iB
INFORMATIEBEVEILIGING
jaargang 15 - 2015
#1


# PRIVACY, ONDERNEMERS EN PROVIDERS

**Treating Risk Prospectively**

**Veiliger met voorkennis**

**Verslag BB Awards**

# IT & Information Security

## Tot hier en niet verder

**Woensdag 11 februari**
**2015**
**Amsterdam ArenA**

## Jaarcongres met topsprekers zoals:

- **Dagvoorzitter Sven Kockelmann**
  Journalist & TV presentator, KRO
- **Reinder Woldring**
  Corporate Security Manager, Gasunie
- **Wim Blauwendraat**
  Audit Director, Philips
- **Ad Krikke**
  Corporate ICT Security Office, DSM
- **Udo Oelen**
  Hoofd toezicht private sector, CPB
- **Fred Streefland**
  Corporate information Security Manager, Exact
- **René Huigen**
  Security officer, KPN

**security.heliview.nl**

# DAT GEBEURT TOCH NIET ECHT

**Tijdens de feestdagen heb ik de gelegenheid gehad om met verschillende mensen te praten over hun beleving van cyber bedreigingen. Volgens het Cyber Securitybeeld Nederland [1] zijn de grootste bedreigingen waar we aan blootgesteld worden spionage door staten en cybercriminaliteit. En het grootscheeps verzamelen van informatie zet onze privacy onder druk. Wat is de blik van de jonge Nederlander?**

In de gesprekken die ik heb valt me op dat er gezocht wordt naar voorbeelden van manifestaties van de bedreigingen. Een scenario waarvan je ziet dat het kan gebeuren is tastbaarder dan een niet bekend geworden manifestatie of een theoretische kwetsbaarheid.

Bruce Schneier heb ik hier ook over horen spreken. We kunnen als mens niet omgaan met de beleving op een kleine kans op een grote impact. Manifestaties van grote kansen op kleine impact zien we genoeg om ons heen. Manifestaties van de grote impact met een kleine kans zien we als koppen van het nieuws. Wat we niet doorhebben is hoe klein die kans is. Wij zijn biologisch niet geëvolueerd om berichten uit de massamedia op kanswaarde in te schatten. Daarom denken we dat we een reële kans hebben op het winnen van de hoofdprijs in de loterij en denken we dat we in het vliegtuig onveiliger zijn dan in de auto.

Dus waar is de jonge Nederlander bang voor? Vooral om informatie kwijt te raken. Foto's die op Facebook staan heb je nog, ook als je harde schijf crasht of je laptop gestolen wordt. Privacyinstellingen zijn ze expert in, maar eigenlijk maken ze zich helemaal niet zo druk over te veel informatie delen. Dat is meer iets voor de ouderen om zich druk over te maken. Ook die paar foto's waarop ze aan het feesten zijn, zou geen belemmering mogen zijn voor het krijgen van een baan. "Kom op, ik heb toch ook een leven."

Spionage door staten en cybercriminaliteit is helemaal de ver van hun bed show. Het cliché "Ik heb toch niets te verbergen" klinkt zelfs. Mensen die een slachtoffer van cryptolocker kennen, vrezen de cybercriminaliteit, opvallend genoeg vrezen anderen dat niet." Malware? "Daar ben ik niet bang voor, ik klik niet op vreemde links." Onderdeel worden van een botnet? "Daar het ik nooit over nagedacht." Een generator kapot hacken? "Dat gebeurt toch niet echt." Totdat ik ze wijs op Project Aurora [2]. Toch is dat nog niet echt genoeg, het is 'maar' een demonstratie...

Ik worstel. Heeft de volgende generatie nu juist zich goed geadapteerd aan het sociale mediatijdperk, of zijn ze ongelofelijk naïef geworden? Ik besluit dat het een beetje van beide is. We kunnen wat van ze leren, zodat we wat minder spastisch worden over informatiedeling in de sociale sferen, maar we moeten nog beter ons best doen om ze duidelijk te maken dat we nog een aantal zaken goed moeten regelen in onze maatschappij.

**Lex Borger,** hoofdredacteur

Links

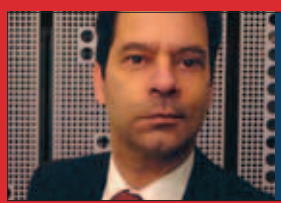
[1] https://www.ncsc.nl/actueel/nieuwsberichten/cybersecuritybeeld-nederland-4.html

[2] http://edition.cnn.com/2007/US/09/26/power.at.risk/

## In dit nummer


# PRIVACY, ONDERNEMERS... EN INTERNETPROVIDERS

Het luid klinkende pleidooi online privacy te versterken door allereerst te kiezen voor andere aanbieders van internetdiensten roept een aantal vragen op. Dat heeft vooral te maken met het feit dat die andere aanbieders beoordeeld moeten kunnen worden, maar er geen sprake lijkt te zijn van eenheid in communicatie en definities.



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

Medio december waren in Amsterdam twee events waar privacy centraal stond. PI.lab [1] organiseerde de jaarlijkse bijeenkomst waarbij inzicht werd gegeven in lopende onderzoeken. Dit gebeurde door workshops en presentaties waarin privacy centraal stond. De andere activiteit was de tiende editie van de Big Brother Awards. Dat ook hier privacy centraal stond behoeft geen nadere uitleg.

## Decentralisatie en distributie van data

Wat deze twee activiteiten verder gemeen hebben is dat onherroepelijk de machtspositie van een beperkt aantal grote partijen ter sprake kwam. Tijdens de keynote van Ian Goldberg [2] op PI.lab werd, net als bij de latere workshop van Mireille Hildebrandt "TETs for PETs, transparency tools for profiling in social networks", duidelijk dat Facebook en Google de nodige aandacht verdienen. De keynote van Aral Balkan [3] tijdens de BBAX [4] deed daar niet voor onder. Hij illustreerde op heldere wijze waarom privacy en dit soort grote bedrijven per definitie nooit een gezonde combinatie zijn. Goldberg en Balkan pleitten voor verschillende oplossingen die een ding gemeen leken te hebben: stap af van de voorkeur voor dit soort giganten, kies voor decentrale opslag van data en andere distributie modellen. Dat klinkt logisch, zeker voor wie de enthousiast ontvangen presentaties van beide heren heeft gevolgd, maar iets ontbreekt. Wat bij dit soort betogen namelijk centraal staat zijn de burger, de consument en die paar grote Amerikaanse ondernemingen. Wat geheel ontbreekt is dat privacy iets is dat ook het bedrijfsleven raakt.

## Focus moet breder

Die constatering is Goldberg voorgelegd: waarom alleen de focus en voorlichting voor de consument. Zou het niet beter zijn eveneens aandacht te besteden aan alle ondernemers. Zij zitten zo mogelijk in een nog lastigere positie dan de doorsnee consument. Zij vergaren en verwerken immers data van derden (de klanten) maar zijn zelf ook weer afhankelijk van leveranciers die dit mogelijk moeten maken. Goldberg was het volledig eens met dat standpunt. Ja natuurlijk moeten – vooral – kleinere ondernemers te horen krijgen hoe zij kunnen bijdragen aan meer en betere privacy voor hun klanten en voor zich zelf. En onvermijdelijk volgde daarop de vraag: wie moet dat dan doen? Moet je van de overheid verwachten dat die frequent voorlichting geeft aan ondernemers door het toezenden van een gedrukt exemplaar van de WBP? Wie kijkt naar de privacy incidenten die afgelopen jaar de landelijke pers hebben gehaald en waarbij Nederlandse ondernemers blijkbaar de fout in zijn gegaan moet de indruk krijgen dat het bijbrengen van zulke basiskennis wel het minste is dat nodig is. Maar de kans dat de overheid dit doet met enig effect is gering. Daarom is het wellicht verstandiger het initiatief te laten aan bepaalde marktpartijen en belangenorganisaties.

## Waarom nationale aanbieders

Er is een type ondernemer dat dan direct genoemd moet worden. Als je namelijk – in lijn met het pleidooi van zowel Goldberg als Balkan – kiest voor decentrale opslag van data kom je vanzelf uit bij partijen van een hele andere omvang dan Google en co. Nederlandse ICT bedrijven, in deze context vooral de providers, zijn heel goed in staat diensten op Nederlandse bodem (wel zo handig als je privacy hoog in het vaandel hebt staan) aan te bieden die privacyvriendelijk zijn. Dat klinkt onvermijdelijk als een verkoopargument, maar het is eigenlijk iets anders. Tijdens de PI.lab bijeenkomst werden de aanwezigen door Rence Damming, de privacy officer van KPN, gewezen op een simpele bevinding: wat klanten van KPN verwachten is Trust. Met andere woorden privacy, als onderdeel van het brede begrip Trust, is een verwachting. Het is dus vraag in plaats van aanbod. Dat KPN daar naar behoren invulling aan geeft en op meerdere plekken prominent aandacht besteedt aan privacy, inmiddels ook in de commerciële uitingen, is daarmee niet meer dan logisch en verstandig.

KPN is echter niet de enige aanbieder van provider diensten in Nederland. Afhankelijk van de definitie zijn het tussen de 800 en 2.000 ondernemers die een of meerdere e-diensten aanbieden waarbij data wordt opgeslagen en/of verwerkt. Hebben die allemaal de zaken net zo goed voor elkaar als KPN? Voldoen zij al in de eerste contactmomenten (lees: het bezoeken van de website) aan de schijnbaar aanwezige verwachting van prospects en klanten om hier iets over te vinden?

## Privacykennis bij de providers

Meten is weten! De eerste constatering is, dat op basis van een steekproef door het bezoeken van twintig willekeurig gekozen provider websites, zeker niet iedereen het belang van privacy lijkt in te zien. In ieder geval is duidelijk dat er op verschillende wijze invulling aan wordt gegeven. Er zijn enkele partijen die in de privacy policy keurig melden persoonsgegevens te verwerken en dit bij het CBP te hebben aangemeld. De meesten maken daar geen melding van. Of zij bekend zijn met WBP en CBP blijft vooralsnog gissen, de verstrekte informatie reikt niet verder dan dat in de leveringsvoorwaarden is opgenomen dat men uiterst professioneel met klantdata omgaat. Een aparte vermelding van het begrip privacy, laat staan een verwijzing naar data minimalisatie als leidraad, op de website via een privacy statement of opname in de FAQ ontbreekt. Als het voor die ondernemers al niet top-of-mind is dat ze hier kunnen dan wel moeten communiceren, hoe kun je dan

verwachten dat zij in staat zijn de klanten (pro-) actief over deze materie te informeren of zelfs te adviseren.

Een aantal providers is vervolgens de bewust open vraag voorgelegd: wat betekent privacy voor je onderneming. TransIP [5], een van de grootste aanbieders van domeinnamen, hostingservices en VPS in het land, werd gekozen omdat het op de voorpagina een intrigerende melding heeft staan: "We gaan voorzichtig om met jouw privacy gevoelige gegevens. Omdat we telefonisch niet met zekerheid kunnen vaststellen wie ons belt, verzoeken we je voor inhoudelijke vragen het controlepaneel te gebruiken." Dit lijkt een mooi voorbeeld te zijn van privacy-awareness uitstralen en zo indirect je klanten bewust te maken dat ook op dit niveau privacy een rol speelt. Maar goed, privacy wat betekent dat (verder) voor TransIP? Het antwoord maakt duidelijk dat men heel goed doorheeft een dubbele rol te vervullen: "Wij beheren niet alleen de persoonlijke informatie van meer dan 120.000 klanten, onze klanten beheren ook persoonlijke of privacy-gevoelige data". Dat betekent concreet: "systemen zodanig in te richten dat wij niet direct bij persoonlijke gegevens kunnen". Verder wordt er nog gewezen op het principe van dataversleuteling en het feit dat TransIP medewerkers zelf niet zomaar bij persoonlijke gegevens kunnen komen.

Een andere aanbieder die is benaderd, Fundaments [6], is een IaaS provider. IaaS staat voor de onderste cloudlaag en daarmee het type provider dat – in tegenstelling tot partijen als TransIP – in principe geen eindgebruikers als klant heeft. Het antwoord op dezelfde vraag was daardoor compleet anders: "Wanneer je privacy serieus neemt, dien je te kijken naar de hele keten van de dienstverlening: een applicatie kan nog zo goed beveiligd zijn, maar als in de onderliggende infra de data te grabbel ligt, is het een schijnbeveiliging. Vanuit deze ketenvisie proberen we de juist de onderliggende infrastructuur en virtualisatie software zo krachtig mogelijk te kiezen."

Het begrip ketenvisie illustreert in dit antwoord treffend de rol van een provider. Hij is een schakel in het geheel, maar wel een waaraan aanvullende eisen gesteld worden die veel minder vaak voorkomen bij partijen elders in de keten. Het is daarom ook verklaarbaar waarom partijen als Fundaments door ISO en/of NEN certificering aantonen de zaakjes voor elkaar te hebben. Overigens was dat een punt waar ook met Goldberg over is gesproken. Zag hij mogelijkheden de nieuwe ISO certificering voor cloud diensten [7] in te zetten om privacy (awareness) van elk type gebruiker te vergroten? Goldberg ziet het als een interessante optie waar hij echter nog te weinig van afwist om een tot een beter onderbouwd oordeel te komen.

Stellen dat je je zaakjes voor elkaar hebt of een intrigerende beschrijving op je website dat je privacy hoog in het vaandel hebt staan, is een manier van communiceren. Vervolgens is gevraagd: hoe pro-actief zijn jullie op dat vlak? Hier werd het verschil tussen de beide providers door de plek die ze in de waardeketen hebben en de diensten duidelijk. Bij de IaaS provider is maatwerk de regel. Dat betekent dat in offertes, contracten en SLA's ruimte is aandacht te besteden aan dat onderwerp. Voorbeeld daarvan was de opmerking dat: "privacy -en beveiligingsmechanismen dienen te worden ondersteund door de leveranciers. De keuze voor leveranciers is daarmee onderhevig aan harde eisen". Voor de meer standaarddiensten die TransIP levert is de communicatie per definitie anders en daarmee ook de mogelijkheid pro-actief te acteren. Desalniettemin, is er een heldere uitgebreide privacy-policy waarnaar vanaf elke pagina wordt gelinkt en er is de policy, "als er vragen over [privacy] worden gesteld zullen wij deze helder beantwoorden".

## Conclusie

Het verschil tussen de providers die reageerden op de vragen (een aantal deed dat overigens niet) en wat er op basis van de steekproef is geconstateerd blijft opvallend. Als burgers en bedrijven meer en betere privacy maatregelen willen voor e-communicatie, digitale opslag en verwerking is er nog een hoop werk te verrichten. De kans dat alle providers hier een rol willen en kunnen vervullen lijkt vooralsnog klein, omdat niet iedereen op het zelfde kennisniveau zit. De vraag of en hoe dit kan worden gerealiseerd is lastig te beantwoorden. Het ontbreekt in ieder geval aan een verplicht bedrijfschap voor providers dat kwaliteitseisen zou kunnen opleggen.

Voor iedereen die privacybewust is en zijn eigen data of klantdata koestert, blijft het zaak alert te blijven en niet elke aanbieder op zijn blauwe ogen te geloven. Gelukkig zijn er partijen die de zaakjes wel voor elkaar hebben en daarover helder communiceren. Alleen al dat laatste is een bruikbaar criterium.

Links

[1] pilab.nl/
[2] en.wikipedia.org/wiki/Ian_Goldberg
[3] aralbalkan.com/
[4] www.bigbrotherawards.nl/
[5] www.transip.nl
[6] www.fundaments.nl
[7] www.iso.org/iso/catalogue_detail?csnumber=60545

# TREATING RISK PROSPECTIVELY

Dit artikel borduurt verder op een aantal concepten die in een eerder verschenen artikel "Tethering Enterprise Interests" [1] centraal hebben gestaan en werkt deze, waar nodig, iets meer uit. Het eerdere artikel stelt dat stakeholder belangen centraal staan in risicomanagement. De stelling is dat het doel van risk management in essentie neerkomt op het managen van prospects. We beogen, gegeven onze belangen als stakeholders, wat in het verschiet ligt zo gunstig mogelijk te laten zijn.

De website thefreedictionary.com geeft een aantal betekenissen van het woord prospect. Voor de doelstellingen van dit artikel zijn de volgende passend:

- **A probability for future success**
- **A vision of the future; what is foreseen; expectation**
- **Something expected; a possibility**
- **Financial expectations, especially of success**

Een prospect naar het Nederlands vertaald zie ik als een vooruitzicht, iets dat in het verschiet ligt.

## Stakeholders en hun belangen

Stakeholders verdelen we geïnspireerd door Principal-Agent Theory [2], in principals en agents. Voor de ontwikkeling en uitvoering van zijn visie en beleid is een principal doorgaans afhankelijk van agents. Deze agents kunnen op hun beurt principals zijn ten opzichte van de partijen waar zij afhankelijk van zijn.


**Figuur 1 - Principals en agents in een organogram**

Een typisch organogram, zoals figuur 1 toont, is een voorbeeld van een diagram waarin principals en agents worden getoond. Agents worden door corresponderende principals gemanaged. We stellen dat principals hun belangen behartigen door het uitstippelen van strategie en bijbehorend beleid. Een belang van een principal en een strategie om dat belang te verwezenlijken levert de principal strategische objectieven op.

*Maurice Gittens, CGEIT, CISA, CISM. Maurice werkt als consultant met informatiemodelleren, informatieverwerking, informatiearchitecturen en informatiebeveiliging. Hij is momenteel project manager bij een Nederlandse Bank. Maurice is te bereiken via maurice@gittens.nl.*

| Strategic Map | Principal Interest 1 | | Principal Interest 2 | |
|---|---|---|---|---|
| | Item of Interest 1 | Item of Interest 2 | Item of Interest 3 | Item of Interest 4 |
| Strategy 1 | Objective 1 | Objective 2 | Objective 3 | Objective 4 |
| | Objective 5 | Objective 6 | Objective 7 | Objective 8 |
| Strategy 2 | Objective 9 | Objective 10 | Objective 11 | Objective 12 |
| | Objective 13 | Objective 14 | Objective 15 | Objective 16 |

**Tabel 1 - Belangen, strategieën en strategische objectieven**

Doorgaans delegeert de principal de realisatie van deze objectieven (deels) aan agents uit. Agents kunnen employees, externe accountants, leveranciers, etc. zijn. Het is een gegeven dat principals en agents lang niet in alle situaties gemeenschappelijke belangen hebben. Tabel 1 geeft een algemene weergave van strategische objectieven zoals deze aan belangen en strategieën te relateren kunnen zijn.

De tabel suggereert dat een principal verschillende strategieën kan overwegen om zijn belangen behartigd te zien. Bij het actionable maken van zijn (deel) strategieën kiest hij als onderdeel van zijn strategische planning, strategische objectieven uit. De inrichting van een risk management regime dat synergetische alignment tussen de belangen van principals en agents waarborgt is een belangrijk doel in het managen van risico op strategisch niveau.

Tabel 2 toont een voorbeeld strategy map. Een principal die zelfontplooiing als primair belang heeft, onderscheid respectievelijk educatie en een inkomstenvoorziening als deelbelangen. Zijn strategie is om zelfstandig ondernemerschap binnen vijf jaar na te streven.

## Prospects: Dreigingen & Opportunities samengevoegd

We definiëren een prospect als een mogelijke toekomstige gebeurtenis die voor een betreffende principal waarde toevoegend en/of waarde dervend kan zijn. We drukken een prospect het liefst uit als geldbedrag. Risico's doen prospects afnemen terwijl opportunities prospects doen toenemen. De centrale aanname bij prospective risk management is dat alle stakeholders hun prospects tegen aanvaardbare kosten willen doen toenemen. Het kader 'Relevante concepten' geeft definities voor concepten die voor prospective risk management relevant zijn. We beginnen voor de volledigheid met een aantal alom bekende begrippen en breiden dat verder uit.

Tabel 3 toont een eenvoudig voorbeeld betreffende een webshop. Het doel van de principal is winstbejag met de exploitatie van een webshop. De tabel toont een lijst met risks en opportunities en ook de prospect voor dit doel.

**In dit voorbeeld zijn de opportunities voor de principal:**

- de inkomsten uit de exploitatie van de webshop. Het exploitatieplan wordt gezien als een lever die de kans op winstgevendheid verbeterd.
- de mogelijkheid de exploitatie inkomsten van de webshop te vergroten via marketing gerichte reclamecampagnes worden als lever gezien om de prospect te verbeteren.

| Strategic Map | Zelfontplooiing | |
|---|---|---|
| | Educatie | Inkomstenvoorziening |
| Zelfstandige ondernemerschap binnen 5 jaar | Afronden studie binnen 3 jaar | Start en exploiteer webshop |

**Tabel 2 - Voorbeeld Strategy Map**

| Objective | Prospect | Threat/Opportunity | Impact | Probability | Lever/Control | Cost of lever/control |
|---|---|---|---|---|---|---|
| Explotatie Webshop | 179320 | Exploitatie Inkomsten | 300000 | 70% | Uitvoering Exploitatieplan | 30000 |
| | | Interne Fraude | -25000 | 2,00% | Employee screening | 500 |
| | | Marketing programma | 10000 | 10% | Reclame | 300 |
| | | Hack op Webshop | -30000 | 1,00% | Website Security | 80 |

**Tabel 3 - Risks en opportunities**

# Relevante concepten

| Concept | Omschrijving |
|---|---|
| Risk | Risico wordt doorgaans gedefinieerd als het product van impact en probability. Hierbij* is het streven om risico tegen aanvaardbare kosten zoveel mogelijk te beperken. |
| Opportunity | Opportunity definiëren we op dezelfde wijze als risico, namelijk als het product van impact en probability. In het geval van opportunity is het doorgaans het streven om dit product tegen aanvaardbare kosten te maximaliseren. |
| Control | Een instrument bedoelt om risico te reduceren. |
| Lever (Engels) | Een instrument bedoelt om opportunities te vergroten. Een lever is in het Nederlands een hefboom. |
| Levering Control | Een control die ook een lever is. Levering controls kunnen in potentie risico reduceren en tegelijkertijd opportunity vergroten. In een ideale wereld zouden alle controls levering controls zijn. |
| Gross risk | Het bruto risico; het risico op waarde derving voor de principal veronderstelt dat er geen controls aanwezig zijn. Een dreiging of in het Engels een threat zien we als synoniem voor een gross risk |
| Net risk | Het netto risico; het risico op waardederving aan de belangen van de principal als er wel rekening met het cumulatieve effect van de controls wordt gehouden. Een netto risico wordt ook een residual risk genoemd. |
| Unlevered opportunity | Een opportunity zonder rekening te houden met het effect van eventueel aanwezige levers. |
| Levered opportunity | Een opportunity juist wel rekening houdend met het cumulatieve effect van eventueel aanwezige levers. |
| Gross prospect | De som van gross risks en unlevered opportunities die in relatie tot een bepaald doel gelden. Opportunities wegen als positief getal mee, risico's juist als negatief getal. |
| Net Prospect | De som van netto risico's en levered opportunities die in relatie tot een bepaald doel gelden. De kosten om controls en levers te realiseren en te exploiteren trekken we van de prospect af. Ook in dit geval opportunities als positief getal mee en risico's als negatief getal. |
| Congruent & incongruent prospects | De belangen van stakeholders heten congruent als deze niet strijdig zijn. Zijn de stakeholder belangen wel strijdig dan heten ze incongruent. Levers en controls heten congruent als ze de prospect voor dezelfde objective verbeteren. |

**Principals behartigen hun belangen door het uitstippelen van strategie en bijbehorend beleid.**

**Volgens het voorbeeld zijn de dreigingen:**

- de dreiging van interne fraude. Employee screening wordt gezien als een control om het risico te beperken.
- de dreiging van hackers. Website security processen en tooling worden als control gezien om dit risico te beperken.

Tabel 3 toont impact en waarschijnlijkheid voor een aantal dreigingen en opportunities. Opportunities wegen als positieve waarde mee en dreigingen als negatieve waarde. De tabel toont kosten voor levers en controls die in mindering op de prospect worden gebracht. In het bovenstaand voorbeeld wordt het netto prospect P volgens formule 1 berekend.

$$P = (\text{som van opportunities}) - (\text{som van dreigingen}) - (\text{som van kosten})$$

**Formule 1 - Netto prospect**

**Voor dit voorbeeld uitgewerkt wordt P:**

P =((300000*0,7)-(25000*0,02)+(10000*0,1)-(30000*0,01))-30000-500-300-80 = 179320

**Uit dit voorbeeld valt af te leiden dat:**

- Een negatieve impact op de principal ook een positieve impact op een agent kan hebben. De medewerker die bijvoorbeeld interne fraude pleegt, zal er met een bepaalde waarschijnlijkheid mee wegkomen. In dit geval is het duidelijk dat de belangen van de medewerker strijdig zijn met die van de principal.
- De principal zal, bijvoorbeeld, willen overwegen of het beter is om geld aan beveiliging te besteden of liever datzelfde bedrag op de beurs investeren.
- Het verschil tussen een dreiging en een opportunity is het teken van de impact.

Het mag evident zijn dat het voorbeeld fictief is en dat de gebruikte cijfers onrealistisch en vrij willekeurig zijn.

## Prospect Map: prospects per stakeholder

Eerder is gesteld dat de belangen van principals en agents niet congruent hoeven te zijn. Een prospect map is een tabel waarin de prospect per stakeholder wordt getoond. Hierbij geven we met een kleur aan of een prospect wel of niet congruent is met de belangen van de principal. Tabel 4 toont een prospect map voor het bovenstaande voorbeeld. We nemen hierbij aan dat alle marketingactiviteiten door de principal worden uitgevoerd, terwijl kosten voor de uitvoering van het exploitatieplan salarisinkomsten voor de medewerker zijn.

| Prospect Map | | Prospect |
|---|---|---|
| Principal | Exploit webshop | 169320 |
| | Marketing | 10000 |
| Employee | Earn salary | 30000 |
| | Commit fraud | 25000 |
| Hacker | Steal goods | 30000 |

**Tabel 4 - Prospect Map**

Groene cellen geven voor de principal congruente prospects aan terwijl rode cellen incongruente prospects aanduiden.
Een prospect map is een goed startpunt voor risk management mede omdat de principal inzage krijgt in mogelijk incongruente belangen van zijn stakeholders. Een belangrijke vraag is hierbij: Wat is de meest effectieve manier om de prospect voor een principal en zijn congruente stakeholder te verbeteren?
(tk)De kans van slagen: Prospect probability
Tot slot deel ik graag nog een gedachte. Om deze gedachte te delen definiëren we eerst de cumulatieve impact voor een objective als de som van impact voor dreigingen en opportunities die bij een bepaalde objective horen, verminderd met de kosten. In het voorbeeld uit tabel 3 is de cumulative impact:
300000+10000-30000-25000 -30000-500-300-80 = 224120.
De prospect probability Q definiëren we in formule 2.

$$Q = \frac{\text{Net Prospect}}{\text{Cumulative impact}}$$

**Formule 2 - Prospect probability**


De prospect probability Q geeft de kans dat de prospect gerealiseerd zal worden. Voor ons voorbeeld geldt:

$$Q = \frac{\textit{Net Prospect}}{\textit{Cumulative impact}} = \frac{179320}{224120} = 0{,}8$$

## Samenvatting

Wat mij betreft is alle risk management een kosten- versus batenanalyse. In dit artikel is een aanpak voor een kosten/baten analyse, onder de naam prospective risk management, gepresenteerd. Deze aanpak beoogd om informatiebeveiliging op strategisch niveau aansluiting te laten vinden met de belangen en zorgen van betrokken principals en agents. Door de effectieve inzet van informatiebeveiliging verbeteren we niet alleen de prospects voor de betreffende principals, maar ook voor onze vakgenoten en onze medeburgers.

Links

[1] Artikel in Informatiebeveiliging "Tethering Enterprise Interests", gepubliceerd in IB8 2013:
https://www.pvib.nl/download/?id=17695862
[2] Wikipedia: Principal Agent Theory:
http://en.wikipedia.org/wiki/Principal-agent_problem

# VEILIGER MET VOORKENNIS

## Deel 1

"Bij uitval van het navigatiesysteem bestaat er geen recht op vervangend vervoer. Er is namelijk geen sprake van uitval van het voertuig. We adviseren reizigers naast het navigatiesysteem ook wegenkaarten mee te nemen." – SOS International

In het huidige informatietijdperk raakt IT alle aspecten van ons leven. Voor organisaties is het belangrijker dan ooit om te weten wat ze aan de zich steeds sneller ontwikkelende technologie hebben en hoe kansen veilig kunnen worden benut. De technologische ontwikkeling heeft ook invloed op de beveiliging van informatie zelf. Welke kennis is dan nodig om informatie veilig te houden? Die vraag beantwoord ik in twee delen.

In het eerste deel start ik met het besturingsparadigma als context voor informatiebeveiliging. Vervolgens geef ik aan wat de rol is van een systematische analyse om risico's goed in te schatten. In de conclusie van dit deel vat ik samen welke kennis organisaties meestal missen bij de invulling van risicomanagement.

In het tweede en laatste deel analyseer ik de kansen en risico's van ontwikkelingen zoals de toenemende complexiteit en het voortdurend opschalen van organisaties en systemen. Ik schets tevens de invloed die kwantumcomputers kunnen hebben op de encryptie van data. Ik sluit af met een samenvatting welke kennis voor informatiebeveiliging nuttig is.

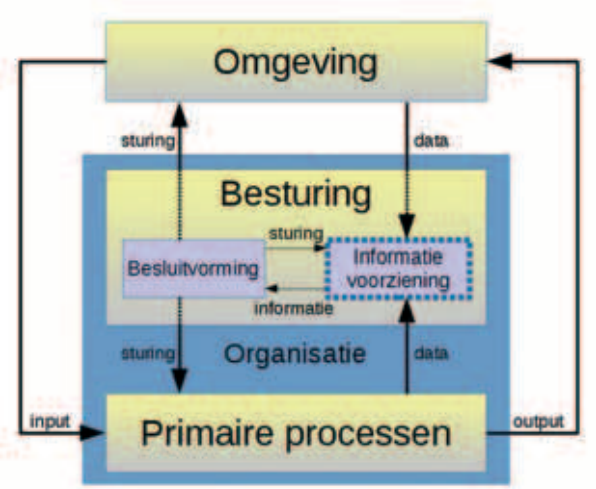
*"One of the functions of an organization, of any organism, is to anticipate the future, so that those relationships can persist over time" – Kevin Kelly*

## Sturen van organisaties

Personen en organisaties die open staan voor de mogelijkheden van nieuwe technologie kunnen grote stappen vooruit maken. Organisaties willen daarom relevante technologische verbeteringen tijdig opmerken, het effect van deze technologie kunnen voorspellen binnen de eigen context, op het juiste moment de juiste beslissing nemen en het effect van veranderingen optimaliseren.

Het besturingsparadigma plaatst de sturing van organisaties in context, zie afbeelding 1. In dit eenvoudige model stuurt het management op basis van informatie het primaire proces en de omgeving, de ondersteunende processen blijven buiten beschouwing. De informatievoorziening produceert deze sturingsinformatie uit in- en externe data. Informatiebeveiliging is voornamelijk geconcentreerd rond de informatievoorziening, inclusief de sturing daarop en rapportage daarover naar het management.

De informatievoorziening is meer gedetailleerd weergegeven in afbeelding 2. De data vanuit het primaire proces als input voor de informatievoorziening bestaat onder andere uit feed forward data (gegevens over de input) en feed back data (bijv. gegevens over eindproducten). Met feed back data kan je later, maar effectiever




**Afbeelding 1 - het Besturingsparadigma als context voor besluitvorming**

bijsturen, omdat dan bijvoorbeeld precies bekend is in hoeverre het eindproduct voldoet aan de kwaliteitsnormen. Sturen op de kwaliteit van het eindproduct met feed forward data is sneller en onnauwkeuriger, omdat de fouten in de input en de verwerking niet kunnen worden gecorrigeerd.

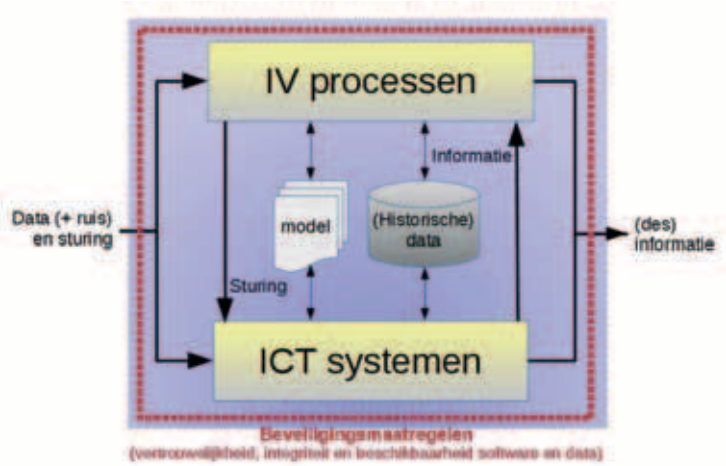
Beiden soorten data zijn complementair aan elkaar en ook allebei nodig, omdat data een onbekende hoeveelheid ruis kan bevatten en foutloze informatiesystemen niet bestaan. Feed forward besturing is gevoelig voor Garbage In, Garbage Out: als de input niet deugt, zal het resultaat ook niet goed zijn. Effectief sturen op basis van feed forward data is daarnaast alleen mogelijk met een model dat betrouwbaar kan voorspellen hoe afwijkingen in de input doorwerken in de kwaliteit van het eindproduct. Feed back data is dus tevens nodig om voorspellende modellen te toetsen en te verbeteren. Ik kom later nog terug op de kwaliteit van modellen.

***"Everything should be as simple as possible, but not simpler" – Albert Einstein***

## Waarom een systematische analyse

De ontwikkelingen in de ICT gaan steeds sneller, zoals blijkt uit het voortduren van de wet van Moore en de steeds korter durende Hype Cycle van Gartner voor nieuwe producten. In het begin van het ICT tijdperk lag de nadruk op het nuttig maken van computers, bijvoorbeeld door met een geschikte programmeertaal processen te automatiseren die informatie uit databases kunnen halen. Het oplossen van steeds

*Henk-Jan van der Molen is freelance docent bij de Security Academy.*
*De auteur wil iedereen bedanken die een positieve inbreng heeft geleverd aan dit artikel, in het bijzonder Jurgen van der Vlugt en Charlotte Rugers.*




**Afbeelding 2 - Informatievoorziening (IV) binnen het besturingsparadigma**

complexere problemen vormt de uitdagingen voor de nabije toekomst, zoals het real time volgen van significante veranderingen in netwerken, het halen van informatie uit grote meerdimensionale en ongestructureerde datasets, het verwerken van grote datastromen, kortom: de extractie van relevante informatie uit de beschikbare verzameling data inclusief ruis. En er is behoorlijk wat data beschikbaar als "ruis". Van alle data die nu beschikbaar is, is negentig procent in de afgelopen twee jaar gegenereerd [1].

Overigens verandert de wetenschap zelf ook door de voortdurende ontwikkelingen op ICT gebied. Vroeger moest je bijvoorbeeld wiskundige problemen handmatig kunnen oplossen, tegenwoordig kan de computer dat proces steeds beter ondersteunen. Daardoor verschuift de aandacht naar het stellen van de juiste vragen, het wiskundig goed kunnen formuleren van praktijkproblemen en het valideren van de berekende oplossing [2].

***"The purpose of abstraction is not to be vague, but to create a new semantic level in which one can be absolutely precise"***
***- Edsger Dijkstra***

Abstracties kunnen niet-relevante ruis verwijderen, zodat het onderzoek zich kan richten op het modelleren van het specifieke gedrag van het systeem. Invloed op de input vertaalt zich dan in de beheersing van het systeem. Een goede abstractie vereenvoudigt het beantwoorden van de vraag "hoe kan ik de werking van een systeem optimaliseren?". Een slechte abstractie maakt de vraag onoplosbaar, of (erger) produceert een fout antwoord dat juist lijkt. Een vaak toegepaste manier van onderzoek is per experiment slechts één variabele te veranderen en te kijken hoe die variabele het gedrag van het systeem beïnvloedt.

Daarnaast helpt een abstractie kennis meer generiek toepasbaar te maken, zodat meer soortgelijke problemen kunnen worden opgelost. Toepassing van een abstract model buiten de context is pas verantwoord als die situatie voldoet aan de uitgangspunten en randvoorwaarden (zeg maar: de bijsluiter) van dat model. De afwijkingen van de nieuwe situatie moeten worden vertaald naar wijzigingen in de scope, parameters en input van het abstracte model. Daarna moeten de conclusies en aanbevelingen uit de analyse van het abstracte model worden terugvertaald naar de praktijksituatie.

Het abstract modelleren van systemen lijkt veel op de zogenaamde "empirische cyclus" in de wetenschap:

1. het beschrijven van relevante waarnemingen uit de praktijk;
2. het opmerken van patronen in de werking van het systeem;
3. het construeren van een logisch model dat de waarnemingen kan verklaren;
4. het voorspellen van nieuw, nog niet waargenomen gedrag van het systeem met dat model;
5. het toetsen van het model door deze voorspellingen te verifiëren in de praktijk.

Een model kan de werking van het systeem correct voorspellen als van alle relevante variabelen de gezamenlijke effecten op het systeem bekend zijn. In de praktijk zullen nooit alle variabelen en hun onderlinge relaties bekend zijn en resteert er in elk systeem een bepaald ruisniveau. Zelfs een correct model kan daarom in de praktijk nooit helemaal nauwkeurig zijn en dat hoeft ook niet. Als de gebruikte modellen met de brondata maar een betrouwbare voorspelling kunnen maken. In het verleden zijn echter regelmatig modellen gebruikt die later onbetrouwbaar bleken. Bijvoorbeeld omdat het model gebaseerd was op verkeerde waarnemingen en pseudo-informatie uit ruis produceerde of het gemodelleerde systeem te chaotisch was om het gedrag betrouwbaar te voorspellen.

***"Errors using inadequate data are much less than those using no data at all" – Charles Babbage***

Waarom dan toch modellen gebruiken, als die beslissers op het verkeerde been kunnen zetten? Dat komt omdat sturen met een redelijk model meestal beter is dan sturen zonder model. Een logisch model helpt ons de wereld om ons heen te begrijpen en te beheersen. Als een model een bepaalde uitkomst niet kan voorspellen omdat die uitkomst afhangt van een samenloop van omstandigheden, kan het model of de bijsluiter worden verbeterd [3].

Toetsing van modellen en systemen blijft altijd nodig, om het nut ervan in de praktijk te bepalen en onnauwkeurige modellen te verbeteren of af te schaffen. Als een structureel onbetrouwbaar model in gebruik blijft, voert de organisatie deze toetsing niet goed uit. Of er is onvoldoende rekening gehouden met de bijsluiter van het model, bijvoorbeeld door het weer van volgende maand te voorspellen of één weersverwachting te maken voor een groot gebied. De betrouwbaarheid van sommige modellen kan verbeteren door de scope in tijd en ruimte te verkleinen.

Voor het bedenken, toetsen, aanpassen aan de context en verbeteren van modellen en systemen zijn analytische vaardigheden nodig en logisch redeneren. Modellen die zonder deze vaardigheden worden gebruikt zullen minder nauwkeurig voorspellen.

***" There is no security on this earth; there is only opportunity"***
***– Douglas MacArthur***

## Beveiliging in de praktijk

Ten opzichte van veel andere landen zijn de loonkosten in Nederland (veel) hoger. Om op kostprijs te kunnen blijven concurreren in "the global village" is een steeds grotere inzet van ICT in bedrijfsprocessen nodig. Zonder de juiste ICT ondersteuning zijn concepten zoals "Just in Time", "Zero Inventory" en "On Demand" niet te integreren in bedrijfsprocessen. Concurreren op basis van innovatie is effectief als de organisatie erin slaagt (concurrentie)gevoelige informatie geheim te houden en de primaire processen ongestoord kunnen doordraaien. De keerzijde van de continue innovatie is dat organisaties steeds afhankelijker worden van ICT systemen.

De voortdurende technologische vernieuwing introduceert naast voordelen ook steeds nieuwe beveiligingsrisico's en dat maakt informatiebeveiliging een dynamisch vakgebied. De volgende vragen en dilemma's vergroten die dynamiek verder:

- Een adequate beveiliging of de afwezigheid van kwetsbaarheden zijn onmogelijk objectief aan te tonen.
- Wegen de verwachte voordelen van veranderingen op tegen de (on)bekende nadelen?
- Hoe complexer een systeem, hoe meer kans dat er beveiligingsgaten aanwezig zijn.
- Een aanvaller heeft aan een kwetsbaarheid genoeg, terwijl een verdediger alle gaten moet dichten.
- Welke risico's loop ik en met welke maatregelen verminder ik die risico's tot een acceptabel niveau?
- Hoe kan ik incidenten het beste signaleren en afhandelen, zodat de impact op mijn bedrijfsprocessen minimaal is?
- Waar kan ik verantwoord bezuinigen op de kosten van mijn beveiliging?

Een beveiligingsincident vermindert de performance van de ICT resources van bedrijfsprocessen en kan gevoelige klantinformatie lekken. Ook het niet tijdig kunnen leveren van de juiste producten of als de kwaliteit lager is dan afgesproken, schaadt de reputatie van het bedrijf en verslechtert de concurrentiepositie. Om de impact van beveiligingsincidenten efficiënt te verminderen, moet de organisatie risicogericht maatregelen nemen. Daarom vullen veel organisaties hun beveiliging in met acties die de volledige PDCA-cyclus afdekken, zie tabel 1.

Cybercriminelen profiteren ook van de technologische ontwikkelingen, waarbij malafide software, tools en diensten op de zwarte markt worden verhandeld. Daardoor kan een steeds breder publiek geavanceerde cyberaanvallen uitvoeren. Dat is onder andere merkbaar bij de detectie van malware, die afhankelijk is van feed back informatie die gedeeld moet worden over meerdere organisaties. Daardoor heeft malware detectie in de afgelopen jaren zoveel achterstand opgelopen, dat up-to-date Antivirus pakketten nog maar ca. 50% van de nieuwste malware detecteren [4]. Die trend lijkt stabiel – wist in 2012 nog 37% van de slachtoffers zelf vast te stellen dat hun systemen waren besmet, in 2013 daalde dat naar 33% [5]. Verontrustend is dat investeringen in cybersecurity vooralsnog de vatbaarheid voor aanvallen nauwelijks vermindert [6]. We zijn nog niet in staat om het rendement van investering in beveiligingsmaatregelen goed te voorspellen. Hierdoor worden individuele systemen steeds kwetsbaarder, waardoor de frequentie van incidenten toeneemt. Gecombineerd met de toenemende afhankelijkheid, groeit de impact en daarmee het risico van cyber incidenten.

***"It is not certain that everything is uncertain"***
***– Blaise Pascal***

| | |
|---|---|
| **Plan** | Opstellen van **beveiligingsbeleid en plannen** om te voldoen aan wet- en regelgeving met o.a.:<br>• doelstellingen, uitgangspunten, taken, inventarisatie en toleranties van risico's;<br>• een strategie en plannen om de beveiliging op het gewenste niveau te krijgen en<br>• regels en standaarden om de beveiliging op het gewenste niveau te houden. |
| **Do** | Het **uitvoeren** van plannen om de beveiliging op het gewenste niveau te krijgen met o.a.<br>• Verwerving, inzet, optimalisatie en uitfasering van resources;<br>• Opleiding, training en oefening personeel;<br>• Het ontwikkelen en toepassen van **standaarden**, zoals best practice beveiligingsnormen, architecturen en procedures, zoals voor:<br>  • het uitvoeren van risico-analyses;<br>  • de preventie van incidenten (o.a. vermijden single-points-of-failure);<br>  • het realtime signaleren en oplossen van kwetsbaarheden, incidenten en aanvallen, en<br>  • het beheerst doorvoeren van veranderingen in de informatievoorziening. |
| **Check**<br>**Act** | Het **monitoren** van de implementatie van het beleid, de plannen, de performance van sturing, (human) resources en standaarden, het uitvoeren van periodieke audits en het evalueren van (bijna) incidenten.<br>Het treffen van preventieve en correctieve **maatregelen** op basis van de analyse van monitoring, audits en andere evaluaties. |

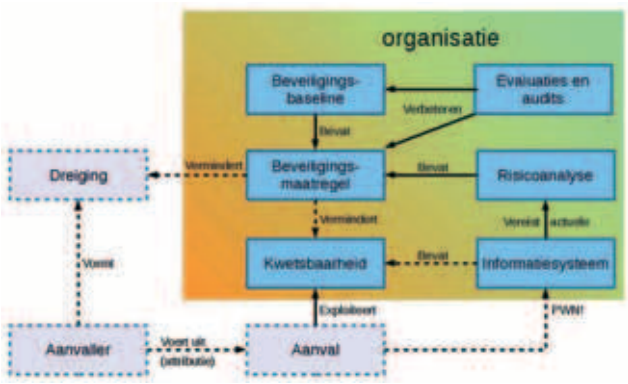
**Tabel 1 - Voorbeelden van beveiligingsacties als onderdeel van de PDCA-cyclus**

In onzekere tijden wil het management van een organisatie gevraagd en ongevraagd advies over risicotrends, zeker als overschrijding van risicotoleranties dreigt. Dat vergt een periodieke en systematische analyse om relevante trends voor informatiebeveiliging te signaleren. Op basis van gezond verstand is informatie alleen goed te beveiligen met de volgende randvoorwaarden:

- beschreven processen – alleen zo is herhaling, controle en continue verbetering mogelijk,
- specifieke en tijdige informatie over eigen kwetsbaarheden en (elders) uitgevoerde aanvallen,
- de mogelijkheid om effectieve en veilige standaarden in te zetten,
- modellen om te voorspellen welk effect veranderingen op de beveiliging hebben en
- regelmatige objectieve evaluaties van (doorgevoerde veranderingen op) beveiligingsmaatregelen.

Voldoen aan het bovenstaande lijstje met eisen voor het oplossen van de vragen en dilemma's heeft echter nogal wat voeten in de aarde. Afbeelding 3 vat de vragen en dilemma's met een eenvoudige aanvalsvector samen, waarbij de gestippelde lijnen en informatiebronnen aangeven dat een organisatie daar slecht zicht op heeft. Een organisatie kent bijvoorbeeld meestal niet alle kwetsbaarheden van een informatiesysteem en hoeveel de operationele beveiligingsmaatregelen deze kwetsbaarheden verminderen. Het signaleren dat een informatiesysteem is gecompromitteerd wordt ook steeds lastiger. Cybercriminelen willen zo lang mogelijk profiteren van gehackte systemen en verifiëren vaak vooraf dat reguliere beveiligingsmaatregelen zoals Antivirus en firewalls hun aanvallen niet opmerken [7]. Het gemiddeld aantal dagen dat aanvallers in 2013 gebruik konden maken van een besmet netwerk voordat ze werden ontdekt is 229 dagen [8].

Er zijn twee gangbare methoden om de schade van incidenten te bepalen [9]. De schade van uitval van een systeem kan bijvoorbeeld worden berekend met de factoren MTBF, MTTD en MTTR (Mean Time Between Failure, Mean Time to Detect, Mean Time to Repair). De MTTR's van de essentiële productiesystemen bepalen of de Recovery Time Objective van de organisatie kan worden gehaald.




**Afbeelding 3 - samenhang vragen en dilemma's van informatiebeveiliging**

Anderzijds kan met een schatting van de SLE (Single Loss Expectancy) vermenigvuldigd met de jaarlijkse frequentie van incidenten de ALE (Annual Loss Expectancy) worden bepaald. De businesscase van een beveiligingsmaatregel wordt dan als volgt ingevuld: schat de ALE met en zonder de maatregel en verminder dit verschil met de eenmalige en jaarlijkse kosten van de maatregel. De impliciete aanname voor dergelijke berekeningen is echter dat de kansverdelingen van de MTTR, MTTD en SLE normaal zijn verdeeld. Deze aanname is echter niet altijd correct, zie het tweede deel van dit artikel.

In dit eerste deel van dit artikel heb ik het besturingsparadigma geïntroduceerd als context voor informatiebeveiliging. Ik heb aangegeven waarom een systematische analyse nuttig is om de effecten van veranderingen te bepalen en welke kennis organisaties meestal missen bij de invulling van risicomanagement. In het volgende deel analyseer ik de risico's en kansen van enkele nieuwe ontwikkelingen, zoals de toenemende complexiteit en het voortdurend opschalen van organisaties en systemen. Ik schets tevens de invloed die kwantumcomputers kunnen hebben op de encryptie van data. In de conclusie vat ik samen welke kennis voor informatiebeveiliging nuttig is en waarom dat zo is.

## Referenties

[1] "Big Data – for better or worse", SINTEF, 2013

[2] Zie bijvoorbeeld wolframalpha.com, sagemath.org en "Homotopy Type Theory – Univalent Foundations of Mathematics" – Univalent Foundations Program, 2013

[3] Als de factoren onafhankelijk zijn, dan is de kans dat ze zich allebei gelijktijdig manifesteren het product van hun individuele kansen. Daarom is volgens Occam's Scheermes de eenvoudigste oorzaak meestal de juiste en kan een eenvoudig model dus goed genoeg zijn. Aangeven wanneer de uitkomst van een model betwijfeld moet worden, verbetert de bijsluiter van het model. En als er tussen afhankelijke factoren een causaal verband bestaat, dan kan het model met die relatie worden uitgebreid.

[4] 'Do Anti virus Products Detect Bots?', Staniford, S., 20 november 2008, http://blog.fireeye.com. Zie ook Retrospective/Proactive Test, AV-Comparatives.org, May 2011, www.av-comparatives.org .

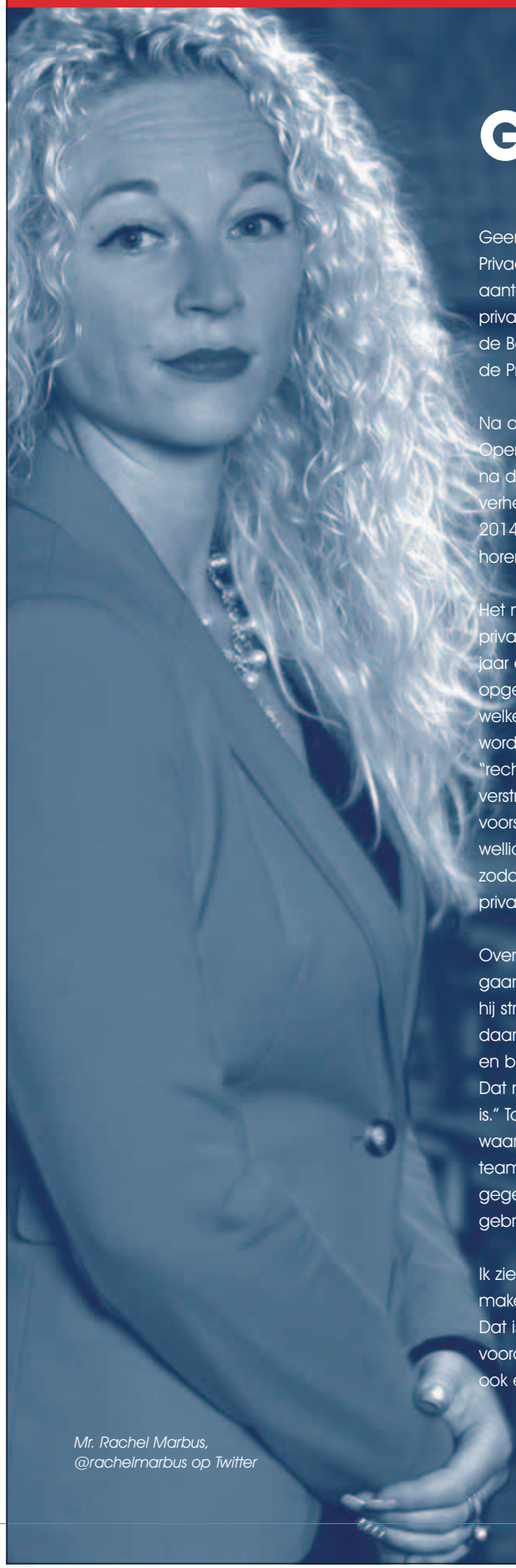
[5] Mandiant 2014 Threat report "Beyond the Breach"

[6] Zie Cyber Security Perspectives 2013.

[7] "Before We Knew It - An Empirical Study of Zero-Day Attacks In The Real World" L. Bilge e.a., 2012

[8] Mandiant 2014 Threat Report "Beyond the Breach"

[9] CISSP Exam Guide, Sixth Edition, Shon Harris



# GLUREN BIJ DE BUREN

Geen idee hoe de Belgen denken over ons Ministerie van Veiligheid en Privacyschendingen, maar ik kan u zeggen dat ik van hen in ieder geval op een aantal gebieden erg onder de indruk ben. Waar wij al jaren kampen met de meest privacy schendende Minister (hij won vorig jaar ALWEER de Big Brother Award…) doen de Belgen het aanmerkelijk beter. Zij hebben namelijk een heuse Staatssecretaris voor de Privacy.

Na de voorlaatste formatie had België een staatssecretaris "op overschot", voor de Open VLD (Open Vlaamse Liberalen en Democraten). Een uitgelezen kans om daar na de nieuwe verkiezingen de privacy te beleggen. Het voorstel mocht zich verheugen op steun binnen de regeringsformatie en zo kreeg België op 7 oktober 2014 haar eerste Staatssecretaris Privacy: Bart Tommelein. Al direct liet hij van zich horen.

Het nieuwjaarsvoornemen luidde: iedere Belgische burger moet eenmaal per jaar een privacybalans op schrift krijgen. Bedrijven en overheden moeten verplicht worden elk jaar een overzicht te zenden waarin vermeld wordt welke gegevens over de burger zijn opgeslagen en wat daarmee gedaan wordt. "Elke burger heeft het recht te weten in welke databank gegevens van hem zitten, wat daarmee gebeurt en hoe je eruit kunt worden verwijderd", aldus Tommelein. Daarmee maakt Tommelein van het passieve "recht op informatie" een actieve plicht voor verwerkers om de informatie te verstrekken. Mocht dit voornemen daadwerkelijk ingevoerd worden, dan kan ik mij voorstellen dat dit een veel groter bewustwording bij burgers teweeg gaat brengen en wellicht ook – op die plaatsen waar er ongebreidelde gegevensverwerking is – zodanige kritiek oplevert dat bedrijven en overheden zich genoodzaakt zullen zien privacyvriendelijker te werk te gaan.

Overigens is dat niet het enige waar de Staatssecretaris zich in 2015 sterk voor wil gaan maken. Ook op het gebied van Informatiebeveiliging en persoonsgegevens wil hij strenge eisen gaan stellen. "Iedereen die persoonlijke gegevens bijhoudt, zal daarvoor een veiligheidsplan moeten opmaken. Ik ga ervan uit dat overheidsinstanties en bedrijven die persoonlijke data beheren, zichzelf nu al beveiligingseisen opleggen. Dat moet voor elke verwerker het geval zijn, hoe groot of hoe klein die organisatie ook is." Tommelein reageert daarmee op de steeds vaker publiek wordende "hacks" waarbij persoonsgegevens online geplaatst en verspreid raken. Hij wil daartoe een team van experts (De hackers taskforce) samenstellen die moet onderzoeken hoe gegevens beter te beveiligen. Een opstapje naar dat strengere beleid zou zijn om het gebruik van onbeveiligde databanken met persoonsgegevens strafbaar te stellen.

Ik zie het nu al zitten met die Staatssecretaris. Hij moet het allemaal nog waar gaan maken, maar het toont wel dat de geest van Privacy leeft in het Belgisch parlement. Dat is in ieder geval iets waar wij Nederlanders wat van kunnen leren. Dus, laten we vooral leren van dat gluren bij de buren, het lijkt mij namelijk een prima plan om hier ook een regeringsfunctionaris voor de Privacy te hebben.

*Mr. Rachel Marbus,*
*@rachelmarbus op Twitter*

VERSLAG

# BIG BROTHER AWARDS 2014

Afgelopen 16 december was weer de jaarlijkse uitreiking van de Big Brother Awards. Dit jaar was de Grote Zaal van de Stadsschouwburg in Amsterdam het toneel van deze jubileumeditie. Vanwege de tiende editie werd eerst een terugblik gegeven op vijftien jaar privacy en Big Brother Awards.

Tussen de bedrijven door speelden verscheidene bands voor de honderden aanwezigen. Zij droegen op het onderwerp privacy toegespitste teksten voor. Ex-Jakhals (DDWD) Bahram Sadeghi was weer de dagvoorzitter die het programma aan elkaar mocht praten.

Maar waar het natuurlijk om ging was de aangekondigde aanwezigheid van Edward Snowden via een live video verbinding vanuit Moskou. Edward Snowden mocht als eerste de nieuwe 'Winston Award' in ontvangst nemen. Voor wie het niet weet: Winston was de hoofdpersoon uit George Orwell's 1984.

## Nominaties

**De genomineerden voor de Expertprijs waren:**

- De Nederlandse scholen, vanwege het doorspelen van privacygevoelige gegevens van leerlingen aan uitgevers van lesmateriaal. Maar eigenlijk gaat het nog verder met het verzamelen van gegevens over gezondheid, leerprestaties, gedrag en zelfs seksuele activiteiten. Deze gegevens worden vervolgens ruim dertig jaar bewaard. 'Vroeger ging je naar school om te studeren, nu om bestudeerd te worden'.
- Het eID stelsel. De experts maken zich zorgen over de centrale opslag van authenticatiegegevens, de beveiligingsproblemen en de toegang van de politie tot informatie.
- Bouwmarkten in omgeving Ede. Wie in een van de veertien bouwmarkten in de omgeving van Ede een koevoet of grote schroevendraaier koopt, wordt bekeken door de politie vanwege mogelijke inbraakplannen. 'Men zoekt niet de dader van een bekende inbraak maar de daden van een bekende inbreker.'

**De genomineerden voor de Publieksprijs waren;**

- Ivo Opstelten. Vanwege het in stand houden van de bewaarplicht, voor het doorzetten van zijn hackplannen en voor het langer willen opslaan van kenteken- en locatiegegevens. Ook het billijken van onrechtmatige opsporingsbevoegdheden in de Blackshades zaak.
- De Belastingdienst. Vanwege de schijnbaar onstilbare honger naar informatie over Nederlandse burgers. Daarnaast kunnen onder andere de AIVD en MIVD talloze gegevens opvragen van alle Nederlanders bij de dienst.
- Lodewijk Asscher. Vanwege de invoering van SyRI. Dat is een systeem dat grote hoeveelheden gegevens aan elkaar kan koppelen om burgers door te lichten. Het gaat dan om arbeidsgegevens, boetes, fiscale gegevens, roerende en onroerende goederen, handelsgegevens, zorgverzekeringsgegevens en nog veel meer. Ondanks een vernietigend oordeel van de Raad van State voerde Asscher de wet toch door.

## Winnaars

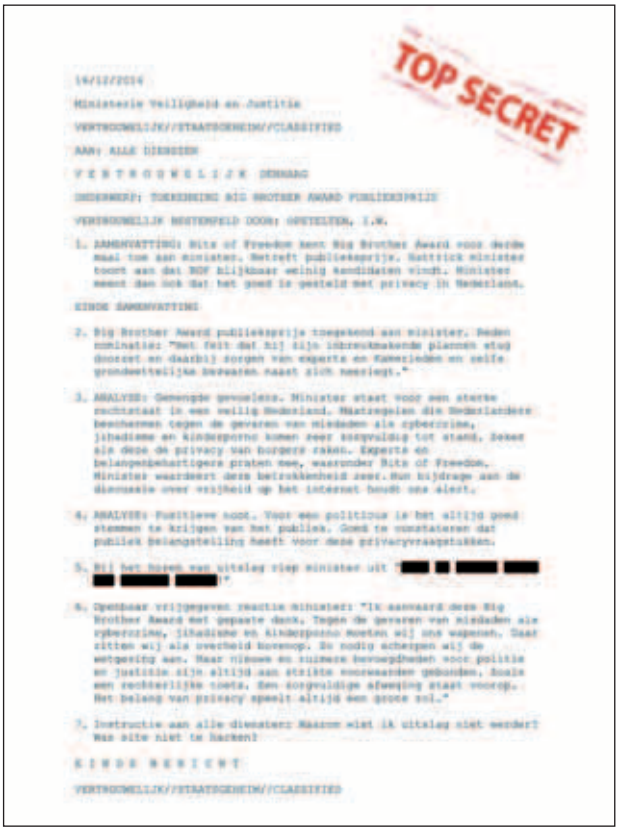
De Nederlandse scholen wonnen de Expertprijs. Deze werd namens de sectororganisatie in ontvangst genomen door Simone Walvisch, vice-voorzitter van de PO-raad. Zij gaf aan de Award te beschouwen als een aanmoedigingsprijs om verder te werken aan de aanpak van dit probleem door de uitgevers onder druk te zetten, met mogelijke hulp van de Tweede Kamer, om de privacy schendingen te stoppen.

Opstelten won voor de vierde keer (de derde keer op rij) de Publieksprijs met maar liefst 66% van de stemmen. Bits of Freedom vindt dat Opstelten zeker recht heeft op een oeuvre prijs met de deze vierde keer. Helaas bestaat die prijs niet, maar Opstelten heeft wel de belofte dat hij met aandacht in de gaten gehouden zal worden.

De schriftelijke reactie (in de vorm van een 'cable') van Opstelten stelde Bits of Freedom erg teleur [1]. Deze 'grappige' tekst viel niet in goede aarde. Uit deze brief blijkt dat Opstelten en het ministerie deze prijs niet erg serieus nemen en het eigenlijk belachelijk maken.

## Aral Balkan

De keynote speaker Aral Balkan hield een vlammend betoog over de verzamelwoede van private partijen zoals Facebook en Google en dat zij eigenlijk het werk uitvoeren dat overheden graag zouden willen. Surveillerende overheden hoeven niet zelf gegevens te verzamelen, dat kunnen ze gewoon halen bij deze private partijen. Aral gaf ook aan hoe alternatieve online diensten ontwikkeld kunnen worden waarbij de mensenrechten gerespecteerd worden. Dat zou de basis moeten zijn.




## Big brother awards / Artikel van het jaar 2014

### Edward Snowden

Aan het eind van avond was er de uitreiking van de Winston Award aan Edward Snowden. 'Ik was van plan vanavond aanwezig te zijn maar zoals jullie weten heb ik een probleem een visum te krijgen' was zijn reactie. Hij maakte zich zorgen om de nieuwe wet over het in de gaten houden van alle communicatie over de kabels (voorstel minister Plasterk). Organisaties worden al in de gaten gehouden door het afluisteren van satellietverbindingen maar nu raakt het de burger omdat juist die de vaste lijnen gebruikt. Volgens stelde Snowden dat men beter over 'freedom' kon spreken dan over 'privacy' omdat dat beter aangeeft waar het eigenlijk om gaat: onze vrijheid. Daarna kon het publiek nog vragen stellen aan Snowden. Het was een geweldig interessante avond waarbij na afloop nog nagepraat kon worden tijdens de borrel. Het hele programma is nog te bekijken op de site van Big Brother Awards [2].

Links

[1] https://www.bof.nl/2014/12/20/terugblik-op-de-tiende-big-brother-awards-bbax/

[2] https://bigbrotherawards.nl/blog/

# Nominaties voor Artikel van het Jaar 2014

Wederom zal het PvIB dit jaar een prijs uitloven voor het 'Artikel van het Jaar'. Er worden drie prijzen uitgereikt, waarbij de eerste prijs een waarde zal hebben van vijfhonderd euro. De meest belangrijke reden om een prijs uit te reiken aan onze auteurs is om waardering uit te spreken en ze te bedanken voor de goede artikelen die ze ons bezorgen.

De jury is samengesteld uit drie gekozen vertegenwoordigers uit de leden. De redactie heeft een voorselectie gemaakt van negen artikelen, de jury zal dus ook flink aan het werk moeten. De jury kiest hieruit drie winnaars en onderbouwt hun keuze in een juryrapport. De jury is dit jaar: **Remco Bakker van CQure** / **Lambrecht Nieuwenhuize van BNG** / **Renato Kuiper van VKA**

Vaste rubrieken en artikelen van redactieleden en juryleden dingen niet mee. Uitreiking van de prijzen wordt opgenomen in het programma van de PvIB-bijeenkomst op 21 april a.s.

**Genomineerde artikelen (op chronologische volgorde):**

| # | Titel | Pag | Auteur |
|---|---|---|---|
| IB1 | De CBP-Richtsnoeren nader beschouwd | 8 | Kersten, F. |
| IB2 | De sterkte van wachtwoorden en hun tekortkomingen | 4 | Heijningen, N. van |
| IB3 | Big Data: herijking noodzakelijk | 10 | Verburg, W. e.a |
| IB4 | Heartbleed | 4 | Rogaar, P. |
| IB5 | De Logius-norm voor DigiD: perikelen bij technisch testen | 10 | Koot, M. |
| IB6 | Phishing: slinkse manieren om een organisatie binnen te dringen | 4 | Duijn, R. van |
| IB6 | Klik, klik, klik het geluid van een gezonde werkvloer | 8 | Niggebrugge, D. e.a. |
| IB7 | Identiteitsfraude is kinderspel | 20 | Genova, M. |
| IB8 | Vulnerability scanning | 8 | Vernède, R. |

VERSLAG

# HET INTERNET IS STUK

In 2014 zijn op gebied van digitale infrastructuur al zeven kritische kwetsbaarheden gevonden:  Heartbleed, Shellshock, Poodle, Apple's SSL goto-fail, MS14-068 en MS14-064 en SSL triple handshake. De alom geaccepteerde en geïmplementeerde technologie OpenSSL kende dit jaar ook al diverse kritische kwetsbaarheden. Gevolg is dat dat bijvoorbeeld versleuteld dataverkeer van betaalmethode Ideal of authenticatie service DigiD over het internet te onderscheppen is. Het internet lijkt wel stuk en hebben hackers nu vrij spel gehad?

Vier maal per jaar organiseert Trust in People het Security Café. De editie van 25 november 2014, werd bij Schuberg Philis op Schiphol-Rijk georganiseerd. In het expertpanel Oscar Koeroo, werkzaam bij de KPN CISO in het Strategy & Policy team en voorheen werkzaam bij het KPN REDteam. Frank Breedijk, werkzaam als Security Officer bij Schuberg Philis. Adrianus Warmenhoven, werkzaam als Security Evangelist bij RedSocks en Professor in Hacking bij Oplerno. Hieronder volgt een impressie van de discussie.

**Wat zijn die kwetsbaarheden in Jip en Janneke taal?**

Oscar Koeroo legt uit dat je bij Heartbleed de mogelijkheid bestaat om het geheugen van een server op te vragen waar data onversleuteld langs stroomt. Zie het als de regen die je ziet als je door een raam naar buiten kijkt. In dit geheugen komen dus ook wachtwoorden en 'private keys' van certificaten voorbij. Credentials zijn goud voor een hacker om ongemerkt een legale weg naar binnen te vinden. 'Private keys' van certificaten zijn ideaal voor man-in-the-middle attacks omdat zij zich identificeren met dit certificaat. Deze kwetsbaarheid bestaat sinds 2011. 'Apple's SSL goto fail' en 'SSL triple handshake' laten ook kwetsbaarheden zien in het beveiligingsprotocol. Waar we dachten veilig te werken over het internet, bleek dat niet het geval.

De Shellshock kwetsbaarheid heeft betrekking op Bash, een open source programma dat commando's kan geven aan verschillende Unix-systemen. Doordat Bash niet controleert op nieuwe legale instanties/programma's, kunnen hackers een eigen applicatie starten en allerlei gegevens uitvragen. IBM/Unix-systemen bevatten vaak grote hoeveelheden kritische 'real-time' data. Naar schatting zijn minstens de helft van de web servers op het internet Unix systemen, een enorme slag voor de veiligheid van het Internet en de data die daar is opgeslagen. Analyse van de broncode toont aan dat deze kwetsbaarheid al sinds 1989 bestaat; het is onduidelijk of, en zo ja hoe vaak, er gebruik is gemaakt van deze route voordat hij ontdekt werd.

De Poodle kwetsbaarheid (Padding Oracle On Downgraded Legacy Encryption) is erop gericht een lagere beveiliging met de server te onderhandelen (bv SSL met kwetsbaarheden i.p.v.

*Gerco Kanbier is directeur van Trust in People – the information protection company.*
*Hij is te bereiken via gerco.kanbier@trustinpeople.com*

TLS). Servers onderhandelen het encryptieprotocol met de Client voor comptabiliteit voor gebruikers met beperkte beveiliging. Als alleen het hoogste niveau wordt toegestaan door de server, dan kunnen gebruikers geen gebruik maken van de functionaliteit totdat ze hun software hebben bijgewerkt. Daarom wordt vaak een lagere beveiliging wel toegelaten. Microsoft heeft ook kritische kwetsbaarheden gevonden en opgelost in bijna alle versies van Windows. Een kwetsbaarheid (MS14-064) maakt het mogelijk om op afstand code uit te laten voeren middels het onderdeel Object Linking en Embedding (OLE), ook deze kwetsbaarheid was minstens negentien jaar oud. Daarnaast was het mogelijk (via kwetsbaarheid MS14-064) om al Windows-gebruiker de rechten van domain controller te verwerven door een kwetsbaarheid in het onderdeel Kerberos KDC.

**"Gebruikersnaam en wachtwoord voor diensten op het internet is niet meer van deze tijd."**

### Wat is de impact voor bedrijven?

Zo'n kritische kwetsbaarheid moet je direct repareren. Alle systemen die kwetsbaar zijn, moeten geïdentificeerd worden en bijgewerkt worden. Dit vereist een behoorlijke inspanning en expertise. Soms is de tegenmaatregel dusdanig dat het ten koste gaat van het gebruikersgemak en is afstemming met hoger management noodzakelijk. Oscar schetst dat KPN te maken heeft met een grote gebruikersgroep die 24 x 7 gebruik maakt van online diensten. Kwetsbaarheden moet je dus wel oplossen binnen de mogelijkheden van de bestaande infrastructuur zonder dat de gebruiker er last van heeft. Je kan niet even de dienst een weekje platleggen.
Zodra het lek gedicht is, is het opgelost. Of toch niet? Adrianus Warmenhoven vertelt dat professionele hackers die binnen zijn, er alles aan doen om onopgemerkt binnen te blijven. Ze verstoppen zich in de krochten van het netwerk, zorgen voor afleiding op plekken die er niet toe doen en bouwen allerlei achterdeuren in, voor het geval dat je één van de geïnfecteerde systemen weet te blokkeren. Hackers weten namelijk ook dat het moeilijk is je gehele infrastructuur telkens opnieuw op te bouwen. Denk maar aan het gedoe als je je computer formatteert en weer in oorspronkelijke staat brengt. Frank Breedijk zegt dat dit voor datacenters de enige manier is om uit te sluiten dat ze niet binnen blijven zitten. Het doet pijn, maar je ontkomt er niet aan om alles opnieuw installeren. Hoe vaker je het, hoe minder pijn het doet en hoe beter je beschermd bent/blijft. Dankzij tools als Chef, Puppet, Ansible en/of Salt kan het herbouwen zelf omgevormd worden naar de standaard werkwijze.

*Hoe weet je dat deze kwetsbaarheden niet misbruikt zijn en hackers zich genesteld hebben in de krochten van uw netwerk met bijvoorbeeld Regin?*
Regin is zeer geavanceerde malware die zich richt op telco's (28%) en bepaalde individuen cq kleine organisaties (48%) gedetecteerd in hoofdzakelijk niet westerse landen (bron: http://www.brightsideofnews.com/). Deze malware is erop gericht data ongemerkt te lekken, screenshots te maken, keylogger informatie te versturen en om dataverkeer te onderscheppen. Software die nog niet toegankelijk is voor scriptkiddies. Echter, België en Duitsland zijn wel besmet geraakt, maar hebben waarschijnlijk telefonie services in het midden oosten. In Nederland lijken we hier geen last van te hebben. Op de achtergrond wordt door het westen wel een voorsprong opgebouwd als het gaat om grootschalige spionage praktijken. De digitale wapenwedloop tussen US, de Russen en de Chinezen is daardoor in volle gang.

### Wat is de Hold Security Case?

Hold Security is een Amerikaans commercieel bedrijf en heeft een grote dataset van toegangsgegevens opgekocht die op ondergrondse illegale fora rondzworven. In augustus 2014 verkreeg ons NCSC deze gegevens om te bepalen of en waar digitaal Nederland kwetsbaar was. Het bleek dat er 5600 Nederlandse websites kwetsbaar waren voor SQL injection en dat er via deze websites 1,3 miljoen Nederlandse emailadressen met wachtwoorden zijn verzameld. Het cybercentrum NCSC moest natuurlijk wel onderzoeken of de vitale infrastructuur in Nederland kwetsbaar is geweest. Hoewel de impact nihil bleek voor overheid en vitale infrastructuur, is in september 2014 nog wel een gecoördineerde actie gestart met onder meer domeinregistrar SIDN om 5600 website eigenaren te informeren en diverse ISP's om 1,3 miljoen emailadres eigenaren per brief te informeren. In de brief stond natuurlijk het advies om je wachtwoord van je emailadres te veranderen. Echter, in deze brief wordt niet gemeld dat dit wachtwoord ook misbruikt kan worden voor toegang tot een andere online dienst. Je zakelijke email en/of lidmaatschap bij een webshop kan dan gemakkelijk gehackt worden als alleen nog je gebruikersnaam achterhaald moet worden.
Omdat het NCSC aangeeft dat er nauwelijks impact is op de vitale infrastructuur in Nederland, concludeer ik dat het 5600 websites in het bedrijfsleven die inactief en/of onvoldoende beschermd zijn. Een professionele website zoals bol.com of


ah.nl zal er dus ook niet bij zitten. Eerder de semiprofessionele websites van de lokale voetbalvereniging, de handwerkclub en/of de backend van vlotte nieuwe apps. Mogelijk zijn ook de kwetsbaarheden van Wordpress en/of Joomla misbruikt. Strafbaar en ogenschijnlijk weinig impact. Toch is dit kwetsbaar voor vitale infrastructuur in Nederland als je het wachtwoord komt te weten van de directeur van een multinational via zo'n onschuldige website.

## Hoe zit dat met dataheling?

Een Russische botnet crawler die wereldwijd kwetsbare 'onbelangrijke' websites hackt om 1,4 miljard emailadressen en wachtwoorden te verzamelen, is illegaal en strafbaar. Deze hackers hebben als doel om geld te verdienen aan de verkoop van vertrouwelijke gegevens. De vraag is of de daders zich iets aantrekken van de Wet Computercriminaliteit in Nederland en of ze ooit internationaal vervolgd gaan worden. Dit soort gezwellen op internet zijn blijvertjes, net als kwetsbare websites. Pakkans is nihil. Een commercieel bedrijf als Hold Security koopt de illegaal verkregen informatie op. Deze koop is net zo strafbaar als het hacken van de websites zelf. Hoewel Hold Security de data hoogstwaarschijnlijk niet misbruikt om toegang te krijgen tot websites of email van slachtoffers, gebruikt Hold Security de data wel voor extra publiciteit. Dit is ook een ongewenste doelbinding in relatie tot de data. Vervolgens wordt deze informatie aangeboden aan het NCSC. Omdat het NCSC als doel heeft de vitale infrastructuur in Nederland te beschermen, denk ik dat het rechtvaardig is dat het NCSC deze informatie mag gebruiken om die dreiging te beoordelen. Echter, als het doel van een organisatie niet is vastgelegd en/of valide is in relatie tot de data, hoe zit het dan? Geeft Hold Security deze informatie namelijk aan een willekeurige derde, dan is dat dataheling. Je kunt je afvragen of het dan nog relevant is of er dan betaald is voor de informatie.
Volgens mij is deze situatie vergelijkbaar met de typische Nederlandse problematiek rondom fietsdiefstal. Als iemand je fiets pikt en na gebruik gratis weggeeft of verkoopt aan een ander, dan is zowel de nieuwe eigenaar als de oorspronkelijke dief strafbaar. Ik vraag mij hoe de Wet Computercriminaliteit dit soort internationale problematiek adresseert en of doelbinding gebruikt wordt om dataheling wel of niet toe te staan.
Het advies van panelleden naar aanleiding van dit incident: Maak gebruikers bewust om verschillende wachtwoorden per website te gebruiken in combinatie met tools die je password onthouden (bv LastPass, 1Password). Frank Breekdijk suggereert nog een bijzonder alternatief door middel van een willekeurige symfonie van karakters als wachtwoord in te voeren en via "wachtwoord vergeten" telkens het wachtwoord opnieuw op te vragen. Maak webhosters & -ontwikkelaars bewust dat websites beter beveiligd moeten worden tegen kwetsbaarheden zoals SQL Injection en XSS. Maak het liefst gebruik van 2 factor authenticatie (bv Authy, Google Authenticator) waardoor een statisch wachtwoord vervangen wordt door een eenmalige toegangscode via een app of sms op je telefoon.

## Hoe leren we van dit soort incidenten?

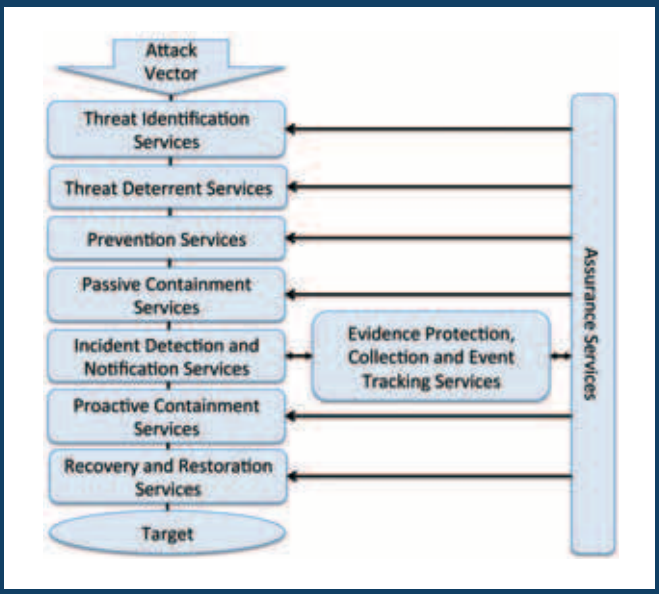
Toch blijft het lastig om (semi) openbaar kennis met elkaar te delen over incidenten. Tijdens een incident-onderzoek mag niemand over het incident praten. Achteraf vind niemand het leuk om fouten toe te geven. Toch is het leerzaam om bijvoorbeeld tijdens zo'n Security Café betrokkenen in het panel aan het woord te laten met als doel er met zijn allen van te leren.

Links

**Security Cafe:** http://www.trustinpeople.com/security-cafe
**Hold Security over CyberVor:**
http://www.holdsecurity.com/news/cybervor-breach
**Kaspersky, Symantec en McAfee over Regin:**
http://www.brightsideofnews.com/
**RIPE:** http://www.ripe.net/

# FORENSICS READY

As we enter into the new year of 2015, it is timely to consider what lessons we might have learned from the previous year. One that seems to be of major importance is that large corporations can increasingly expect to get hacked, and when they do they need to investigate how, by whom and why it happened. Take for example the recent Sony embarrassment. A major film stolen (IPR theft on a large scale), threats of attack on public cinemas (leading to withdrawal of the public release because of safety considerations) and as a result world governments exchanging insults in a major diplomatic incident. That's quite an impact!




It seems that many enterprises are still way behind the curve in their thinking. Far from being a 'Black Swan', this was a predictable attack scenario, but it seems that many still have their heads buried deep in the sand with no real appreciation of the possibilities or the consequences. So in this issue we shall explore the concept of 'forensic readiness' as another SABSA Business Attribute.

It is well established that digital forensics is an important tool in our armoury of security controls. There are many specialists offering services in this area. However, when they reach the scene of the crime they often find that evidence is either hard to find or badly contaminated. If we are to identify exactly what happened and by whom the attack was mounted, then we can do much to prepare for collecting evidence and protecting its integrity as being 'admissible' – another important SABSA Business Attribute. Legal and diplomatic proceedings need to be based on sound, incontrovertible forensic evidence, the integrity of which can be demonstrated beyond reasonable doubt.

This is not just 'another control' – it is something that needs to be designed into the entire systems architecture, but legacy architectures are not well conceived in this respect. It highlights the need for a business-driven security architecture that is based on a business risk assessment rather than a mere technical risk view. The impacts from the Sony incident are massive, but expert technical security analysts would never predict that without close engagement with their business colleagues, because they do not think in those business terms.

Developing successful security architecture is a multi-disciplinary activity that requires input from business stakeholders, experts in several specialised technical fields and architects who should be able to bring all of it together into one holistic view of how to manage business risk in a digital environment. The main architectural concept needed here a layered control strategy, as described in SABSA publications. Most organisations focus too much attention and investment on 'preventive controls', but a much more balanced approach is required. The diagram illustrates a layered 'defence-in-depth' control strategy in which evidence collection and preservation features as and integral part of the architecture.

It seems that we are still a long way from achieving this level of architectural sophistication in the real business world, and that SABSA thinking needs to be promoted to a much wider community. Well, that's the job of The SABSA Institute, recently launched for public membership, and one day that goal will be realised.

**The Attributer**

Verantwoorde onthullingen #12

# TROTS OP ONZE DIGITALE POLDEROPLOSSINGEN

Op 19 december kregen we weer een brief van Ivo Opstelten over hoe het ervoor staat met responsible disclosure; "beleid voor het op verantwoorde wijze openbaar maken van ICT-kwetsbaarheden in informatiesystemen en softwareproducten die door goedwillende melders of hackers worden ontdekt en gemeld." Het gaat goed met dat beleid, want steeds meer partijen doen eraan mee. Bij de Rijksoverheid, telecom, banken, hosters, verzekeraars en nog vele anderen zijn nu meldpunten voor gevonden kwetsbaarheden. Het NCSC is hierin de spil. Het centrum bemiddelt bij meldingen en heeft er zelf ook 136 afgehandeld.

Chris van 't Hof
Voor meer verantwoorde onthullingen.
www.cvth.nl/vo

Er is veel gebeurd sinds het verschijnen van hun leidraad responsible disclosure twee jaar geleden. Ook toen kregen we een brief van onze minister van Veiligheid en Justitie. Hij schreef op 5 december 2012: "Centraal bij het werken met responsible disclosure staat het verhelpen van de kwetsbaarheid en het verhogen van de veiligheid van informatiesystemen. Daarbij gelden een aantal algemene uitgangspunten. Zo is het bijvoorbeeld niet gepast om schade aan te richten of verder te gaan dan het aantonen van de kwetsbaarheid. In zo'n geval is het niet gepast om onnodig grote databestanden te stelen als al is aangetoond dat het databestand benaderbaar is." Dat standpunt is niet veranderd en werd bevestigd door de rechtszaken die erop volgden.

Aanleiding voor de brief was destijds de onthulling van beveiligingsproblemen bij het Groene Hart Ziekenhuis. Een hacker had aangetoond dat hij bij persoonlijke data kon, omdat het netwerk verouderd was. Brenno de Winter onthulde dit op 7 oktober 2012 op nu.nl. Het ziekenhuis stelde meteen een crisisteam aan en liet onderzoek doen. Toen bleek dat er malware was geïnstalleerd en grote hoeveelheden patiëntgegevens waren gedownload, deed het ziekenhuis aangifte en werd de hacker opgepakt.

In diezelfde periode moest ook Henk Krol voor de rechter verschijnen. Hij had enkele patiëntdossiers gedownload om te laten zien dat hij met slechts vijf cijfers in de database van Diagnostiek voor U kon en bracht dat direct in de media. Ook

Diagnostiek voor U deed aangifte en Krol werd vervolgd. Beide zaken leidden tot veel protesten in de media en de Tweede Kamer. Waarom werden de melders aangepakt en niet de organisaties die slecht omgingen met de persoonsgegevens? Net op dat moment kwam de leidraad uit.

Voornaamste kritiek op de leidraad was dat die ethische hackers geen garanties geeft. Organisaties zijn vrij om hun eigen regels op te stellen voor verantwoorde onthullingen, zonder dat ze verplicht zijn iets met de meldingen te doen. Het OM behoudt zich ondertussen het recht om onderzoek te starten naar de rechtmatigheid van de ethische hack. Uitgangspunt daarbij is dat computervredebreuk is toegestaan als het een hoger maatschappelijk doel dient en de hacker handelt volgens de principes van subsidiariteit en proportionaliteit. Oftewel: hack alleen om aan te tonen dat de beveiliging niet klopt, doe het met de minst ingrijpende middelen en download zo min mogelijk persoonsgegevens.

De zaak Krol diende in januari 2013. De rechter vond dat Krol wel ethisch had gehandeld door in te loggen, dossiers uit te printen, te anonimiseren en zijn vondst in de media te brengen – ook al gaf hij Diagnostiek voor U nauwelijks tijd om voorbereidingen te treffen. Wat hij deed was nodig om de misstand in de beveiliging van persoonsgegevens aan te tonen en hij voldoet daarmee aan de subsidiariteitseis. Maar dat hij diverse keren had ingelogd en ook voor het oog van journalisten dossiers downloadde vond de rechter disproportioneel. Hij kreeg hiervoor een boete van 750 Euro. Diagnostiek voor U had nog een fikse schadevergoeding geëist, maar daar ging de rechter niet in mee.

De zaak Groene Hart duurde wat langer, want op de in beslag genomen computer werd ook kinderporno gevonden, wat leidde tot een nieuwe zaak. Gelukkig heeft de rechter in haar oordeel van 17 december 2014 de twee zaken gescheiden, anders zou het wel rommelige jurisprudentie zijn geworden. De hacker handelde volgens haar in eerste instantie ethisch omdat hij geen financieel belang had bij de hack en het lek heeft gemeld via een journalist die bekend staat om onthullingen. Zo hebben ze een beveiligingsprobleem geagendeerd bij een ziekenhuis dat hierin tekortschoot en dienden ze een hoger maatschappelijk belang.

De rechter ziet het als noodzakelijk voor dit doel dat hij een server heeft gehackt en als bewijs enkele dossiers heeft gedownload met een programmaatje dat gezien kan worden als malware. Dat kon niet met minder ingrijpende middelen. Dat hij echter de dagen erna weer inlogde en dossiers ging downloaden, gewoon uit nieuwsgierigheid, was niet noodzakelijk en een disproportionele inbreuk op de privacy van de patiënten. Daarvoor wordt hij veroordeeld tot 120 uur taakstraf wegens computervredebreuk.

De leidraad responsible disclosure laat dus veel open en die ruimte wordt nu ingevuld door de rechtspraak. Bij gebrek aan wetgeving, moeten we het voorlopig doen met de voortschrijdende jurisprudentie. Dat is heel naar voor de hackers en gehackten die zo'n ingrijpend proces moeten doormaken. Maar ik zie ook niet direct een wet komen die opgaat voor alle gevallen, omdat de situatie telkens anders is. Responsible disclosure blijft een polderoplossing waarbij iedereen zich wel een beetje, maar niemand helemaal in kan vinden. Dat is ook inherent aan cyber security: iedereen is een beetje verantwoordelijk voor een deel en daardoor uiteindelijk niemand echt voor het geheel. Hopelijk kunnen rechtszaken voorkomen worden door goed overleg en hebben strijdlustige advocaten en activistische journalisten het nakijken. De leidraad en bemiddeling van het NCSC helpen daar zeker bij, want steeds meer meldingen worden achter de schermen afgehandeld.

Dit is het digitale polderlandschap zoals het erbij ligt begin 2015. Ook dit jaar staat er veel op de agenda voor responsible disclosure. De leidraad wordt geactualiseerd, getoetst bij de ICT community en verder uitgedragen. Onder andere bij twee conferenties: de Global Conference on CyberSpace en de NCSC One Conference. Hiervoor wordt ook onderzocht hoe ethisch hacken zich verhoudt tot de rechtssystemen van andere landen. In 2016 zal Nederland zijn EU voorzitterschap gebruiken om responsible disclosure internationaal uit te dragen. Het is dan wel een digitale polderoplossing, maar we zijn wel het eerste ter wereld dat het zo doet. Daar mogen we best trots op zijn.

Ondertussen zit ik tijdens de Kerstvakantie mijn boek hierover af te ronden, want 11 maart krijgen alle bezoekers van Security Bootcamp een exemplaar van "Helpende Hackers". Misschien volgend jaar maar een versie 2.0?

**Chris van 't Hof**
www.helpendehackers.nl

# Achter het nieuws

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


# HELPEN DWANGSOMMEN?

Steeds meer Europese privacy autoriteiten draaien de duimschroeven aan bij grote privacyverslinders zoals Google en Facebook [1]. Medio december liet het CBP van zich horen met een last onder dwangsom die Google moet dwingen om voor februari 2015 zijn privacybeleid in lijn met de Nederlandse wet te brengen [2]. Hiermee treedt Nederland in de voetsporen van andere Europese landen, zoals Duitsland, Spanje en Frankrijk.

**Lex Dunn**

Ik denk niet dat Google schrikt van een boete van vijftien miljoen euro. Dat komt bij hun uit de kleine kas. Sterker nog, ze willen immuniteit voor de komende meldplicht voor datalekken, net zoals IBM trouwens (zie Webwereld [3]). In het verleden heeft Google al diverse malen persoonsgegevens uit diverse bronnen gecombineerd om te "profileren", een woord dat in mijn optiek een steeds negatievere lading krijgt. En het ziet er niet naar uit dat Google op zijn lauweren gaat rusten, ze zullen ongetwijfeld verder diensten ontwikkelen en voor hun interessante bedrijven opkopen.

Het aandeel van Google in zoekmachinegebruik is nog steeds meer dan tachig procent, zegt een recent onderzoek van iProspect en RMI (zie AG [4]). Maar daarnaast iis Google bezig met de ontwikkeling van de zelfrijdende auto, en wil Google de hele aarde voorzien van hoge snelheid draadloos Internet. Kortom: Google krijgt een steeds groter inzicht in onze gedragingen, onze voorkeuren, onze connecties, onze verplaatsingen, en daarmee in onze persoonlijkheid. Waar dat toe kan leiden is treffend beschreven door George Orwell in "1984" (overigens al in 1949 gepubliceerd) en door Cory Doctorow in zijn SF roman "Little Brother".


Lex Borger


Tom Bakker


Maarten Hartsuijker


Lex Dunn

## Tom Bakker

Ik verwacht niet dat Google en Facebook wakker liggen van dit soort boetes. Wellicht zijn ze niet zo blij met de negatieve publiciteit die ze zo krijgen. Hun koers zullen ze nooit willen veranderen om de doodeenvoudige reden dat de ingeslagen weg gewoon hun businessmodel is: verzamelen van zo veel mogelijk persoonsgegevens voor profiling om dat weer te kunnen doorverkopen.

Kijk maar naar de aangekondigde wijzigingen in de privacyvoorwaarden die Facebook per 1 januari gaat invoeren. Alle content op Facebook wordt van Facebook. Ook nieuwe -handige– Google diensten hebben tot doel nog meer gegevens te kunnen verzamelen. Tijdens de Big Brother Awards (BBA) gaven Aral Balkan en Edward Snowden een interessante analyse hierover.  Zie ook het verslag over de BBA elders in dit blad. Balkan noemde Google/Facebook gebruikers 'Lab Rats'. Een ander gehoord citaat: "We zijn net zomin een klant van Facebook als een varken klant is van Unox."

## Maarten Hartsuijker

Met de feestdagen nog maar net achter ons belooft 2015 een erg interessant privacy jaar te worden. De nieuwe Europese privacyverordening staat voor de deur. En het CBP sluit 2014 af door in december nog voor wat vuurwerk te zorgen richting Google en Facebook.

Hoewel vijftien miljoen voor Google geen groot bedrag is, denk ik dat het bedrijf toch wel met zorgen kijkt naar de wijze waarop Europa scherper in de toepassing van haar privacybeleid is geworden. Google heeft de afgelopen jaren hard gewerkt aan manieren om data over mensen te verzamelen. Elke Google Maps en Google Analytics vertoning vertelt ze weer wat meer over ons internetters. En daar kunnen we zelfs als we geen direct gebruik van Google diensten maken maar bar weinig aan doen. Hetzelfde geldt voor Facebook. Ook als je daar geen account hebt, is de kans zeer groot dat jouw persoonlijke gegevens via jouw vrienden worden aangeleverd. Want onzorgvuldig met je privacy (en die van anderen) omgaan was makkelijker dan ooit te voren. Je hebt het nauwelijks door dat de bedrijven via WhatsApp of je Android telefoon door je adresboek, berichten en foto's struinen.

Wat mij betreft zou er meer werk mogen worden gemaakt van het recht om vergeten te worden. Voor onze privacy zou het goed zijn als we er van op aan kunnen dat verzamelde gegevens na korte tijd verlopen en verwijderd worden. En dat een DNT instelling in een browser voldoende is om profilering te voorkomen. Google, Facebook: is dat teveel gevraagd?

## Lex Borger

Het is goed dat het CBP zijn tanden laat zien. Ze kiezen wel de twee grootste partijen op de markt uit waarvan iedereen al weet dat ze al je klikgedrag monitoren in ruil voor gratis diensten… Ik vraag me af of dat effectief is. Bits of Freedom heeft een heel andere waardering van privacy, zie het verslag van de Big Brother awards elders in deze uitgave.

Google en Facebook zijn uiteindelijk best wel transparant over wat ze van plan zijn te verzamelen, het meest opvallend is dat wij 'slachtoffers' niet massaal reageren met het opzeggen van onze accounts. Dat zou volgens mij meer verschil maken dan een miljoenenboete. Er zijn genoeg alternatieven om wat meer privé te zoeken en we kunnen ook wel voort met wat minder Facebook updates.

Het recht om vergeten te mogen worden is nuttig, maar heeft nog veel publieke discussie nodig voordat dit dwingend toegepast kan worden. Los van de – in mijn ogen – technische onmogelijkheid hiervan, wordt hier een privébelang afgewogen tegen een publiek belang. Een tegenvoorbeeld: Prinses Mabel's relatie met Klaas Bruinsma mocht van de massa niet vergeten worden [5].

Een ander aspect wat van mij ook meer aandacht mag krijgen is het gebruik van privacy-bevorderende technieken, zoals encryptie, DANE, OCSP Stapling en het verplicht honoreren van do-not-track headers. Een dwangsom voor het niet honoreren van do-not-track headers vind ik eigenlijk interessanter klinken dan de huidige dwangsommen. Maar zo ver zijn we nog niet.

### Links

[1] https://www.bof.nl/2014/12/16/facebook-in-het-vizier-van-het-cbp/
[2] http://ictmagazine.nl/4706/cbp-boete-google/
[3] http://webwereld.nl/beveiliging/84861-google--ibm-willen-immuniteit-voor-datalekken
[4] http://www.automatiseringgids.nl/nieuws/2014/52/google-nog-steeds-veruit-populairst
[5] http://www.dailymail.co.uk/news/article-479098/Royal-couple-change-Wikipedia-entry-brush-drugs-scandal.html

# Artikelen

| | | | |
|---|---|---|---|
| [A] | Baaten, D. | HTTPS over Open Wi-Fi blijft kwetsbaar | IB6:19 |
| [A] | Bakker, J. e.a. | Succesvol opereren op het grensvlak van techniek en business | IB3:20 |
| [A] | Berg, J. van den | Cyber Security vraagstukken | IB4:20 |
| [O] | Bobbert, Y. | Schoenmaker blijf bij je leest | IB3:24 |
| [O] | Bolk, F. | Heartbleed en het risico van open source software | IB5:20 |
| [O] | Bolk, F. | Reactie op open brief | IB7:10 |
| [O] | Borger, L. | De nieuwe malware aanpak | IB8:27 |
| [A] | Brandt, D. e.a. | Succesvol opereren op het grensvlak van techniek en business | IB3:20 |
| [A] | Breedijk, F. | De Security Survival Pyramid | IB6:30 |
| [I] | Clark, K. e.a | Aart Jochem & Kas Clark | IB4:8 |
| [I] | Craandijk, C. | Jaya Baloo: de hack heeft ons wakker geschud | IB3:6 |
| [I] | Craandijk, C. | NCSC: 100% veiligheid bestaat niet | IB8:4 |
| [A] | Dominguez, F. e.a. | Klik, klik, klik het geluid van een gezonde werkvloer | IB6:8 |
| [A] | Duijn, R. van | Phishing: slinkse manieren om een organisatie binnen te dringen | IB6:4 |
| [A] | Duijn, R. van | Tien veel voorkomende netwerkrisico's en pro-actieve maatregelen | IB6:14 |
| [O] | Eijkhoudt, A. e.a. | Open brief aan Frans Bolk | IB7:7 |
| [A] | Eygendaal, R. | Security met Li-Fi | IB3:4 |
| [A] | Eygendaal, R. | De volgende fase van SIEM: SAWSOC | IB8:14 |
| [V] | Garskamp, R. | IDentity.Next 2013 | IB1:28 |
| [A] | Genova, M. | Identiteitsfraude is kinderspel | IB7:20 |
| [A] | Gittens, M. | Tethering Enterprise Interests | IB1:16 |
| [O] | Ham, J. van der e.a. | Open brief aan Frans Bolk | IB7:7 |
| [A] | Hartsuijker, M. | IT en Cars | IB4:12 |
| [A] | Hartsuijker, M. | Analyseren en aanpassen van SSL configuraties | IB8:16 |
| [A] | Heijningen, N. van | De sterkte van wachtwoorden en hun tekortkomingen | IB2:4 |
| [O] | Heus, M. e.a. | Open brief aan Frans Bolk | IB7:7 |
| [A] | Jochem, A. | Een virtuele bucket line | IB5:23 |
| [I] | Jochem, A. e.a. | Aart Jochem & Kas Clark | IB4:8 |
| [I ] | Kagie, S. | Michel Henneke: Voorkom DNS-aanval met .nl control of een registry lock | IB5:15 |
| [V] | Kanbier, G. | Security Café: Inlichtingen en onze privacy | IB1:24 |
| [V] | Kanbier, G. | Security Café: Fraude & security | IB3:26 |
| [A] | Kanbier, G. | Data Risk Management | IB7:12 |
| [A] | Kersten, F. | De CBP-Richtsnoeren nader beschouwd | IB1:8 |
| [O] | Klaver, M. e.a. | Open brief aan Frans Bolk | IB7:7 |
| [O] | Koeroo, O. e.a. | Open brief aan Frans Bolk | IB7:7 |
| [A] | Kompanje, H. | Beveiliging is niet alleen een zaak van de IT-afdeling | IB1:20 |
| [A] | Koot, A. | Waar begint de cirkel | IB3:14 |
| [I] | Koot, A. | John McClurg | IB4:14 |
| [A] | Koot, M. | De Logius-norm voor DigiD: perikelen bij technisch testen | IB5:10 |
| [O] | Lahaye, J. e.a. | Open brief aan Frans Bolk | IB7:7 |
| [V ] | Luiijf, E. | Nationale Cyber Security Strategie 2 | IB2:16 |
| [V] | Mendrik, J. | Een bloeiend Privacy Platform | IB2:25 |
| [A] | Niamat, R. | Wat betekent het voor internetbedrijven "vitale infrastructuur" te zijn? | IB1:4 |
| [V] | Niamat, R. | Secure Cloud 2014: Een bijzondere conferentie over een bekend thema | IB6:22 |
| [O] | Niamat, R. e.a. | Open brief aan Frans Bolk | IB7:7 |
| [A] | Nieuwenhuize, L. e.a. | Hoe krijg je ze mee? | IB7:16 |
| [A] | Niggebrugge, D. e.a. | Klik, klik, klik het geluid van een gezonde werkvloer | IB6:8 |
| [V] | Noord, F. van e.a. | Kwalificatiestelstel van Informatiebeveiligers | IB2:18 |
| [A] | Noord, F. van e.a. | Kwalificatiestelsel op basis van e-CF | IB4:24 |
| [A] | Orsouw, P. Van e.a. | Big Data: herijking noodzakelijk | IB3:10 |
| [A] | Oud, E. | ISO27001 herzien | IB2:10 |

Jaaroverzicht 2014

| | | | |
|---|---|---|---|
| [A] | Pols, P. e.a. | Klik, klik, klik het geluid van een gezonde werkvloer | IB6:8 |
| [A] | Rampersad, D. e.a. | Hoe krijg je ze mee? | IB7:16 |
| [A] | Rogaar, P. | Heartbleed | IB4:4 |
| [A] | Siebelink, N. | Het begint met goede hygiëne | IB7:4 |
| [V] | Spruit, M. e.a. | Kwalificatiestelstel van Informatiebeveiligers | IB2:18 |
| [A] | Spruit, M. e.a. | Kwalificatiestelsel op basis van e-CF | IB4:24 |
| [V] | Veenman, C. e.a. | Het Forensic Intelligence Network of Excellence (FINE) | IB8:18 |
| [A] | Verburg, W. e.a | Big Data: herijking noodzakelijk | IB3:10 |
| [A] | Vernède, R. | Vulnerability scanning | IB8:8 |
| [V] | Worring, M. e.a | Het Forensic Intelligence Network of Excellence (FINE) | IB8:18 |
| [A] | Zwinkels, C. | Hoe gaan we om met regelgeving? | IB5:4 |

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

## Thema's

IB1 Complexe samenleving
IB2 Weerbaarheid
IB3 Security by design
IB4 Cybereducatie
IB5 NL Cyberland
IB6 Hacken
IB7 Shellshock
IB8 Dreigingen & kwetsbaarheden

## Achter het nieuws

Een nieuw jaar, nieuwe bedreigingen? - IB1:30
Bewaarplicht telecomdata nog wel van deze tijd? - IB2:28
Advertenties op websites verbieden? - IB3:28
Heartbleed kwetsbaarheid - IB4:28
Nederland kan spijkers met koppen slaan in het cyberdomein - IB5:28
Internet of Things - IB6:33
Heartbleed, Shellshock: is open source onveilig? - IB7:28
Terugblikken en vooruit kijken - IB8:28

## Column Attributer

Integrity Protected - IB1:15
Owned - IB2:15
Risk Managed - IB3:19
Patched - IB4:27
BYOD Enabled - IB5:24
Smart Secured - IB6:27
Shellshocked - IB7:27
Justified - IB8:23

## Column Berry

Alles zelf op het internet doen - IB1:35
Winkelen wordt eng - IB2:31
Wat moet ik nu? - IB3:31
Betrouwbare Beroepen - IB4:31
Slimme hackers of domme gebruikers - IB5:31
To hack or not to hack - IB6:35
De cybercrimineel - IB7:31
Wie is u? - IB8:31

## Boekbespreking

No place to hide - IB6:32
Grip op ICS security - IB8:21
Wake up and smell the value: witboek voor leiders - IB8:22

## Column Privacy

De wedergeboorte van privacy - IB1:7
Het recept voor privacyvriendelijk innoveren - IB2:9
Achter de linies - IB3:9
Wat nu als je ineens niet meer bestaat? - IB4:7
De digitale wereld is een grenzeloze datagraaibak - IB5:8
Parc@ing: ik weet waar je je bips parkeert poesje! - IB6:13
Hoe om te gaan met een onveilige haven? - IB7:15
Je zult maar ziek zijn - IB8:13

## Verantwoorde onthullingen

#4: "I Hacked KPN, and all I got was this lousy t-shirt." - IB1:27
#5: Dongit en het DigiD Debacle - IB2:22
#6: Dismantling Megamos - IB3:22
#7: Student geeft universiteit dure les - IB4:16
#8: Autorisatie Infinitas Uitgeverijen makkelijk te omzeilen - IB5:18
#9: Te goedkoop voor security? - IB6:28
#10: Terugkijken - IB7:24
#11: Beg en de Bug Bounty - IB8:24

## Voorwoord

Complexe samenleving - IB1:3
Privacy weerbaarheid - IB2:3
Security sprint - IB3:3
Browser afhankelijkheid - IB4:3
Privacy issues - IB5:3
De Berlijnse muur - IB6:3
Business value - IB7:3
Inefficiënte informatieoverload - IB8:3

# COLOFON

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

PvIB
Platform voor InformatieBeveiliging

**REDACTIE**
Lex Borger (hoofdredacteur, werkzaam bij i-to-i)
e-mail: hr@pvib.nl
Motivation Office Support bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

**REDACTIERAAD**
Tom Bakker (Digidentity BV)
Kas Clark (NCSC)
Lex Dunn (Capgemini)
Maarten Hartsuijker (Classity)
André Koot (Strict)
Rachel Marbus (NS, IT Advisory)
Bart van Staveren (UWV)

**ADVERTENTIE ACQUISITIE**
e-mail: adverteren@pvib.nl;
of neem contact op met MOS
(Motivation Office Support)
T (033) 247 34 00
ibmagazine@pvib.nl

**VORMGEVING EN DRUK**
VdR druk & print, Nijkerk
www.vdr.nl

**UITGEVER**
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
F (033) 246 04 70
e-mail: secretariaat@pvib.nl
website: www.pvib.nl

**ABONNEMENTEN 2015**
De abonnementsprijs in 2015 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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


ISSN 1569-1063

# HARDLEERS

Soms denk je dat ieder mens, maar zeker ieder bedrijf leert van de fouten die ze in het verleden hebben gemaakt. Neem nu (zomaar een willekeurig voorbeeld) een bedrijf als Sony. Een aantal jaren geplaagd door een hack op hun zogenaamde Playstation waarbij het niet alleen een probleem was met de bereikbaarheid van de "playground" van de Playstation fanaten, maar eveneens de diefstal van heel veel accounts inclusief de creditcardgegevens. Sony maakte later bekend dat er 77 miljoen accounts waren gestolen. De hack in 2011 heeft erg veel impact gehad op de bedrijfsvoering van Sony. Het vertrouwen bij veel klanten was weg en de winsten van Sony lagen erg onder druk. Topmannen werden weg bevorderd of gewoon ontslagen.

Nu is ieder bedrijf of ieder mens zelf lerend, hetgeen al op zeer vroege leeftijd begint. Een kleuter die zijn vingers tegen de kachel houdt,  zal dat over het algemeen niet voor een tweede keer doen, ezels stoten zich ook slechts eenmaal aan een steen, maar de arrogantie van Sony kent geen grenzen.

Wederom heeft er een grootschalige hack plaatsgevonden (of vindt nog steeds plaats) waar veel documenten zijn ontvreemd. Sony doet eerst luchtig over de hack, maar naarmate de tijd vordert worden ze stiller. Sony's medewerkers moeten met hun persoonlijke emailadressen gaan communiceren, omdat het eigen netwerk niet meer opgestart kan worden.

Er verschijnen films in het illegale circuit die nog niet eens gepubliceerd zijn, afbeeldingen van paspoorten van acteurs die voor Sony hebben gespeeld zwerven rond op het internet. Contracten van acteurs zijn inmiddels voor een ieder inzichtelijk en worden gebruikt om de onderhandelingspositie van nieuwe acteurs te versterken. Sony heeft in een perspublicatie laten weten dat erg kinderachtig te vinden. Sony heeft op basis van dreigementen, van naar verluidt Noord Koreaanse hackers, moeten besluiten om de film "The Interview" terug te trekken uit de bioscopen. Een strop van honderden miljoenen dollars. Sony geeft aan dat de film ook niet uitgebracht zal worden op DVD of Blue Ray. Hiermee toont Sony aan er helemaal niets van te begrijpen. Ik heb de film inmiddels gedownload en bekeken en ik vind het niet een heel sterke film. Er wordt een belachelijke wereldleider nog belachelijker gemaakt dan hij al is. Ik begrijp de drukte niet. Sony denkt dat niemand de film te zien krijgt. Sony denkt dat niemand de nog uit te brengen Sony Experia telefoon heeft gezien waar James Bond 5 miljoen euro voor krijgt als hij die in de nog te filmen James Bond gaat gebruiken. Google er maar eens op en je zult hem aantreffen.

Overigens zie ik wel heel veel redenen om het toestel niet aan te schaffen. Voordat je het weet zwerven mijn gegevens over internet, ik lek ze liever via de iCloud van Apple. Ik wens Sony een veilig 2015 toe en hoop voor ze dat ze 2016 gaan halen. Ik heb in ieder geval besloten de netwerk kabel maar uit mijn Sony Bravia HDTV te trekken, ga wel op mijn laptop kijken.

**Berry**

Secure Link
Infrastructure Security Solutions



# Gezocht!
# Security Engineers

SecureLink groeit en is op zoek naar Security Engineers die ons team komen versterken!

Als Security Engineer heb je diepgaande kennis op het gebied van security en networking. De combinatie van enerzijds de security technologie en anderzijds de integratie met networking is iets waar jij al jouw energie en expertise in kwijt kunt. Je krijgt de ruimte zelfstandig complexe security en networking projecten van A tot Z uit te voeren.

Benieuwd? Kijk dan op www.securelink.nl/vacatures




## Kom jij ons team versterken?

Sinds de oprichting van SecureLink in 2003 managen en realiseren wij als security en networking integrator met ruim honderdtachtig SecureLinkers, verdeeld over drie vestigingen in Nederland en België, enterprise security architecturen én een hoger security niveau.

## Go Secure!

SecureLink Nederland B.V. | Trapezium 224 | 3364 DL Sliedrecht | T +31 88 1234 200 | info@securelink.nl