INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 2 - 2011

AANPAK VAN KINDERPORNOGRAFIE OP INTERNET

HIGH SECURITY, HUMAN SIGNIFICANCE

FACEBOOK VOLGT IEDERE INTERNETGEBRUIKER: LIKE THIS!

CLOUD BEVEILIGINGSVERWACHTINGEN VOOR 2011

NOMINATIES VOOR ARTIKEL VAN HET JAAR 2010

VOORWOORD

Beste lezers,
Mijn eerste voorwoord als hoofdredacteur. Voor mijzelf een mijlpaal, maar voor jullie als lezers hopelijk een herkenning en voortzetting van datgene waar het blad Informatiebeveiliging al weer geruime tijd voor staat: interessante inhoud leveren voor de leden op ons vakgebied. Ik wil deze traditie voortzetten en het blad tot iets maken wat zichzelf in stand kan houden. De tijd om daar nu iets over te melden is te kort geweest, daarover dus in een latere uitgave meer.
Wie in mijn voorwoord een leeswijzer voor het blad verwacht komt bedrogen uit. Het blad heeft mijn voorwoord niet nodig om toegankelijk te zijn. Ik wil iets prikkelends neerleggen bij jullie, zoals een amuse. Hierbij dan mijn eerste.
Aan het begin van het jaar word je geconfronteerd met heel veel voorspellingen vanuit verschillende bronnen. Ik lees die graag. Een voorspelling lijkt er dit jaar uit te springen. We krijgen meer aanvallen zoals Stuxnet. Dat denk ik juist niet. Stuxnet was zo geavanceerd en al die informatie is u bekend, er zal een aantal jaren nodig zijn voordat dit kunstje weer getopt zal kunnen worden. Moeten we ons dan veilig wanen? Nee! Ik waag me aan een paar voorspellingen.
Dit jaar komt er een geslaagde publieke aanval op het GSM-verkeer. Men slaagt er in om een aantal belangrijke mobiele gesprekken op te vangen en dit ten nadele van de bellers publiekelijk uit te buiten. Het is al aangetoond dat het mogelijk is. We gaan het nu ook op korte termijn zien gebeuren.

Microsoft en Adobe zijn voor de internetonderwereld al jaren het meest lonende doelwit. Komend jaar gaat er een grote malwareplaag komen op ten minste een van de grote nieuwe mobiele platformen: Apple's IOS of Google's Android.
Ik had ook nog iets willen zeggen over een responsible disclosure schandaal, maar dat is inmiddels binnen. Dat zou scoren voor open doel zijn.
Als laatste verwacht ik dat we in het komende jaar ook eindelijk zullen begrijpen wat 'cloud security' nu echt inhoudt en het daarover ook met elkaar eens worden. Of is dit een wens? Ik twijfel nog…

Dit soort voorspellingen creëert impliciet ook de belofte dat ik hier over een jaar op terug moet komen. Dat ga ik zeker doen en ik kijk er zelfs naar vooruit!

Lex Borger
hoofdredacteur

Foto omslag: CarbonNYC via Flickr

INHOUDSOPGAVE

AANPAK VAN KINDERPORNOGRAFIE OP INTERNET

Mr. J.J. (Jan-Jaap) Oerlemans is juridisch adviseur bij Fox-IT. Tevens is hij promovendus bij de Universiteit Leiden. Jan-Jaap is bereikbaar op oerlemans@fox-it.com.

Robert M. heeft de Nederlandse samenleving met zijn neus op de feiten gedrukt wat betreft het probleem van kinderpornografie. In december 2010 kwamen de gruwelijke details naar voren in de zedenzaak van het jaar. Niet alleen heeft hij zich zeer waarschijnlijk aan peuters vergrepen, hij exploiteerde daarnaast wellicht ook een netwerk waarbinnen mensen kinderpornografie konden uitwisselen. Robert M. kan daarom worden vervolgd voor zowel bezit, verspreiding en vervaardiging van kinderpornografie alsmede kindermisbruik.

Helaas is Robert M. een 'atypisch' geval. Meestal worden 'eenvoudige' downloaders voor het bezit van kinderpornografie vervolgd. Het huidige beleid ter bestrijding van kinderporno is daarom een druppel op de gloeiende plaat op de wereldwijde markt van kinderpornografie. De politie en het OM komen niet meer toe aan de vervolging van verspreiders en vervaardigers van kinderporno en hierdoor blijven de ergste kinderpornogebruikers buiten het beeld van opsporingsinstanties.

Uitdijing van de strafbaarstelling van kinderpornografie

Kinderpornografie is een afbeelding (foto of video) van een seksuele gedraging waarbij iemand die kennelijk jonger is dan achttien jaar is betrokken. Die seksuele gedraging hoeft geen daadwerkelijk misbruik van een minderjarige te zijn, maar kan bijvoorbeeld ook een foto van een geslachtsdeel van een minderjarige zijn. Op dit moment is het bezitten, vervaardigen, verspreiden, invoeren, doorvoeren, uitvoeren, openlijk tentoonstellen van, betrokken zijn met en toegang verschaffen tot kinderpornografie in artikel 240b van het Wetboek van Strafrecht strafbaar gesteld.

De strafbaarstelling van kinderporno is in de loop der jaren enorm uitgebreid. In 2000 is bijvoorbeeld de leeftijd voor kinderpornografie naar aanleiding van een internationaal verdrag van 16 jaar naar 18 jaar verhoogd. Waar in 1985 de maximale gevangenisstraf voor kinderpornografie nog 3 maanden betrof, kan men nu maximaal 8 jaar gevangenisstraf krijgen als een gewoonte wordt gemaakt van de hierboven beschreven gedragingen. Er is sprake van een gewoonte indien de verdachte gedurende een langere periode het materiaal voorhanden heeft gehad. In de meest recente wetswijziging is (terecht) het toegang verschaffen van kinderpornografie strafbaar gesteld. Hierdoor valt ook het online bekijken - via 'streaming video' – van kinderporno onder artikel 240b. Virtuele kinderporno is sinds 2002 strafbaar gesteld. Dat betekent dat er geen echte kinderen meer betrokken hoeven zijn om te spreken van 'kinderpornografisch materiaal'. Bij virtuele kinderpornografie moet het gaan om 'realistisch' materiaal, dat voor kinderen

> Feit is alleen wel dat het probleem alleen maar groter wordt

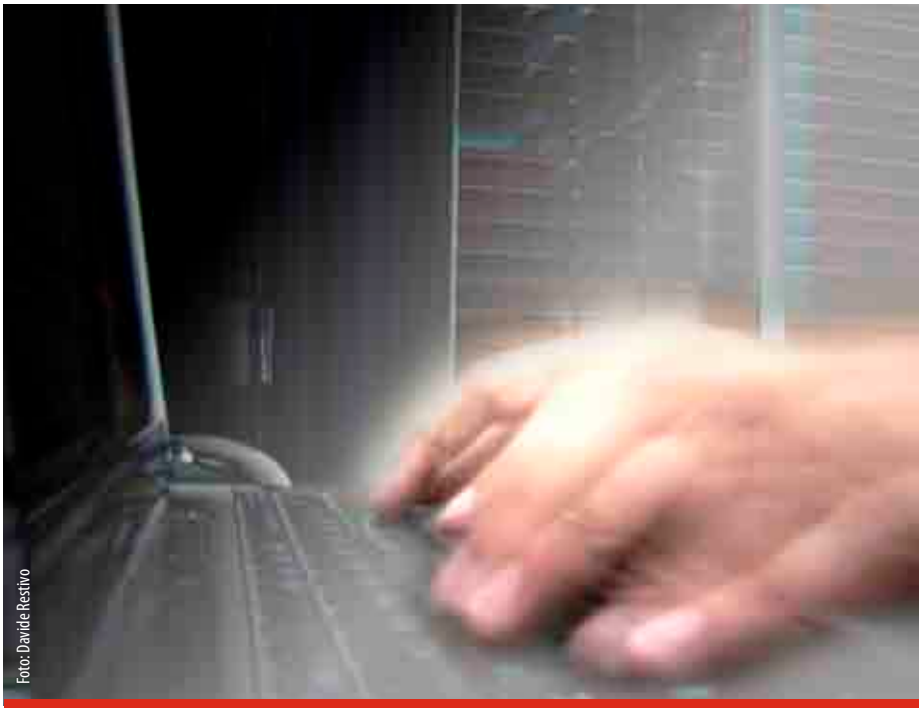


Foto: Davide Restivo

Keyboard fingers

niet van echt te onderscheiden is. Door de rechtbank 's-Hertogenbosch werd een filmpje met een driedimensionaal geanimeerd kind dat seksuele handelingen verrichtte als kinderpornografie gekwalificeerd[1]. Cartoons en andere onrealistische animaties waarbij minderjarigen zijn te zien vallen vooralsnog in Nederland niet onder kinderpornografie.

De uitdijing van de strafbaarstelling kinderpornografie kan worden gezien als een reactie op de maatschappelijke verontwaardiging bij kinderpornografie. Praktisch iedereen vindt kinderpornografie moreel verwerpelijk. Per slot van rekening vindt bij de productie van kinderporno vaak kindermisbruik plaats. Feit is alleen wel dat het probleem alleen maar groter wordt. De stormachtige ontwikkeling van het internet in de afgelopen decennia heeft geleid tot een revolutie in de verspreiding van kinderpornografie. Waar eerst kinderpornografie in seksshops werd verkocht of via een postbedrijf werd verspreid, kan kinderpornografie nu razendsnel in de vorm van bits en bytes over de hele wereld via het internet worden verspreid. Door de exponentiële groei in de opslagcapaciteit van gegevensdragers en snellere internetverbindingen kan kinderpornografie in enorme hoeveelheden worden verspreid en gedownload. Collecties van duizenden of tienduizenden afbeeldingen en video's met kinderpornografie komen tegenwoordig vaak voor. Recentelijk zijn zelfs collecties van meer dan een miljoen afbeeldingen en video's met kinderpornografie aangetroffen[2]. Evenzo zorgelijk is dat volgens het 'Verbeterprogramma kinderporno' het in beslag genomen kinderpornografisch materiaal de laatste jaren steeds grover en gewelddadiger lijkt te worden.

Blijkbaar heeft de huidige aanpak van kinderpornografie onvoldoende effect op de markt van kinderpornografie om een effectieve slag toe te brengen.


foto: Teofilo

Scale of justice carrying putto (Triumph of the Republic)

Aanpak van kinderpornografie

In 2008 en 2009 gingen de meeste zaken puur om het bezit van kinderpornografie en dat was ook het enige dat in deze zaken ten laste werd gelegd en bewezen is[3]. Lünnemann en anderen zeggen hierover in hun rapport: *"Alle respondenten wijzen erop dat meestal eindgebruikers worden vervolgd en dit blijkt eveneens uit het dossieronderzoek."*[4] Dat de focus van de vervolgingen in de praktijk ligt bij de bezitters van kinderpornografie blijkt verder ook uit het Verbeterprogramma Kinderporno[5] en de Korpsmonitor Kinderporno[6]. Afgelopen november hield het Openbaar Ministerie nog een themazitting 'bezit van kinderporno' waarbij acht bezitters werden vervolgd. In het persbericht hierover redeneert het OM over de bezitters als volgt: *"Hierdoor zijn zij volgens het OM mede verantwoordelijk voor het in stand houden van het maken en verspreiden van kinderporno. Kort gezegd; zolang er kopers zijn, zijn er ook mensen die het materiaal produceren of verspreiden."*

Het vervolgen van enkele bezitters (vergeleken met het werkelijke aantal downloaders op wereldwijde schaal) is slechts een druppel op de gloeiende plaat in de markt van kinderpornografie. Het vervolgen van vooral bezitters van kinderpornografie brengt daarom geen effectieve slag op de wereldwijde markt van kinderpornografie. Dit wordt in de Richtlijn Kinderpornografie bevestigd: *"Alhoewel ook het bezit van kinderporno al bijdraagt aan de instandhouding van een 'markt' voor kinderpornografisch materiaal, leveren laatstgenoemde activiteiten de relatief grootste bijdragen aan de instandhouding van een 'markt' voor kinderpornografisch materiaal, de seksuele exploitatie van kinderen en de voortduring van het slachtofferschap van misbruikte kinderen."*

> Huidige aanpak van kinderpornografie onvoldoende effect

Officieel is de Richtlijn Kinderpornografie richtinggevend voor het vervolgingsbeleid in kinderpornografiezaken. Gezien het hoge aantal zaken met betrekking tot artikel 240b moet er nu eenmaal geprioriteerd worden en deze richtlijn biedt hiervoor uitstekende aanknopingspunten. Naast dat meer prioriteit moet gaan naar verspreiders en vervaardigers van kinderpornografie

kan worden geprioriteerd op basis van drie factoren:

- de aard van de afbeeldingen (is er sprake van een seksuele handeling of wordt bijvoorbeeld ingezoomd op een geslachtsdeel van een kind?);
- de leeftijd van de slachtoffers (prepuberale kinderpornografie moet meer prioriteit krijgen dan 12 jaar en ouder);
- de periode waartussen de activiteiten werden gericht (bij nieuw materiaal is er sprake van nieuw misbruik van kinderen en daar moet meer prioriteit aan worden verleend).

Zoals is aangegeven worden in de praktijk vooral 'eenvoudige' downloaders voor kinderpornografie vervolgd. Dit roept natuurlijk de vraag op: *waarom wordt de richtlijn niet nageleefd?*

> Het vervolgen van enkele bezitters is een druppel op de gloeiende plaat

Capaciteitsgebrek

Eerder is aangegeven dat de collecties van kinderpornografieverzamelaars uit honderdduizenden afbeeldingen kunnen bestaan en steeds maar groter worden. Het analyseren van deze verzamelingen door middel van digitaal forensisch onderzoek duurt ontzettend lang en kost veel capaciteit. Daar komt bij dat in omvangrijke onderzoeken het vaak niet om een, maar meerdere downloaders gaat. De Landslide-zaak uit 2002 illustreert dat bijvoorbeeld goed. Het bedrijf Landslide Productions Inc. beheerde een website waarop abonnementen voor toegang naar kinderpornowebsites werden verkocht. Tijdens het onderzoek naar dit bedrijf bleek dat er alleen al 35.000 mensen in de Verenigde Staten waren geabonneerd[7]. In het Verenigd Koninkrijk werd naar ongeveer 6500 Britse abonnees een onderzoek ingesteld[8].
Ook wordt wel aangevoerd dat zedenrechercheurs pas na onderzoek weten of het om een bezitter, verspreider of vervaardiger gaat. Volgens het jaarbericht van het OM blijft door capaciteitsgebrek bij de politie de bestrijding van kinderporno in veel gevallen beperkt tot het aantonen van bezit en blijven, vanwege de grote werkvoorraad, vervaardigers en verspreiders nog te veel ongemoeid.

Toch lijkt het niet alleen maar 'noodzaak' te zijn. In zijn beleid lijkt het OM bewust aan te sturen op de vervolging van bezitters en niet zo zeer op basis van de richtlijn te prioriteren. Dat blijkt wel uit de benaming van zijn themazitting van afgelopen november: '*bezit* van kinderporno'. Als succesverhaal in zijn jaarbericht van 2009 haalt het OM bovendien een zaak aan over 'twijfelmateriaal' (het ging hier om geklede kinderen in erotische poses) dat de rechter onder kinderpornografie heeft geschaard. Op basis van de Richtlijn Kinderpornografie moet hieraan juist de *minste* prioriteit worden verleend. Verder blijkt uit onderzoek van Leukfeldt en anderen dat bijna een kwart (23,8%) van de onderzochte groep kinderpornoverdachten in de leeftijdsgroep van 12-24 jaar valt. Het is goed voor te stellen dat een puber met een smartphone een naaktfoto van zijn vriend of vriendin maakt en de foto doorstuurt naar vrienden 'om stoer te doen'. In dat geval kan vervolgd worden voor bezit, verspreiding en vervaardiging van kinderpornografie. Met een overheidscampagne zouden pubers en adolescenten er op moeten worden gewezen dat dit gedrag strafwaardig is en de privacy van de betrokkenen aantast. Maar ik vind het geen goed idee deze mensen via het strafrechtelijk circuit aan te pakken. De focus zou moeten blijven liggen op die vormen van kinderpornografie waar de Richtlijn Kinderpornografie de meeste prioriteit aan verleent. Zaken met een lage prioriteit, zoals zaken met 'eenvoudige downloaders', virtuele kinderpornografie en twijfelgevallen moeten wat mij betreft geseponeerd worden of op een andere manier worden afgedaan om capaciteit vrij te maken voor de vervolging van verspreiders en vervaardigers. Op dit moment worden veel kinderpornografiezaken nog op regionaal niveau opgepakt, met grote verschillen in het beleid van de regiokorpsen. Gezien de vaak (technisch) complexe zaken en internationale dimensie van het probleem moet kinderpornografie naar mijn mening op landelijk niveau - en niet op regionaal niveau - worden aangepakt.

Kennisgebrek

Helaas is een tendens zichtbaar dat de handel in kinderporno verschuift naar locaties op internet waar de informatie moeilijker te observeren is[9]. Kinderpornogebruikers maken namelijk steeds vaker slim gebruik van nieuwe technische mogelijkheden en verschillende jurisdicties en dat frustreert de opsporing. Kinderpornografie kan

Foto: Bill Tyne

bijvoorbeeld binnen besloten peer-to-peer-netwerken (ook wel darknets genoemd) worden uitgewisseld. Aangezien men alleen op uitnodiging in dergelijke netwerken kan komen vindt deze uitwisseling grotendeels buiten het beeld van opsporingsdiensten plaats.
De meer technisch onderlegde kinderpornogebruikers maken bovendien veel gebruik van versleuteltechnieken. Het communicatieverkeer kan bijvoorbeeld worden versleuteld, zodat een internettap grotendeels onbruikbaar wordt. Data op een gegevensdrager kan ook worden versleuteld. In de media is veel ophef geweest over het gebruik van cryptografie door Robert M. Hij gebruikte naar verluidt het programma 'Truecrypt' om bepaalde data op zijn harde schijf te versleutelen, waar vermoedelijk kinderpornografie op te vinden was. Verdachten zijn niet verplicht een sleutel af te geven, omdat zij niet hoeven mee te werken aan hun eigen veroordeling[10]. Gelukkig heeft Robert M. zijn sleutel vrijwillig afgestaan, zodat in elk geval een deel van de kinderpornografieverzameling kan worden geanalyseerd.
Ten slotte speelt er een groot jurisdictieprobleem op internet. Kinderpornografisch materiaal kan binnen een paar uur veelvuldig in verschillende landen worden gehost. Dit frustreert de opsporing, omdat de inzet van opsporingsbevoegdheden van de Nederlandse politie en justitie bij de grens ophoudt. Dit geldt ook voor opsporingshandelingen op internet. Door middel van een rechtshulpverzoek aan een ander land mogen opsporingsbevoegdheden soms toch worden ingezet, maar rechtshulpverzoeken brengen altijd vertraging met zich mee. De snelheid waarmee dit soort verzoeken worden afgehandeld is afhankelijk van de prioriteitstelling van de zaak in het aangezochte land.


Lady Justice

Politie en justitie kunnen maar moeilijk omgaan met deze complexe vorm van cybercrime. Kinderpornogebruikers die niet van dit soort technieken en jurisdictieverschillen gebruikmaken, zijn gemakkelijker op sporen en te vervolgen en dat speelt de opsporing in de kaart[11]. Een zedenrechercheur noemt de meeste verdachten in een interview met het politieblad 'Blauw' zelfs 'sukkels'[12]. Overigens wordt er ook vanuit de politiek naar mijn mening weinig constructief gehandeld. In het meest recente debat van 10 januari 2011 ligt de focus opnieuw op het terugdringen van het aantal plankzaken met vooral downloaders[13]. Staatssecretaris Teeven: *"De meeste aandacht bij het verbeteren van de aanpak van kinderporno gaat nu primair uit naar het terugdringen van de werkvoorraad. (…) Ik onderschrijf nog steeds met alle andere partners in het veld de wens en de noodzaak om de focus in de opsporing verder te verleggen van downloaders naar misbruikers en producenten. Op dit moment is de politie echter substantieel meer capaciteit kwijt aan het verwerken van het werkaanbod van grotendeels downloadzaken."* Wel wordt gespeeld met de gedachte dat downloaders een bezoek krijgen van de politie met daarbij een voorstel een hulptraject in te gaan. Zolang politici niet bereid zijn het probleem te onderkennen, kan kinderpornografie niet effectief worden aangepakt. Er moeten nu eenmaal keuzes worden gemaakt. Niet alle zaken met kinderpornografie kunnen worden opgepakt.

Complexe vorm cybercrime moeilijk voor politie en justitie

Kortom, teneinde de meer technisch onderlegde kinderpornografiegebruikers aan te pakken moet er meer kennis en expertise bij politie en justitie over de aanpak van cybercrime komen. Gaan de politie en het OM (al dan niet door politieke druk) door met hun huidige focus op de 'eenvoudige downloader', dan verzuipt men in het aantal kinderpornografiezaken zonder dat de juiste personen worden opgepakt.

Andere aanpak van kinderpornografie
Traditioneel doet de politie vooral aan reactieve opsporing. Naar aanleiding van een melding of andere zaak begint de politie in overleg met een officier van justitie een opsporingsonderzoek en wordt een computer of andere gegevensdrager in beslag genomen. Op de gegevensdrager kan kinderporno worden gevonden en na digitaal forensisch onderzoek is duidelijk hoeveel en welk materiaal het precies betreft. Alleen met 'doorrechercheren' kan worden nagegaan of de kinderpornogebruiker een bezitter, verspreider of vervaardiger is, welk materiaal het betreft en kan eventueel het slachtoffer worden geïdentificeerd.
De politie kan in opdracht van de officier van justitie zich echter ook van begin af aan richten op verspreiders

en vervaardigers door aan *proactieve* opsporing te doen. Hierbij wacht de politie geen melding van kinderpornografie af, maar neemt zelf het initiatief. Aangezien de wereld van kinderpornografie zich in vergaande mate ondergronds afspeelt, komen opsporingsinstanties al gauw tot de inzet van bijzondere opsporingsbevoegdheden. Daarbij kan bijvoorbeeld gedacht worden aan de bevoegdheid van infiltratie om een netwerk van kinderpornografiegebruikers in kaart te brengen. Hierbij speelt het dilemma dat soms strafbare feiten moeten worden gepleegd om toegang te verschaffen tot een dergelijk netwerk. Juridisch gezien zou infiltratie, ondanks de formaliteiten en zware waarborgen die voor deze bijzondere opsporingsbevoegdheid gelden, mogelijk moeten zijn. In het kader van de pseudokoopbevoegdheid zou men zich ook met een 'politiecreditcard' toegang kunnen verschaffen tot een website of andere locatie waarop kinderpornografie wordt aangeboden. Wanneer het IP-adres bekend is, kunnen identificerende gegevens gevorderd worden bij een Internet Service Provider (ISP) of andere instantie. Indien de kinderpornogebruiker bijvoorbeeld een proxyserver gebruikt om zijn IP-adres af te schermen dan zou men bijvoorbeeld loggegevens bij de proxydienstverlener kunnen vorderen. Is de kinderpornografiegebruiker uiteindelijk geïdentificeerd, dan kan met een internettap zijn communicatieverkeer in kaart worden gebracht. Indien de verdachte gebruikmaakt van versleuteling, kunnen toetsaanslagen (en wachtwoord) worden afgevangen met een keylogger. Op die manier kan het versleutelde verkeer weer leesbaar worden gemaakt. Op dit moment is dat echter alleen mogelijk door het huis van de verdachte te betreden en dan een keylogger op zijn computer te plaatsen. De keylogger kan dus niet op afstand (door in te breken op de computer van de verdachte) worden geplaatst. Dit komt wat ouderwets op mij over en de wetgever zou kunnen overwegen dit plaatsen op afstand met een wetswijziging mogelijk te maken. Echter, uit onderzoek naar de knelpunten in de bestrijding van cybercrime blijkt dat op dit moment voor de politie en het OM nog onvoldoende duidelijk is hoe (bijzondere) opsporingsbevoegdheden op internet überhaupt kunnen worden ingezet[14]. Toch zijn er, voor zover ik weet, geen initiatieven genomen deze mogelijkheden in kaart te brengen. Ook in de toelichting op het nieuwe conceptwetsvoorstel Computercriminaliteit III wordt dit probleem geconstateerd, maar in het conceptvoorstel wordt daar verder niets mee gedaan[15].

Focus van downloader naar verspreiders en vervaardigers

Ten slotte kan men door slim gebruik te maken van de strategische positie die bedrijven zoals ISP's en aanbieders van betalingsdiensten hebben, kinderpornografie effectiever opsporen. In de vorige alinea is beschreven dat bijvoorbeeld (identificerende of andere) gegevens gevorderd kunnen worden. Die gegevens zijn vaak van cruciaal belang in een opsporingsonderzoek. In tegenstelling tot de regering ben ik wat minder enthousiast over publiek-private samenwerking. Het filteren van kinderporno door middel van zwarte lijsten na bemiddeling van het 'Platform Internetveiligheid' is bijvoorbeeld geen onverdeeld succes te noemen. Uit onderzoek blijkt dat deze filtertechniek niet effectief is en gemakkelijk kan worden omzeild. Met deze technische oplossing gaat men slechts het gevolg van kinderpornografie tegen. Liever zou ik zien dat met recherchewerk op internet kinderpornografie bij de bron wordt aangepakt.

Tot slot

Hopelijk maakt de Robert M.-zaak duidelijk waar werkelijk het probleem van kinderpornografie ligt. Verspreiders en vervaardigers mogen niet ongestraft hun gang gaan, maar om dat te bereiken moet eerst het beleid ter bestrijding van kinderpornografie worden veranderd.

[1] Uitspraak van de Rechtbank 's-Hertogenbosch van 4 februari 2008 (LJN BC3225).

[2] Zie bijvoorbeeld de uitspraak van de rechtbank Rotterdam van 9 december 2009 (LJN BK6022) en rechtbank Rotterdam van 10 juni 2009 (LJN BI7331).

[3] Dit is gebaseerd op de analyse van 274 uitspraken op http://www.rechtspraak.nl op de zoekterm '240b' in het tijdsbestek van 2000 tot en met 2009. Zie J.J. Oerlemans, Opsporing en bestrijding van kinderpornografie op internet, 2010 (Juncto reeks: nr. 59), p. 123-143.

[4] K. Lünnemann e.a. Kinderen beschermd tegen seksueel misbruik, Utrecht: Verwey-Jonker Instituut 2006, p. 108.

[5] Politie, landelijk project kinderporno, Verbeterprogramma Kinderporno, 2008, p. 14.

[6] D. Janssen & P. Reijnders, Stand van zaken 2009, Korpsmonitor Kinderporno, Landelijk beeld, versie 1.1., 18 november 2009, p. 20.

[7] M. Taylor & E. Quayle, Child pornography: an internet crime, Hove: Brunner-Routledge 2003, p. 5.

[8] Y. Akdeniz, Internet Child Pornography and the Law, Ashgate 2008, p. 26 en 27.

[9] Zie W.Ph. Stol, 'Trends in Cybercrime', Justitiële verkenningen 2004, (8), p. 88.

[10] Zie uitgebreid B.J. Koops Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?, Deventer: Kluwer, 2000 (ITeR-Reeks, nr. 31).

[11] Zie ook W.Ph. Stol, 'Trends in Cybercrime', Justitiële verkenningen 2004, (8), p. 78.

[12] 'Een eeuwige strijd, Kinderporno neemt snel toe', Blauw – Recherche, 3 februari 2007, nummer 3, p. 20: Het zijn dan ook vooral de 'sukkels' die Marcel Nek naar eigen zeggen tegenkomt in zijn werk. (…) 'De echte slimmerds zijn heel moeilijk te achterhalen.'"

[13] Verslag van het algemeen overleg over de brief met het eerste voortgangsbericht 2010 over de aanpak van kinderpornografie. Kamerstukken II 2010/11, 32500VI, nr. 75.

[14] Brief van de minister van Justitie 'Naar een veiliger samenleving'. Kamerstukken II 2008/09, 28684, nr. 232.

[15] Zie voor meer informatie J.J. Oerlemans, 'Het conceptwetsvoorstel versterking bestrijding computercriminaliteit nader bezien', Tijdschrift voor Internetrecht, nr. 5, 2010.

De belangrijkste missie van IDentity.Next is om een open en onafhankelijk platform te kunnen bieden dat staat voor ondersteuning en faciliteren van innovatieve benaderingen in de wereld van de digitale identiteit. Met als voornaamste doel disseminatie van kennis, expertise en ervaring door het organiseren van evenementen en workshops enz. op een verscheidenheid aan thema's, gemaakt van en door expertises binnen de wereld van IT en Business en Marketeers.

DE EERSTE IDENTITY.NEXT IN DEN HAAG

Robert L. Garskamp is werkzaam als projectmanager bij Everett en founder of IDentity.Next. Hij is per e-mail bereikbaar via robert.garskamp@everett.nl

Op 8 december 2010 vond de eerste IDentity.Next plaats op een zeer unieke locatie in Den Haag, de Fokker Terminal. Bij Identity.Next kwamen honderd deelnemers bijeen om zich te laten inspireren, te netwerken en ontwikkelingen met elkaar te kunnen uitwisselen rondom het onderwerp 'de digitale identiteit'. Het PvIB was een vriend van dit evenement, waardoor ook veel PIVB-leden aanwezig waren. Een event hanteerde deels de unconference-formule. De kracht van dit format zorgt ervoor dat er ruimte is voor ontmoetingen met kennisexperts, samenwerking, interactie, discussie en creativiteit. Daarbij ontstaat vanzelf de mogelijkheid om te luisteren en te spreken met deskundigen en professionals en zelf deel te nemen aan debatten en discussies. Met het unconference format, wordt de agenda, in relatie met de thema's, op de dag zelf vastgesteld.

IDentity.Next werd geopend door Robert Garskamp, de organisator van dit event. Keynote spreker was Sander Duivestein. Hij is onder meer trendwatcher en analyst binnen VINT maar ook schrijver van columns (Frankwatching, Metro, enz.) en boeken (zoals 'Me the Media: Rise of the Conversation Society'). Sander had een inspirerend verhaal over de ontwikkelingen van de technologie rondom Digitale Identiteit. Sander is al diverse malen in het nieuws geweest onder andere vanwege het gebruik van het Twitter-account van Wouter Bos. Sander deed uit de doeken hoe hij op een simpele manier het Twitter-account op naam van Wouter Bos had gemaakt en hoe hij dat gebruikte om (mede op basis van de openbare agenda van Bos) plausibele, maar ook minder plausibele berichten te verspreiden. Hij liet dus ook zien wat de gevaren hiervan zijn. De rode draad van de presentatie van Sander was vooral dat het gebruik van (sociale media-) technologie accelereert en van toepassing is voor welke generatie dan ook.

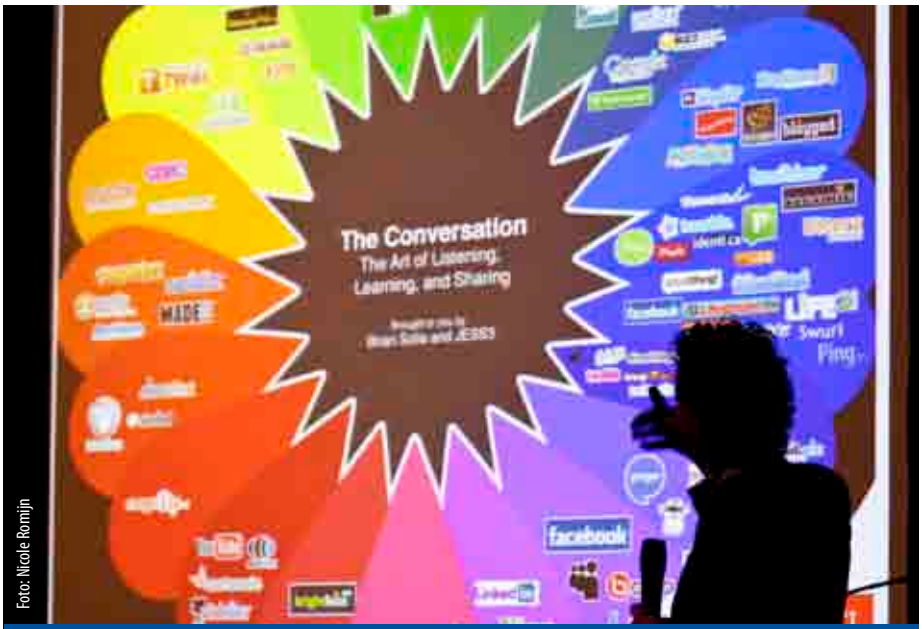


Foto: Nicole Romijn

Sander over trends

Na een break werd er met het ochtendprogramma gestart dat uit een aantal tracks bestond. De tracks waren gekoppeld aan de thema's van die dag. De thema's waren:

- 'Social consumer': de laatste ontwikkelingen in social commerce en user centric identity. Consumenten zijn in control van hun data en informatie en zijn hiermee in staat om social tooling te gebruiken binnen de keten zoals online retail.
- 'MobileMe': brengt mobiliteit en identiteit samen. Als we onderweg zijn bellen we, sturen we e-mails en

sms'jes en geven we betaalopdrachten. Het digitale identiteitsvraagstuk wordt in deze context steeds complexer. Wie heeft de controle over informatie en in hoeverre is dat noodzakelijk? En is mijn mobieltje misschien wel het ideale middel om mijn digitale identiteit te beheren?
- 'Private Eye': het privacy aspect. Ervaren we het wel als een probleem? En zo ja, wie moet daar dan iets aan doen? Internet providers, sociale netwerken en overheidsdiensten maken dagelijks gebruik van informatie. Maar waar ligt de regie als het gaat om privacy? Al deze vragen worden in verschillende contexten bekeken.
- 'E-citizen': is een single identity voor burgers en werknemers van bedrijven de beste weg om van de volgende generatie eOverheidsdiensten gebruik te maken? De initiatieven op dit vlak zijn vaak even veelbelovend als controversieel.

Elke track bestond uit gerenommeerde sprekers uit binnen- of buitenland, die werkzaam zijn binnen de wereld van de digitale identiteit: Stefan Voges (Yunoo), Axel Nennker (Deutsche Telekom AG), Marcel van Galen (Qiy), Mike Small (Kuppinger Cole), Rachel Marbus (BetterID4ALL en redactielid PVIB),

Foto: Nicole Romijn

Agendamuur Open Space unconference

Pascal van Hecke (van Hecke.info), Rob Brand (Ministerie Economische zaken, Landbouw en Innovatie), Timan Rebel (Mobypicture), Marc Sel (director PWC).

Deelnemers konden hun tweets plaatsen met hashtag #identitynext en die werden direct op het grote scherm in de ontmoetingsplek van IDentity.Next getoond.

Unconference

Na de lunch nam Kaliya Hamlin het heft in handen voor het faciliteren van het unconference deel van IDentity.

Foto: Nicole Romijn

Twitter backchannel

Next. Kaliya (ook bekend als Identitywoman) heeft jarenlange ervaring met het modereren van unconference events. Er zijn diverse methoden die hiervoor kunnen worden gebruikt. Kaliya maakte gebruik van het Open Space-model. Samengevat betekent dit dat allereerst de agenda moet worden vastgesteld. Om dit te kunnen doen moesten alle aanwezigen in een kring uitleggen wat hun belang is om een onderwerp te bespreken en welke problemen/ontwikkelingen men op tafel wil leggen, gerelateerd aan de thema's binnen IDentity.Next. Aanwezigen kunnen dan op de muur aangeven welk onderwerp besproken zou moeten worden binnen een sessie. De muur wordt dan uiteindelijk de agenda van die middag. Hierop komen alle onderwerpen te staan, sessies en de duur ervan. Wanneer iedereen (die zich geroepen voelde) dit heeft gedaan kan de agenda als definitief worden beschouwd. Elk van de aanwezigen mag dan besluiten aan welke sessie wordt deelgenomen. Er is verder geen limiet aan het (minimaal en maximaal) aantal mensen per sessies. Wel heeft elke sessie een gespreksleider en wordt er aan een van de deelnemers gevraagd aantekeningen te maken.
Nadat de sessies waren bepaald konden de deelnemers via de agenda


Foto: Nicole Romijn

Prijsuitreiking aan Ziggur

bepalen aan welke sessies ze wilden deelnemen. Onderwerpen die tijdens de sessies werden besproken waren onder andere multiple (linked) id's; need for a common vocabulary; no standards on user consent, default settings for sharing attributes; I want to be the owner of my own data; How should we address Liability?; what is the business case for Service Providers entering the Identity Provider Market; NationalID or 'CitizensID' scheme; Partial identity is key; e-ID's in gov't and private sector BCP; B2B & cloud authz. De notulen van al deze sessies staan online op de website van IDentity.Next.

Award

Aan einde van de dag vond de uitreiking plaats van de Novay Identity Award. Een award voor het beste nieuwe concept of product op het gebied van digitale identiteit. Met deze prijs ondersteunen IDentity.Next en het ICT-onderzoeksinstituut Novay, innovaties die de toekomst van onze digitale identiteiten vormgeven. Er was een jury samengesteld onder leiding van Hermen van der Lugt (directeur Novay). De overige juryleden waren: Yme Bosma (Hyves), Jaap Kuipers (Diginotar) en Dennis van Ham (KPMG). Uit de vele inschrijvingen heeft de jury drie genomineerden geselecteerd voor deze award: Het STORK-project (Secure idenTity acrOss boRders linked), de NVB Awareness campagne 'Veilig Internetbankieren: OK' en Ziggur.nl. Het STORK-project (www.eid-stork.eu) is een Europees project dat werkt aan het interoperabel maken van de diverse nationale elektronische identiteitsoplossingen voor e-overheidsdiensten. De NVB-campagne creëert op een originele manier bewustzijn bij gebruikers over de gevaren van identiteitsdiefstal en adviseert wat ze daar zelf aan kunnen doen. Ziggur is een nieuwe dienst die gebruikers controle geeft over wat er met hun online identiteit gebeurt na hun overlijden.

De jury heeft uiteindelijk Ziggur als winnaar geselecteerd. Het jury rapport vermeldt hierover het volgende: "Ziggur heeft een innovatieve dienst ontwikkeld die aan een belangrijke behoefte tegemoet komt van zowel degene die overlijdt, als van de nabestaanden. Ziggur heeft een praktische benadering hiervoor, die het makkelijk en veilig maakt voor de gebruikers. De jury hoopt met het toekennen van de prijs deze onlangs gestarte dienst een duwtje in de rug te geven." Gerrit Jan Bloem (directeur Ziggur) nam uiteindelijk deze zeer mooie award (een beeld van keramiek op een marmeren sokkel ontwerpen door Alexandra Veneman) van Hermen van der Lugt (Novay) in ontvangst.

Onder het genot van een hapje en drankje en ondersteund door live muziek werd de dag uiteindelijk afgesloten. De aanwezigen gingen naar huis met een rugzak vol (nieuwe) bagage en het vooruitzicht dat er in 2011 weer een IDentity.Next-conferentie zal gaan plaatsvinden.

Meer informatie: www.identitynext.nl


Foto: Nicole Romijn

Netwerken bij Identity.Next

COLUMN

BRIEF AAN HOOFDCOMMISSARIS BIK

Geachte hoofdcommissaris Bik,

Ik vind het zo jammer dat u ergens gewoon gelijk heeft, maar tegelijk ook een heleboel niet. Dat u oneigenlijke argumenten gebruikt voor goede doelen. Ben het namelijk heel erg met u eens hoor. Criminelen moet je kunnen aanpakken. Vooral van die slechte heerschappen (want dat zijn het toch vaak) die kleine kinderen misbruiken en daar foto's en video's van maken en dat verspreiden onder een immer groeiende kring hele nare sujetten. Dat zijn zaken die me raken. Uw schoonmaakwoede kan ik ook erg waarderen. Geen bergen drugs meer in onze wijken en op straat. En het lozen van illegaal afval op onze zee aanpakken. Geweldig! Ik surf namelijk heel graag in schone wateren. Ja, dan vind ik ook echt dat de politie veel meer middelen en mogelijkheden zou moeten hebben om daarop te rechercheren, door te zoeken, meer te vinden om die criminelen te vangen en veroordeeld te krijgen. Maar waarom moet u nu van die rare opmerkingen maken over Big Brother? Ik citeer u uit de Volkskrant (mijn excuses als u woorden in de mond zijn gelegd, maar het stond er toch echt…) "Wie heeft het nog over Big Brother in deze tijd van Facebook en internet? De overheid moet alle beschikbare informatie kunnen gebruiken om criminelen te pakken." Mag ik het dan nu, hier, even met u over Big Brother hebben?

Ik word hier namelijk zo verdrietig van. Want u heeft een goede boodschap, echt waar. Alleen verspeelt u weer zoveel krediet door dit soort opmerkingen. Ik zal u uitleggen waarom. Ten eerste, Big Brother is onze overheid. Facebook en het internet zijn wij. De overheid is er voor, door en namens ons (het wij). Wij hebben daarom een Grondwet. De machtsverhouding tussen de overheid en 'wij' is niet gelijk en daarom zoeken wij balans in die Grondwet. Leggen wij de overheid regels op. Het is u niet toegestaan zomaar in onze basisrechten te treden. Wij – het volk – hebben onder meer een recht op privacy. U moet wel een heel goede reden hebben daarin te mogen treden. Sterker nog, die reden moet in de wet te vinden zijn. Die hebben wij niet voor niets. Of bent u misschien voor het afschaffen van de wet? Ik kan het me niet voorstellen. Dat lijkt me niets voor u, dienaar en hoeder van de wet, pakker van wetsovertreders.

Ten tweede, wat ik doe op Facebook of het internet is mijn vrije keuze. Dat recht heb ik ook. Mits ik binnen de grenzen blijf van wat de wet mij toestaat (dat geldt dus voor ons beiden). Ik mag er zelf foto's op zetten, vertellen waar ik ben en met wie (handig is dat misschien niet altijd), ik mag commentaar leveren op datgene wat anderen daar vertellen en ik mag mezelf en mijn leven delen met wie ik wil. Privacysettings bestaan ook niet zomaar en worden heus door mensen gebruikt. En ik ben ook niet automatisch een boef als ik veilig anoniem ontraceerbaar wil communiceren via proxyservers of als ik mijn materiaal wil versleutelen zodat niet iedereen er zomaar bij kan geraken. Maar, eerlijk is eerlijk, ik heb u ook geen toestemming gegeven om in mijn leven te komen. Voor zover ik weet, heb ik u geen aanleiding gegeven te graven in alles wat over mij bekend is. De laatste keer dat ik controleerde was ik nog nimmer ergens verdacht van. Waarom wilt u toch zo graag een ons juristen welbekend paradigma omdraaien? In mijn colleges strafrecht heb ik toch echt geleerd dat 'een mens onschuldig is totdat het tegendeel bewezen is'. Ik ben er zo bang voor dat door de opmerkingen die u maakt, en anderen met u, het inmiddels aan het verworden is tot 'iedereen is verdacht, tenzij u zelf het tegendeel weet te bewijzen'.

Ik kan best nog een tijdje doorgaan. Er zijn nog wel meer redenen te bedenken waarom u krediet verliest met uw opmerkingen over Big Brother. Maar misschien moeten we daarover maar eens in het echt discussiëren. Ik hoop eigenlijk ook dat we wat meer op een lijn komen daardoor, want weet u, ik heb het eerder al gezegd: u heeft een goed punt. Maar misschien kunt u nog wat hulp gebruiken om ervoor te zorgen dat het ook echt zal landen en dat er eindelijk wat verandert. Leest u vooral ook het artikel van J.J. Oerlemans over de aanpak van kinderporno in deze editie, ik kan het u van harte aanbevelen.

Met vriendelijke groet,
Rachel Marbus

(U kunt mij vinden op Twitter onder @RachelMarbus en u mag me daar best volgen hoor, dat is prima).

Foto: Mast3r

VERSLAG

OWASP BENELUX 2010

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

Jaarlijks organiseren de OWASP chapters in Nederland, België en Luxemburg samen een conferentie. In 2010 werd deze gehouden op 1 en 2 december in Eindhoven op het terrein van de Fontys Hogeschool. De eerste dag is een trainingsdag. Ik ben hier niet aanwezig geweest. Ik was er wel op de tweede dag, zij het met een flinke vertraging. Dit was de eerste sneeuwdag van het seizoen. Gelukkig was ik niet de enige.

Ik kwam binnen na de eerste koffiepauze en had daarmee de OWASP-update-presentaties gemist. Maar daar is in deze uitgave al een ander artikel aan gewijd. De dag heeft een track en is een snelle afwisseling van buitenlandse sprekers die een, meestal pijnlijk, dossier over een aspect van veilige webapplicaties presenteren. Zaken waar je je soms bij afvraagt hoe het mogelijk is dat dit anno 2010 nog steeds mogelijk is.

Clickjacking, VoIP & SIP protocol, backdoors, cashback-systemen, file sharing, social networking... Het gevoel wat me op Blackhat bekruipt, bekruipt me hier ook. Je durft gewoonweg niet meer het internet op te gaan. Toch maar even gecontroleerd dat WiFi op mijn telefoon en tablet uitstaan.

Aan de andere kant hoor je ook dat we in staat zijn het Bredolab botnet op te rollen en toch echt wel een verdediging kunnen opzetten. Hierdoor krijg je weer moed en inspiratie, ik word eraan herinnerd dat ik mijn carrière begonnen ben als programmeur en ga weer denken in programmeerprincipes. Heel verfrissend.

De afsluiting is, ondanks de late start, toch op tijd. Er was ook een gezamenlijk gevoel dat we in zulk weer niet uit wilden lopen. Martin Knobloch en Ferdinand Vroom sloten het congres namens de Dutch Chapter waardig af. Wie volgend jaar van de partij wil zijn moet naar Luxemburg.

Al met al is OWASP een deal. Alles is gratis en je krijgt kwaliteit voorgeschoteld. Ook op dit congres. Aangezien ik niet geloof in een free lunch moet ik nu wel op enige wijze OWASP gaan steunen. Ik kan dat eenieder die met webapplicaties te maken heeft ook van harte aanbevelen. Inmiddels zijn ook de presentaties te downloaden vanaf de website.

Links

www.owasp.org/

www.owasp.org/index.php/BeNeLux_OWASP_Day_2010

www.owasp.org/index.php/BeNeLux_OWASP_Day_2010#tab=Conference.2C_December_2nd

HIGH SECURITY, HUMAN SIGNIFICANCE

INFORMATIEBEVEILIGING IN TWENTE

Wolter Pieters, Universiteit Twente

De Universiteit Twente staat voor high tech en human touch, en dat laat ook het security-onderzoek zien. Dat de mens de zwakste schakel is wisten we natuurlijk al, maar de interactie tussen beveiligingstechniek en samenleving gaat verder dan dat. Hoe kunnen we informatiebeveiliging inzetten om maatschappelijke problemen aan te pakken? Hoe zorgen we dat de ingezette technieken geen nieuwe vormen van misbruik uitlokken? En hoe kunnen we iets zinnigs zeggen over de veiligheid van systemen inclusief de sociale omgeving in organisaties?

Centraal in het beveiligingsonderzoek in Twente staat de Distributed and Embedded Security groep, van de faculteit Elektrotechniek, Wiskunde en Informatica. Hier komen cryptografie, formele methoden en toepassingsgericht onderzoek samen in de ontwikkeling van nieuwe technieken. Op het gebied van risicomanagement en security in organisaties wordt veel samengewerkt met de Information Systems groep, en voor data security zijn er gezamenlijke projecten met Databases. Regelmatig treden we naar buiten via opinieartikelen in kranten, of in radio- en TV-interviews, bijvoorbeeld rond de veiligheid van het verkiezingsproces. De onderzoeksgroep Design and Analysis of Communication Systems haalde internationaal het nieuws met hun onderzoek naar de beperkte anonimiteit van WikiLeaks-supporters.

Gezondheid en welzijn

Een belangrijk aandachtspunt in het onderzoek is het inzetten van informatiebeveiliging voor technieken die gezondheid en welzijn bevorderen. Daarbij denk je natuurlijk in eerste instantie aan het beveiligen van medische gegevens wanneer die uitgewisseld worden om de zorg beter te organiseren. Daarnaast wordt gewerkt aan nieuwe architecturen voor telemedicine en telecare, waarbij (medische) zorg efficiënter wordt vormgegeven met behulp van IT. Gezien de gevoeligheid van medische gegevens speelt security hierin een belangrijke rol. Niet alleen

Introductie Nieuwe serie Onderzoek en Onderwijs

Het PvIB is niet alleen een gezellige beroepsvereniging waar we onder elkaar praten over de veilige dingen des levens, maar ook een beroepsvereniging die een actieve bijdrage wil leveren aan het ontwikkelen van het vakgebied. Dat doen we vooral door kennis te (laten) delen, onder meer via dit blad. Maar ook dagen we mensen uit om kennis te ontwikkelen. Zo is het PvIB een van de trekkers achter de opleidingenmarkt en is het PvIB betrokken bij het professionaliseren van de beroepsgroep en het onderwijsveld, ook in internationaal verband. Maar denk ook aan de uitreiking van de Joop Bautz Information Security Award voor baanbrekend onderzoek en aan de award voor het Artikel van het Jaar.

Dit jaar willen we in een serie artikelen aandacht schenken aan de Nederlandse instituten die een actieve bijdrage leveren aan het ontwikkelen van kennis op ons vakgebied. Dat blijkt niet gering te zijn, er zijn meer initiatieven dan wij dachten. De activiteiten van de Radboud Universiteit mogen algemeen bekend zijn, maar er is echt veel meer. In de komende nummers van dit blad besteden we aandacht aan die activiteiten. We hebben hogescholen, universiteiten en onderzoeksinstituten gevraagd voor ons uit de doeken te doen op welke manier ze een bijdrage leveren. De aftrap in dit nummer is van Wolter Pieters (voormalig winnaar van de Artikel van het Jaar-award!), die ingaat op wat er allemaal gebeurt op de Universiteit Twente. We hopen u met deze serie een goed beeld te geven van wat er in ons land aan ontwikkelingen plaatsvindt. Waarschijnlijk ook meer dan u dacht.

Namens de redactie,
André Koot

vertrouwelijkheid, maar ook integriteit (je moet niet stiekem andere medicijnen kunnen voorschrijven).

Dat er in het kader van welzijn ook hele andere mogelijkheden zijn laat het Natural Teggs-project zien. Hier ligt de nadruk op meer transparantie in de voedingsindustrie. Met de resultaten van dit project kunnen eieren worden gevolgd van boerderij tot supermarkt. Zo kunnen consumenten betere informatie krijgen over de eigenschappen van de producten die ze kopen, en kan bijvoorbeeld fraude met de classificatie (zoals biologisch) worden voorkomen.

Critical control systems

Veel onderzoek richt zich op de beveiliging van de aansturing van processen. Hierbij gaat het onder andere om intrusion detection in industriële settings (SCADA). Wanneer er een directe verbinding is tussen het internet en, bijvoorbeeld, de drinkwatervoorziening, is het essentieel dat aanvallen tijdig opgespoord worden. De StuxNet-worm heeft laten zien dat dit niet alleen een theoretische mogelijkheid is. Omdat de protocollen veelal geheim zijn, kan de detectie alleen plaatsvinden op basis van afwijkingen van het netwerkverkeer ten opzichte van

Informatiebeveiliging inzetten om maatschappelijke problemen aan te pakken

normale patronen, zogeheten anomaly-based intrusion detection (Bolzoni et al., 2009). Een spin-off bedrijf van de universiteit, genaamd Security Matters, ontwikkelt deze technieken verder.

Als toekomstige toepassing wordt gekeken naar communicatie tussen voertuigen. Hiermee zou het bijvoorbeeld mogelijk zijn real-time waarschuwingen te geven voor files, maar uiteindelijk zelfs om voertuigen automatisch te laten remmen. In beide gevallen kan hier misbruik van worden gemaakt door frauduleuze berichten te sturen, zodat medeweggebruikers een andere route kiezen of zelfs op elkaar botsen. De communicatie tussen de voertuigen moet dus voldoende beveiligd zijn. Aan de andere kant bestaan er ook grote maatschappelijke bezwaren tegen het kunnen volgen van voertuigen, dus ook privacy moet een plaats krijgen in het ontwerp. Neem daarbij dat de communicatie slechts over een beperkte afstand mogelijk is, dat ook de bandbreedte beperkt is, en dat er zeer veel voertuigen tegelijk op de weg zijn, en er ontstaat een uitdaging van formaat (Dietzel et al., 2010).

Social and enterprise networks

Een derde aandachtspunt is beveiliging van nieuwe netwerkstructuren, die bestaande concepten van informatiebeveiliging uitdagen. In ons

privéleven hebben we het dan met name over sociale netwerkdiensten, zoals Facebook en Hyves. Aan de ene kant zouden we als beveiligers graag betere bescherming bieden voor privacy en security in dit soort omgevingen, aan de andere kant worden dergelijke maatregelen al snel te ingewikkeld voor gebruikers. Het Kindred Spirits-project heeft als doel verschillende privacy-niveaus automatisch te garanderen op basis van overeenkomsten tussen gebruikersprofielen. De profielen zelf zijn dan versleuteld, en gebruikers kunnen alleen profielen ontsleutelen als deze voldoende overeenkomen met dat van henzelf (privacy-preserving matching; Tang, 2010). Een ander idee dat we uitwerken is het regelen van toegang op basis van wat de gebruiker al van een profiel weet (data-based access control; Pieters en Tang, 2009).

Meer transparantie in de voedingsindustrie

Ook binnen organisaties ontstaan nieuwe vormen van netwerken. De grenzen tussen organisaties en hun IT-infrastructuur vervagen. Externe medewerkers moeten toegangsrechten kunnen krijgen, en de gegevens die zij moeten kunnen opvragen staan 'in the cloud'. Wat betekenen deze vormen van virtualisatie (niet alleen van servers, maar ook van organisaties!) voor de beveiliging? Hoe bepaal je de security-eisen (Morali en Wieringa, 2010)? Cloud computing vormt daarbij een belangrijk aandachtspunt, en de Universiteit Twente was de initiator van zowel de workshop on Security and Privacy in Cloud Computing (Brussel, januari 2009; zie Pieters, 2011) als het Dagstuhl seminar over Secure Architectures in the Cloud (Dagstuhl, December 2011). Beide zijn gericht op het vormen van een community om over deze vragen na te denken. Daarnaast is in samenwerking met Kennispark en Caase.com het kenniscentrum Centre-4Cloud opgezet (www.centre4cloud.nl).

Aanpak

Voor deze toepassingen worden zowel bouwstenen als analysetechnieken ontwikkeld. Bij bouwstenen gaat het dan om cryptografische technieken en daarop gebaseerde protocollen. In het bijzonder besteden we aandacht aan technieken die werken met beperkte middelen, zoals geheugen, bandbreedte en energie. Met analysetechnieken kunnen we de veiligheid van systemen vaststellen, hetzij op basis van een risicoanalyse vooraf, hetzij op basis van real-time metingen. Vaak worden resultaten getoetst in simulaties of case studies. Regelmatig zijn wij op zoek naar geïnteresseerde bedrijfspartners voor het uitvoeren van deze validatie. De lezer kan uiteraard contact opnemen als hij/zij daar meer over wil weten. Een van de actuele resultaten

?

is een model waarmee op basis van de organisatie-infrastructuur bedreigingen kunnen worden geanalyseerd, inclusief social engineering (Dimkov et al., 2010a). Daarnaast hebben we ook een methode ontwikkeld om de gevonden bedreigingen daadwerkelijk te testen, door middel van penetration testing met social engineering (Dimkov et al., 2010b).

Op het gebied van biometrie is er samenwerking met de Signals and Systems groep. Gezichtsherkenning bij cameratoezicht, vingerafdrukken, en andere vormen van unieke identificatie kunnen helpen om systemen beter te beveiligen, maar de opgeslagen gegevens introduceren zelf ook weer beveiligingsrisico's. Je kunt immers geen nieuw biometrisch kenmerk aanvragen als je oude is uitgelekt. Een van de resultaten van deze samenwerking is een systeem om veilige informatie-uitwisseling met mobieltjes mogelijk te maken door foto's van elkaar te nemen (Buhan et al., 2009).

Voor het onderzoek naar ethische aspecten werken we samen met de afdeling Wijsbegeerte. Een van de hieruit voortgekomen ideeën is de toepassing van het voorzorgsbeginsel op informatietechnologie (Pieters en Van Cleeff, 2009). Het principe stelt dat bij mogelijke schadelijke gevolgen van technologische ontwikkelingen mitigerende maatregelen nodig zijn, ook als niet met zekerheid kan worden vastgesteld in welke mate deze gevolgen optreden. Aan de ene kant kan een dergelijk principe het belang van informatiebeveiliging in beleid verankeren, bijvoorbeeld door eisen te stellen aan privacybescherming en scheiding van verantwoordelijkheden. Aan de andere kant kan het ook richtlijnen geven over hoe wij als informatiebeveiligers security-eisen voor informatiesystemen zouden moeten opstellen, terwijl we nog niet precies weten hoe de systemen gebruikt zullen worden.

Een nieuw initiatief is samenwerking met de afdeling Social Risks and Safety Studies op het gebied van de preventie van cybercrime (Hartel et al., 2010). Technieken uit het onderzoeksgebied crime science worden hierbij toegepast op informatiebeveiliging. Er zijn hierbij vijf categorieën van maatregelen: increase efforts, increase risks, reduce rewards, reduce provocations, remove excuses (www.popcenter.org/25techniques/). Het gaat hierbij om het beïnvloeden van gebruikersgedrag door ontwerpmaatregelen, een 'softe' variant van security vergeleken met encryptie en access control. Deze beïnvloeding heeft in wereldwijd onderzoek naar productontwerp al veel aandacht gekregen, maar is nog relatief onbekend binnen de informatiebeveiliging. Een aardig overzicht is te vinden op http://nudges.org.

Penetration testing met social engineering

Toekomst

De bredere visie op informatiebeveiliging lijkt wereldwijd terrein te winnen. Maatschappelijke aspecten én de rol van menselijk gedrag zijn essentieel in het beter begrijpen van het vakgebied. Technische ontwikkelingen kunnen zo beter worden afgestemd op maatschappelijke behoeften en de beperkingen die door gebruikers worden opgelegd. De Twentse aanpak kan daar ook in de toekomst een belangrijke bijdrage aan leveren.

Literatuur

Bolzoni, D. and Etalle, S. and Hartel, P.H. (2009) *Panacea: Automating Attack Classification for Anomaly-based Network Intrusion Detection Systems.* In: Recent Advances in Intrusion Detection (RAID). pp. 1-20. LNCS 5758. Springer Verlag.

Buhan, I.R. and Boom, B.J. and Doumen, J.M. and Hartel, P.H. and Veldhuis, R.N.J. (2009) *Secure pairing with biometrics.* International Journal of Security and Networks, 4 (1/2). pp. 27-42.

Dietzel, S. and Schoch, E. and Kargl, F. and Könings, B. and Weber, M. (2010) *Resilient Secure Aggregation for Vehicular Networks.* IEEE Network, 24 (1). pp. 26-31.

Dimkov, T. and Pieters, W. and Hartel, P.H. (2010a) *Portunes: representing attack scenarios spanning through the physical, digital and social domain.* In: Proceedings of the Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS'10). pp. 112-129. LNCS 6186. Springer Verlag.

Dimkov, T. and Pieters, W. and Hartel, P.H. (2010b) *Two methodologies for physical penetration testing using social engineering.* In: Proceedings of the Annual Computer Security Applications Conference (ACSAC). pp. 399-408. ACM.

Hartel, P.H. and Junger, M. and Wieringa, R.J. (2010) *Cyber-crime Science = Crime Science + Information Security.* Technical Report TR-CTIT-10-34, Centre for Telematics and Information Technology, University of Twente, Enschede.

Morali, A. and Wieringa, R.J. (2010) *Risk-Based Confidentiality Requirements Specification for Outsourced IT Systems.* In: Proceedings of the 18th IEEE International Requirements Engineering Conference (RE 2010). pp. 199-208. IEEE Computer Society.

Pieters, W. (2011) *Security in the clouds: a bird's eye view.* To appear in Data Protection: An Element of Choice, proceedings of the 2010 conference on Computers, Privacy and Data Protection (CPDP). Springer.

Pieters, W. and van Cleeff, A. (2009) *The Precautionary Principle in a World of Digital Dependencies.* IEEE Computer, 42 (6). pp. 50-56.

Pieters, W. and Tang, Q. (2009) *Data is key: introducing the data-based access control paradigm.* In: Data and Applications Security 2009. LNCS 5645. Springer Verlag.

Tang, Q. (2010) *User-friendly matching protocol for online social networks.* In: ACM Conference on Computer and Communications Security. pp. 732-734. ACM.

FACEBOOK VOLGT IEDERE INTERNETGEBRUIKER: LIKE THIS!

Arnold Roosendaal is partner bij FennellRoosendaal Onderzoek en Advies en gespecialiseerd in juridische implicaties van ICT-toepassingen. Daarnaast is hij werkzaam als promovendus en onderzoeker bij het Tilburg Institute for Law, Technology, and Society (TILT) aan Tilburg University. In zijn promotieonderzoek kijkt hij naar implicaties voor privacy en autonomie van individuen als gevolg van het gebruik van digitale representaties.

Slecht nieuws voor internetgebruikers die privacy belangrijk vinden en daarom een beknopt Facebookprofiel of zelfs helemaal geen profiel op Facebook hebben. Er is geen ontsnappen aan! De immens populaire Like Button stelt Facebook in staat om elke internetter te volgen.

Het gebruik van zogeheten third party cookies om individueel surfgedrag te volgen is op zich niks nieuws. Derde partijen kunnen, wanneer ze inhoud voor een website aanleveren, ook cookies plaatsen op de computer van bezoekers van die website. Wanneer de cookie eenmaal geplaatst is, wordt deze bij elk volgend verzoek om content, van de servers van de betreffende derde partij meegestuurd. Gebruikers hebben vaak geen weet van de geplaatste cookies, juist omdat ze niet direct zichtbaar zijn.
Op basis van een cookie kan de computer van de bezoeker worden herkend wanneer verschillende websites worden bezocht. Wanneer het internetgedrag van een gebruiker in kaart wordt gebracht kunnen aan de hand daarvan interesses en eigenschappen worden bepaald. Dat vormt een profiel op grond waarvan bijvoorbeeld gerichte advertenties worden getoond. Vanuit commercieel oogpunt kunnen die profielen dus bijzonder waardevol zijn. Hoe gedetailleerder een profiel is, des te gerichter kan er worden geadverteerd. Het is daarom niet verwonderlijk dat er steeds slimmere technieken worden ontwikkeld om gedrag van internetgebruikers in kaart te brengen. Bekend zijn de zogeheten webbugs, kleine bestandjes van 1x1 pixel, dus onzichtbaar voor de gebruiker, die bij het laden een cookie plaatsen of lezen. Maar naast deze bugs, die vaak door advertentiebedrijven worden gebruikt, komen er ook nieuwe technieken met vergelijkbare mogelijkheden. Hier zit het slimme van de techniek hem juist in de zichtbaarheid die een schijnbare onschuldigheid etaleert. Ik heb het hier over de Like button van Facebook.

De Facebook 'Like' button

De Like button van Facebook is een 'thumbs-up'-symbool met het woord 'Like' ernaast. Volgens Facebook: *"The Like button lets a user share your content with friends on Facebook. When the user clicks the Like button on your site, a story appears in the user's friends' News Feed with a link back to your website."*[1] De code waarmee de button kan worden geïmplementeerd in een website is gratis beschikbaar en kan dus eenvoudig door website-eigenaars worden gebruikt om bezoekers de site of onderdelen ervan te laten promoten. Als de bezoeker op de button klikt kan hij op Facebook inloggen via een popupscherm. Daarna wordt de link op de profielpagina van de Facebook-gebruiker geplaatst. Wanneer een gebruiker al is ingelogd gebeurt dat direct na het aanklikken van de button.
De Like button is één van de zogeheten social plugins die Facebook in april 2010 op haar F8-conferentie introduceerde. De button moest Facebookgebruikers in staat stellen om op

1 developers.facebook.com/docs/reference/plugins/like

eenvoudige wijze interesses te delen door te verwijzen naar artikelen en sites. Sindsdien is de button op tal van sites te zien. De waarde van de button is ook vanuit commercieel oogpunt aanzienlijk. Sites die de Like button hebben geïmplementeerd rapporteren groei in bezoekersaantallen van soms meer dan 200% en de tijd die op sites met de button wordt gespendeerd om artikelen te lezen is vaak ook met 80% toegenomen.[2] De populariteit van de buttons in combinatie met de enorme commerciële waarde maakt het aannemelijk dat het aantal Like buttons alleen maar explosief toe zal blijven nemen.

Cookies, herkenning en identificatie

Zoals aangegeven kunnen cookies door partijen worden geplaatst die niet de eigenaar zijn van de bezochte website. Dat gebeurt dan via het leveren van content voor zo'n site, zoals advertenties, routekaarten of video's. Wanneer een website wordt bezocht, wordt elk onderdeel van die site apart van de server geladen. De third party content wordt direct van de servers van de derde partijen opgevraagd door middel van een http request. Zo worden dus vaak niet één, maar vele sites bezocht, zonder dat het direct zichtbaar is. Elke partij die inhoud voor een site levert kan daarbij een cookie meesturen die op de computer van de gebruiker wordt geplaatst. Vanaf dat moment wordt die cookie elke keer dat content van de desbetreffende server wordt opgevraagd meegestuurd in de http request. Omdat elke cookie een uniek nummer heeft kan een computer worden herkend. Wanneer een partij op veel verschillende websites inhoud aanlevert kan een gebruiker dus op basis van de cookie gevolgd worden over het web. Omdat de interactie met de server plaatsvindt bij het laden van een pagina is het niet relevant of een stukje content wordt aangeklikt of überhaupt klikbaar is.

Als we nu kijken naar de Facebook Like button zijn er enkele scenario's mogelijk. Ten eerste een scenario waarin de gebruiker lid is van Facebook. Deze gebruiker heeft bij het aanmelden een cookie van Facebook ontvangen met een unieke ID die gekoppeld is aan het account. Deze cookie wordt dus telkens meegestuurd naar Facebook wanneer content van de Facebook-servers wordt opgevraagd. Elke keer als een website met een Like button wordt bezocht is dat dus het geval, ongeacht of de button ook wordt aangeklikt.

Een tweede scenario is wanneer de gebruiker geen lid is van Facebook. In dat geval is er geen Facebook cookie op de computer van de gebruiker aanwezig. Bij het opvragen van de Like button wordt ook geen cookie geplaatst. Echter, een grote hoeveelheid websites heeft Facebook Connect geïmplementeerd en daarmee wordt wel een cookie geplaatst. Na plaatsing wordt deze cookie dus, hetzelfde als hierboven, steeds meegestuurd naar de Facebook-servers en is het mogelijk om de gebruiker te volgen. Het enige verschil is dat in dit geval de gegevens niet aan een account kunnen worden gekoppeld.

Wat als een gebruiker besluit om een account te creëren? Dat is scenario drie. De gebruiker heeft al een cookie van Facebook op zijn of haar computer. Wanneer een account wordt aangemaakt wordt deze cookie eerst via de inlogpagina van Facebook vervangen door een aantal tijdelijke cookies. Vervolgens krijgt de gebruiker bij het aanmaken van het account een unieke user-ID die in een cookie naar de computer van de gebruiker wordt verzonden. De oude cookies kunnen achter de schermen door Facebook aan de ID worden gekoppeld en zo aan de nieuwe account. Vanaf dit moment geldt de gebruiker als Facebook-lid en wordt de user-ID steeds meegestuurd naar de servers van Facebook wanneer content wordt opgevraagd.

Tot slot, scenario vier, is het mogelijk dat een gebruiker zijn Facebook-account opheft. Hier dient een onderscheid te worden gemaakt tussen het deactiveren en het daadwerkelijk verwijderen van een account. In het eerste geval wordt het account slechts onzichtbaar gemaakt voor Facebook-leden, maar blijft alles op de servers van Facebook beschikbaar. Daardoor is het mogelijk om het account toch weer te activeren, inclusief alles wat erop staat, mocht de gebruiker spijt krijgen van de beslissing om met Facebook te stoppen. Op de Facebook-servers blijft het account dus actief. Dit betekent dat gegevens over webgedrag nog steeds aan het account kunnen worden gekoppeld.

> Slimme techniek in zichtbaarheid die een schijnbare onschuldigheid etaleert

In het tweede geval is reactivering niet mogelijk. De gebruiker moet een speciale procedure volgen om het account te laten verwijderen en dat duurt veertien dagen. Wanneer op enig moment gedurende die periode toch wordt ingelogd, wordt het opheffingsproces stopgezet. Op welke wijze het account precies verwijderd wordt en of en wat er op de Facebook-servers overblijft is onduidelijk. In ieder geval heeft de gebruiker nog steeds de user-ID cookie op zijn computer staan. Deze dient dus te worden verwijderd. Verder moeten ook alle andere services die gekoppeld zijn aan het account, bijvoorbeeld een slideshare.com account waar met de Facebook-gebruikersnaam en -wachtwoord kan worden ingelogd, ontkoppeld worden. Wanneer de gebruiker alles heeft stopgezet en de cookies heeft verwijderd is het alsof er geen account is en treedt scenario twee in werking. De cookies worden dus gebruikt om een computer of Facebook-lid te herkennen. Wanneer iemand verschillende apparaten gebruikt om zich aan te melden op zijn Facebook-account, bijvoorbeeld een PC, een laptop en een smartphone, dan krijgen deze

2 www.facebook.com/notes/facebook-media/value-of-a-liker/150630338305797

verschillende apparaten eenzelfde cookie met een user-ID. Zo kunnen deze apparaten herkend worden als zijnde van een en dezelfde persoon. Bij niet-leden zullen de apparaten verschillende cookies hebben en dus niet alleen op grond daarvan gekoppeld kunnen worden. Voor Facebook zal dat in eerste instantie weinig verschil maken, omdat de gegevens van deze gebruikers waarschijnlijk geaggregeerd worden om een grotere sample te krijgen op basis waarvan gerichte advertenties aan leden kunnen worden aangeboden.

Naast de Facebook Like button is er nog een aantal andere soortgelijke buttons op het web. Voorbeelden zijn Twitter's Tweet button, de Digg button en Google's Buzz button. Toch zijn deze buttons niet allemaal hetzelfde. Zoals eerder beschreven wordt Facebook Connect gebruikt om cookies te installeren op de computers van internetgebruikers. Er is dus een extra mechanisme om het volgen via de Like button mogelijk te maken. Twitter heeft niet zo'n systeem. Dat betekent dat het noodzakelijk is om daadwerkelijk een keer op de homepage van Twitter te zijn geweest om een cookie te ontvangen die vervolgens bij http requests voor de Tweet button wordt meegestuurd. Een account is ook hier niet noodzakelijk, maar een (klein maar belangrijk) verschil is wel dat iemand een keer langs de Twitter homepage gekomen moet zijn en dat er toch iets van een connectie is, al is het minimaal.

Traceerbare sporen

Geen manier om aan de aandacht van Facebook te ontsnappen

Een ander belangrijk verschil is dat Facebook surfgedrag kan koppelen aan accounts van haar leden. Deze accounts bevatten vaak al veel waardevolle persoonlijke informatie, maar deze informatie wordt dus nog extra verrijkt met gegevens over surfgedrag, zonder dat de leden dat weten. Met het oog op privacy bewust geen account op Facebook aanmaken of slechts een zeer beperkte hoeveelheid informatie op die account plaatsen is dus geen manier om aan de aandacht van Facebook te ontsnappen.

Een laatste punt van aandacht is dat Facebook hard op weg is om een digitale identiteitsprovider te worden. Er is al een aantal diensten waarvoor een Facebook-account gewenst of vereist is om er gebruik van te maken. Een voorbeeld is het eerder genoemde Slideshare.com. Naarmate het aantal diensten dat zo wordt aangeboden toeneemt, worden internetgebruikers sterker afhankelijk van Facebook en mogelijk genoodzaakt om een account op Facebook aan te maken. De greep op internetgebruikers wordt daarmee enorm versterkt.

Wat is het probleem?

Het meest voor de hand liggende probleem is dat gegevens over gebruikers worden verzameld zonder dat zij daar weet van hebben. Die gegevens worden vervolgens verwerkt tot profielen. Daarmee kunnen advertenties worden gepersonifieerd met gevolgen voor gebruikers wat betreft welke informatie

Surveillance camera's

ze wel of juist niet te zien krijgen. Vanuit het perspectief van privacy en individuele autonomie zijn daar de nodige vraagtekens bij te plaatsen. Dit is echter een al langer bestaand probleem, dus ik wil hier op juist een ander aspect ingaan.

De Like button heeft een speciale eigenschap waardoor er een verschil is met andere technieken waarmee gegevens worden verzameld. Die eigenschap is de zichtbaarheid. Juist vanwege die zichtbaarheid worden tegengestelde verwachtingen gewekt van wat er in de praktijk gebeurt. Ten eerste zullen gebruikers die geen Facebook-account hebben in de veronderstelling zijn dat die button van Facebook is en dat zij er 'dus' niks mee te maken hebben. Je moet dan immers lid zijn. Ten tweede zullen degenen die wel lid van Facebook zijn denken dat er niks gebeurt zolang ze niet op de button klikken. Het is immers een tool die alleen iets doet als je hem gebruikt. Beiden niet waar dus, terwijl de zichtbaarheid van de buttons juist deze verwachtingen oproept. Dit in tegenstelling tot de genoemde web bugs die onzichtbaar zijn.

Het probleem is dat er geen keuze is voor internetgebruikers. Vergelijk het met een winkel waar cameratoezicht plaatsvindt. Je ziet dan de camera hangen en normaal ook een sticker bij de deur die waarschuwt voor dit toezicht. Als je niet op video opgenomen wilt worden kun je besluiten om niet naar binnen te gaan. Bij de Like button is er geen waarschuwing. Je weet vooraf niet of de button op een website staat. Als je hem ziet en besluit er niks mee te doen, ben je toch te laat. De button is in die zin vergelijkbaar met de sticker die waarschuwt, maar is tegelijkertijd de camera die meteen vastlegt wie er gewaarschuwd wordt. Daarmee lijkt er een keuze geboden te worden die er helemaal niet is.

Conclusie

Met de Like button en andere social plugins heeft Facebook een grote slag geslagen in de strijd om de macht over het internet. Facebook heeft toegang tot het surfgedrag van mogelijk iedere gebruiker. Daarnaast genieten de social plugins een enorme populariteit dankzij de commerciële waarde voor aanbieders van content en de functionaliteit voor Facebook-leden. Als we daarbij voegen dat Facebook zich ook een rol heeft aangemeten als digitale identiteitsprovider is duidelijk dat de positie van Facebook erg sterk is. Enerzijds weet zij gebruikers te bereiken en anderzijds weet ze die gebruikers ook sterker afhankelijk te maken en stap voor stap aan zich te binden omdat de diensten van Facebook op steeds meer punten een noodzakelijke voorwaarde worden voor toegang tot diensten. Iedereen heeft een connectie met Facebook. Wie die connectie zelf niet maakt wordt door Facebook een handje geholpen. Er is geen ontkomen aan!

Like

CLOUD BEVEILIGINGSVERWACHTINGEN VOOR 2011

Randy Barr is als Chief Security Officer (CSO) van Qualys verantwoordelijk voor beveiliging, risicomanagement en zakelijke continuïteitsplanning voor Qualys. Randy is lid van de Cloud Security Alliance, stuurgroep van het Common Assurance Maturity Model, Worldwide Executive Council, ISSA CISO Executive Forum, en heeft meer dan 13 jaar ervaring in het implementeren van gebruiksprocedures voor beveiliging en het voldoen aan regels. Randy is rechtstreeks te bereiken op randy.barr@qualys.com

Cloud computing was in 2010 een veelbesproken onderwerp. De voordelen beginnen duidelijk te worden en leveranciers bieden levensvatbare oplossingen aan die echte voordelen opleveren. Zo langzamerhand begrijpen bedrijven het concept cloud computing en beginnen zij het daadwerkelijk in de praktijk te brengen, waarbij ze hun toepassingen en IT-infrastructuren verhuizen naar de cloud. Ondanks een toename in gebruik van cloud computing is er nog steeds een aantal uitdagingen, met name op het gebied van beveiliging. Aan het begin van 2011, terwijl steeds meer bedrijven over gaan op cloud computing, zijn er vijf belangrijke gebieden die naar verwachting het nieuws zullen halen.

Beveiliging als onderscheidende factor in cloudoplossingen

Nu de markt klaar is om cloud computing te omarmen, zullen cloudleveranciers proberen om hun oplossingen te laten opvallen. Ingebouwde beveiliging zal een onderscheidende factor worden nu vendors zich gaan richten op het leveren van meerwaarde aan de klant. Tenslotte is een leverancier die de klant eenvoudige, efficiënte oplossingen levert voor wat voorheen ingewikkeld en duur was, een van de meest aantrekkelijke voordelen van cloud computing. In de wetenschap dat beveiliging een punt van zorg is, en dat beveiliging en compliance voor bedrijven vaak ingewikkelde en kostbare aangelegenheden zijn, verwachten we dat leveranciers beveiliging zullen toevoegen aan hun aanbod.

Mobiele apparaten als doelwit

Veel mobiele apparaten hebben een rechtstreekse connectie met de cloud. Bijvoorbeeld met een Appstore, voor opslagservices of voor e-mail. Bovendien worden bedrijfscloud-voorzieningen in toenemende mate beheerd via mobiele apparaten. Hackers en cybercriminelen zullen altijd inspringen op groeitrends om de eenvoudigste manier te vinden voor het stelen van gegevens of om IT-systemen in hun macht te krijgen. We zagen hetzelfde in 2010 met de opkomst en verfijning van malware-aanvallen om webapplicaties te exploiteren. Nu meer mensen mobiele apparaten gebruiken om toegang te krijgen tot bedrijfstoepassingen, gaan hackers hun aanvallen op die apparaten richten. Hoewel we nieuwe beveiligingsoplossingen voor mobiele apparaten kunnen verwachten, is het zeer waarschijnlijk dat er eerst een groot incident moet komen, waarbij de gaten in de beveiliging van mobiele apparaten worden blootgelegd, voordat ze worden gedicht. Hieronder enkele denkbare scenario's.

> Cloud-vendors gaan zich onderscheiden met ingebouwde beveiliging

a) Mogelijk onveilige back-up in de cloud en aanwezigheid van zeer vertrouwelijke gegevens op mobiele apparaten. Er zijn interessante onderlinge afhankelijkheden in het gebruik van verschillende cloud-diensten op mobiele apparaten, die mogelijk verschillende beveiligingsmodellen en aannames hanteren.
Dankzij functionaliteit als ondersteuning op afstand kan het hacken van een cloudleverancier de poort openzetten naar grootschalige toegang tot vertrouwelijke gegevens op mobiele apparaten.

b) Verlies of diefstal van een mobiel apparaat (een zeer waarschijnlijk incident) waarmee toegang tot cloud-diensten en gegevens op root-niveau mogelijk is. Mobiele Apps leveren vaak directe en geautomatiseerde toegang tot cloud-diensten en -gegevens. Als het mobiele apparaat van een persoon met adminrechten wordt gestolen, kan dit een ernstige bedreiging zijn voor zeer vertrouwelijke gegevens of zelfs complete cloud-diensten die door zo'n persoon worden beheerd vanaf een mobiel apparaat. Apps voor

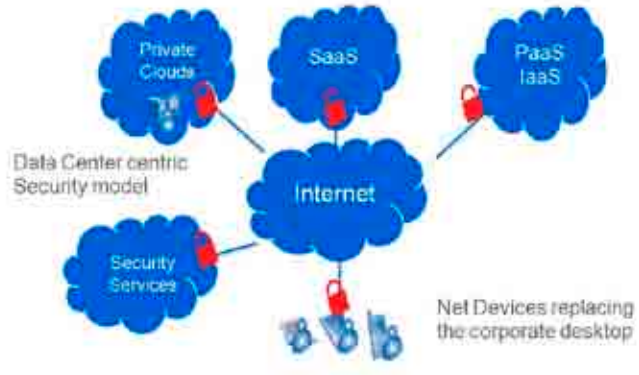
extern beheer op mobiele apparaten zijn er volop.

c) Gedownloade mobiele Apps die met een kwaadaardige softwarecode zijn geïnfecteerd, met mogelijk zeer uitgebreide distributie op een enorm aantal mobiele apparaten tot gevolg. De geïnfecteerde toepassingen kunnen ertoe leiden dat onbevoegden toegang krijgen tot de geïnfecteerde smartphones. Als de gebruikers de smartphones inloggegevens van cloud-diensten laten onthouden, vormen de geïnfecteerde smartphones daarmee indirect een bedreiging voor de gegevens binnen de cloud-diensten.

d) Mobiele Worm/botnets. Proof-of-concepts daarvoor zijn al geleverd op Symbian, iPhone en Android. Dit kan mogelijk zelfs leiden tot Denial-of-Service-aanvallen op cloud-diensten. Zie bijvoorbeeld: downloadsquad.switched.com/2010/03/11/8000-iphone-and-android-devices-hacked-to-form-a-botnet/

Nieuwe beveiligingsstandaarden en -eisen

De eisen van klanten en regelgeving zullen cloud-leveranciers ertoe aanzetten wijzigingen aan te brengen in de standaardrapportages aan klanten. Gedurende het komende jaar zullen cloud-leveranciers de waarde gaan inzien van een standaard benadering van rapporteren. Tot het moment dat de standaarden zijn vastgesteld zullen



cloud-leveranciers echter SAS-70 rapportages en ISO-certificeringen blijven benutten.

Omdat bij het kiezen van cloud-diensten ook de security ervan zal worden geëvalueerd, zullen normen uiterst belangrijk worden om klanten te helpen inschatten hoe veilig hun gegevens worden bewaard. Cloud-gebruikers zullen hun bestaande processen voor de beoordeling van de beveiligingsaanpak van cloud-leveranciers blijven benutten, maar ook zullen ze gaan kijken naar de meest populaire organisaties die richtlijnen en standaarden ontwikkelen, zoals de Cloud Security Alliance (CSA), ENISA, het Common Assurance Maturity Model (CAMM), en het nieuwe Federal Risk and Authorization Management Program (FedRAMP). Om er een paar te noemen.

Security-normen belangrijk om klanten te helpen bij keuze leveranciers

Certificeringen en assessment tools

Vandaag de dag bestaat er een aantal initiatieven waarbij wordt gewerkt aan standaarden en richtlijnen, zoals de CSA. Er zal extra aandacht ontstaan voor certificeringen in 2011. We krijgen discussies te zien rond de noodzaak voor de certificering van cloud-leveranciers.

In 2011 zullen bedrijven actiever de beveiliging van hun cloud-leveranciers gaan beoordelen. Hoewel daarvoor nu al enkele tools voorhanden zijn, kunnen we verwachten dat er voor cloud-gebruikers meer beschikbaar zullen komen. Sommige van de huidige tools maken het voor gebruikers mogelijk om de bestaande spreadsheets met een opsomming van vragen voor hun cloud-leveranciers te vervangen. Andere producten bevatten een beoordeling van de netwerkbeveiligingsaanpak van de leverancier. Cloud-gebruikers zullen ook tools gaan toepassen die het mogelijk maken hun bestaande processen voor de doorlopende beoordeling van hun cloud-leveranciers te stroomlijnen, terwijl ze ook informatie samenvoegen om inzicht te krijgen in het risicobeeld van hun leveranciers.

Proactieve communicatie over beveiliging

In de beveiligingsindustrie spreekt men bij beveiligingsmanagement vaak over 'people, process & technology (PPT)'. We zullen waarschijnlijk zien dat vendors gaan samenwerken met bedrijven om zich te richten op specifieke zorgen over de cloud, hoewel 'mensen' en 'proces' dan nog hulp kunnen gebruiken. Dit geldt vooral voor het toenemende gebruik van IT door consumenten, die hun eigen mobiele apparaten willen gebruiken om toegang te krijgen tot bedrijfsgegevens via de cloud. Hoewel de productiviteitsvoordelen hiervan schijnbaar eindeloos zijn, zal proactieve communicatie met werknemers noodzakelijk zijn om het bedrijfsnetwerk als geheel te beschermen. Dit zou protocollen kunnen omvatten die gevolgd moeten worden bij verlies van een smartphone of diefstal van een laptop, of procedures om browsers up-to-date te houden en zo de kans op een malware-infectie te verkleinen.

Al met al lijkt 2011 een opwindend jaar te worden voor het gebruik van cloud computing. Ik ben ervan overtuigd dat door samenwerking in de industrie, security verder zal evolueren om het veilige gebruik van deze fantastische nieuwe technologieën mogelijk te maken.

Voor verdere vragen en discussie omtrent dit onderwerp nodig ik u graag uit op https://community.qualys.com/index.jspa.

SUCCESVOLLE INTEGRITEITBEHEERSING DOOR BEÏNVLOEDEN MENSELIJK HANDELEN

Peter Schimmel is partner bij Grant Thornton Forensic & Investigation Services B.V.
Hij is bereikbaar op Peter.Schimmel@gt.nl.

Mensen zijn niet uit zichzelf eerlijk. "Vertrouwt niet op prinsen, op des mensen kind, bij hetwelk geen heil is." Weinigen herkennen zichzelf in deze versregel uit psalm 146. Wij zijn zelf immers altijd integer, want wij kunnen ons handelen en dat van onze naasten rechtvaardigen. Wij zijn te vertrouwen. Bij derden gaat het wel eens mis, maar dat gaat om incidenten, uitzonderingen op de regel. Derden zijn daarom ook te vertrouwen. Een beetje integer bestaat toch niet? Dus is iedereen integer?

Het wordt tijd voor het inzicht dat wij uit ons zelf helemaal niet zo zuiver zijn in ons handelen. Niemand wordt wakker met de gedachte: "hé, laat ik vandaag weer eens lekker eerlijk zijn". Wij allen, vrijwel zonder uitzondering, zijn in staat tot fout of, meer modieus, stout gedrag. Het zogenaamde Milgram-experiment aan de universiteit van Yale, waar deelnemers werden verleid schijnbaar dodelijke stroomstoten toe te dienen aan een onschuldig slachtoffer, toont aan hoe gemakkelijk het merendeel van de mensen zich laat verleiden tot ondenkbare handelingen. Het gaat om een risico van materieel belang. Vertrouwen in mensen, onze medewerkers, onze collega's, mag daarom geen vanzelfsprekendheid zijn. Vertrouwen dient de uitkomst te zijn van een gedegen proces. En mochten wij daar zelf niet *in* geloven, gezien de wet- en regelgeving moeten we daar dan wel *aan* geloven.

De bron van het fraude- en integriteitrisico is niet autonoom

De oorsprong van het risico dat mensen (on)opzettelijk stoute dingen doen, is niet autonoom. De oorsprong zelf is namelijk beïnvloedbaar en daarmee afwijkend van ieder ander operationeel risico. Daarmee verdient dat risico ook een andere aanpak.
Wat is een risico met een autonome oorsprong? Stel dat regen als een risicobron en nat worden als het risico wordt gezien en een paraplu als een beheersmaatregel, dan kan een persoon droog blijven onder de paraplu, zonder dat de regen afneemt. De beheersmaatregel verandert niets aan de oorzaak, maar neemt slechts het gevolg weg. Het weer is autonoom en daardoor niet beïnvloedbaar. Beheersingsmaatregelen kenmerken zich door het wegnemen van de mogelijkheid, de gelegenheid, dat het bedrijfsproces last ondervindt van het risico. Het gaat dan om preventieve maatregelen en het monitoren van de kwaliteit van die maatregelen.
Het fraude- en integriteitrisico is in feite het mensrisico. De mens is opportunistisch en berekenend en daardoor niet autonoom. De mens reageert op beheersmaatregelen, positief en negatief, door zich anders te gaan gedragen. Een slot op de deur, ter voorkoming van binnentreden, kan ertoe leiden dat de mens op zoek gaat naar een raam dat toegang geeft tot de ruimte die met de deur is afgesloten of dat via het plafond toegang wordt gezocht. Dat betekent enerzijds dat aan de preventieve maatregelen hogere eisen moeten worden gesteld, maar dat anderzijds wellicht op een andere wijze met dit specifieke risico omgegaan dient te worden.
In tegenstelling tot het weer, laat de mens zich afschrikken of juist verleiden iets te doen. Dit betekent dat er maatregelen bestaan die voorafgaan aan klassieke preventieve maatregelen.

Als het om beheersing van het fraude- en integriteitrisico gaat, ligt daar dan ook de sleutel tot het succes. Je kunt zelfs komen tot een vorm van positieve 'social engineering', een vorm van beïnvloeding van sociaal gedrag en van attitudes.

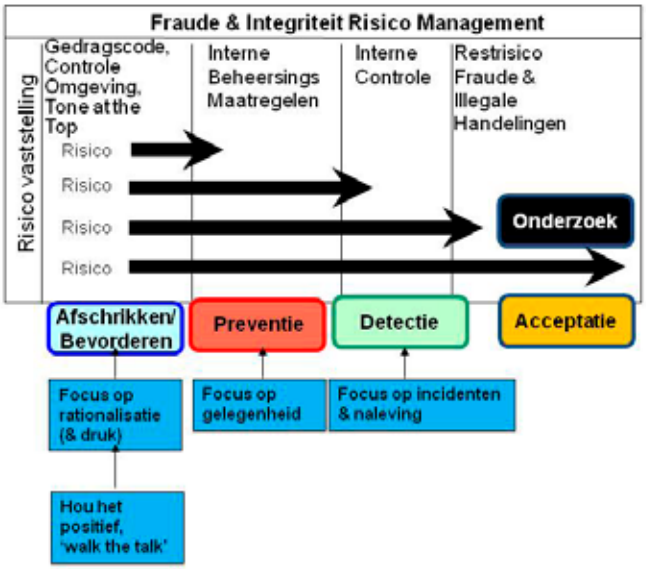
Beheersing van fraude- en integriteit, een model

Eenieder die ooit een cursus fraudebeheersing heeft gevolgd, is bekend met de zogenoemde fraudedriehoek. Als een persoon gelegenheid, druk en rationalisatie ervaart om tot een bepaalde handeling te komen, dan is de kans reëel dat die handeling ook wordt verricht. Als een van die elementen ontbreekt, dan kan is de kans dat de handeling zich voordoet minder groot.

Met kennis van de elementen van de fraudedriehoek zijn accountants en veiligheidsfunctionarissen hard aan de slag gegaan om vooral de gelegenheid tot het verrichten van ongewenste handelingen te dichten, door maatregelen van administratieve organisatie en interne beheersing, net zoals ze dat

zouden doen bij andere operationele risico's. Dat helpt maar ten dele, omdat het niet-autonome karakter van de oorzaak van het risico wordt miskend. Maar, gelegenheid maakt de dief, toch? Nee, helaas zo simpel is dat niet. Denk aan jezelf. Als een vers brood onbeheerd bij de bakker op de toonbank ligt en er even niemand in de winkel is, hoe waarschijnlijk is het dan dat jij dat brood meeneemt zonder te betalen? Die waarschijnlijkheid neemt toe als jij of je gezin honger heeft. Maar dan nog, is dat een rechtvaardiging om dat brood zomaar mee te nemen? Nee, je moet een dergelijke handelingen ook nog met je eigen geweten in overeenstemming kunnen brengen. Die rechtvaardiging is makkelijker als je weet dat iedereen in een dergelijke situatie dat brood meeneemt of als je meent zwaar maatschappelijk achtergesteld te zijn zodat proletarisch winkelen daarom een recht is.

Omdat niet de gelegenheid de dief maakt, maar het motief om te stelen, verdient het aanbeveling eerst te voorkomen dat het motief ontstaat of tot handelen leidt, alvorens te denken aan preventie en detectie van de handeling zelf. De eerste verdedigingslinie bij fraudebeheersing draait dan ook volledig om het creëren van een cultuur, waarin het minder waarschijnlijk is dat de deelnemers van de organisatie tot stoute dingen zullen overgaan. In die verdedigingslinie horen de zogenoemde 'soft controls' op basis van een gedragscode, die wenselijk gedrag bevorderen en onwenselijk gedrag afschrikken. Resterend ongewenst gedrag dient in de tweede verdedigingslinie door preventieve maatregelen te worden afgevangen. Fout gedrag dat niet valt te voorkomen moet dan actief worden opgespoord in de derde linie, waarna de keuze volgt om dat gedrag dan maar te accepteren of door handhaving of verder onderzoek aan te pakken. Modelmatig ziet dit model er als volgt uit:



Volgens dit model gaat aan preventie van ongewenst gedrag een aantal belangrijke maatregelen vooraf, die niet zozeer met de gelegenheid tot stout doen te maken hebben, maar met het motief om op een bepaalde manier te handelen. Maar wat motiveert de deelnemers van de organisatie om op een bepaalde manier te handelen. Wat drijft de mens tot bepaald gedrag?

Het gedrag van de leider en het gedrag van de massa drijven het gedrag van het individu

Wat doet mensen ergens toe bewegen? Een werkbare visie die een mogelijk antwoord geeft op die vraag, is beschreven door de Amerikaanse psycholoog Lawrence Kohlberg. Kohlberg heeft zich toegelegd op de ontwikkeling van het morele denken. Kohlberg onderscheidt in die ontwikkeling een preconventionele, een conventionele en een postconventionele fase. Kleine kinderen zijn preconventioneel, ze weten nog niet wat goed of fout is, wat gebruikelijk is of ongebruikelijk. Zij leren de conventies met vallen en opstaan, door straffen en belonen, tot het moment dat ze als vroeg-adolescent hun onschuld verliezen en de gebruiken gaan begrijpen, althans volgen. Dat volgen gaat heel ver, want zij leren dat je door het volgen van de gebruiken kennelijk succesvol bent. Kleding, schoenen, gedrag en loopbaankeus worden afgekeken van de rolmodellen; conventies van de massa bepalen het individuele gedrag. Het individu meent door die massa te volgen modieus te zijn en ontleent daaraan een gevoel van erbij horen, geaccepteerd worden, succes.

Straffen en belonen is in deze conventionele fase geen succesvol sturingsmiddel meer, aanspreken op succes wel. Sterker nog, een conventioneel mens door middel van straffen en belonen aansturen kan leiden tot regressie in het gedrag. Volwassenen gaan zich dan als kinderen gedragen. Daarom, stuur volwassenen aan door te wijzen hoe succesvol zij kunnen zijn door het volgen van conventies die zich uiten in het gedrag van de rolmodellen, bij voorkeur de leiding.

Het succesvolste rolmodel is de uiteindelijke leider, vandaar dat 'tone at the top' (voorbeeldgedrag) en 'tone from the top' (leiderschapstijl) zo van belang zijn bij de aansturing van organisaties. De gedachte vat post dat hij de conventies bepaalt en daarom zelf mogelijk postconventioneel is. Postconventionaliteit zet de collectieve normen opzij, want bepaalt die zelf. De suggestie is dat dit het ultieme stadium is dat een mens in zijn morele ontwikkeling kan bereiken, en dat dit uitzonderlijk is. Dit klinkt positief, maar bedenk dat postconventioneel ook heel goed zedeloos of immoreel kan betekenen.

> De beheersmaatregel verandert niets aan de oorzaak

Dat wij bijna allen door conventies worden gedreven, tonen oude foto's van onszelf. Uit die foto's blijken haardracht,

brilkeuzes en woninginrichting die altijd passen in een specifiek tijdbeeld waarin bijna iedereen vergelijkbare keuzes bleek te maken, terwijl wij dachten origineel te zijn.

Door schade en schande wijs?
Helaas gaat de uitdrukking 'door schade en schande wijs' in geval van fraude- en integriteitbeheersing zelden op. Er heerst veel naïviteit. Incidenten suggereren wat betreft benaming de uitzondering op de regel, wat tot incidentmanagement leidt. De gedachten dat organisaties op vertrouwen moeten worden gedreven of dat een beetje integer niet bestaat, doen nog verdere afbreuk aan toereikende integriteitbeheersing. 'Een beetje integer bestaat niet', een uitspraak van voormalig minister Dales, heeft een zodanige betekenis gekregen dat deze uitspraak voor velen een onwrikbare werkelijkheid is geworden. Waar deze retoriek in het begin van de jaren negentig behulpzaam was om het thema integriteitbeheersing op de agenda te krijgen, zit het nu effectieve verbetering van integriteit in de weg. Vanuit integriteit- en fraudebeheersing is de gangbaar geworden zwart-wit redeneertrant riskant. Willen organisaties en hun toezichthouders er in slagen om het integriteit- of frauderisico in de greep te krijgen, dan zullen ze analoog moeten leren denken, op een glijdende schaal, in plaats van digitaal. Door zwart-wit, in goed en fout te denken, verleiden organisaties zichzelf rijk te rekenen aan integere medewerkers, want volgens die visie is iedereen integer zolang het tegendeel niet is bewezen. En als het tegendeel wordt bewezen, kan worden geredeneerd, gaat het om een incident, een uitzondering die de regel bevestigt.
Zoals eerder gesteld, is vrijwel iedereen te verleiden tot het ondernemen van 'stoute' dingen. Je hoeft de statistieken wat betreft huwelijks(on)trouw of studies naar liegen er maar op na te slaan en je krijgt een ontluisterend beeld. Mensen zijn geen robots, maar denkende wezens van vlees en bloed, met lusten en behoeften, die niet altijd de verleidingen kunnen weerstaan of sociaal geaccepteerd willen worden en daarom meedoen aan activiteiten die ze eigenlijk niet onderschrijven. De gedachte van een beetje integer speelt daarbij een belangrijke rol: het foute kan door het goede worden gerechtvaardigd. Juist omdat zovelen een beetje stout zijn, zouden organisaties veel sterker dan ze tot op heden doen,

Een beetje integer bestaat niet

hun personeel moeten verleiden zich vooral op het goede te richten, indachtig dat zij dat niet uit zichzelf doen. Betrouwbaarheid, eerlijkheid en fatsoen zijn geen vanzelfsprekendheden. Integriteit vereist actieve beheersing. Actieve beheersing vereist inspanning en investering. Wijs wordt je pas als je investeert in kennis en vaardigheden.

Wat levert integriteit- en fraudebeheersing op?
Investeren in integriteit wordt door velen als een motie van wantrouwen in het personeel gezien. Bovendien, wat levert het nou eigenlijk op?
De gedachte aan een vermeende motie van wantrouwen maakt slechts duidelijk dat (de leiding van) een organisatie nog heel ver af staat van het erkennen dat fraude en onrechtmatig handelen inherent zijn aan het economisch deelnemen aan de maatschappij. Lees de krant en kijk televisie en leer dat fraude en integriteitinbreuken van alle dag zijn. Stoute mensen horen er bij, zoals ziekte van personeel er bij hoort. Inderdaad, je kan nooit iets aanpakken als je het bestaan ervan niet onder ogen ziet. Stoppen met roken lukt ook niet als je niet wilt beseffen of wilt geloven dat roken slecht is voor de gezondheid.
Het is niet meetbaar welke schade wordt voorkomen door goede fraude- en integriteitbeheersing. Je kunt immers niet meten wat er niet is. Hooguit is een vergelijking met het verleden te maken, maar werden de incidenten toen wel ontdekt? Ontdekte incidenten in het heden zijn ook geen graadmeter van succes van beheersing, omdat die mogelijk anders ook wel uitgekomen waren.
Goede fraude- en integriteitbeheersing uit zich in een plezierige loyale werkomgeving, waarin mensen weten waar ze aan toe zijn en zich kunnen en willen verantwoorden. Dit uit zich niet slechts in de organisatie, maar ook in verhoudingen die de individuen hebben namens de organisatie met derden. Goed en succesvol integriteitbeleid komt tegemoet aan individuele wensen en verlangens en geeft richting aan wenselijk gedrag. Waar klassiek beleid vooral eisen ('druk') stelt op basis van wet- en regelgeving ('demands'), zijn huidige inzichten in integriteit- en fraudebeheersing in belangrijke mate ook gebaseerd op de individuele behoeften, verlangens en verwachtingen ('desires'). In feite worden individuen door goed beleid verleidt tot wenselijk gedrag en dragen op die manier bij aan een weerbare organisatie.
Te soft? Goede fraude- en integriteitbeheersing uit zich voorts in lagere afkoopsommen voor niet functionerende medewerkers, betere en eenvoudigere verantwoording aan toezichthouders, lager ziekteverzuim, minder verloop personeel en verminderde aansprakelijkheid (boetes!) in geval van stoute werknemers.

Hoe kan ik integriteitbeleid in mijn organisatie ontwikkelen?
Fraude- en integriteitbeheersing is geen kwestie van inhuur van gelijkgestemden uit een goed nest, het wegsluiten van gevoelige documenten, het voeren van een ernstig gesprek over waarden en normen plus af en toe een incidentonderzoekje. Fraude- of integriteitbeheersing begint met te begrijpen wat integriteit eigenlijk is en het organisatiegericht nemen en blijven nemen van geëigende stappen.
Iemand is integer als hij of zij doet wat er van hem of haar wordt verwacht. Deze simpele stelling leidt tot een van

de meest ingewikkelde vraagstukken. Wat is een reële verwachting in een bepaalde situatie? Bestaan er universele waarden? Welke mate van naleving wordt er verwacht? Is de mate van naleving meetbaar te maken? Hoe is de naleving te bevorderen? Wat te doen als met opzet inbreuk wordt gemaakt op de verwachtingen? Kortom, veel vragen die heden ten dage op het allerhoogste niveau van een onderneming moeten kunnen worden beantwoord. Integriteit is een containerbegrip dat duidt op wenselijk gedrag op een bepaald moment, in een bepaalde situatie. Er zijn wel universele waarden die aan integriteit ten grondslag liggen, zoals terug te vinden in de universele rechten van de mens, maar daarmee kan je het beheersingsproces in een organisatie niet aansturen. Iedere relevante organisatie dient zich ervan

Conventies van de massa bepalen het individuele gedrag

te overtuigen wat voor die organisatie valt te definiëren als wenselijk gedrag. Die definiëring volgt daarbij de voor die organisatie relevante situaties waarbij menselijk gedrag van belang is. Een commerciële organisatie zal zich daarom buigen over de omgang met klanten en een overheidsorganisatie die vergunningen verleent, zal een visie ontwikkelen hoe om te gaan met de burger. De klant zal van organisatie tot organisatie heel anders kunnen zijn, zoals de burger van gemeente tot gemeente fors zal kunnen verschillen.

Pas als wenselijk gedrag goed is gedefinieerd voor een specifieke organisatie is het mogelijk een beeld te vormen van wat als integer wordt beschouwd. Organisaties leggen het als wenselijk geachte gedrag vast in gedragscodes. Die codes zijn de uitkomst van een gedegen proces, dat is te zien als de uitkomst van een integriteitrisicoanalyse.
Een code, die het positieve benadrukt, rekening houdt met de verlangens en verleidingen van individuen die samen de organisatie vormen, is de eerste stap in een integriteitbeheersingstraject. Daarom, geen betuttelende of hoogdravende code, maar een code die recht doet aan het karakter van de groep van vlees en bloed mensen die het betreft en daardoor uitnodigt tot wenselijk gedrag. Als je die code leest zou je onmiddellijk bij die organisatie willen werken. De code moet vervolgens tot leven worden gewekt, in leven worden gehouden, regelmatig aan de actualiteit worden aangepast, worden gehandhaafd en in primaire processen worden verankerd. De naleving dient zichtbaar en meetbaar te worden gemaakt. Pas als aan al die vereisten wordt voldaan, dan kan met recht vertrouwen worden uitgesproken in de individuen en kan beschaming van vertrouwen worden aangepakt.

Hoe krijg ik mijn verwachtingen tussen de oren van mijn werknemers?
Bij succesvolle fraude- en integriteitbeheersing wordt gebruikgemaakt van de beïnvloeding van 'desires'. Het fraude- en integriteitrisico is in feite de uitkomst van menselijk handelen. Menselijk gedrag is beïnvloedbaar, mits het gedrag past in de cultuur van de omgeving. Zoals hiervoor al is aangegeven, dient een organisatie de bij haar horende verwachtingen wat betreft gewenst gedrag vast te stellen. Bij de verdere verankering van dat gedrag begint het met hoe de leiding van een organisatie zich geloofwaardig volgens die verwachtingen presenteert, niet alleen in officiële uitingen, maar ook in de dagelijkse omgang of in het e-mailverkeer, binnen en buiten de organisatie. De uitgangspunten van het bewuste gedrag van de leiding dient terug te komen in beoordelingssystemen, in beloningsystemen en in interne- en externe bedrijfscommunicatie.
Veel organisaties lukt het om eenmalig een project op te zetten ter verbetering van de beheersing van het fraude- en integriteitrisico. Helaas, bij gebrek aan proceseigenaar, bij gebrek aan budget of de idee 'dat wij dat wel zelf kunnen', bij gebrek aan focus of de verdeling van verantwoordelijkheden voor het fraude- en integriteitrisico over vele personen, ebben de baten van dergelijke project daarna snel weg, tot een groot incident het onderwerp weer op de agenda zet.
Probleem bij eenmalige integriteitprojecten is dat een tweede keer de geloofwaardigheid fors is aangetast door het tussentijdse gebrek aan aandacht. Daarom, zelfs als het wettelijk niet is vereist, dan is blijvende aandacht door middel van strak gemanagede fraude- en integriteitbeheersing een vereiste, want psalm 146 stelt terecht dat niet op des mensen kind kan worden vertrouwd, met soms desastreuze gevolgen voor de organisatie.

Investeren in integriteit wordt door velen als een motie van wantrouwen in het personeel gezien

ACHTER HET NIEUWS

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

NATIONALE CYBER SECURITY STRATEGIE

In december 2009 vroegen de leden Knops, Voordewind en Eijsink in de Tweede Kamer al om een cybersecurity strategie. Het kabinet Rutte ging van start met de belofte om te komen tot een integrale aanpak van cybercrime. Op 1 maart moet hij er zijn. De Nationale Cyber Security Strategie, kortweg NCSS. Er is in januari een consultatie met bedrijven, overheidsdiensten en wetenschappers geweest. Een indrukwekkend gezelschap in een Haagse sociëteit. De NCSS regelt in grote lijnen hoe we de dreigingen rond internet willen aanpakken zodat het een veilige basis biedt voor economische groei. De NCSS heeft direct betrekking op het werk van veel informatiebeveiligers. We hebben vier leden van de redactie gevraagd te reageren op: 'Een Nationale Cyber Security Strategie zal ervoor zorgen dat informatiebeveiligers in de BV Nederland weer rustig kunnen slapen.'

Lex Dunn:
Zal ik weer rustig slapen als de NCSS er is? Ik denk het niet. Sterker nog, ik vrees dat er meer slapeloze nachten bij gaan komen. Hoe dat zo? De NCSS, en met name het eronder liggende actieplan, wil meer samenwerking bereiken tussen de partijen in Nederland die zich met 'cybermalheur' (zoals ik het noem) bezighouden. De informatie-uitwisseling tussen private en publieke partijen zal worden verbeterd, waardoor er meer inzicht ontstaat in kwetsbaarheden en actuele bedreigingen. En ik ga ervan uit dat dit niet minder zal zijn dan we nu weten. Ondanks deze 'bijwerkingen' is de NCSS een goede zaak.
Op de eerste plaats verwacht ik dat er meer bewustzijn zal ontstaan bij alle internetgebruikers, zowel de professionele als de thuisgebruikers. Dit zal ongetwijfeld leiden tot meer vragen aan ons, professionals. Op de lange termijn zal het effect hiervan positief zijn. Het zal echter in de praktijk wel iets meer vergen dan nog een Postbus 51-filmpje.
Ten tweede verwacht ik dat het mogelijk wordt een nauwkeurige kaart te maken van het bedreigingenlandschap, waaraan we met zijn allen bloot staan. Dat zal ertoe leiden dat we meer gericht onze beperkte middelen ter bestrijding van cybermalheur in kunnen zetten. En misschien zal die kaart het mogelijk maken om eindelijk eens de 'zware jongens' te slim af te zijn, in plaats van achter ze aan te hollen om de brokken op te ruimen.
Ten derde hoop ik dat de NCSS ertoe bijdraagt dat we objectief kunnen kijken naar cybermalheur, en ons minder laten leiden door sensationele artikelen in de pers. Emotioneel reageren aan de hand van subjectieve waarneming leidt meestal niet tot het gewenste resultaat.
Tot slot het internationale aspect. Ondanks het 'nationale' in de benaming is het uitdrukkelijk de bedoeling om internationaal aansluiting te zoeken. Cybermalheur is nu eenmaal geen nationaal feestje meer.

Rachel Marbus:
Een integrale aanpak van cybercrime. Het klinkt bijna te mooi om waar te zijn. Als jurist weet ik dat zaken integraal aanpakken vrij lastig kan zijn. Zie eerst maar eens alle neuzen dezelfde kant op te krijgen en als dat gelukt is, moet het ook nog in de praktijk worden gebracht. Bedenk hierbij dat tussen dromen en daden nog een zee van uitvoeringsproblemen ligt.
Maar juist omdat de afgelopen jaren is gebleken dat de noodzaak tot integrale aanpak steeds groter wordt - criminelen worden steeds geavanceerder en de cybercriminaliteit neemt toe - vermoed ik dat het deze keer beter zal gaan. De samenwerking met private partijen is toe te juichen. Daar zit immers een enorme bron van kennis waarmee een brug kan worden geslagen. De Bredolab-samenwerking toont aan dat het niet alleen kan, maar dat het ook succesvol kan zijn.
Toch heb ik nog wel gemengde gevoelens. Zeker als al het nieuws en de plannen rondom cybercrime in ogenschouw worden genomen. Ja, beter ingerichte en gecoördineerde bevoegdheden voor opsporing lijken me noodzakelijk. Maar tegelijk boezemt het mij ook angst in. Er zal grote aandacht moeten zijn voor de balans tussen opsporing en de rechten van burgers (en mogelijke verdachten), temeer daar de afbrokkeling van de rechten en vrijheden van diezelfde bur-

gers ook al langer een trend lijkt te zijn. Een uitbreiding van bevoegdheden zal dan ook streng wettelijk vastgelegd moeten worden met bijbehorende controlemechanismen. En toch hoop ik dat er serieus naar die bevoegdheden zal worden gekeken. Want die integrale aanpak kan in combinatie met betere opsporingsbevoegdheden en handhavingsmogelijkheden er hopelijk voor zorgen dat het tij keert. Eigenlijk hoop ik dat zowel de overheid als de private sector het daardoor zo druk krijgen dat er van slapen de komende tijd niet zo heel veel meer komt.

Gerrit Post: Wat verwacht ik van zo'n strategie? Samengevat ben ik er niet erg gerust op. Het wordt een Haags compromis met allerlei mitsen en maren. Veel jargon, zo abstract mogelijk opgeschreven én gezien de statuur en achtergrond van het zittende kabinet veel zelfregulering. Uiteindelijk levert dat weinig op. Dat is verontrustend omdat de risico's steeds verder toenemen en overzicht en inzicht, niet alleen bij de overheid, verder afnemen.
Wat zou ik willen zien? Feitelijk kun je hier gauw mee klaar zijn. In 2009 is er in de VS ook een NCSS tot stand gekomen. Wij lopen dus al twee jaar achter en moeten nog beginnen. We zouden de NCSS kunnen vertalen en implementeren. Dat gaat niet werken in het Nederlandse. De Amerikaanse NCSS is vooral Amerikaans, en laat weinig aan het toeval over. Het is nog maar de vraag hoe ze het daar gaan 'rooien'. Vooral het toezicht heeft het in zich verstikkend te worden. Dat strookt niet erg met onze hang naar zelfregulering.
Hoe dan? Het begint met inzicht in het te beschermen gebied. De digitale snelweg kent ook provinciale en lokale aftakkingen. Ieder niveau zou op zijn eigen manier moeten worden beveiligd. De hoogste niveaus uiteraard het zwaarst. De digitale backbone van de BV Nederland moet veilig zijn en ongevoelig voor aanvallen van zowel buiten Nederland als doorgegeven vanuit de lagere niveaus.
Maak dus een praktische onderverdeling van de nationale digitale infrastructuur in bijvoorbeeld drie niveaus. Stel voor ieder van de niveaus een security baseline vast die neerkomt op het invoeren van een soort Information Security Management System zoals ISO27000 dat voorstelt, toegesneden op de betreffende sector van de infrastructuur. Regel implementatie en toezicht en zorg voor een plaats in het nationale functioneringscircuit. Regel de financiering.
De rust die dan ontstaat zal tijdelijk zijn. Invoering en onderhoud van de NCSS wachten…

Ronald van Erven: Een Nationale Cyber Security Strategie is zeker een goede zaak en wel om vier redenen.
Informatiebeveiliging en cybercrime is een zeer breed vakgebied met veel raakvlakken in diverse branches. Gelet op de toenemende afhankelijkheid van informatie is het beleggen van focus en eigenaarschap onder de vlag van een NCSS een goede zaak.
Ook kan een NCSS er voor zorgen dat kennisdeling binnen de overheid en tussen de overheid en diverse branches wordt bevorderd. De insteek is nu vooral preventief en er moet een balans komen tussen preventie en evaluatie. Ik heb wel eens de indruk dat deze laatste moeilijk is bij de overheid. Dit vergt namelijk een praktische mentaliteit.
Er zijn teveel partijen binnen de overheid bezig met het vakgebied informatiebeveiliging en cybercrime. Zover ik mij nog uit mijn telecomtijd kan herinneren zijn er de GovCERT, HighTec crime team, AIVD, MIVD, NCO-T, Informatieknooppunt Cybercrime, o-IRT-O, ECP-EPN, SOVI, ICT response board, NICC, KLPD en diverse ISAC (informatie knooppunten). Excuses als ik nog enkele vergeten ben. Efficiëntie op diverse vlakken wordt eenvoudiger onder één organisatie. Ik denk dat de overheid er goed aan doet om al deze instanties, onder de vlag van de NCSS, samen te brengen tot één Informatiebeveiliging- en Cybercrime-organisatie. Wellicht brengt dit dan een ministerie van Informatie voort.
Dat door de komst van een NCSS de informatiebeveiliger rustig kan gaan slapen is de komende vijf jaar nog niet aan de orde. Dat is een best-case-scenario. Kortom, in het voorjaar 2011 is er, na twee jaar, een NCSS met een actieplan. Dat is een goede eerste stap.

Links:

Presentaties van InfoSecurity 2010:
www.slideshare.net/infosec10/auke-huistra-infosecuritynl-3-november-jaarbeurs-utrecht
www.slideshare.net/infosec10/koen-gijsbers-infosecuritynl

Brief van Minister Opstelten aan de Tweede Kamer over GovCERT Trendrapport 2010:
https://zoek.officielebekendmakingen.nl/kst-28684-292.html

Een thesis over de verantwoordelijkheden van de Overheid in Cybersecurity uit 2009:
www.prodef.nl/pdf/Thesis_Cyber_Security.pdf

De presentatie van Ronald Prins (Fox-IT) van de PvIB Trends sessie van eind vorig jaar:
www.pvib.nl/download/?id=17669268&download=1

NOMINATIES VOOR ARTIKEL VAN HET JAAR 2010

Benoeming van het artikel van het jaar begint een traditie te worden. Dit is al weer de derde keer dat het PvIB hiervoor een prijs uitlooft.

Er worden opnieuw drie prijzen uitgereikt, wat de jury de ruime gelegenheid moet geven om gepaste waardering uit te spreken. De reden om een prijs uit te reiken is om naar onze auteurs waardering uit te spreken en ze te bedanken voor hun artikelen. De kwaliteit was hoog in 2010, de jury zal dus ook flink aan het werk moeten. We hebben de jury van vorig jaar teruggevraagd:

- Uit het onderwijs: Leo van Koppen van de Haagse Hogeschool
- Als lezer: Kees Hintzbergen van 3-Angle
- Als auteur: John Rudolph van Verizon Business

De redactie heeft een lijst van negen artikelen genomineerd. Vaste rubrieken en artikelen van redactieleden dingen niet mee. De criteria die we de jury meegeven zijn ongewijzigd en van oplopend belang. De redactionele begeleiding helpt bij de eerste drie criteria. De laatste twee criteria gaan over de creatieve inbreng van de auteur. Uitreiking van de prijzen wordt opgenomen in het programma van de ledenvergadering en workshop op 19 april.

Beoordelingscriteria:

1. Is de opzet van het artikel juist voor de soort (inhoudelijk of opiniestuk)?
2. Is het artikel helder en begrijpelijk geschreven, met passende illustraties? Is de stijl consistent, zoals serieus of satirisch? Of het nu een praktijkbeschrijving is of een wetenschappelijke beschouwing betreft, is de leeservaring prettig?
3. Is het duidelijk wat de doelgroep is voor het artikel? Is het artikel te volgen voor een lezer buiten de subgroep?
4. Heeft het artikel visie en/of nieuwe gezichtspunten op een onderwerp?
5. Zet het de doelgroep aan het denken? In hoeverre slaagt de auteur er in om de lezer aan het denken te zetten?

Genomineerde artikelen (op chronologische volgorde):

1. Jaap van der Veen. De opbouw van IB-patronen. Informatiebeveiliging 1, 11
2. Peter Hoogendoorn en Jean-Pierre Vincent. Het business oriented autorisation model. Informatiebeveiliging 2, 11
3. Wendy Goucher. In marketing's Shoes. Informatiebeveiliging 3, 4
4. Erno Duinhoven. Een iPhone van de zaak. Informatiebeveiliging 3, 12
5. Leon Kuunders. Identity management en privacy. Informatiebeveiliging 4, 25
6. J. M. T. Wijnberg. Paspoortwet brengt burgers in gevaar. Informatiebeveiliging 4, 38
7. Ella Broos. Nederland is niet immuun voor autoritaire tendensen. Informatiebeveiliging 4, 43
8. Cor Rosielle. Trust Audits. Informatiebeveiliging 7, 19
9. Jan de Boer. Social engineering deel 8: De misleader aan het werk. Informatiebeveiliging 8, 4

COLOFON

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

Redactie
Lex Borger (hoofdredactie, werkzaam bij Domus Technica),
e-mail: lex.borger@domustechnica.com
Cynthia Kremer (eindredactie, Motivation Office Support bv, Nijkerk)
e-mail: ibmagazine@pvib.nl

Redactieraad
Said El Aoufi (Metapoint)
Tom Bakker (Delta Lloyd)
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
Rob Greuter
Maarten Hartsuijker (ANWB)
Aart Jochem (GOVCERT.NL)
André Koot (Univé-VGZ-IZA-Trias)
Rachel Marbus (BetterID4all)
Gerrit Post (G & I Beheer BV)

Advertentieacquisitie
e-mail: adverteren@pvib.nl

Vormgeving en druk
Van de Ridder Druk & Print, Nijkerk
www.vanderidder.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
De abonnementsprijs bedraagt 115 euro per jaar (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

GOEDE VOORNEMENS

De overgang van 31 december naar 1 januari wordt altijd gevierd met champagne, oliebollen en appelflappen. Zo ook bij ons thuis en uiteraard ook met de zogeheten goede voornemens. Berry heeft voor dit jaar ook een aantal goede voornemens en die wil ik graag met u delen. Niet alle voornemens zullen u interesseren maar mogelijk interessant is dat ik op alle machines alleen nog maar officiële software ga draaien. Mijn telefoon, mijn laptop en mijn bureaumachine gaan alleen software herbergen die ik zonder enige schroom kan laten zien aan de Business Software Alliance (BSA). Deze club is ooit eens opgericht door software- en hardwareleveranciers en heeft tot doel om softwarepiraterij in het bedrijfsleven te stoppen en toe te zien of de licentiekosten wel allemaal worden afgedragen. Software is natuurlijk een vreemd product. Je maakt een exemplaar en gaat deze meerdere keren dupliceren totdat je aan de vraag in de markt kunt voldoen. Met andere woorden, iedere extra kopie kost niets en levert wel het volledige licentiebedrag op. Een slimme leverancier verspreidt zijn spullen via internet. Op een website downloadt de klant de software en na betaling wordt de sleutel om de software daadwerkelijk te installeren toegezonden. Lekker handig voor zowel klant als leverancier.

Toch zie je al heel snel dat er een beweging ontstaat die het als sport ziet om de officiële wegen iets anders te bewandelen en het hele stappenplan uit te voeren behalve de betaalstap. Ik heb dit ook lange tijd gedaan en natuurlijk schaam ik mij daar hevig voor. Zoals eerder aangehaald zal ik mijn voornemen dan ook tot uitvoer gaan brengen. Ik zal niet meer op internet gaan zoeken naar illegale sleutels voor software maar tegelijkertijd moet ik ook zeggen dat die duistere hoeken waar je deze informatie vindt ook wel erg leuk zijn als je ziet wat je er allemaal tegenkomt. De afgelopen jaren ben ik de meest vreemde en rare zaken tegengekomen. Creditcardgegevens, handleidingen om beperkingen van hardware af te halen, de wegen naar illegale softwaresites, sites waarin supporters van voetbalclubs opgeroepen worden naar een bepaalde plek te gaan om de supporters van de tegenstander te gaan ontmoeten, sites waarop betaaltelevisie ineens gratis wordt, en zo zou ik nog tien pagina's kunnen volschrijven.

Ik begin met het eenvoudigste en pak mijn telefoon, kijk er meewarig naar, sluit hem uiteindelijk toch op mijn computer aan en reset hem naar de fabrieksinstellingen. Een kwartier later is alle software er af en heb ik weer heel veel geheugen vrijgemaakt op mijn telefoontje. Een aantal apps zal ik wel gaan missen maar even zoeken en na een dag heb ik al die handigheidjes weer terug, nu in de legale vorm. Trots laat ik de telefoon aan mijn vrouw zien die mij niet begrijpend aankijkt en mij vraagt wat er bijzonder is aan de telefoon die ik al lang heb en die ze al vaak gezien heeft. Ze twijfelt of ik een van de voornemens die ik ook had en met haar gedeeld had alweer vergeten was.

Als tweede pak ik mijn nieuwe laptop en kijk welke software, via donkere wegen verkregen, eraf moet. Het valt mee. Eigenlijk alleen een officepakket van een zeer grote leverancier. Eraf halen gaat sneller dan het plaatsen en ook de alternatieven zijn eenvoudig te vinden. Ik maak dit document met een open source tekstverwerker die verbazend compleet is en die tijdens het toetsen het lekkere gevoel van legaal werken geeft. Inmiddels is de tweede machine in mijn huis helemaal legaal gemaakt en met een glimlach zit ik achterover in mijn stoel te staren naar mijn laptop. Ik besluit mijn euforische gevoel niet te delen met mijn vrouw en denk na welke van de twee resterende machines ik nu ga legaliseren. Het zijn twee machines die eigenlijk helemaal opgebouwd zijn uit illegale softwarecomponenten waarbij het besturingssysteem het eerste obstakel is. Ik besluit eens te gaan neuzen op internet en zoek op plekken waar ik nog nooit eerder ben geweest, namelijk software verkopende webwinkels. Ik kom erachter dat de door mij gewenste versie van het besturingssysteem maar liefst 300 euro kost en dat valt wel een beetje tegen. Dit is het moment waarop mijn voornemens hard botsen met eerder gehanteerde principes namelijk dat software niets mag kosten. Ik besluit mijn voornemen eerst maar eens voor de helft uit te voeren en deze resterende machines volgende week onder handen te nemen. Maar ja dan ben ik weer aan het werk en heb ik er eigenlijk geen tijd voor. Dan doe ik het wel op een later moment besluit ik. Alweer een voornemen die de eindstreep niet haalt. Een beetje teleurgesteld in mijzelf sluit ik de machine af, maar ik weet dat ik dat gevoel snel kwijt zal zijn.

Groetjes,
Berry

SOPHOS

SECURITY SO COMPLETE YOU FEEL INVINCIBLE

WORRY LESS. ACCOMPLISH MORE.

CRYPSYS Data Security is de expert op het gebied van security oplossingen en distributeur van Sophos. Neem contact met ons op via sales@crypsys.nl of via 018 362 44 44 voor een gratis evaluatie versie! Voor meer informatie kunt u ook terecht op onze website: **www.crypsys.nl**

CRYPSYS data security