. ing. Ronald Koorn RE. Partner bij KPMG IT Advisor en gericht op vraagstukken op gebied van informatiebeveiliging, privacy, ICT-beheersing en ICT-compliance.
koorn.ronald@kpmg.nl
Drs. Jeroen van Kerkhof. Mede-eigenaar van Re5 Europe BV, specialist in dataveilige IT-retourlogistiek. Daarvoor was hij verantwoordelijk voor de Europese retourdistributie van de asset managementtak van Hewlett Packard.
jeroen@re5europe.nl

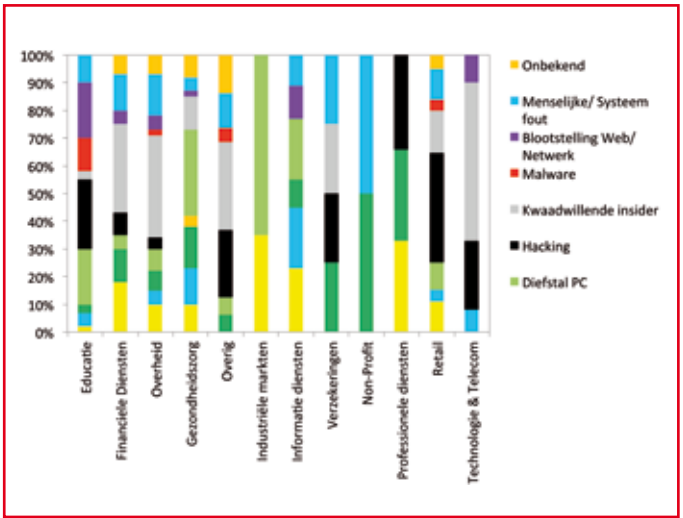
Op basis van recent onderzoek heeft De Nederlandsche Bank (DNB) vastgesteld dat slechts bij 15% van de onderzochte financiële ondernemingen informatiebeveiliging volledig op orde is. Met een circulaire wil DNB het onderwerp informatiebeveiliging in de financiële sector onder de aandacht brengen. Onderdeel van het toetsingkader is de bescherming van informatie bij het afstoten van gegevensdragers. Dit speelt natuurlijk evenzo voor gevoelige gegevens in andere sectoren, vandaar dat dit artikel relevant is voor alle organisaties die haar hardware veilig wil afvoeren of hergebruiken.

Organisaties lijken zich in toenemende mate te realiseren wat het risico is wanneer er hardwaremutaties zijn, zoals vervanging of herinzet. Maar in deze periode van ICT-uitbesteding, cloud computing, virtualisatie en internetbeveiliging lijkt informatiebeveiliging bij hardwaremutaties en -verplaatsingen toch nog steeds een ondergeschoven kindje te zijn. Uit Amerikaans onderzoek is gebleken dat 45% van de organisaties niet over beleid voor gegevensarchivering en -verwijdering beschikt. Aan de andere kant geeft recent Europees onderzoek van dezelfde organisatie aan dat 68% van de Nederlandse managers beperkte (financiële) risico's ziet van onveilige gegevensverwijdering (NAID2012). Dat gegevensverlies door foutieve omgang met gegevensdragers niet louter een theoretisch maar praktisch belangrijk onderwerp is blijkt uit onderzoek van KPMG (KPMG2010); in de meeste sectoren wordt tussen een derde tot meer dan de helft van het verlies van informatie veroorzaakt door het verkeerd afvoeren of verlies en diefstal van PC's (figuur 1 en figuur 2). Deze statistieken geven een abstract beeld, individuele beveiligingsincidenten maken het concreter. Ook al spreken de hackingincidenten in de landelijke media meer aan, in kader 1 is een aantal voorgevallen en gepubliceerde incidenten met gegevensverlies opgenomen. Nalatigheid en lankmoedigheid blijken daarbij belangrijke oorzaken.

> In de meeste sectoren wordt tussen een derde tot meer dan de helft van het verlies van informatie veroorzaakt door het verkeerd afvoeren of verlies en diefstal van PC's



Figuur 1: Oorzaken verlies van informatie



Figuur 2: Oorzaken verlies van informatie per sector

Kader 1: Incidenten

Online inbraken krijgen de meeste persaandacht maar ook met achtergebleven gegevens vinden vele beveiligingsincidenten plaats. Een korte bloemlezing:

- Amerikaanse bank verliest computertape met bankgegevens van 3,9 miljoen rekeninghouders
- Computertapes met gegevens van 800.000 burgers van de Department of Child Support Services (DCCS) van de staat Californië is verloren tijdens oefening met IBM en Iron Mountain. De tape bevatte adresgegevens, Amerikaanse BSN-nummers, rijbewijs- of identificatienummers, zorgverzekering en informatie van de werkgever.
- Officier van Justitie Tonino zet zijn PC met gevoelige privébestanden en vertrouwelijke Justitie-gegevens op straat, welke vervolgens in handen komt van Peter R. de Vries
- T-Mobile verliest CD met gegevens van 17 miljoen klanten
- Een Amerikaanse universiteit verliest persoonsgegevens van 600 alumni door het kwijtraken van twee laptops met onversleutelde gegevens.
- Server met medische gegevens van 55.000 patiënten was door een opruimingsbedrijf niet gewist of vernietigd. Door een overstroming was het opruimingsbedrijf gevraagd het laboratorium leeg te ruimen en de apparatuur af te voeren.
- Een man formatteert meerdere malen zijn laptop en bedenkt niet dat er belangrijke gegevens op staan, die vervolgens uitlekken
- De harde schijf van een geleast kopieerapparaat bevatten persoonsgegevens van meer dan 400.000 medewerkers, tot aan identiteits- en medische gegevens aan toe.
- Een harde schijf die veiligheids- en visagegevens van artsen bevatte is via een veiling verkocht. Door het ontbreken van een hardwareregistratie werd het gemis van deze gegevensdrager pas ontdekt toen het in de pers werd gemeld.
- Motorola vergat de gegevens van de vorige eigenaar van circa 100 Xoom-tablets te wissen alvorens ze werden doorverkocht aan nieuwe eigenaren.

Waar liggen de gegevensrisico's?

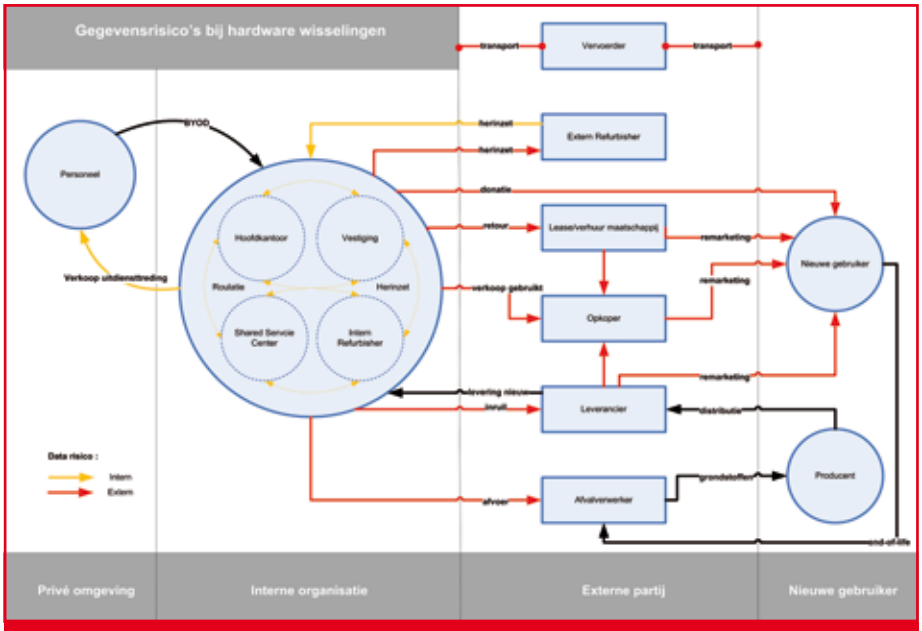
We kunnen stellen dat er een gegevensrisico ontstaat zodra hardware in beheer of eigendom wordt overgedragen. Want dan kunnen vertrouwelijke gegevens samen met de gegevensdragers verdwijnen.
De maatregelen om dit te voorkomen zijn vaak ontoereikend. De manier waarop de gegevensdragers rouleren of de organisatie verlaten is verschillend en is vaak afhankelijk van het organisatiebeleid en/of de wijze waarop de hardware is gefinancierd (figuur 3).

Interne gegevensrisico's

De mate waarin gegevens vertrouwelijk zijn kan per onderdeel van een organisatie verschillen.
Zo worden persoons- en bedrijfsgevoelige gegevens zoals in gebruik op een HR-afdeling of bij de directie vaak als vertrouwelijker geclassificeerd dan gegevens op andere afdelingen. (Zie voor rubricering van persoonsgegevens en de beveiliging daarvan o.a. in publicatie van College Bescherming Persoonsgegevens [CBP2001].) Het is dus raadzaam om te kijken of met het herinzetten van hardware geen informatie 'verhuist' naar vestigingen, afdelingen of derde partijen waarvoor deze informatie (te) vertrouwelijk is.
Daarnaast is Bring Your Own Device (BYOD) in Nederland geen trend meer, maar realiteit: 85 procent van de Nederlandse werknemers gebruikt inmiddels een privéapparaat voor werkdoeleinden ([Cisco2012]). Weliswaar worden toegangsprotocollen geschreven om veilig met privéapparaten in een bedrijfsnetwerk te kunnen werken, maar bestanden kunnen over het algemeen gewoon lokaal worden opgeslagen. Daarom dienen gegevensdragers die formeel dus buiten de eigen organisatie vallen meegenomen te worden in de scope van informatiebeveiliging bij hardwaremutaties. Want wat gebeurt er met de opgeslagen informatie als de eigen 'device' vervangen wordt of als de betreffende medewerker de organisatie verlaat?

Externe gegevensrisico's

Bij de meeste mutaties in hardware speelt een externe dienstverlener een rol. Transporteurs worden meestal alleen ingeschakeld voor het vervoer en dus niet voor de gegevensverwijdering. Andere partijen nemen in het proces wel de verantwoordelijkheid voor de verwijdering en – indien van toepassing – ook voor de doorverkoop of afvoer van apparatuur.
In alle gevallen geldt het risico dat hardware met vertrouwelijke informatie verloren gaat gedurende het transport door onzorgvuldigheid of diefstal. Daarnaast is er



Figuur 3: Gegevensrisico's bij hardwarewisselingen

het risico dat informatie niet, niet volledig of niet volgens de juiste richtlijnen wordt verwijderd. En vervolgens onbedoeld ter beschikking aan derden kan komen.
Verder bestaat het risico van diefstal vanaf de locatie van de externe dienstverlener en het moedwillig verzamelen van vertrouwelijke informatie door (een medewerker van) de externe dienstverlener met als doel deze te gelde te maken.
De marketingwaarde per record bij verkoop levert interessante opbrengsten op.
Het merendeel van de huidige informatiebeveiligingsmaatregelen richt zich echter op de 'gegevens in ruste', dus goed afgeschermde systemen, databases, platformen of fysiek afgesloten rekencentra. Met uitzondering van de veelal goed beveiligde interfaces met andere organisatie/systemen, is er in mindere mate aandacht voor 'gegevens in transit', vooral als het niet-reguliere verplaatsingen en buiten gebruikstelling van hardware, tapes, devices, e.d. met onversleutelde gegevens betreft. Als de gehele informatielevenscyclus wordt beschouwd ligt het accent van informatiebeveiliging op de reguliere verwerkingsstappen, maar zou het bewustzijn van de risico's aan het eind van de levenscyclus van gegevens sterker mogen.

Wat is de mogelijke impact?
Het in ongewenste handen komen van bedrijfs- of privacygevoelige informatie kan natuurlijk verregaande financiële consequenties hebben.
Allereerst hoeft het gegevensverlies niet altijd opgemerkt te worden. Dat maakt het lastig om de exacte financiële consequenties vast te stellen. Maar bedrijfsgevoelige gegevens zoals over overnamekandidaten en de profijtelijkheid van klanten zijn van onschatbare waarde, juist als ze in handen komen van bijvoorbeeld concurrenten.
Voor het wel vastgestelde verlies van informatie kan de schade vaak wat beter worden geschat.
Sowieso zijn daar de kosten voor de interne afhandeling van de schadegevallen. Maar kostbaarder nog zijn de incidenten die leiden tot aanzienlijke reputatieschade, schikkingen of sanctiemaatregelen door toezichthouders. Zoals in [Ponemon2010] is vermeld zijn de kosten bij gegevensverlies wederom gestegen, ditmaal naar circa 95 euro per verloren gegaan record.
Het College Bescherming Persoonsgegevens (CBP) maakt zich net als haar Britse evenknie (ICO) sterk voor forsere boetes en bijvoorbeeld een publicatieplicht voor beveiligingsincidenten in alle sectoren. Daarmee kan ook de reputatieschade ernstige proporties aannemen. De opvolger van de huidige Europese privacyrichtlijn is een verordening die overheden in staat stelt om aanzienlijke financiële sancties op te leggen. Ze kunnen oplopen tot maar liefst 2% van de wereldwijde omzet (bijvoorbeeld Shell zou een boete van meer dan 7 miljard euro kunnen oplopen!).

> Sancties kunnen oplopen tot maar liefst 2% van de wereldwijde omzet

Aandachtspunten
Al met al genoeg redenen om bewust te zijn van de risico´s bij hardwaremutaties. Kernpunten van de richtlijnen op het gebied van gegevensmanagement zijn een sluitende registratie van de aanwezige gegevensdragers en het definitief verwijderen van gegevens wanneer een gegevensdrager elders opnieuw wordt ingezet of wordt afgevoerd. Afgezien van de primaire gegevensdragers is het natuurlijk ook van belang dat ook alle andere kopieën, zoals gerepliceerde gegevens (i.g.v. dubbel rekencentrum), back-ups, gearchiveerde gegevens en dergelijke worden gewist.
Maar hoe pak je een goed beheer van gegevensdragers in de praktijk aan?
Het toetsingskader informatiebeveiliging voor DNB themaonderzoek [DNB2012] geeft bijvoorbeeld houvast. Hierna volgt een aantal aandachtspunten.

> Waar 'vernietiging' wordt vereist blijkt gedegen 'wissen' ook te mogen

Registratie
Allereerst is het verstandig om gegevensclassificatie toe te passen – minimaal op hoofdlijnen. Dat biedt de mogelijkheid om bijvoorbeeld voor gevoelige gegevens een afwijkende informatiebeveiligingsprocedure te hanteren ten opzichte van gegevensdragers met publieke gegevens. Bovendien kan de ernst van een eventueel incident beter worden getaxeerd en kunnen proportionele maatregelen worden getroffen.
Daarnaast is het essentieel om een complete, sluitende registratie te hebben van alle aanwezige gegevensdragers. Alleen dan kan worden gegarandeerd dat de informatie ook daadwerkelijk van elke gegevensdrager wordt verwijderd.
Een initiële inventarisatie lijkt op zich nog eenvoudig te realiseren op basis van bijvoorbeeld merk, omschrijving en serienummer. Maar het gevaar schuilt in gegevensdragers die niet als zodanig geïdentificeerd worden. Dan gaat het bijvoorbeeld over losse server disks, printers met geheugen, smartphones, extra harde schijven in desktops (al dan niet aangesloten) en externe harde schijven voor back-ups. (Middel)grote organisaties hebben al moeite met de registratie van softwarelicenties, laat staan van gegevensdragers en de inhoud daarvan.
Ook is het belangrijk om in dit stadium geen onderscheid te maken in wie de daadwerkelijke eigenaar van de hardware is. Voor geleaste of gehuurde producten gelden immers dezelfde gegevensrisico's als voor producten in eigendom. Bij elk van de financieringsvormen is het dus van belang dat de administratie van de apparatuur sluitend is.
Cruciaal is ook dat elke mutatie wordt vastgelegd en vooral dat voor elke gegevensdrager wordt gecontroleerd en geadministreerd dat informatie definitief verwijderd is volgens door de organisatie goedgekeurde richtlijnen. Dit alles vergt heldere procesomschrijvingen, veel discipline in de uitvoering en een goede samenwerking met een eventuele externe dienstverlener.

Fysieke vernietiging
Voor het eigenlijk verwijderen van informatie zijn er meerdere alternatieven. Daarbij is er grofweg de keuze tussen het fysiek vernietigen van de gegevensdra-

ger en een softwarematige verwijdering van informatie. Wat onbekend is is dat veelal beide vormen zijn toegestaan (zie ook kader 2). Waar 'vernietiging' wordt vereist blijkt gedegen 'wissen' ook te mogen (de definitie van vernietiging in ISO 15489 luidt namelijk: "Het proces van verwijderen of wissen van archiefbescheiden zonder dat zij weer gereconstrueerd kunnen worden").

Kader 2: Overheidseisen aan gegevensverwijdering

Naast de DNB-eisen voor de financiële sector kent ook de publieke sector een aantal richtlijnen rond bewaartermijnen en – in mindere mate – gegevensverwijdering, deze betreffen:

Archiefwet 1995:
Deze wet bevat algemene richtlijnen voor archivering en vernietiging, waarbij er sterk de nadruk ligt op papieren archieven. Met vernietigingslijsten per overheidsorgaan of -sector wordt specifiek aangegeven welke gegevens moeten worden vernietigd. De wijze van vernietiging is niet bepaald.
Voorschrift Informatiebeveiliging Rijksoverheid (en daarbinnen de Code voor Informatiebeveiliging – ISO 27001/2)
De eisen aan verwijdering, vernietiging of wissen van gegevens bij de eis "Veilig afvoeren en hergebruiken van apparatuur" zijn relatief algemeen van aard; er wordt niet aangegeven of gegevens(dragers) hardwarematig danwel softwarematig moeten worden verwijderd. Ook niet voor hogere gevoeligheidsklassen.

VIR-BI (VIR Bijzondere Informatie voor gerubriceerde overheidsgegevens):
Bij het onderwerp "Gegevensdragers veilig afstoten" staat vermeld dat alleen bij het niveau 'Staatsgeheim Zeer Geheim' gegevensdragers fysiek moeten worden vernietigd. Alle andere gegevensdragers moeten worden gewist met een door de Beveiligingsambtenaar voor de desbetreffende rubricering goedgekeurde methode. Veelal wordt van vernietiging van 'Staatsgeheim Geheim' of hoger gerubriceerde gegevens een proces-verbaal opgemaakt. Met uitzondering van gegevensdragers van 'Staatsgeheim Zeer Geheim' gegevens kunnen gegevensdragers van staatsgeheimen binnen de eigen organisatie worden hergebruikt. Deze gegevensdragers dienen eerst te zijn gewist. Hergebruik buiten de eigen organisatie is dan niet toegestaan.

Wet bescherming persoonsgegevens & gerelateerde CBP-richtlijn Achtergrondstudies en Verkenningen 23: Beveiliging van persoonsgegevens (§ 4.12):
Verwijdering van persoonsgegevens (incl. gevoelige gegevens) mag fysiek of softwarematig gebeuren. Er dient een vernietigingsprotocol, ondertekende geheimhoudingsverklaring van 3e partijen en toestemming van de verantwoordelijke te zijn, alsmede te worden vastgelegd welke functionaris, op welk tijdstip, welke gegevens heeft vernietigd en wie daartoe opdracht heeft gegeven. Gegevensdragers mogen de organisatie alleen verlaten als de persoonsgegevens erop zijn vernietigd. Onder toezicht van de verantwoordelijke mag de vernietiging van de persoonsgegevens elders plaatsvinden.

Verder worden in de Wet Politiegegevens en de NEN7510 specifieke eisen in de politie- resp. zorgsector vereist. In de NEN7510 staat in § 9.2.6 Veilig verwijderen of hergebruiken van apparatuur aangegeven:
Pas voor het wissen van opslagmedia met gevoelige (medische) gegevens, in plaats van standaardmethoden, fysieke vernietiging toe. Of vernietig, verwijder of overschrijf de informatie met technieken die het onmogelijk maken de oorspronkelijke informatie terug te halen. Zie ook data sanitation standards, bijvoorbeeld van het National Institute of Standard and Technology (NIST) (zie schema 9).

Fysieke vernietiging gebeurt door een gegevensdrager te beschadigen met bijvoorbeeld een moker, machinaal te vernietigen ('shredderen') of te 'degaussen'. Bij die laatste optie wordt de gegevensdrager onbruikbaar gemaakt door de moleculaire structuur door middel van sterke magnetische velden te veranderen (vergelijkbaar met de magnetische 'stip' bij winkelkassa's die een bankpas onbruikbaar kan maken). Bij het shredderen zijn er volgens de European Association for Data Media Security (EADMS) verschillende veiligheidsklassen te onderscheiden. De klasse-indeling is gebaseerd op de mate waarin versnipperd wordt, waarbij categorie E volgens deze standaard het veiligst is (zie kader 3).

Softwarematige verwijdering
Een alternatief voor fysieke vernietiging is de softwarematige gegevensverwijdering. Dat is in elk geval niet het formatteren van een gegevensdrager of het herinstalleren van de besturingssoftware. Want dat biedt geen garantie dat gegevens definitief zijn verwijderd.
Er zijn daarentegen vele softwaretools specifiek voor het wissen van gegevens beschikbaar. Hierbij wordt eigenlijk altijd de oorspronkelijke gegevens volgens

Kader 3: Normeringen fysieke vernietiging

EADMS 2008 (European Association for Data Media Security)
Beschrijft 5 fysieke destructie methodes gebaseerd op 5 risicoclassificeringen, van A t/m E. Het laagste niveau A (doorboren) wordt aangeraden voor particulieren en kleine bedrijven. Niveau E (versnipperen tot 10mm^2) voor de meest vertrouwelijke informatie, zoals zeer geheime overheidsinformatie.

NIST 800-88 (National Institute of Standards and Technology)
'Degaussing' voor gegevens met een minder hoge beveiligingsclassificatie volstaat . 'Shredderen' van een medium wordt aangeraden voor de hoogste beveiligingsclassificatie van de gegevens.

Kader 4: Normeringen softwarematige verwijdering

US Department of Defense – Sanitizing (DoD)
Standaard van het Amerikaanse Ministerie van Defensie voor de gehele beveiliging van de overheid. Gegevensverwijdering was hier een onderdeel van.

HMG Infosec Standard No 5
Beveiligingsstandaard voor overheidscomputersystemen in het Verenigd Koninkrijk. Kent twee variaties voor gegevensverwijdering: de 'baseline standard' (enkele overschrijving) en de 'enhanced standard' (drie overschrijvingen).

BSI (Bundesamt für Sicherheit in der Informationstechnik)
Is een raamwerk voor computerbeveiliging van de Duitse overheid. Stelt dat een enkele overschrijving met vaste of willekeurige patronen voldoende is voor normale eisen ten aanzien van bescherming, omdat forensisch laboratorium onderzoek aangetoond heeft dat dan geen gegevens meer gereconstrueerd kan worden.

NIST 800-88/ATA secure erase
Beveiligingsstandaard van het National Institute of Standards and Technology (USA). Praktische handleiding voor hoe om te gaan met gegevensverwijdering. Schrijft enkelvoudige overschrijving voor, wat op basis van studies (…) als voldoende genoemd wordt.

bepaalde patronen overschreven.
Het aanbod loopt uiteen van eenvoudig te downloaden freeware (o.a. Killdisk, Dban) tot en met professionele software voor gegevensverwijdering (o.a. Blancco).
Het is belangrijk om software te gebruiken die veilige gegevensverwijdering garandeert. Diverse internationale instanties hebben normen gedefinieerd om dit te toetsen (zie kader 4). Deze normen worden inmiddels ook volop gehanteerd door andere organisaties en helpen om een goede software te selecteren.

De keuze van gegevensverwijdering
Welke wijze van gegevensvernietiging het beste is, zal per organisatie verschillen. Qua betrouwbaarheid hoeft er in elk geval geen verschil te zitten in softwarematige en fysieke vernietiging. Voor veel organisaties speelt mee dat er gevoelsmatig behoefte is om te kunnen zien dat een gegevensdrager vernietigd is. Waardoor vaak gekozen wordt voor 'shredderen'. Bij een softwarematige verwijdering is dit bewijs veel minder duidelijk, al worden ook wel garantiecertificaten afgegeven.

De vraag is echter of fysieke vernietiging in de toekomst nog acceptabel is. Het is vaak duurder, onder andere doordat wederverkoopwaarde verloren gaat. Maar het conflicteert in toenemende mate met het groeiende belang van Maatschappelijk Verantwoord Ondernemen (MVO). In de meeste gevallen wordt de levensduur door fysieke vernietiging immers bewust verkort, met een vervroegde en potentieel omvangrijke afvalstroom tot gevolg. Bij een softwarematige verwijdering kan de hardware worden hergebruikt, wat over het algemeen beter past bij de MVO-doelstellingen. Zeker als een combinatie wordt gemaakt met het opzetten van bijvoorbeeld een donatieprogramma aan goede doelen in Nederland of ontwikkelingslanden.

Fysieke vernietiging conflicteert in toenemende mate met het groeiende belang van Maatschappelijk Verantwoord Ondernemen (MVO)

De overtreffende trap van veilig transport is een gegevensvrij transport

Overdracht van hardware
Volgens het DNB-toetsingskader dient de organisatie ervan overtuigd te zijn dat er geen gegevens verloren kunnen gaan gedurende het gehele proces van afvoer of overdracht. Hierbij is een onderverdeling te maken in een administratieve component en het transport.
Voor wat betreft de administratie kan op basis van de eerder genoemde registratie worden vastgelegd welke hardware precies wordt gestuurd naar welke partij. Dat zal over het algemeen een opkoper, een lease/verhuurmaatschappij of vernietigingsbedrijf zijn. Van deze partijen kan worden verlangd dat zij na verwerking een rapportage van verwerkte producten en vernietigde gegevens verschaffen. Dit is te vergelijken met de verstuurde producten, zodat na een verschillenanalyse de registratie vervolgens definitief kan worden bijgewerkt.
Met betrekking tot het transport zijn er verschillende soorten van beveiliging te onderscheiden. Of een 'tracking & tracing'-systeem ook echt een betere beveiliging inhoudt mag worden betwijfeld, maar het zorgt er in elk geval voor dat het transport zelf al dan niet 'real-time' gevolgd kan worden.
Dan is het in de logistieke wereld zeker geen uitzondering om (delen van) het transport uit te besteden aan collega-vervoerders. Om dit te voorkomen is gebruik te maken van een 'deur tot deur'-service, met de afspraak dat het gehele transport door de opdrachtnemer zelf wordt uitgevoerd. Dat houdt de lijnen ook qua aansprakelijkheid helder. Bij 'dedicated' vervoer wordt een transport exclusief voor een opdrachtgever uitgevoerd, waarbij er dus geen verwisseling van zendingen van andere verladers kan plaatsvinden. Door voertuigen vervolgens te verzegelen kan de veiligheid gedurende transport verder verhoogd worden.
Maar de overtreffende trap van veilig transport is een gegevensvrij transport. In dat geval zijn de gegeven dus al verwijderd voordat producten worden vervoerd. Bijkomende voordelen zijn dat de impact van een eventueel incident veel kleiner is en dat de controle op de beveiligingsprocedures hierdoor eenvoudiger wordt.

Documenten

Het proces van afvoer of overdracht kan eigenlijk pas waterdicht zijn als ook de overdrachtsdocumenten op een juiste wijze zijn opgesteld. Bij transport kan in principe alleen met een vrachtbrief formeel worden geregeld wat de inhoud van een zending is.

Aangeven van alleen het palletaantal is dan niet voldoende. Om disputen en daarmee afwijkingen in de registratie te voorkomen, is het cruciaal om precies te omschrijven welke gegevensdragers overgedragen worden aan een transporteur. Daarmee kan ook formeel worden vastgelegd over welke producten na verwerking precies teruggerapporteerd moeten worden.

Aansprakelijkheid

In veel gevallen zullen er externe dienstverleners ingezet worden in de operationele uitvoering van een overdrachtsproces. Naast duidelijke afspraken over dat proces is het belangrijk om ook de aansprakelijkheid onderwerp in het gesprek over de leveringsvoorwaarden te maken. Zoals we eerder gezien hebben kan de schade bij een incident behoorlijk in de papieren lopen en dan is het goed om vantevoren te weten in welke gevallen en voor welke bedragen een externe partij aansprakelijk gesteld kan worden.

Daarbij is het goed om te weten dat een transporteur normaal gesproken onder de Nederlandse Algemene Vervoers Condities (AVC) of de Europese CMR-condities werkt. Daarin wordt de aansprakelijkheid gemaximeerd tot een bedrag afhankelijk van het daadwerkelijk gewicht van een zending. Een additionele transportverzekering geeft dekking op basis van de waarde van de producten. De schade als gevolg van gegevensverlies is meestal niet gedekt.

Conclusie

Het bewustzijn van gegevensrisico's aan het eind van de levenscyclus van gegevens of hardware moet op management niveau toenemen. Onder andere als gevolg van groter wordende financiële en PR-consequenties van incidenten, wordt wel veel aandacht wordt besteed aan het beveiligen van gegevens(dragers) binnen de organisatie. Het risico is dat gegevensdragers met gevoelige informatie ongewenst in handen komen van derden wanneer ze heringezet of afgestoten worden.

Om dit te voorkomen heeft het correct registreren en up-to-date houden van alle gegevensdragers en type gegevens daarop de hoogste prioriteit. Dit geldt ook voor gegevensdragers buiten servers, storagenetwerken en werkplekapparatuur, zoals printers en privédevices. En ongeacht de wijze waarop de betreffende hardware is gefinancierd of door welke partij de apparatuur wordt beheerd. Organisaties moeten dus zowel de registratie van hun hardware als van de (gevoelige) gegevens daarop – eindelijk eens – op orde brengen.

De beste wijze van gegevensvernietiging verschilt per organisatie, softwarematige gegevensverwijdering kan even betrouwbaar zijn als het vernietigen van gegevensdragers zelf. Waar 'vernietiging' in richtlijnen wordt vereist blijkt grondig 'wissen' ook te mogen. Het hergebruik van hardware is tenslotte te prefereren vanuit het oogpunt van efficiëntie en Maatschappelijk Verantwoord Ondernemen. Ook al maken alle mobiele apparatuur en BYOD het er niet eenvoudiger op, het is te allen tijde belangrijk om controle te hebben over de bewegingen van uw hardware en de gehele levenscyclus van gegevensdragers en (gevoelige) gegevens. Daarvoor zijn heldere afspraken met externe dienstverleners essentieel. Denk hierbij aan het vraagstuk van aansprakelijkheid bij incidenten, een zorgvuldige registratie van hardware die vertrekt (inclusief correcte transportdocumenten) en controle van de rapportages over de verwerking.

Ons advies: niet(s) vergeten!

Het correct registreren en up-to-date houden van alle gegevensdragers en type gegevens daarop heeft de hoogste prioriteit

Referenties

[CBP2001] CBP: Achtergrondstudies en Verkenningen 23: Beveiliging van persoonsgegevens http://www.cbpweb.nl/downloads_av/av23.pdf

[Cisco2012] http://www.cisco.com/web/NL/news/berichten2012/news_persberichten_031312.html

[DNB2012] Toetsingskader Informatiebeveiliging voor DNB thema-onderzoek 2012, met download "Toetsingskader Security Management 2012": www.toezicht.dnb.nl/3/50-203304.jsp

[ISO2001] ISO 15489: Informatie en documentatie - Informatie- en Archiefmanagement http://www.nen.nl/web/Actueel/NENISO-1548912001-nl.htm; gerelateerd daaraan:

- *ISO 19005: Document management – Electronic document file format for long-term preservation*
- *NEN 2082:2008 – Eisen voor functionaliteit van informatie- en archiefmanagement in programmatuur*

[KPMG2010] Data loss barometer (www.datalossbarometer.com), November 2010

[NAID2012] Data disposal attitudes and practices (2010 – 2011) (http://www.naidonline.org/forms/whitepaper/417_NAID-Europe_Research_Summary.pdf , National Association for Information Destruction (NAID) Europe, Februari 2012

[Ponemon12] 2011 Cost of data breach study (UK), Ponemon Institute, maart 2012

Links

www.blancco.com
www.cpbweb.nl
www.datalossdb.org
www.eadms.org
www.logistiek.nl
www.mvonederland.nl
www.security.nl
www.sva.nl
www.toezicht.dnb.nl

ISO 22301 MAATSCHAPPELIJKE VEILIGHEID

VEREISTEN VOOR EEN GECERTIFICEERD BUSINESS CONTINUITY MANAGEMENT SYSTEEM (BCMS)

Gert Kogenhop is directeur van bcm+, een bedrijf dat is gespecialiseerd in training, consultancy en implementatie van Business Continuity Management Systemen conform de norm BS 25999 en 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 een gecertificeerd trainer op het gebied van leidinggeven. Gert is bereikbaar via www.bcmplus.nl of per e-mail: gk@bcmplus.nl

Sinds november 2007 is BS 25999-2:2007 de enige certificeerbare norm voor Business Continuity Management (BCM). Na publicatie van ISO 22301:2012 (Societal security – Business continuity management systems – Requirements) op 15 mei jl. is daar verandering in gekomen. De norm van het British Standards Institution (BSI) zal per 1 november 2012 worden ingetrokken ter faveure van de in 163 landen geaccepteerde ISO norm. Tot die datum is het mogelijk een certificering conform BS 25999 af te ronden. Ook daarna zal een soepele overgang naar de ISO norm worden bewerkstelligd in samenwerking met BSI tot medio 2014.

Wat is BCM volgens ISO 22301?
De definitie wijkt niet substantieel af van de Britse versie, die tot op de dag van vandaag werd gebruikt, en wordt hierin omschreven als: "holistisch managementproces dat potentiële gevaren voor een organisatie identificeert en tot welke gevolgen deze gevaren mogelijk kunnen leiden met betrekking tot de operationele activiteiten. Het schept een kader voor het opbouwen van organisatorische weerstand en veerkracht, leidend tot een effectieve reactie welke de belangen van betrokkenen, reputatie, merk en waarde creërende activiteiten veiligstelt". Met holistisch wordt in dit kader het geheel en de onderlinge samenhang bedoeld, van zowel de organisatie zelf als de directe omgeving, zowel fysiek als de (logistieke en organisatorische) keten met afhankelijkheden beide kanten op. Hier zit tevens het grote verschil met bijvoorbeeld BCM binnen ISO/IEC 27001. Het gaat om de totale organisatie en meer.

Is ISO 22301 anders dan BS 25999?
Als gekeken wordt naar de inhoud van de nieuwe ISO norm wijkt deze technisch gezien niet echt af van de BSI-norm. Enkele definities van gebruikte termen zijn toegevoegd of gewijzigd, terwijl ook enkele zijn verdwenen. Dit laatste omdat deze niet worden toegepast in de ISO-norm of omdat de invulling vrij wordt gelaten. Zaken als het beleidsplan, de feitelijke continuïteitsplannen, de Bedrijfs Impact Analyse (BIA) en Risico Beoordeling (RB), de reactiestructuur en organisatie van het controleren, beoordelen, herzien, onderhouden en continu verbeteren van het managementsysteem zijn enigszins aangescherpt en veranderd op detailniveau, maar leiden zeker niet tot substantiële veranderingen en inspanningen tijdens een eventuele conversie.

> De structuur van ISO 22301 is wezenlijk anders dan die van de BS 25999

De structuur van ISO 22301 is wezenlijk anders dan die van de BS 25999. Het zes-stappenplan is niet meer terug te vinden, echter de Plan-Do-Check-Act (PDCA) cyclus wel. De grootste wijzigingen zijn vooral terug te vinden op de volgende gebieden:

- Systeembeheer (management);
- Betrokkenheid van het bestuur van de organisatie (top management);
- Communicatie voor, tijdens en na een ernstig incident (disruptive incident).

De nadruk ligt duidelijk op het vaststellen van de doelstellingen van het BCMS (fig. 1). Het meten en controleren van de prestaties, voortgang en gerealiseerde resultaten is een veel belangrijker onderdeel in deze norm. Het vastleggen van de verwachtingen van het bestuur van de organisatie heeft een prominente positie. Meer aandacht wordt geschonken aan de planning en voorbereiding van de inzet van mensen en middelen benodigd voor het zo optimaal mogelijk waarborgen van de bedrijfscontinuïteit. Meer dan voorheen geldt: "Voorbereiding is 90% van het resultaat".
Het feit dat de bestuurders van de organisatie volledig betrokken dienen te zijn bij het begrijpen en vaststellen van de benodigdheden (requirements), het bepalen van de doelstellingen en het meten van de resultaten, zal zeker leiden tot een eerdere en betere acceptatie van BCM als wezenlijk onderdeel van "Good Governance", maatschappelijk verantwoord ondernemen.

De inhoud en aanpak conform ISO 22301

Plan

Conform de PDCA cyclus (fig. 2) wordt gestart met de Plan (vaststellen) fase. In deze fase wordt allereerst aandacht besteed aan "context van de organisatie". Zaken met betrekking tot onder andere de activiteiten van de organisatie, functies, producten, diensten, samenwerkingsverbanden, logistieke keten en de relaties met belanghebbenden worden vastgelegd. Dit alles in relatie tot de mogelijke gevolgen van een ernstig incident. In de internationale norm spreekt men overigens nu over "interested parties" en niet meer over "stakeholders". Voorts dient er in het beleidsplan een volledige afstemming te zijn met de missie, visie en doelstellingen van de organisatie en het gewenste risicoprofiel (risk appetite). Tevens dient er rekening te worden gehouden met de behoefte en verwachtingen van de relevante (externe) belanghebbenden en eventueel van toepassing zijnde wet- en regelgeving. Zoals al eerder aangegeven wordt binnen de ISO norm de nadruk duidelijk gelegd op de betrokkenheid (commitment) van het bestuur van de organisatie. Binnen het onderdeel "Leiderschap" wordt hier vorm aan gegeven middels het verantwoordelijk stellen van de bestuurders voor onder andere het:

- vaststellen van het beleidsplan;
- zorg dragen voor het linken van het BCMS aan de strategische richting;
- integreren van het BCMS in alle processen;
  - beschikbaar stellen van de benodigde mensen en middelen;
  - vaststellen van de rollen, verantwoordelijkheden en bevoegdheden van betrokkenen;
  - sturen en ondersteunen van continue verbeteringsinitiatieven;
- communiceren van voortgang en resultaat.

De bestuurders dienen, zoals gesteld, de strategische doelstellingen van het BCMS vast te stellen alsmede de grondbeginselen. Deze bestaan uit het definiëren van de minimale prestatieniveaus met betrekking tot het leveren van producten en/of diensten en bedrijfsactiviteiten, op een dusdanig niveau dat het behalen van de doelstellingen van de organisatie wordt gegarandeerd. Dit alles dient meetbaar te zijn, rekening houdend met betrokken belanghebbenden, en gecontroleerd en bijgestuurd te worden, indien van toepassing.

Als laatste onderdeel binnen de Plan fase dienst men zaken vast te leggen met betrekking tot de uitvoering en ondersteuning. Het gaat hier om de dagelijkse gang van zaken, het zeker stellen dat de juiste mensen en middelen voor elke taak worden ingezet. Onder andere het beschikken over gekwalificeerde mensen met voldoende kennis, vaardigheden en ervaring. Daarna de juiste ondersteuning in de vorm van eventueel mensen van buiten de organisatie, specialisten. Het is van het grootste belang dat iedereen binnen de organisatie beseft wat het belang is van een goed functionerend BCMS en dat men zich bewust is van mogelijke gevolgen bij niet, onvoldoende of zelfs verkeerd reageren (awareness). Belangrijk is zeker in dit geval de communicatie aangaande in eerste instantie het implementatieproces en vervolgens het beheren van het BCMS. Dit alles als vanzelfsprekend ondersteund door een informatiesysteem (document management system) dat een waterdicht "audit trail" garandeert.

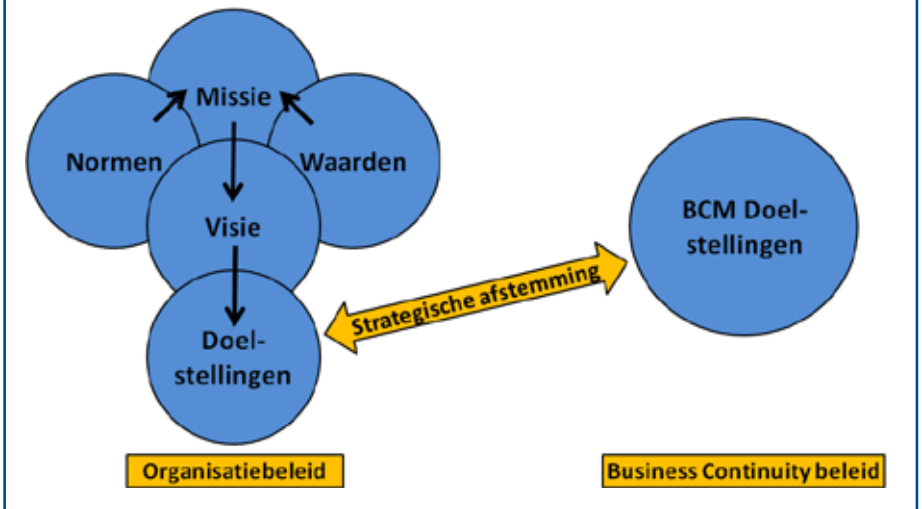
> Binnen de ISO-norm ligt de nadruk duidelijk op de betrokkenheid van het bestuur

Do

De executie van het BCMS is de Do (implementeren en uitvoeren) fase. Dit bevat onder andere de vaststelling van de:

- Bedrijfs Impact Analyse (BIA);
- Risico Beoordeling (RB);
- Business Continuity strategie;
- Business Continuity procedures (BCP);
- test- en oefenprocessen.

Het is van het grootste belang dat continu wordt beoordeeld of de activiteiten in dit kader in lijn liggen met de algemene richting waarin de organisatie zich beweegt. Tevens de wensen en eisen van belanghebbenden, inclusief eventueel van toepassing zijnde wet- en regelgeving. Bij het bepalen van de strategie is het een voorwaarde te kiezen voor haalbare oplossingen, ook al klinkt dat zo logisch en vanzelfsprekend. Afstemming binnen de organisatie, de mensen op de werkvloer, is van doorslaggevend belang bij het implementeren van een (mogelijk/hopelijk) succesvol BCMS. Men dient in



Figuur 1: Strategische afstemming ISO 22301

deze fase prioriteiten te stelllen keuzes te maken over de beschikbaarheid van zaken als mensen, werkplekken, informatie (data), machines en materialen, alsmede zakenpartners, leveranciers en klanten. Dit is uiteindelijk terug te vinden in de te kiezen reactiestructuur, wat regelingen en afspraken bevat aangaande het vaststellen van de gevolgen (impact) en daaraan gekoppelde respons. Dit kan zijn: het in werking stellen van de initiële actie/reactie handelingen, coördineren en communiceren, herstel en/of mogelijk activeren van alternatieve werkwijzen of uitwijk. Het communicatieplan, zowel intern als extern, dient robuust en flexibel te zijn. De tijdigheid en wijze waarop wordt gecommuniceerd is van doorslaggevend belang bij de uitvoering van het actieplan. Voorbeelden te over, helaas, waar dat in het (nabije) verleden vreselijk mis is gegaan. Het is dan ook goed vast te stellen dat de norm hier op een adequate wijze aandacht voor vraagt.

Check

In de Check (controleren en beoordelen) fase ligt de nadruk op het evalueren van de prestatie/uitvoering. In de norm is opgenomen dat men continue moet controleren op het BCMS alsook periodieke beoordeling en herziening ter verbetering. Controle is vereist op onder andere het behalen van de doelstellingen, het meten van de prestaties (processen, procedures en werking) en het voldoen aan hetgeen gesteld in de norm. Dan is het goed dat de organisatie de resultaten analyseert en na evaluatie van de uitkomsten verbeter- en correctieve acties initiëert (audit trail). Als vanzelfsprekend is een interne auditprocedure een vaststaand onderdeel van de vereisten. Deze dient gericht te zijn op zowel de interne doelstellingen als de vereisten gesteld in deze internationale norm.

> Niet alle veranderingen zijn verbeteringen en niet alle nieuwe bezems vegen per definitie schoner

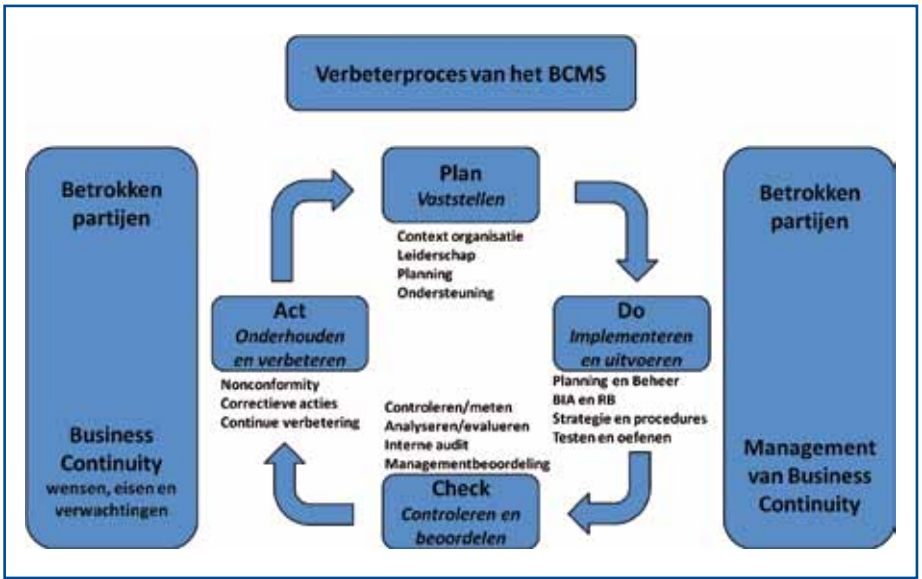
Een van de grootste verschillen met BS 25999 komt tot uiting als we kijken naar de periodieke beoordeling door de bestuurders (management review). In de ISO-norm is deze meer gedetailleerd als het gaat om de vereisten. Duidelijk is wederom de focus op betrokkenheid (commitment) van de bestuurders. Men moet het proces ook zeer serieus nemen en niet als sluitpost op de agenda te plaatsen. De uitkomst van deze beoordeling is de input voor de laatste fase.

Act

In de Act (onderhouden en verbeteren) fase dient elke afwijking (nonconformity) met een actieplan te worden beloond. Na vaststelling van de afwijking moet men correctieve maatregelen nemen, deze strikt volgen en opvolgen. Het onderhoud en herzien van alle onderdelen van het BCMS behoort zeker ook te worden meegenomen in deze fase. Een continu verbeterproces is een vereiste, waar ook de bestuurders van de organisatie niet te licht over moeten denken. Het gaat in dit geval om activiteiten in de organisatie die een bijdrage leveren aan de effectiviteit (het behalen van de doelstellingen) en efficiency (een optimale mix van kosten en baten) van veiligheidprocessen en procesbeheersing, met als doel een hoger rendement voor de organisatie en haar belanghebbenden. Al met al is deze fase vooral gericht om te leren van het heden en verleden om beter voorbereid de (onzekere) toekomst tegemoet te kunnen treden. Regeren is vooruitzien!

Ergo

De meningen zijn verdeeld over het antwoord op de vraag of de ISO 22301 norm "beter" is dan de BS 25999 norm. Zeker is dat men gekozen heeft voor een andere aanvliegroute om tot feitelijk hetzelfde resultaat te komen. "Zo optimaal mogelijk waarborgen van de bedrijfscontinuïteit". De nadruk ligt terecht nu meer op de betrokkenheid van de bestuurders van de organisatie, wat de positie en ontwikkeling van BCM ten goede zal komen. Naar de bescheiden mening van de auteur zal moeten blijken in de nabije toekomst of deze (nieuwe) ISO norm zal leiden tot een succesvollere aanpak en bijbehorende resultaten, daar niet alle veranderingen verbeteringen zijn en niet alle nieuwe bezems per definitie schoner vegen. Feit is dat de internationale acceptatie van een certificeerbare norm zeker een positieve bijdrage levert aan de acceptatie van Business Continuity Management als waardevol managementinstrument op zich. Waarvan akte!



Figuur 2: PDCA cyclus in ISO 22301

GOED HUISVADERSCHAP IN DE STRIJD TEGEN CYBERCRIME

Yuri Bobbert Msc is onderzoeker aan het IT Alignment & Governance Institute van de Universiteit van Antwerpen op het gebied van Business Information Security Governance en Managing Director van B-Able.

Internationale actie tegen cybercrime is dringend nodig, concluderen leiders van overheden en grote bedrijven. Tijdens het World Economic Forum in Davos waarschuwden ze dat criminelen snel omschakelen naar internet, terwijl overheden treuzelen met de bestrijding (Bron: Volkskrant, 26 januari 2012)

De samenwerking tussen burgers, overheden en bedrijfsleven is een juiste en broodnodige stap in de strijd tegen cybercriminaliteit. Ons steeds groter wordende digitale huishouden kent een duistere kant die gekenmerkt wordt door criminele activiteiten, fraude en zelfs digitale oorlogvoering. Zo werden, op nota bene Valentijnsdag, bedrijfswebsites in Bangladesh niet gespaard. Met een simpele druk op een knop legde een massale hack in een dag maar liefst 20.000 sites plat. Geen wonder dat het World Economic Forum zich buigt over dat wat wel eens de volgende nachtmerrie kan zijn voor het bedrijfsleven. Zeker omdat we zien dat de afhankelijkheid van informatiesystemen alleen maar toeneemt en dat parallel daaraan de informatievraag

World Economic Forum 2012

exponentieel groeit. (Bron: IDC) Zowel het CBS als Europol rapporteerden eerder al over de toenemende schade en de koppositie die Nederland in dit slecht huisvaderschap vervult. Sommige landen, die al langer te maken hebben met criminaliteitscijfers die extremere proporties kennen dan de EU landen, zijn inmiddels verder op het gebied van governance op IT security

Rob Wainwright, directeur van Europol

vlak. Een land als Zuid-Afrika heeft al sinds begin deze eeuw "corporate governance" kaders voor risicomanagement op technologie vormgegeven en geëffectueerd (King report [1]). Dit om niet in de praatfase te blijven hangen maar CEO's in een vroeg stadium in de doe- fase te krijgen. Een recent onderzoek, dat is uitgevoerd door het ITAG (IT Alignment and Governance Institute), wijst uit dat het merendeel van de CIO's als ook Security Officers niet pro-actief bezig is zijn of haar organisatie te consulteren over toekomstige technologieën (i.e. Near Frequency Communication & Payment, Machine to Machine communication etc.) en de vertaling hiervan naar nadelige bedrijfsimpact bij security gerelateerde incidenten (bijvoorbeeld hack attacks). Iets wat de CEO redelijkerwijs wel mag verwachten van zijn CIO als het gaat om strategische informatieplanning en de "Governance" daarvan. De verwevenheid van Corporate Governance, Enterprise Governance of IT, Risk Governance alsmede Business Information Security Governance neemt hand over hand toe. De urgentie om te komen tot praktisch effectieve en eenvoudig toepasbare Governance praktijken (Governance practices) is essentieel willen CEO's de aankomende hoeveelheid zettabytes aan informatie adequaat kunnen blijven beschermen zonder dat hun bedrijfsvoering hier hinder van ondervindt. IDC verwacht dat de totale hoeveelheid digitale informatie dat in een jaar wordt gemaakt en gerepliceerd zal uitgroeien tot 35 zettabytes in 2020, van minder dan 1 zettabyte in 2009 (Economist, 2011). Het World Economic Forum benadrukt dan ook dat bedrijven sterk onderling verbonden risico's in cyberspace en zogenaamde "networked ecosystems" in kaart moeten brengen. Iets wat we kunnen vertalen naar een "digitale stakeholder analyse". Een van de meest principiële corporate governance praktijken die nimmer door EU bedrijven worden toegepast maar wel degelijk een CEO of CFO inzage geeft in zijn digitale -risicovolle- zakenpartners (i.e. Stakeholders) binnen zijn "networked ecosystem". Nuttig ook om digitale risico's die andere, maar voor jouw bedrijfsvoering kritieke, informatiesystemen kunnen brengen te identificeren. CEO's kunnen, met een logische preventieve blik, vandaag al beginnen met het vormgeven van risico management kaders als het gaat om Cybercrime. Mits men uiteraard vanuit goed huisvaderschap preventief wenst te acteren in plaats van reactief achter de feiten aan te lopen.

Referentie

King report:
http://www.iodsa.co.za/PRODUCTSSERVICES/KingReportonGovernanceinSA.aspx

EEN NIEUWE PRAGMATISCHE KIJK OP GOVERNANCE RISK EN COMPLIANCE SOFTWARE

Ing. Marcel Lavette CISA EMITA is managing director van CompLions B.V. en is te bereiken via m.lavalette@complions.nl.

Een nieuwe ontwikkeling in het aanbod van Governance Risk en Compliance (GRC) software is een benadering die gericht is op de processen die bijdragen aan de GRC doelstellingen. Een voorbeeld van zo'n proces is Informatiebeveiliging. Veel van de huidige GRC oplossingen zijn erop gericht om interne beheersing te realiseren over alle bedrijfsprocessen heen. Dit heeft meestal complexe, tijdrovende implementaties en hoge investeringen tot gevolg. Een bottom-up benadering is in sommige gevallen eenvoudiger te realiseren en biedt de mogelijkheid om gefaseerd GRC doelstellingen te realiseren.

Weinig tooling beschikbaar

In de praktijk is er voor deze benadering nog maar weinig tooling beschikbaar. Dit ondanks de grote rol die processen als informatiebeveiliging of IT risicomanagement spelen in de GRC behoefte van een organisatie. Voor de IT-organisatie is er veel meer keuze uit servicemanagement tooling. Voor Informatiebeveiliging is het zeer beperkt en dat wat er is dekt veelal niet de gehele lading. Het is te beperkt, te complex en is meer ontwikkeld vanuit een GRC context en veelal duur. In het laatste geval blijkt het voor onderliggende processen als Informatiebeveiliging lastig te zijn pragmatisch de Plan-Do-Check-Act activiteiten vanuit normen als ISO 27001 uit te voeren.

Plan-Do-Check-Act

Een nieuwe benadering voor ondersteuning van deze procesactiviteiten van een (informatie)beveiligingsorganisatie, is de borging van het gehele proces op basis van de PDCA-cyclus als geheel.

Vanuit de Plan-fase naar de Do-fase

CompLions B.V. uit Deventer brengt sinds 2 jaar de ISMScontrol tooling op de markt. Deze tooling biedt ondersteuning aan alle activiteiten van een managementsysteem, zoals onder andere ISO 27001/NEN7510 dit vereist. Tot de basisfunctionaliteit behoren een risicomanagementsysteem Plan-fase (op basis van een Business Impact Analyse en Dreigingen Analyse) en een maatregelenselectiesysteem. Dit selectiesysteem werkt op basis van kenmerken die aan maatregelen op te geven zijn zoals BIV-classificaties, dreigingen en SLA-wensen en die wel of niet matchen met risicoanalyses en configuratie-items. Het systeem is geïntegreerd met een risicoafwegingen maatregelacceptatiemechanisme, waardoor een koppeling ontstaat tussen risicoanalyses op basis van Business Impact Analyses en Dreigingen Analyses en de selectie van maatregelen. Geaccepteerde maatregelen kunnen in de Do-fase van het systeem verder worden afgehandeld.

Maatregelen en normen

Een belangrijke plus voor gebruikers van ISMScontrol is dat het systeem uitgaat van een maatregelenset, waarvan de maatregelen gekoppeld worden aan norm controls van normen zoals PCI DSS, BS2599/ ISO 22301, ISO 9001, ISO 14001, ITGC, WBP, DBB-IT, ISAE-3402, HKZ, NIAZ etc.
ISO 27001 of NEN7510 zijn naar keuze standaard beschikbaar. Daarnaast is het ook mogelijk eigen normen toe te voegen.

Het koppelen van maatregelen hoeft maar eenmalig te gebeuren waardoor het inrichten van een compliance en control raamwerk relatief eenvoudig is geworden en een onderhoudsarme activiteit. Van maatregelen worden vervolgens de implementatiestatus en effectiviteitsscores bijgehouden die door vertaald worden naar de norm control. Hierdoor ontstaat een goed beeld per norm over de status en effectiviteit.

ISMS control Dashboard

Certificering

Diverse organisaties hebben inmiddels met behulp van ISMScontrol een certificaat behaald op één van de genoemde normen of gebruiken de tooling voor het managen ervan. ISMScontrol voorziet in standaard (management)rapportages zoals een Management Review rapportage, Verklaring van Toepasselijkheid, normmaatregelen en auditrapportages Hierdoor is het direct toe te passen en sluit het aan op de dagelijkse praktijk van een ISMS waardoor het proces en standaarden als ISO 27001 en NEN7510 sneller en beter te beheersen zijn.

PINCODE VOOR JE PACEMAKER

Jules Prast draaide jarenlang mee in de top van het bedrijfsleven en bereisde vele landen van de wereld. In 2008 kwam hier abrupt een einde aan als gevolg van sarcoïdose, een chronische ziekte van het immuunsysteem. Sindsdien runt hij zijn eigen coachingspraktijk PrastConsult. Jules is te bereiken via jules@prastconsult.com.

Pacemakers zijn met de tijd meegegaan. Het zijn nu kleine computers die draadloos kunnen worden uitgelezen en geprogrammeerd. Daarmee begeeft de pacemaker zich op het terrein van de informatiebeveiliging. Je moet er toch niet aan denken dat je pacemaker wordt gehackt! Gelukkig kondigde computerbeveiligingsfirma McAfee onlangs aan, dat de universiteit van Princeton in de Verenigde Staten nieuwe software heeft ontwikkeld die een firewall creëert voor pacemakerdragers.

Inderdaad. Een firewall voor pacemakerdragers. Sinds 2008 ben ik zelf drager van een pacemaker. Op de plaats waar deze in mijn borstkas zit, wordt bij controles in het ziekenhuis, een soort computermuis gelegd. Het is zowel een zender als een ontvanger die via een draad verbonden is met een apparaat dat een pacemaker kan besturen. Op een microchip binnenin, onthoudt mijn pacemaker tot een jaar lang iedere geregistreerde afwijking van het hartritme. Die gegevens worden tezamen met de stand van de batterij uitgelezen. Zo kan de cardioloog besluiten of de pacemaker aan vervanging toe is of dat de instellingen ervan moeten worden bijgesteld.

Modem

Tegenwoordig kan ik thuis ook zelf controles verrichten. Ik heb van het ziekenhuis een modem gekregen met precies zo'n 'computermuis' eraan. Iedere paar weken sein ik mijn data over naar de computer van het ziekenhuis. Ook tussentijds kan ik dit doen wanneer ik mijn hartritme niet vertrouw. Zelf kan ik de data niet analyseren. Maar als er iets mis is, dan krijg ik dezelfde dag nog bericht. Een veilig gevoel.

In de krant heb ik al eens eerder gelezen over een proef die een lobbygroep op het gebied van privacy had laten uitvoeren om pacemakers te hacken. Op drukke punten, in winkelcentra en op vliegvelden, was men gaan staan

met een laptop en een draadloze ontvanger. Af en toe kwam er een niets vermoedende pacemakerdrager voorbij van wie het signaal werd gedetecteerd. Als je maar dicht genoeg in de buurt bleef van het slachtoffer, dan was uitlezen van de gegevens een koud kunstje. Ik vind het een nogal enge gedachte dat dit me kan overkomen. De vertrouwelijkheidsschending is één ding, maar wat als een of andere onverlaat je pacemaker gaat herprogrammeren?

> Het idee dat een whizzkid op afstand je pacemaker uitzet

Doodmoe

Ik beschik over een ultramoderne pacemaker, eentje waarmee je ook in een MRI-scanner kunt. Mijn toch al innovatief ingestelde cardioloog wilde per se zo'n superdeluxe uitvoering voor mij. Wanneer ik een MRI-scan moet ondergaan, komt er een medewerker van de afdeling cardiomeettechniek om mijn pacemaker voor de duur van het onderzoek in een veilige, stationaire stand te zetten. Dan kan er niets fout gaan. Na afloop moet ik dan de gang door en de hoek om naar een kamertje waar deze medewerker op me wacht om de pacemaker weer te activeren. Dan weet ik meteen waarom ik het apparaatje ook alweer heb. Het verschil is onmiddellijk voelbaar. Ook op die korte afstand word ik doodmoe en duizelig omdat het hart niet in staat is om op eigen kracht voldoende vermogen te genereren voor de inspanning.

Het idee dat een grapjas of een rotjochie met whizzkid-neigingen in een winkelcentrum op afstand je pacemaker uitzet, is onverdraaglijk! Voor mensen die helemaal niet zonder kunnen, is dat levensgevaarlijk. Zo doen zich met het voortschrijden van de technische mogelijkheden voorheen onbekende uitdagingen voor.

Enige tijd geleden kreeg ik al een brief van de fabrikant dat extra controles nodig zijn vanwege een softwarefout in sommige pacemakers van mijn type. Innovatie heeft zijn prijs. Zou ik binnenkort een brief krijgen dat ik op het internet de nieuwe firewall software kan downloaden en installeren? Een pincode bij mijn pacemaker zou ook wel bijdragen aan mijn gemoedsrust.

COLUMN

KOEKJE ERBIJ? NEE? NOU, DAN BEZOEKT U ONZE WEBSITE TOCH LEKKER NIET!

Toen ik in 1998 rechten ging studeren, wist ik het heel zeker: IT & Recht, dat is echt het allerspannendste rechtsgebied dat bestaat. Althans, het bestond toen nog amper en dat was dus exact waarom het zo spannend was. Colleges waren gewijd aan discussie over wetsvoorstellen, over de voors en de tegens, over hoe dat dan zou moeten allemaal, en over de vraag of online hetzelfde recht zou moeten gelden als offline. Nu is het 2012 en worden de eerste wetten van toen in de herzieningsbak gesmeten omdat blijkt dat de wereld van de technologie sneller loopt dan het recht en ook omdat bepaalde ideeën over regulering toch niet helemaal lekker matchen met de online praktijk. En dan hebben we nu een cookiewet. Voor mij oprecht een van de dieptepunten uit het discours, een drama uit de krochten van diegenen die het niet begrijpen en een farce voor hen die het niet willen begrijpen of die gewoon doen alsof ze het niet begrijpen.

Mag ik het zeggen? We hebben prachtig gefaald hier. Met zijn allen. Dat werd me alleen maar meer duidelijk op het moment dat ik voor het eerst na het van kracht worden van de cookiewet een bezoek wilde brengen aan fok.nl. Toen ik de website bezocht, kreeg ik eerst een mooie pop-up met wat uitleg en onderaan een keuzeoptie: links onderin stond in klein grijs font de tekst "ik wil geen cookies!" en rechts onderin schreeuwde in enorm groen een groot blok "deze melding sluiten en niet meer weergeven". Nu ben ik geen ontzettende anti-cookie dame, maar dat kleine grijze font veranderde in een ongehoord verlokkelijk stukje tekst. Uiteraard moest ik daarop klikken om te zien wat er zou gebeuren. En toen viel mijn mond open van verbazing. Ik mocht niet meer door naar de foksite. Volgens de websiteaanbieder kon mij niet gegarandeerd worden dat ik gevrijwaard zou blijven van cookies en dus was het einde oefening. Wat?

Niet dat ik nu per se naar de foksite wilde, maar de toegang ontzegd worden omdat ik als consument van mijn wettelijk recht gebruik gemaakt had… "In wat voor wereld leven we eigenlijk" hoorde ik mezelf hardop zeggen. Nou, in een wereld waarin onze Nederlandse wetgever een wet heeft gemaakt over toestemming voor het plaatsen van (niet-functionele) cookies. Een toestemming die strenger is vormgegeven dan noodzakelijk onder de Europese wet waarop deze gebaseerd is. Een wet die tijden onderwerp van verhit debat is geweest juist omdat er onenigheid ontstond over die vereiste toestemming. Waar eerst nog bedacht werd dat dit wel allemaal via de browsers geregeld kon worden (u klikt gewoon 1 keer in uw browser op "ja" of "nee" en dan is het klaar), werd dit uiteindelijk niet afdoende gevonden. Het niet blokkeren door consumenten kon niet worden opgevat als toestemming. En dus moest er echt iets expliciet in beeld verschijnen op het moment dat een website bezocht werd. Dat er een opt-in moet zijn voordat persoonsgegevens verwerkt worden, is iets waar ik als privacyjurist alleen maar blij om kan zijn. Openheid en transparantie worden gestimuleerd en data subjecten (gewoon u en ik dus) kunnen dan beslissen of ze dat wel allemaal zo willen. En dat de wetgever privacy zeer serieus neemt, valt ook alleen maar toe te juichen. Maar tegen welke prijs?

Websiteaanbieders buitelden over elkaar om te zeggen dat ze ook niet precies wisten hoe ze dit recht nu moesten vormgeven. Een rondgang van Webwereld op de eerste dag van de cookiewet liet dan ook zien dat praktisch geen van de door hen bezochte websites iets geregeld had. OPTA, verantwoordelijk handhaver in deze, had beloofd te komen met richtlijnen over de toepassing in de praktijk (menigeen had gehoopt op een "doet u dit nu maar, dan is het goed"), maar het bleef stil. Klaarblijkelijk wist OPTA zelf ook niet hoe ze het gospel moest verkondigen, want – oh ironie – op de cookiewetdag had de toezichthouder zelf ook haar zaakjes niet op orde en bleek er een mooie niet-functionele cookie werkzaam op de eigen website. En dan te bedenken dat het handhaven van die wet een van de drie speerpunten in het beleid van OPTA is, althans, dat vermeldde zij zelf op haar website (ja, die site met dat cookie dus). Enfin. Ik moet u zeggen dat deze wet een unicum is in alle opzichten. Nog nooit heb ik in al die jaren sinds ik voor het eerst in de collegebanken zitting nam meegemaakt dat een IT & Recht-wet bij het in werking treden al zo overduidelijk in de herzieningsbak gedumpt moest worden.

Mr. Rachel Marbus, @RachelMarbus op Twitter

IS CLOUD STORAGE TOO FLUFFY FOR YOUR MOBILE DEVICE?

Joe Sturonas, CTO van PKWARE, schrijft over de risico's van informative in de cloud. Dit keer beschouwt hij de BYOD-trend, waarin hij stelt dat het niet "jouw" apparaat is, maar "ons" apparaat, dat device management niet gelijk staat aan beveiliging van deze apparaten en dat gebruik van de cloud door deze apparaten niet uit te sluiten is. Daarom sluit hij af met twee belangrijke vragen die we onszelf horen te stellen.

By Joe Sturonas, Chief Technology Officer for PKWARE. PKWARE offers software solutions to critical IT problems, namely the explosive growth of data, the need to secure data, and the emergence of data in the cloud. He can be reached at Joe.Sturonas@pkware.com.

With the proliferation of mobile devices, companies are increasingly adopting "Bring Your Own Device" (BYOD) policies – whereby employees use their personal phones and tablets to access corporate applications and data. Gartner has projected that by 2014, ninety percent of organizations will support corporate applications on personal devices. This raises significant security challenges for enterprise IT departments on how to secure and protect corporate data on a wide range of mobile devices.

Knowledge workers in an enterprise are notorious for finding the path of least resistance in order to be productive, much like a river finds the path of least resistance in a valley. The river will find its way around a large boulder until it erodes the boulder to gravel. Today, knowledge workers use mobile devices to fuel efficiency like never before. And in an ironic twist, smart phones and tablets have become the network computers that IT organizations have been trying to propagate for years.

More and more, employees are bringing their personal technology devices into the workplace to access company information. As a result, companies are challenged to enable collaborative access to sensitive information while ensuring data security and privacy. The trend significantly blurs the line between enterprise and personal computing, and further complicates the job of governance, risk and compliance management. Left unbridled, this practice can lead to a significant loss of sensitive information.

The river will erode a large boulder to gravel

In many organizations, there has been a tremendous focus on security technologies, such as *Data Loss Prevention (DLP),* with which organizations attempt to detect sensitive data at rest and in motion within the fortified borders of the enterprise network. Frequently, and quite often in parallel, knowledge workers are moving data to their BYOD smart phones and tablets, bypassing the MIS/IT policy and procedures completely. Picture your data management guru repairing a leak in the middle of a dam, while at the same time, water cascades by the gallons over the top of his/her head.

The not so hidden costs

Yes, at face value it seems like an excellent deal…*employee purchases wireless device, not us*. But, not so fast, there's a host of security and compliance costs associated with mobile BYOD. Typically, BYOD brings the iOS® iPhone® and iPad®, BlackBerry®, and Android™ tablets together into one shop. Now CIOs have to invest in a multi-platform mobile device management solution as well as other software, and possibly a virtual private network (VPN) layer.

And, while most mobile devices have some type of management tool to help

locate a lost phone, perform a remote lock or wipe, or even change the pass code remotely, the tools may not meet your enterprise standards. What's more, you can't force fit an Android phone into a BlackBerry Enterprise Server paradigm.

Aberdeen analyst Hyoun Park adds, "The cost of compliance - ensuring governance, risk management and compliance - is also more difficult when devices must be chased down individually." It's quite different for an organization to inventory and set-up a hundred devices from a hundred directions than a bulk upload of machines from one vendor.

Avanade, a business technology services firm, surveyed more than 600 IT decision makers late last year and discovered that more than 50% of the companies reported experiencing a security breach as a result of consumer devices.

According to Jim Reavis, executive director of the Cloud Security Alliance, "The challenge for administrators is to provide business data to end user devices while keeping that data separated, segmented and managed."

Time to sharpen your pencil when examining the overall cost savings of employee owned devices, don't forget to factor in additional management time, increased risks for a breach and the need for policy enforcement.

50% of companies experienced a security breach because of BYOD

A Closer Look- taking the "Y" out of your

The BYOD culture can create very interesting situations. For example, when an employee purchases a device, it is thought of as *their own* device. But in reality, if they really want to increase their own productivity, they will want access to company resources via the device requiring a connection to enterprise data network devices.

Consider theses sceneries to see how companies quickly turn "your" into "our" device.

Before the employee has permission rights to connect the BYOD to the company network, the employee may need to agree that the BYOD be managed by policy. Such policy often includes mandatory password protected screen timeout, data encryption, and the ability to wipe the device if it is lost or stolen. The policy granularity can go very deep and may actually encroach on personal data. So at this point, is it really still the employee's device?

A company may "snoop" your device

Recent headlines spotlight a very large international company that allowed BYOD, but prohibited the use of voice recognition command software.

The rationale cited a remote server that translates the spoken queries into text, a process not done locally on the phone. Fears loomed around the potential for data leakage if the voice recognition was used for sensitive data and the phone provider (aka the third party systems) did not treat it as such. A natural language interface is often viewed as a very useful feature of a smart phone. And it could easily be deprecated by the policy administrator, thus becoming a cost of policy enforcement in order to access enterprise data. Is this still the employee's device?

If an employee agrees to use a device for company business, they might need to call on a corporate IT person for assistance or support. More likely than not, that IT person will have some access rights to the personal information, if even temporarily. A company may also set forth certain rights to "snoop"

on the device, requiring random access and possible review of private files, e-mails, web history, even passwords. Now, is it the employee's device?

Lastly, pretend the BYOD device has been found to be out of compliance with agreed upon security standards. As a result the device is quarantined, and access to corporate networks shutdown, a virtual lockout of everything, even family phone numbers, needed by the employee. Now, is it the employee's device?

Device management ≠ data security

Regardless if the BYOD culture gets the traction many expect, it is still a force that requires attention. A recent survey by Gartner suggests global companies have BYOD on their radar. The 2011 survey results found CIOs believe 38 percent of laptops, tablets and mobile phones will be employee-owned in the US and 20 percent in the UK in two years. The survey also showed BYOD demand was highest in countries where Gen Y employees make up more of the workforce.

With all the buzz around Mobile Device Management (MDM), it might be tempting to believe your data will be locked down with use of these tools. Not always the case. Determining efficiencies and creating management dashboards to control a sea of smart phones does not equate to data security. Instituting a policy that wipes a device clean if lost might be just a few seconds too late at the hands of a professional hacker.

> The content consuming devices need the content producing devices

Perhaps there is comfort in knowing the MDM strategy articulates the acceptable apps employees can access. Think again. Even the best efforts will fall short trying to control the plethora of employee owned devices and enforcing policy. For example, the Android Malware Genome Project hopes to improve the efficiency of mobile malware detection-- claiming mobile security software can miss as much as 80% of malware with the best apps letting approximately 20% slip by today.

Those challenges may quickly pale in significance when you consider the dangerous combination of employee owned devices accessing corporate information connected to third party cloud services and using cloud storage.

100% Chance of cloud cover

Why is cloud so closely related to mobile? Mobile devices are for the most part, content consumption devices where content (emails, documents, books, articles, etc) is mostly consumed (read) on these devices. The content producing devices-- such as desktops and laptops-- need to be available to the content consuming devices.

> Data has to actually get to the cloud

The very productivity potential of the mobile device requires automatic content delivery, not premeditated, through cloud storage services that synchronize data from each device and the cloud. Consider this result:

An employee works on a desktop to prepare a presentation needed for the next day. That evening, he wants to go over the presentation one last time. He takes out his smart phone, downloads the latest presentation from the cloud storage where it was last updated from the desktop, and reviews the presentation. The next day when he arrives at the office, he goes into the conference room with his tablet, accesses the latest file, connects to a projector and presents to his peers.

While cloud storage synchronization might sound like a very intimate activity with very little security exposure, the reality is that unless the data is encrypted, the data could be very exposed.

And, depending on the cloud storage service that is being used, it might actually be public. Exactly the case when a 2011 software update mishap yielded a four hour security breach, temporarily allowing any password to access any user account in the vendor's cloud storage system.

Because mobile devices are mainly content consumption devices they don't have the same resources in terms of memory. What's more, almost all mobile data plans are capped in terms of the amount of data that can be transferred in a month. This means the majority of data must reside in the cloud which allows the user to pick and choose the data they need on the mobile device, conserving the memory and bandwidth.

Cloud concerns

Data is often comingled on shared servers and exposed to users you don't know. If your Cloud storage provider encrypts your data but holds the key, anyone working for that Cloud storage provider can gain access to your data. Cloud providers have root access to all your unencrypted data in the cloud, and they are not your employees.

Data also has to actually "get to" the cloud, which usually means leaving your trusted infrastructure and overcoming compounded transfer vulnerabilities as data moves to and from the cloud.

Contactless transactions

More data vulnerabilities are present with Near Field Communications (NFC) and Bluetooth Low Energy, both short-range communication technologies which are integrated into mobile phones. Cleverly coined a "virtual wallet", retailers are looking to capitalize on this opportunity to personalize the consumer experience. Although the transmission range is fairly short, such as waiving your phone over a NFC capable device for a coupon or payment, worries are still justified about personal information stored in NFC tags.

This wireless exchange of data between a reader (a phone) and a target (a microchip embedded in an object) is essentially a subset of radio frequency identification (RFID). Man-in-the-middle attacks are at the forefront of concern, where a participant in one transaction drops some form of malware onto the phone, subsequently infecting other phones that the original interacts with later. And the bottom line…any broadcasted data can be intercepted, period.

Key ideas

Using Public/Private key pairs (X.509 digital certificates and/or PGP key pairs) can greatly increase the ease of use for regular crypto use. Using Public/Private key pairs eliminates the need to have to manage a dozen or more passwords in order to decrypt information.

> The cost and complexity of implementing secure data exchange can get overwhelming

With Public/Private key pairs used for encryption/decryption operations, the public key is used for encryption. Public keys are intended to be public and can exist in local key stores or in LDAP directories where they can be searched and used for encryption operations.

The use of Private keys for mobile devices is a bit more delicate. For certain, concern arises that if the private key must exist on the mobile device itself, that the mobile device be sufficiently protected so that the private key could not be exposed if the mobile device were lost or stolen. Best practices to ease anxieties include policy around timeouts and screen locks that require authentication in order to protect the private key on a mobile device.

In contrast, mobile interaction does not always require the private key to reside on the device for decryption operations. For example, where attachment

processing is managed by a server it is only necessary for the private key to exist on the server, which is essentially out of control of the owner of the private key. This can have some serious security implications depending on the nature of the data and the applications that are securing the data.

Think outside the device-- data-centric not device-centric

A device-centric strategy is a costly infrastructure to keep up and almost destined for failure. There's no dispute, organizations are confronted with increasing amounts of sensitive data and ever changing compliance statutes. Simple encryption solutions, in a complex world of mobile devices won't get the job done. Faced with a wide variety of computing platforms and operating systems, the cost and complexity of implementing secure data exchange can get overwhelming. Damaging costs due to a breach could essentially cripple an organization.

Think outside the device for a more realistic strategy and protect data at its native-use level. The only way to protect data in the cloud is if you encrypt the data before it leaves and you maintain control of the private key.

This approach ensures that virtually any type of sensitive data kept in file, folder, or email format is protected while the data is in transit or at rest.

A data-centric security strategy helps organizations address their daily data security challenges, including protecting sensitive data and meeting compliance requirements. When used in conjunction with a compression tool, less bandwidth is required for transmissions and less storage space is required in the cloud. This helps companies reduce overall costs and operational overhead.

The regulatory standards issues that you deal with today in your own data center are just as important in the Cloud. Compliance with PCI DSS, EU Privacy Act, Sarbanes-Oxley, and FIPS140-2, etc. are just as imperative. If you know that the data is encrypted before it goes into the Cloud, you may be compliant with any number of these regulations. Even if the Cloud vendor is hacked or someone uses an administrative password improperly, your data is still impregnable at that location. A breach? No worries, really. You can prove your data is protected.

Important questions

Since the productive use of mobile devices requires spontaneous access to data that must reside in the cloud, then ask yourself a couple important questions:

1. Do you trust your cloud provider?
2. Do regulations on certain data allow you to trust your cloud provider?

If you answered "no" or even "maybe" or hesitated, it's time to encrypt the sensitive data. Then, you don't need to trust your cloud provider.

Data-centric security, allows you to decrypt the data on your mobile device when you need to consume the information, and leave it encrypted otherwise. As "data-centric" becomes the standard for information security, it eases concerns over the platform, the device, the transmission for moving and storing that data.

Reversing BYOD is not an option

Bill Bodin, IBM® chief technology officer for mobility, summarized that whatever the challenges of supporting workers' equipment might bring, reversing BYOD practices is not an option for IBM nor the business world in general. "The genie is out of the bottle," he said.

ACHTER HET NIEUWS: WACHTWOORDEN

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

"Het lekken van wachtwoorden is een gegeven. Deal with it."
Bijna elke homo digitalis is de afgelopen weken weer eens met zijn/haar neus op de feiten gedrukt: wachtwoorden hebben de neiging om in breder publiek bekend te worden. Of dit inherent is aan het verschijnsel wachtwoord, moet nog wetenschappelijk worden onderzocht. Het is echter feit dat een groot deel van de hashes van LinkedIn wachtwoorden op een of andere wijze recentelijk in het publieke domein terecht zijn gekomen. Omdat we (te) veel wachtwoorden moeten onthouden, hebben mensen de neiging om wachtwoorden te "hergebruiken", zoals een politicus ook ronduit toegaf in de pers. Hij gebruikte hetzelfde wachtwoord voor zowel LinkedIn als voor PayPal. Wat moeten wij als securisten hier nu mee?

Lex Dunn
Problemen moet je aanpakken bij de bron, en dan ook niet aarzelen om drastische maatregelen te nemen. Wachtwoorden zijn een probleem: ze moeten aan allerlei moeilijke regels voldoen, de gebruiker moet vele wachtwoorden verzinnen en onthouden, ze worden bij anderen bekend (opzettelijk gedeeld, of onopzettelijk door afkijken of diefstal), of ze zijn bij voorbaat al gecompromitteerd omdat leveranciers de wachtwoorden van standaard accounts in hun documentatie vermelden. Dus even fors ingrijpen: we schaffen wachtwoorden af. Probleem opgelost. <einde cynische mode>. Zo simpel ligt het natuurlijk niet. Als je wachtwoorden af zou schaffen, hoe zorg je dan voor authenticatie van de gebruiker? Er zijn diverse oplossingen voorgesteld, sommige daarvan bestaan al in de praktijk. Bijvoorbeeld SMS-codes, one-time pads zoals de TAN-codes, one-time password tokens - waar je overigens weer een PIN, dus wachtwoord, voor nodig hebt - en andere zijn nog in onderzoek of al afgeschoten (grafisch, door het aanraken van verschillende punten in een afbeelding, RFID-chips in het lichaam, NFC-technieken middels je mobieltje, analyse van snelheid en manier van tikken op het toetsenbord). In mijn optiek hebben alleen oplossingen die twee-factor-authenticatie bieden, een toekomst. Bijvoorbeeld het gebruik van een one-time password token, die middels een PIN wordt ontsloten (twee factoren: bezit van het fysieke token, en kennis van de PIN code). Waarom? Als hierbij een van beide factoren wordt gestolen of openbaar wordt, is falsificatie nog niet mogelijk, want je moet beide factoren hebben of kennen. Dan moet de gebruiker natuurlijk wel danig geïnstrueerd worden om die PIN code NIET op het token te schrijven, en als bedrijf moet je dus NIET het token en de PIN-code beide per post verzenden. Maar voorlopig zullen we nog moeten leven met het bekend worden van wachtwoorden (of zoals in geval van LinkedIn de hashes, maar met rainbow tabel lookup en zwakke MD5-hashes is dat net zo erg als het lekken van de wachtwoorden zelf). Complicerende factor daarbij is dat die wachtwoorden steeds vaker buiten ons domein vallen (Yammer, Facebook, Twitter en dergelijke).

Ronald van Erven

Enige jaren geleden heb ik van Sony een usb-stick gekocht met een finger-print reader. Deze werkte met een vinger-swipe ipv vingerscansysteem.
Op de usb-stick stond een soort kluisje waar je je wachtwoorden in kon doen met de url van specifieke websites of applicaties. Op je pc moest je een stukje software installeren en als je dan op een site kwam waar je op kon inloggen zag dit stukje software dat en riep de versleutelde usb-stick aan. Dit zelfde gold bij inlogvelden van applicaties of beveiligde Officedocumenten. Na de vinger-swipe opende het kluisje en werd de bijbehorend pincode of wachtwoord ingevuld.
Natuurlijk is dit systeem niet feilloos. op diverse punten is aftappen van verkeer mogelijk. Het voordeel voor mij was dat het werkte als een huissleutel. En als je niet hoefde in te loggen haalde je je sleutel uit het usb-slot.
Helaas met de overgang naar mijn Apple-computertje was ik deze functionaliteit vergeten mee te nemen in het aanschafproces en ben ik terug naar de dagen van 1001 wachtwoorden met elk zijn eigen kwaliteitskenmerken. Zover ik het zie zal het nog vele jaren duren voordat er een universeel inlogprincipe en (technische) mechanismen zijn. Tot die tijd zijn we nog overgeleverd aan de wachtwoordsettings die ICT-beheerders met de beste intenties en vaak naar eigen inzicht doorvoeren.

André Koot

Wachtwoorden. Het zijn ondingen. Ik heb wel 50 verschillende accounts met iets minder verschillende wachtwoorden. Gelukkig kan ik in de meeste gevallen nog onthouden welk wachtwoord ik voor welk account moet gebruiken, dat is het voordeel van hergebruik. En volgens een recent wetenschappelijk onderzoek ben ik bijna zo oud dat ik ook nog eens complexe wachtwoorden gebruik, maar als nog later meneer Alzheimer langskomt, dan weet ik dat ook zo niet meer. Nee, ik ben niet blij met wachtwoorden. En het vervelende is dat elk bedrijf mij weer voorziet van een 'mijn-omgeving', waar ik helemaal geen behoefte aan heb; ik wil een 'ik-omgeving' waar bedrijven informatie aan mogen leveren. Via een RSS-bericht, of een tweet, of in een digitale kluis, als het maar niet een 'mijn' is.
Gelukkig zijn er partijen die hergebruik van identiteiten mogelijk maken en die mij niet opzadelen met een nieuwe identiteit voor hun 'mijn-omgeving'. Zo kun je soms op een site (met behulp van het Oauth-protocol) inloggen met een Twitter of Facebook of, tsja, LinkedIn account. Op voorhand prima. Als zo'n site mijn identiteit en wachtwoord niet zelf beheert, dan hebben ze die dus ook niet en dan kunnen ze die ook niet kwijtraken. Maar - en dat is dan eigenlijk de randvoorwaarde - dan moeten die Identity Providers op hun beurt wel minstens zo zorgvuldig omgaan met mijn identiteit. Misschien moeten we dat dan maar eens aan de LinkedIn's van deze wereld laten weten: Ik wil graag mijn identiteit bij jou gebruiken, maar daar moet je wel wat voor doen!

Lex Borger

LinkedIn en PayPal -- nee, die had ik niet gecombineerd. Maar ik heb wel een aantal wachtwoord-resets moeten doen... Het wachtwoord is dus failliet. Aan de ene kant is het nog steeds het meest eenvoudige authenticatiemiddel; toepasbaar over elke interface. Aan de andere kant is het niet meer te doen om al je wachtwoorden te onthouden. We kiezen te makkelijke wachtwoorden, hergebruiken ze, schrijven ze op, vergeten ze... We doen alles wat ze afzwakt. Een wachtwoord is niet meer wat het was: "iets wat je weet." En wat is de stap na een faillissement? Een doorstart.

In deze doorstart is een wachtwoord tot een radertje geworden in een nieuwe authenticatieketen. Het is "iets wat je hebt" geworden, met nog steeds bijna alle interface voordelen. De enige manier om nog al je wachtwoorden te onthouden is met een hulpmiddel. Het is niet meer overal toepasbaar, maar overal waar ik toegang heb tot 1Password, het hulpmiddel dat ik gebruik. En ik moet er maar op vertrouwen dat alle cryptografie die daarbij voor de beveiliging zorgen goed geïmplementeerd is. Het grote schrikbeeld daarin is op een dag opstaan met het bericht dat 1Password al weken gebroken is en alle wachtwoorden van iedereen op straat liggen...

BOEKVERSLAG

PRIVACYRECHT IS CODE

Deze review is gedaan door Henriëtte Westerling. Zij is adviseur informatiebeveiliging bij RIVM en kan bereikt worden via h.woltman@student.tudelft.nl.

Boekverslag van Privacyrecht is code – Over het gebruik van Privacy Enhancing Technologies van J.J.F.M. Borking, uitgegeven bij Kluwer, Deventer, 2010, ISBN: 978 90 13 07561-8, 421 pagina's.

Voor mijn afstuderen aan de postdoctorale studie Master of Security Science & Management van Delft Toptech van de TU Delft heb ik diverse boeken gelezen. Een boek die vanwege zijn overview aan onderwerpen met betrekking tot privacyrecht en de link naar informatiebeveiliging daarbij uitsprong is 'Privacyrecht is code'. De auteur, John Borking, is bekend als expert op het gebied van Privacy Enhancing Technologies (PET). Sinds de jaren negentig houdt hij zich met vraagstukken rondom Privacy Enhancing Technologies bezig. In juni 2010 is hij gepromoveerd aan de Universiteit Leiden met dit boek over PET als proefschrift. In het boek stelt de auteur dat zonder structurele en preventieve technologische maatregelen onze privacy niet te beschermen zal zijn, waarbij zijn stelling is dat niet de techniek de wet moet voorschrijven, maar de wet de techniek. Het doel van het boek is na te gaan of het technologisch haalbaar is, onder meer door toepassing van PET, om de rechtsbeginselen met betrekking tot de gegevensbescherming in het ontwerp van de architectuur van informatiesystemen op te nemen. De auteur verkent in het boek twee zaken. Aan de ene kant onderzoekt hij of privacybeschermende informatiesystemen preventief kunnen worden ingezet om onze persoonsgegevens en onze persoonlijke ruimte effectief te kunnen beschermen. Aan de andere kant onderzoekt hij hoe PET (tegenwoordig overigens 'privacy by design' genoemd) kunnen worden toegepast in informatiesystemen om onze privacy adequaat te beschermen.

De probleemstelling

De probleemstelling die in het boek is beantwoord luidt:
"*Hoe kunnen in informatiesystemen de persoonsgegevens van burgers zodanig effectief worden beschermd, dat zij erop kunnen (blijven) vertrouwen dat hun persoonsgegevens niet onrechtmatig worden verzameld, verwerkt, opgeslagen en verspreid door de verantwoordelijke en de bewerker?*".

Om deze vraag te beantwoorden, staat de auteur stil bij diverse onderzoeksvragen die hij per hoofdstuk behandelt. Zo staat hij in het eerste hoofdstuk stil bij de omgevingsanalyse. Waaruit blijkt dat in postindustriële landen, zoals de Verenigde Staten, Canada, Australië, Japan en de landen van de Europese Unie, informatie- en communicatiesystemen worden gebruikt, die op een steeds verfijndere manier gegevens over personen verzamelen, opslaan, uitwisselen, (her)gebruiken, identificeren, analyseren en monitoren. Uit de resultaten van de omgevingsanalyse blijkt onder meer dat burgers en consumenten zich er zorgen over maken dat de overheid en het bedrijfsleven hun persoonlijke gegevens mogelijk misbruiken. Zij zijn niet in staat na te gaan wat er met hun persoonsgegevens gebeurt en aan wie die worden verstrekt. De auteur stelt dat het voor de hand ligt dat zij controle willen hebben over het gebruik van hun persoonsgegevens. Om de bescherming van persoonsgegevens niet tot een papieren tijger te laten verworden en burgers controle over de verwerking van hun persoonsgegevens te laten behouden stelt de auteur dat het noodzakelijk is de privacyrechtsregels met structurele en preventieve technische maatregelen te ondersteunen.

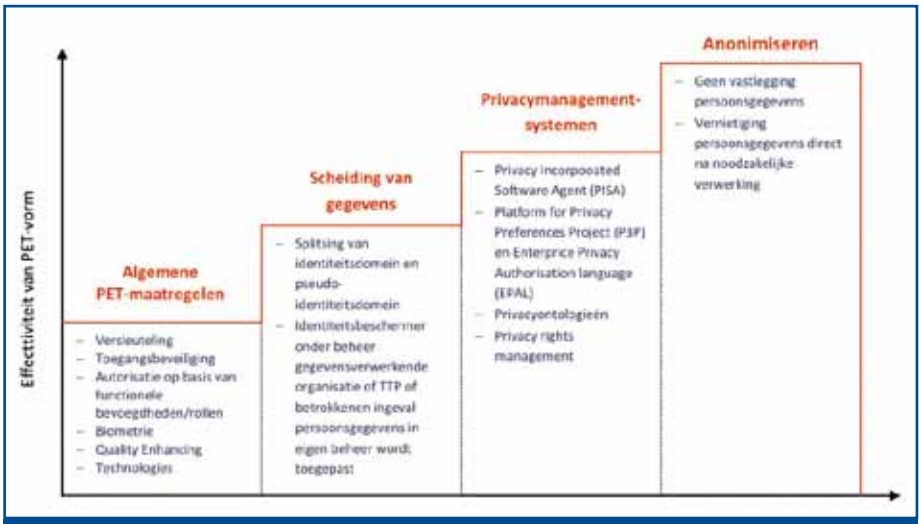
Privacyrealisatiebeginselen

Nadat eerst de sleutelbegrippen als 'privacy', 'persoonlijke ruimte', 'identiteit' en 'persoonsgegevens' zijn verkend, worden in hoofdstuk twee de algemene uitgangspunten over persoonlijke informatie die ten grondslag liggen aan de privacybescherming in kaart gebracht. Daar laat John Borking de privacyrealisatiebeginselen uit voortkomen met juridische specificaties, met subeisen, die in het ontwerp van privacygevoelige systemen moeten worden meegenomen. Hierbij gaat het bijvoorbeeld om de beginselen van gegevensminimalisering, doelbinding en transparantie. Interessant vanuit informatiebeveiligingsoogpunt is in dit hoofdstuk het vergelijk dat gemaakt wordt tussen het beveiligen van informatie en de privacyrealisatiebeginselen. Hieruit blijkt dat vertrouwelijkheid niet synoniem is aan privacy. Vertrouwelijkheid gaat volgens de auteur geheel voorbij aan

		Privacy criterion								
		Registering of processing	Transparent processing	As required processing	Lawful basis for data processing	Data quality conservation	Rights of the parties involved	Data traffic with countries outside EU	Processing personal data by processor	Protection against loss and unlawful processing of personal data
Information-security	Availability									+
	Confidentiality		++					++++	+	++++
	Integrity					++++	+		+	+++

++++ very strongly related +++strongly related ++ moderately related + weakly related

Tabel 1: De overlap informatiebeveiliging en de privacybeginselen



Figuur 1: - De Pet-trap (Bron: Borking, 2010:196)

de rechtmatigheid van de te verwerken gegevens. Zie onderstaande tabel voor de verschillen en overeenkomsten tussen privacy en informatiebeveiliging. Informatiebeveiliging dekt vanuit de drie peilers beschikbaarheid, vertrouwelijkheid en integriteit nergens volledig het domein van de privacybescherming. Drie velden worden zelfs met informatiebeveiliging helemaal niet bestreken dat zijn: de melding, de transparantie en de rechtmatige verwerking van persoonsgegevens inclusief het toestemmingsvereiste.

Privacyrisicomodellen

Nadat de auteur ingegaan is op de gevolgen van de risicotoezichtsamenleving waarin we volgens hem nu leven, bespreekt hij in hoofdstuk vier vervolgens verschillende privacyrisicomodellen en bedreigingsanalyses (de zogeheten privacy impact analyse -PIA's) met de risico's en bedreigingen die kleven aan het verwerken van persoonsgegevens. Deze neemt hij op in een overzicht met privacybedreigingsontologie. Ook in dit hoofdstuk gaat Borking in op de verschillen en overlappen tussen de discipline als informationele privacy en informatiebeveiliging. Hij verwijst hierbij naar Koorn & Ter Hart die het bijna synoniem zien van beveiliging en privacy als misvatting opmerken: 'Als we de beveiligingsmaatregelen hebben getroffen volgens de Code voor informatiebeveiliging, dan hebben we direct de privacybescherming geregeld'. Een belangrijk spanningsveld tussen informatiebeveiliging en informationele privacy betreft volgens Borking het privacyrealisatiebeginsel van transparantie (o.a. inzagerecht) en de toegangsbeveiliging, omdat de inzage van documenten een beveiligingsrisico oproept.

Privacy Enhancing Technologies

Wat Privacy Enhancing Technologies inhoudt, welke reikwijdte het heeft en welke keuzen in de PET-maatregelen te nemen zijn brengt de auteur in hoofdstuk vijf naar voren. PET manifesteren zich in vier vormen. Iedere vorm heeft specifieke functies met betrekking tot gegevensbescherming. In dit hoofdstuk focust hij vooral op de rol en inrichting van de 'Identity Protector' (IDP). Zie figuur voor de PET-trap.

Voorbeelden privacyveilige informatiesystemen

Hoe de zogeheten privacyveilige informatiesystemen in de praktijk daadwerkelijk gerealiseerd zijn, wordt in het boek beschreven aan de hand van enkele voorbeelden. Zo beschrijft de auteur de metazoekmachine Ixquick van een ziekenhuis, het ziekenhuisinformatiesysteem Victim and Tracing System (ViTTS) en privacy vriendelijke software-agent PISA (een Europees onderzoeksproject). Waarom privacyveilige informatiesystemen en PET nauwelijks worden geïmplementeerd analyseert Borking aan de hand van diverse belemmeringen. Zo merkt hij op dat organisaties in een vicieuze cirkel zitten: zolang PET zich nog niet heeft bewezen, acht men het risico van mislukken te groot, worden PET niet toegepast en kunnen PET zich niet bewijzen. Ook benoemt Borking een gebrek aan beproefde businessmodellen als belemmering om in PET te investeren. Om te investeren in PET is volgens hem een positieve businesscase vereist die de financiële haalbaarheid aantoont. Een aantal methoden en specifieke investeringsformules worden door de auteur aangehaald. Ook het maturiteitsniveau van een organisatie wordt als belemmering benoemd. Of PET binnen een organisatie kan worden toegepast hangt af van de maturiteit die de organisatie heeft op het gebied van Identity & Access Management en privacybescherming.

Adoptiepoces van innovaties

In het boek is tevens aandacht besteed aan het adoptieproces van innovaties en wordt een inkijk gegeven in de adoptiefactoren van een innovatie als PET. Het boek sluit af met conclusies en aanbevelingen voor privacyveilige informatiesystemen. Zoals meer voorlichting, aanscherping van de rol van de toezichthouder en het advies tot het oprichten van een PET-centrum.

Waardering

Een kritische noot ten aanzien van het boek is te plaatsen bij de vluchtigheid waarmee sommige onderwerpen in het boek geïntroduceerd en besproken worden. Door de vele onderwerpen en invalshoeken die de auteur in het boek behandelt is de samenhang tussen de onderwerpen soms onvoldoende belicht.

Naar mijn mening biedt de auteur met dit boek een breed overzicht aan materiaal, achtergrondinformatie, casussen, verdieping over privacyrecht en allerlei dimensies van 'Privacy Enhancing Technologies'. Waarbij de belangrijkste boodschap is dat privacybescherming alleen van de grond kan komen wanneer al bij het ontwerp van systemen rekening wordt gehouden met de beginselen van gegevensbescherming. Het boek kan als brugfunctie gezien worden tussen het vakgebied informatiebeveiliging en de meer juridische insteek van privacyrecht. Het is daarmee niet alleen interessant vanuit een juridisch perspectief. Voor de informatiebeveiliger die te maken heeft met analyses met betrekking tot persoonsgegevens, architectuur van informatiesystemen en het beveiligen van informatie biedt het boek een overview aan privacyrecht, privacy impact analyse.

ONSIGHT IT SECURITY CONGRES 2012

Jan Jaap van der Neut werkt als business consultant bij Onsight met als specialisatie de organisatie van security management. Hij is te bereiken via Jan.Jaap.van.der.Neut@onsight.nl.

Op 22 mei organiseerde Onsight zijn jaarlijkse IT Security congres in het Gelredome in Arnhem. Méér dan 270 klanten hadden zich vooraf geregistreerd. Op de dag zelf waren er ruim 200 bezoekers, waarmee het aantal van het jaar ervoor ruimschoots overtroffen werd. Onsight organiseert dit jaarlijkse congres om zijn klanten en andere geïnteresseerden in een informele sfeer op de hoogte te brengen van de laatste ontwikkelingen op het gebied van IT security. Een imposant voetbalstadion als het Gelredome biedt goede faciliteiten en draagt indirect bij aan het succes van een dergelijk evenement.

Het programma bevatte uiteenlopende onderwerpen die invulling gaven aan de diverse vraagstukken die Onsight dagelijks bij zijn klanten tegenkomt zoals:

- IT security-trends en -ontwikkelingen
- 'Het nieuwe werken' en 'Bring your own device'
- Privacy, security en wetgeving
- Security monitoring
- Antifraude
- Social media
- Cybercrime

Naast sprekers van Onsight zelf waren er ook interessante presentaties van onder andere Check Point, RSA, F5, Qualys, Thales, Versafe en ObserveIT. Rachel Marbus trad op als inspirerende dagvoorzitter. In de middag vond een round table plaats over cyber security. De dag sloot af met een interessante presentatie door de AIVD over digitale spionage. Zo bood het programma een uitgebreid aantal onderwerpen met zowel een technische als een niet-technische insteek. En dat past bij de huidige aard van security dat in alle geledingen van organisaties en de samenleving tot uiting komt.

Een verslag van een aantal presentaties op die dag:

Secure Bring Your Own Device

Jan Jaap van der Neut startte het programma met een toelichting op Secure Bring Your Own Device. Hij schetste dat het gebruik van eigen mobiele apparatuur grote druk op IT-afdelingen zet. Security-risico's spelen hierbij een belangrijke rol. Het gebruik van eigen mobiele apparatuur is een onderdeel van de werkplekstrategie van een organisatie. Dat houdt in dat remote access, application delivery, mobile device management en security allemaal onderdeel van BYOD zijn. Alleen een integrale aanpak is robuust en veilig genoeg om BYOD succesvol te maken. Daarbij speelt mee dat de gebruikers individueel een grotere verantwoordelijkheid krijgen. De wijze waarop zij veilig vertrouwelijke informatie verwerken is bepalend voor het succes van BYOD. Onsight adresseert

> Alleen een integrale aanpak is robuust en veilig genoeg om BYOD succesvol te maken

deze aspecten in workshops met directies, managers en medewerkers en begeleidt zo de juiste besluitvorming.

Cyber Threats & Trends

Vincent van Kooten, Expert Cyber Threat & Fraudepreventie bij Onsight, presenteerde over cyber threats & trends. In het beschreven security-landschap spelen cyber threats een belangrijke rol. Ze richten zich steeds vaker op individuele gebruikers en steken geraffineerd in elkaar. Vincent neemt onderstaande trends waar met betrekking tot cyber-aanvallen:

- Steeds meer bedrijven komen in het nieuws na het lekken van data;
- De frequentie van aanvallen gaat omhoog;
- Phishing en malware kits zijn steeds makkelijker te verkrijgen;
- Detectie van aanvallen is moeilijker;
- Niet alleen de financiële sector is doelwit;
- Veel organisaties hebben geen idee of ze doelwit of slachtoffer zijn.

Daarnaast merkt Vincent op dat veel organisaties niet zijn voorbereid op een grote data breach. Denk bijvoorbeeld aan een urgency mailbox waar klanten of gebruikers melding kunnen maken van incidenten en verdachte zaken. Ten tijde van een crisis zijn IT-afdelingen niet in staat om die informatiestroom te verwerken, laat staan vast te leggen.

Security Prism

Peter Pronk, Technisch Directeur bij Onsight, lichtte de behoefte aan geïntegreerde security intelligence toe. Organisaties investeren veel tijd en geld in verschillende security-oplossingen die vaak langs elkaar werken. Security Information and Event Management (SIEM) biedt hiervoor slechts ten dele een oplossing. Daarbij speelt dat slechts een klein deel van de SIEM-trajecten de beoogde doelstellingen behaalt. Ook is de aard van de security-informatie ontoereikend om snel en adequaat beslissingen te kunnen nemen bij zeer geraffineerde cyber-aanvallen. De Security Prism combineert daarom security-informatie uit de bekende security-oplossingen met geavanceerde antifraude-informatie en waargenomen verkeerspatronen om tot een totaalinzicht te komen. In het Security Operations Center van Onsight vindt de correlatie en analyse van de veelzijdige informatie plaats. Organisaties krijgen zo de juiste inzichten om snel te kunnen besluiten en handelen.

> Security management is meer dan de statische plan-do-check-act-cyclus uit ISO 27001

Digitale spionage

De AIVD sloot de dag af met een interessante presentatie over digitale spionage. Daarbij gaf de spreker aan welke risico's dit met zich meebrengt voor het bedrijfsleven. Zij ging tevens in op de wetgeving met betrekking tot inlichtingendiensten in landen zoals Groot-Brittannië, de Verenigde Staten, Frankrijk en Rusland. Daaruit bleek dat veelal economische motieven de basis voor deze wetgeving vormen. Ook werden enkele cases toegelicht, zoals die waarin Chinese studenten of wetenschappers tijdelijk in het bedrijfsleven werken en heimelijk vertrouwelijke gegevens en kennis vergaren.

Afsluiten van de dag

Na het intensieve programma konden de bezoekers aan de hand van een drankje de dag afsluiten. Veel bezoekers gaven aan dat het een goede en informatieve dag voor hen was geweest. Marcel Knippen, Directeur van Onsight, was verheugd met de grote opkomst. Voor hem was het de bevestiging dat het congres een goede manier is om de markt goed te kunnen informeren. De veelzijdigheid aan onderwerpen, sprekers en leveranciers maakten de dag tot een succes.

Links:

Informatie over Onsight: www.onsight.nl

De presentaties van het congres: www.onsight.nl/onsight_it_security_congres_2012/Programma

Informatie over digitale spionage en de taken van de AIVD: www.aivd.nl

PAST-PRESENT-FUTURE, JUBILEUM EDITIE BLACK HAT SESSIONS 2012

Gerrit Post RE. en Tom Bakker RE RI CISA CISM. Tom en Gerrit zijn beiden redacteur van Informatiebeveiliging. Gerrit is zelfstandig gevestigd security consultant en IT-auditor. Tom is werkzaam bij Allianz Nederland Groep.

Alweer voor de tiende keer organiseerde Madison Gurkha dit jaar, op 4 april, de Black Hat sessions in de Reehorst, Ede. De sessions bedoelen een seminar te zijn "waarbij interessante gastsprekers uit Nederland en daarbuiten hun kennis delen over de nieuwste ontwikkelingen op het gebied van technische IT-beveiliging". Of MG in die ambitie is geslaagd valt lastig te zeggen. Zeker is wel dat het voor uw reporters een zeer nuttige belevenis is geweest, die smaakt naar meer.

We hebben zoveel mogelijk getracht alle bijeenkomsten bij te wonen en aangezien er 2 parallelle stromen waren is dat goed gelukt. Tijdens het seminar was er ook een informatieplein/-markt waar aanbieders van diverse diensten vertegenwoordigd waren. Ook PvIB was hier aanwezig in de persoon van Debbie Reinders. Zij had een goed meetbare doelstelling: 10 nieuwe leden. Of dat uiteindelijk ook gerealiseerd is…?

De Black Hat sessions lijken wel een beetje op de "echte" Black Hat Europe. De doorsnee lezing is echter naar onze mening toegankelijker en is, zoals MG ook zelf aangeeft, door iedereen te volgen, ongeacht het niveau van technische kennis. De organisatie is prima, goede locatie en verzorging. De video's van de presentaties staan inmiddels allemaal online evenals de handouts (indien beschikbaar). Zo hoort het! (http://www.blackhatsessions.com/)

De keynote was (uiteraard) voor Brenno de Winter. Brenno weet op een relaxte manier vreselijke dingen te zeggen en hij beschikt over een heel scala van praktijkgevallen om zijn gehoor te schetsen wat er aan de hand is. In zijn verhaal bleef het "Future" aspect echter een beetje onderbelicht. Dat is op zich ook wel weer begrijpelijk. In dit continu razendsnel veranderende vakgebied is het bijzonder lastig om al te ingewikkelde toekomstvoorspellingen te doen.

Wim Verloop en Huub Roem gaven inzicht in de problematiek rond een forensisch onderzoek dat zij hebben uitgevoerd naar aanleiding van een incident. Vooral de logistieke problemen rondom dat onderzoek waren interessant. Zo was er maar korte tijd voor onderzoek mogelijk. Tekort aan extra harde schijven vanwege productieproblemen in Japan (Fukushima), benodigd 133 TB – 266 TB totaal inclusief kopieën). Geen toegang tot de data bij de hosting partij van de klant etc.

Arthur Donkers en Ralph Moonen gaven vervolgens hun visie in "Mobile Hacking and Security", een uittreksel uit een workshop die ze eerder in Maleisië gaven en die in september nogmaals in Nederland georganiseerd zal worden. Een goed, sober, verhaal. Ze gaven in ieder geval vanuit de praktijk een doorkijkje naar zaken die ons mobile bestaan nu al bedreigen waaruit je zonder veel moeite een beeld van de toekomst kunt vormen. BYOD lijkt – in hun optiek - iets in de trant van "you can't live with it and you can't live without it". Maar het is waarschijnlijk niet te vermijden. Android lijkt dan weer in het nadeel ten opzichten van IOS, qua hackmogelijkheden. Saillant detail: Blackberry werd door een aantal sprekers weggezet als "iets voor kinderen" . Als volwassen – tevreden – Blackberry-gebruiker zit je dan wel raar te kijken.

Bert Hubert ging in op "The end of secure computing on general purpose hardware". Met dat laatste werd overigens alles bedoeld dus naast de normale werkstations ook bijvoorbeeld smartphones en tablets. Het beeld dat Bert schetst is inktzwart. In feite zijn we volgens hem al "aan de goden overgeleverd". Banken zijn bezig om langzaam het risico van online bankieren naar ons – de consument - te verplaatsen. Dat lijkt overigens bevestigd te worden door uitlatingen van bankiers. Sommige buitenlandse maatschappijen blokkeren je creditcard al automatisch als je langer dan een paar dagen in het buitenland verblijft. In het kort zijn uw systemen voor Kwetsbaarheden Uiterst Transparant. Maar we blijven ze toch gebruiken, sterker nog we breiden het

Presentatie door Huub Roem

Presentatie Social Engineering door ir. Walter Belgers

gebruik uit en volgens Bert daarmee ook de potentiële security gaten omdat de starre hardware, ontwikkelaars er toe noopt software aanpassingen te doen die die gaten veroorzaken. Goed beschouwd zou je daarom bijvoorbeeld online bankieren niet moeten doen evenals het EPD en internet stemmen. Er zijn teveel risico's. Dedicated devices zou een oplossing kunnen zijn. De consumenten zouden dan worden uitgerust met een EPD-tablet, een banking smartphone en een communications phone die bijvoorbeeld op de Nokia 6310 zou kunnen lijken. Als u er nog één heeft liggen… U bent gewaarschuwd!
Het menselijk falen is vaak de oorzaak van vele incidenten. Walter Belgers ging in over de dreigingen en tactieken van Social Engineering. Net als in de serie van Jan de Boer van 2010 in dit blad werd veelvuldig verwezen naar de acht manieren (in de Nederlandse vertaling zes!) van manipulatie van Robert Cialdini. Walter ging verder over hoe een mystery guest te werk moet gaan met inachtneming van de lessen van Cialdindi.
De mens toch weer als zwakste schakel!
Alhoewel erg technisch van aard was de

Debbie Reinders

lezing van Job de Haas over verscheidene aspecten van "Hardware Security Testing" geweldig interessant. Er zijn ruwweg 3 manieren om hardware te pesten: logisch, fysiek en via "side channel". Logisch heeft alles te maken met de implementatie van systemen: operating system, cryptografie. Fysiek (ook wel invasive) kun je gebruik maken van eigenschappen van bijvoorbeeld ROM's of andere chips door sporen op een moederbord weg te etsen of juist aan te brengen. In programmeerbare hardware kun je ook ingrijpen. Onder "side channel" verstaat Job het waarnemen van effecten in de buitenwereld die een interessante gebeurtenis signaleren. Bijvoorbeeld het waarnemen van een sterk verhoogd watergebruik op woensdagavond om 9:30 zou zomaar op de pauze van een voetbalwedstrijd kunnen duiden. Iets dergelijks kun je ook met een multimeter of een oscilloscope in computer hardware waarnemen. De toepassing van de zaken die Job schetst ligt over het algemeen ver van de gangbare praktijk van een security professional maar is wel alledaagse realiteit voor de leverancier van set-top-boxes voor betaald televisie kijken. Als het relatief eenvoudig is om de hardware te kraken dan loopt het verdienmodel ernstig gevaar.
Edwin van Buuren van het NCSC (v.h. Govcert) gaf een overzicht van dreigingen zoals die gepubliceerd zijn in het trendrapport Cybersecuritybeeld Nederland 2011. 'Meer kwaadaardig en minder zichtbaar' is de trend. Daarvoor gaf hij een uiteenzetting over het dit jaar opgerichte NCSC.
Cryptografie stond centraal in een verhaal over RFID door Roel Verdult. Ondertitel 'The failures of propriety cryptography' gaf aan dat bedrijven hun eigen (onveilige) algoritmes ontwerpen met het idee van 'het is geheim dus veilig'.
Na een inleiding over de bekende crypto systemen zoals DES en 3DES had Roel vele voorbeelden waar het mis is gegaan met propriety cryptography (denk aan de OV-chip). Ook werd duidelijk dat de sleutellengte alleen niet zaligmakend is maar dat onderliggende design fouten vaak het onveilig maken. Het was wel een erg technisch verhaal met name het stuk over de poging om iClass en PicoPass te kraken. Daarover is ook een publicatie verschenen. Maar ook voor niet ingewijden was het goed te volgen.
Koen Martens ging in op "Hacken: toen, nu en straks". Naast leuke anekdotes over "toen" was prominent in zijn verhaal de roep om een klokkenluidersstatus voor hackers omdat ze aan de ene kant een niet te missen factor zijn in de verbetering van beveiliging maar aan de andere kant in toenemende mate onder druk komen te staan door verscherping van de vervolging, niet in de laatste plaats in de VS aangeblazen door het WIKILEAKS gebeuren.
Aardige uitspraak van Koen was die over Ivo Opstelten waarvan hij opmerkte dat die nog was van voor de computers…
De afsluitende presentatie was voor Stefan Castille en Frans Kollée. Zij blikten kort terug op de historie. In 2004 lag de wereld nog redelijk open zoals een demo van Walter Belgers en Hans van de Looy op een Windows 2K omgeving aangaf. Nu zou eenzelfde poging op een Windows 2K8 omgeving veel minder opleveren. Er is dus zeker bijgeleerd. Wel zijn er nu weer nieuwe mogelijkheden ontstaan zoals ze in hun demo's bewezen. Vooral aardig was de demo met het apparaatje dat een aantal aanwezigen in de tombola hadden getrokken, een usb-hub. Stefan en Frans lieten zien dat zo'n ogenschijnlijk gevaarloos apparaat echt wel risico's met zich kan brengen. Hoe je daar tegen te wapenen werd overigens niet echt duidelijk.
Samengevat een zeer leerzame, gezellige dag. Goed verzorgd door Madison Ghurka op een prima locatie. En die doelstelling voor Debbie? Niet helemaal gehaald maar wel flink aan naamsbekendheid van PvIB gewerkt.

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 Domus Technica),
e-mail: lex.borger@domustechnica.com
Motivation Office Support bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

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

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 2012
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

DE THUISTAP

Kortgeleden ben ik even naar de binnenstad geweest om een aantal aankopen te doen. Ik besloot met de stadsbus te reizen hetgeen niet direct een hobby van mij is. Na 5 minuten wachten kwam de stadsbus en na inwisseling van 2 euro kreeg ik mijn kaartje. Ik ging achterin de bus zitten omdat ik wel overzicht wil houden. Je ziet een aantal mensen verveeld naar hun telefoon kijken en anderen kijken met een lege blik door de vieze ruiten van de bus. Ineens werd mijn aandacht getrokken naar een meisje met een blauwe jas die in een heftig telefoongesprek zat. Het meisje sprak luidkeels in haar telefoon alsof zij een poging deed degene aan de andere kant van het telefoongesprek te bereiken zonder het gebruik van de telefoon. Meer en meer mensen kregen in de gaten dat er zich een drama afspeelde bij het meisje in de blauwe jas en zelfs de chauffeur zag ik zo nu en dan in zijn spiegel kijken. Uiteindelijk bleek iedereen (min of meer gedwongen) mee te luisteren met het meisje met de blauwe jas. Haar verkering was die dag uitgegaan en verdere details wil ik u graag besparen.

Toen ik uitstapte dacht ik dat het vreemd was dat het meisje met de blauwe jas helemaal geen problemen had dat de hele bus haar gesprek had kunnen volgen. Haar Facebookpagina zal ook wel een openbaring van persoonlijke feiten zijn. Het afluisteren van dit gesprek was een min of meer gedwongen actie en toen schoot mij een bericht door het hoofd waarin Justitie aangaf dat ze over 2011 meer dan 25.000 telefoongesprekken stiekem had afgeluisterd. Dat zijn bijna 70 gesprekken per dag zonder dat de eigenaar van de telefoon er iets van weet, overigens betreft het hier alleen de geregistreerde taps, de staatsgeheime taps worden niet in de tellingen meegenomen. Ter illustratie: in de VS worden ongeveer 2200 gesprekken per jaar afgeluisterd. De VS telt echter ruim 20 keer zoveel inwoners. In Nederland worden derhalve 200 keer zoveel gesprekken afgetapt per inwoner als in de VS. Dat is een extreem verschil en wij maar denken dat men overzee deze praktijken meer uitvoert.
Ik heb maar eens uitgezocht welke criteria Justitie in Nederland hanteert. Eigenlijk wist ik voor mijn zoektocht al wel dat daar alleen maar holle kreten als staatsveiligheid, criminaliteit, opsporing en dergelijke uitkwam. Geeft Justitie dan echt niet aan wanneer een telefoontap toegestaan wordt? Neen, er zijn geen richtlijnen bekend buiten Justitie. Daarover nadenkend vroeg ik mij af wanneer Justitie mijn gesprekken gaat tappen. Doen ze dat als ik te vaak verkondig dat ik het veel bejubelde lenteakkoord niet sociaal vind en dat er waanzinnige bezuinigingsvoorstellen in zitten? Wordt Justitie achterdochtig als ik te vaak (louter en alleen beroepshalve) naar hackersites toe ga? Als ik naar de site van Geert Wilders ga (louter en alleen ter illustratie van de voorbeelden) worden dan de telefoontjes getapt die ik met mijn vrouw heb over het merk Pindakaas die ik moet meenemen uit de winkel ? Of maak ik het al te bont als ik op zondagavond de containers al buiten zet in plaats van op maandagochtend en als ik de honden niet aangelijnd door onze woonwijk uitlaat?
Ik weet het niet, ik durf niet te zeggen wanneer je begint op te vallen bij Justitie. Ik weet niet wanneer ze mijn mobiele nummer invoeren in hun computer om al mijn gesprekken te tappen.
Ik heb werkelijk geen idee of Justitie weet welke pindakaas mijn vrouw lekker vindt. Je zal toch bij Justitie werken en als taak hebben de telefoongesprekken te analyseren. Hardop roepend naar hun collegae dat Berry weer de verkeerde pindakaas meeneemt. Om de mannen van Justitie een beetje te vermaken heb ik inmiddels de gewoonte om aan het eind van een gesprek een nietszeggende kreet te slaken om de heren eens flink te laten puzzelen, denk dan aan "het paard is over de heuvel" of "1+1=3" of "de rozen zijn verwelkt" .
Mocht iemand van Justitie nu meelezen dan kan ik ze aangeven dat mijn kreten helemaal niets betekenen en dat ze mijn telefoon niet hoeven te tappen. Buiten de eerder genoemde vergrijpen doe ik niets wat Justitie zou moeten interesseren. Helemaal niets.
Voor de zekerheid ga ik de telefoon van mijn kinderen of mijn vrouw maar gebruiken, ondanks het feit dat mijn vrouw weleens naar Dr. Phil kijkt, denk ik niet dat haar telefoon getapt wordt.

Groetjes, Berry

SOPHOS

simple + secure

Individually great, altogether – better

Security products that cover every aspect of your business, individually great, but if you put them altogether – they're even better.

endpoint | web | e-mail | encryption | mobile | network

distributeur: CRYPSYS Data Security | 0183 - 62 44 44 | sales@crypsys.nl | www.crypsys.nl