04/2011

INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 4 - 2011

BLACK HAT BRIEFINGS EUROPA 2011

ONZORGVULDIGE WETGEVING COMPUTERCRIMINALITEIT?

ANDROID-GEBRUIKER KWETSBAAR

VAN SAS70 NAAR ISAE 3402

CYBERSECURITY EN RISICOMANAGEMENT

FOX-IT

... for a more secure society

Fighting cybercrime

Protecting secrets

Finding digital evidence

Innovating internet interception

Ben jij de nieuwe foxer?

Fox-IT is het meest innovatieve IT Security bedrijf in Nederland en dé expert op het gebied van cybercrime, crypto, digitaal rechercheonderzoek en internet interceptie. Met een enthousiast team van zo'n 100 betrokken en gedreven medewerkers vertalen wij de ambities van onze klanten in concrete ICT oplossingen. Innovativiteit, vertrouwelijkheid, een excellente reputatie en de drive tot ontwikkeling zijn de kernwaarden binnen ons bedrijf.

Actuele vacatures:

- Senior Accountmanager / Sales manager
- HR Business partner
- Senior Security Expert Audits
- Linux beheerder met Windows affiniteit
- Software developer Cybercrime
- Software developer Forensics
- Medewerker Support Implementatie & Beheer
- Security Analyst Cybercrime
- Medewerker Security Monitoring (parttime)

Meer weten? Kijk op www.werkenbijfox-it.nl of mail naar vacature@fox-it.com

Fox-IT Olof Palmestraat 6 Delft 015 - 284 79 99 www.fox-it.com

VOORWOORD

In de uitvoering van mijn werk kom ik veel verschillende soorten beveiligers tegen. De detaillisten die ieder risico tot in de fijnste details willen doornemen en afdekken, de managers die de top 10 willen isoleren en de rest verwaarlozen, de architecten die de grote lijnen abstract willen invullen met visie, en de techneuten die iedere kwetsbaarheid technisch kunnen en willen oplossen. En vaak vergeten: de procesmedewerkers die worden blootgesteld aan de maatregelen die alle voorgaande groepen verzinnen. Een hele variëteit aan betrokkenen…

Je kunt met al deze partijen in discussie gaan. Hoe die discussies verlopen heeft veel te maken met de kennis en ervaring enerzijds en de betrokkenheid anderzijds. Zijn de beveiligers ook goed betrokken, dan krijg je strak opgezette, soepel uitvoerbare beveiliging waar alle betrokkenen zich in kunnen vinden. Ik ken een paar grote bedrijven waar dit duidelijk het geval is.
Is er een groot verschil met beveiligers tegenover betrokkenen, dan krijg je wat ik noem 'statuut-achtige' discussies. Ik doel hier op het motto van het statuut tussen Nederland en de (niet meer bestaande) Nederlandse Antillen: "Steunend op eigen kracht, doch met de wil elkander bij te staan". De kant van de eigen kracht van de betrokkenen is duidelijk, maar het 'bijstaan' door de beveiligers komt dan vooral over als de roep van een autoriteit op afstand. Dit wordt ook wel de ivoren toren genoemd. Het resultaat is strak noch soepel.
De ideale situatie is als iedereen betrokken is. De conversatie gaat dan over de kernzaken. Eenieder kan zijn standpunt inbrengen en verdedigen en er wordt met wederzijds respect een goed compromis bereikt. Beveiligen is tenslotte meestal een compromis, en zelden een doel op zich. In dat geval groeit de kennis en ervaring vanzelf.
Het omgekeerde is niet het geval. Veel kennis en ervaring leidt niet tot meer betrokkenheid. Het staat in mijn ervaring, opgegroeid op Curaçao, juist in de weg. Dat werkte al niet in de koloniale verhoudingen en het werkt niet met beveiligen.
Dit is de paradox voor ons beveiligers, die de kennis en ervaring hebben…

Lex Borger
hoofdredacteur

Rijkseenheidmonument ter ere van het statuut van de Nederlandse Antillen.

Foto omslag: Kevin Walsh

INHOUDSOPGAVE

VERSLAG

BLACK HAT BRIEFINGS EUROPA 2011

Frank Breedijk werkt als Security Officer voor Schuberg Philis, een leverancier van Mission Critical Outsourcing services. Hij is verantwoordelijk voor het toezicht op en de implementatie van het informatiebeveiligingsbeleid. Daarnaast is hij actief op Twitter (@seccubus), blogt hij voor www.cupfighter.net en is hij de auteur van de open source beveiligingstool Seccubus.

Op 17 en 18 maart 2011 vond in Barcelona de 11e Europese editie van de Black Hat conferentie plaats. Deze conferentie gaat al een flink aantal jaren mee en heeft, ook in een jaar waarin de ontwikkelingen rond informatiebeveiliging op hun hardst lijken te lopen, nog steeds niet aan actualiteit ingeboet. Op Black Hat Europe werden dit jaar 16 nieuwe tools of nieuwe versies van tools onthuld en in negen presentaties werden tot nu toe nog onbekende kwetsbaarheden verder uit de doeken gedaan
Black Hat is vorig jaar verhuisd van Amsterdam naar Barcelona om ruimte te bieden aan drie in plaats van twee *tracks*. Dit jaar werd één track geheel gevuld met workshops.

Zelf heb ik alleen presentaties bijgewoond, met name die in de tracks 'Application Dissection' en 'Infrastructure Rationale'. Ik heb van medebezoekers begrepen dat de andere tracks ook zeker de moeite waard waren.

Rafal Los: kwetsbaarheden business logic
Rafal Los gaf de presentatie 'Defying Logic - Theory, Design, and Implementation of Complex Systems for Testing Application Logic', over kwetsbaarheden in de *business logic* van applicaties. Hij raakte in dit onderwerp geïnteresseerd bij een online aanschaf. Hij maakte een fout bij het intikken van zijn creditcardgegevens, en vervolgens werd zijn bestelde artikel niet geleverd, maar werden de bijbehorende loyalty points wél bijgeschreven.
Fouten in de business logic van applicaties zijn over het algemeen schadelijker dan die in de technische implementatie. Om business logic-fouten op te lossen, is het vaak nodig een applicatie geheel opnieuw te ontwerpen of te schrijven en er zijn soms ook fysieke gevolgen.
Zo was het voorheen mogelijk om via internet een negatief aantal koffiecapsules te bestellen. Gevolgen: een negatieve afboeking van de creditcard, spookvoorraad voor de leverancier en mogelijk een zeer grote koffielevering omdat de tellers van de inpakmachines niet op negatieve getallen ingesteld zijn. Rafal onderzoekt voor zijn werkgever HP of het mogelijk is dit soort fouten geautomatiseerd op te sporen en demonstreerde de vooruitgang op dit gebied.

Rafal Los - CC by Xavier Mertens.

Marco Balduzzi: HPP vulnerabilities
Marco Balduzzi onderzocht met zelf ontwikkelde *tooling* de aanwezigheid van zogenaamde *HTTP Parameter Pollution (HPP) vulnerabilities* in de 5.000 meest populaire websites.
HPP *vulnerabilities* zijn al zo'n 11 jaar bekend, maar tóch bevatte maar liefst 30 procent van de sites, waaronder die van Google en Paypal, nog steeds een of meerdere pagina's met deze kwetsbaarheid.

Raul Siles: SAP vulnerabilities
Op de eerste dag kwamen met name

Room overview - CC by Xavier Mertens.

de SAP-systemen erg onder druk te liggen. Raul Siles liet in zijn presentatie 'SAP: Session (Fixation) Attacks and Protections (in Web Applications)' zien dat er *vulnerabilities* aanwezig zijn in diverse producten, zoals Joomla (inmiddels hersteld) en een op WebLogic gebaseerd intranet. Bij dit product was overigens geen sprake van een programmeer-, maar van een configuratiefout. Deze komt waarschijnlijk veel voor, aangezien het uitbannen van de kwetsbaarheid een niet-standaard-combinatie van parameters vraagt.
De aanwezigheid van deze kwetsbaarheid in SAP werd in zeer veel details uit de doeken gedaan. SAP is de laatste tijd vooruit gegaan op het gebied van beveiliging en brengt nu net als Microsoft op de tweede dinsdag van de maand zijn patches uit, maar het oplossen van kwetsbaarheden in live systemen is nog steeds een langzaam proces. Dit komt mede omdat SAP zijn producten standaard zeven jaar ondersteunt en klanten hier nog eens twee jaar support bij kunnen kopen. Hierdoor moet SAP patches op zeer veel versies uittesten en implementeren.

Andreas Wiegenstein: SAP manipuleren met ABAP
Andreas Wiegenstein gaf de tweede SAP presentatie 'The ABAP Underverse - Risky ABAP to Kernel communication and ABAP-tunnelled buffer overflows'. Hij nam ons mee in de wereld van ABAP, een proprietary taal waarmee veel SAP-consultants modificaties aan klantsystemen uitvoeren en waarin ook grote delen van SAP zelf geschreven zijn. ABAP biedt veel (gedocumenteerde) mogelijkheden om de data in het SAP-systeem te manipuleren. Hierbij worden netjes de regels met betrekking tot het rechtenmodel en *client separation* (het scheiden van data van verschillende klanten) gerespecteerd. De ABAP *runtime* ondersteunt echter ook niet-gedocumenteerde calls naar de ABAP *kernel*. Sommige van deze calls, Andreas noemde er acht, maken het mogelijk alle data in het SAP-systeem te manipuleren, ongeacht de security instellingen van SAP. Het kleinste ABAP-programma om de volledige controle over een SAP-systeem over te nemen is slechts 36 tekens lang. Een verbeterde versie die geen sporen op het systeem achterlaat, was met 56 tekens iets langer. Naast het misbruiken van de functionaliteit van de ABAP-taal, bleek het ook mogelijk via deze taal *buffer overflow attacks* uit te voeren op de SAP-kernel zelf.

Bruce Schneier: Cyber War of niet?
Bruce Schneier sloot dag een af met een *keynote* over *Cyber War*. Hierbij stond de vraag of er zo'n oorlog gaande is centraal. Bruce is van mening dat de term cyber war gehyped is. We leven in een wereld waar middelen die voorheen alleen voorbehouden waren aan landen nu ook binnen het bereik van 'niet landen' zijn, zoals bijvoorbeeld Anonymous. En we weten nog niet goed hoe we hiermee om moeten gaan.

Wim Remes: visualisatie van security
Op dag twee hield Wim Remes een minder technische, maar zeker interessante lezing over het gebruik van visualisatietechnieken door security professionals. Hij riep het publiek op meer te luisteren naar de hierover reeds ontwikkelde kennis. Hierbij is bijvoorbeeld de *inkt-to-info ratio* een goede maatstaf. Anders gezegd: hoeveel inkt is er nodig om de informatie weer te geven? Voegt het toevoegen van meer inkt (zoals 3D, rasterlijnen, kleur en mooie lettertypes) iets toe aan het overdragen van de informatie?

Claudio Criscone: virtualisatie kwetsbaarheden
Claudio Criscone's presentatie 'You are Doing it Wrong: Failures in Virtualization Systems' ging over kwetsbaarheden in virtuele infrastructuren. Virtualisatie en beveiliging gaan hand in hand, maar beveiliging richt zich dan vaak op de *hypervisor* (hoe voorkom je bijvoorbeeld dat de ene virtuele machine de andere ziet) of beveiliging binnen de virtuele machine. De beveiliging van de beheerlaag lijkt echter een onder-

Wim Remes - CC by Xavier Mertens.

geschoven kindje te zijn. Het security model dat bepaalt wat een beheerder wel en niet mag, wordt vaak opgesteld door diezelfde beheerders in plaats van de beveiligers. Volgens Claudio is dat niet wenselijk; daarom ontwikkelde hij het programma vGatekeeper. Dit creëert aan de hand van een lijst van toegestane acties Apache en mod_security configuraties die alleen deze acties toestaan. Zo kan bijvoorbeeld het uitzetten of het aanmaken van een virtuele machine worden geblokkeerd.

Black Hat tickets- CC by Xavier Mertens.

Jason Geffner:
non-exportable PKI keys

Jason Geffner liet in zijn presentatie 'Exporting non-exportable RSA keys' zien hoe je in een Microsoft omgeving *non-exportable PKI keys* toch kunt exporteren. Via een zeer knap staaltje *reverse engineering* toonde hij aan dat het zonder speciale hardware onmogelijk is sleutels aan het besturingssysteem beschikbaar te stellen zonder dat deze uit het geheugen te lezen zijn. Zijn tool is binnenkort via de Black Hat site te downloaden.

Al met al was deze editie van Black Hat weer zeer de moeite waard. Goede inhoud en eenvoudige toegang tot de sprekers dankzij de kleinschaligheid. En natuurlijk werkte het zonnige weer in Barcelona ook mee

Links

Black hat Europe: www.blackhat.com/html/bh-eu-11/bh-eu-11-home.html
Presentaties en ander materiaal van deze conferentie: www.blackhat.com/html/bh-eu-11/bh-eu-11-archives.html
Seccubus – www.seccubus.com

COLUMN

PRIVACYINBREUKEN ZIJN GOED!

Playstationgate, EPD afgeschoten, opslag biometrische paspoortdata gekilled, TomTom-heisa over geanonimiseerde gegevens, de CIOT-database (on)rechtmatig bevragen, iPhone volgt 'your every move'. En zo kan ik nog wel even doorgaan. Je zou kunnen zeggen dat het slecht gesteld is met de privacy en dat we ons ontzettend zorgen moeten maken. Ach, van die school ben ik niet. Ik ben namelijk blij. Wat zeg ik? In jubelstemming!

Het is het privacyminnend volk eindelijk gelukt. We staan op de agenda en niet zo'n klein beetje ook. Langzaam maar zeker voelt mijn onderbuik dat het tij aan het keren is. Niet langer worden zaken weggemoffeld, verdoezeld, in de doofpot gestopt of gewoon ontkend. Privacy is belangrijk, privacy is nieuws en privacy begint tussen de oren van de gemiddelde Nederlander ingebed te raken. Hele televisieprogramma's worden er inmiddels aan gewijd. Zo was onlangs Reporter in de ban van Facebook en privacy naar aanleiding van de paper van Arnold Roosendaal over de 'like button' en de privacy implicaties voor zowel gebruikers als niet-gebruikers van de sociale netwerksite (zie ook zijn artikel in nummer 1 IB 2011). Viviane Redding, vicepresident van de Europese Commissie, sloeg in datzelfde programma nog eens met de spreekwoordelijke vuist op tafel. De EU is haar privacywetgeving aan het herzien en buitenlandse mogendheden moeten niet denken dat ze in de toekomst nog zo makkelijk weg zullen komen met het schenden van de privacy van 'haar' Europese onderdanen.

En ook ons Nederlands privacytrots in bange dagen laat weer wat vaker haar tanden zien. Het College Bescherming Persoonsgegevens legde Google een last onder dwangsom op in verband met het wifi-snoopen. De boete kan oplopen tot een miljoen euro als Google haar zaakjes niet op orde brengt. De Sociale Inlichtingen en Opsporingsdienst (SIOD) kreeg er ook van langs vanwege het onrechtmatig koppelen van gegevens van burgers voor fraudebestrijding. Boetes die kunnen oplopen tot 100.000 euro als de privacyschending niet wordt gestaakt. En, in een recent rapport schoffelde het College de gegevensuitwisseling via het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) vol onderuit. De autorisaties tot het systeem (wie mag de gegevens inzien) en ook de beveiliging laten zeer te wensen over. De politie denkt daar natuurlijk heel anders over, want het zou slechts gaan om 'vormverzuim'. Toch vreemd dan dat bij een steekproef door het CBP van elf gevallen, er negen gevallen van onrechtmatige bevraging werden geconstateerd.

Maar goed. Blij ben ik er dus mee. Nu zult u zich misschien afvragen waarom die privacydame van het PvIB nu zo blij is met die massale inbreuken op de privacy van burgers en consumenten… Ik kan het simpel verwoorden: we pikken het niet langer! Politici (ik noem Jeanine Hennis en Sophie in 't Veld) bevechten de privacyonrechtvaardigheden en vinden een gewillig gehoor in politieke kringen. Journalisten ruiken nieuws, het journaal opent met allerhande privacymisstanden en de dagbladen schrijven de kolommen vol met datalekken en aanklachten tegen een te nieuwsgierige overheid. Burgerrechtenorganisaties zoals Bits of Freedom worden een stuk serieuzer genomen, ook al worden ze daardoor nog weleens geweerd bij een persconferentie (tegenstand is namelijk niet altijd gewenst of leuk). 'Ze' zijn bang geworden voor al die mensen die in toenemende mate tekeer gaan tegen mooi bedachte plannen die onze privacy schenden. Prima. Laat ze bibberen, laat ze vrezen. Wij vertellen erover op Twitter, zenden berichten door, doen publieke aanklachten tegen de gegevenshonger. En als je dan de mist ingaat, krijg je de publieke schandpaal als gevolg. Want wat is een van de meest effectieve middelen tegen privacyschenders? Juist. Openbaarheid en transparantie. Als u mijn privacy schendt, doen wij aan 'naming and shaming' in de hoop dat u, privacyschender, daar steeds banger van wordt en van tevoren bedenkt hoe u kunt voorkomen dat zaken misgaan. Dat is nog altijd beter dan genezen.

Mr Rachel Marbus
@rachelmarbus op Twitter

CONCEPTWETSVOORSTEL COMPUTERCRIMINALITEIT III: ONZORGVULDIGE WETGEVING?

Mr. J.J. (Jan-Jaap) Oerlemans is juridisch adviseur bij Fox-IT. Tevens is hij promovendus bij de afdeling eLaw@Leiden, centrum voor recht in de informatiemaatschappij, Universiteit Leiden. Jan-Jaap is bereikbaar op oerlemans@fox-it.com.

Ligt de grootste taak van bestrijding van computercriminaliteit door de wetgever bij de vervolging van mensen voor het stelen van naaktfoto's van BN'ers? Of misschien bij een nieuwe opsporingsbevoegdheid om grensoverschrijdend 'terughacken' mogelijk te maken? In dit artikel wordt een tipje van de sluier opgelicht over hoe de regering daar afgelopen jaar over dacht.

In de zomer van 2010 is namelijk een internetconsultatie van het conceptwetsvoorstel Computercriminaliteit III gehouden[1]. In het conceptwetsvoorstel wordt onder andere het bevel tot Notice-and-Take-Down door de officier van justitie als bevoegdheid gecreëerd en het helen van gegevens strafbaar gesteld. De formulering en toelichting op de artikelen laat echter nog te wensen over.

> Tóch denk ik dat de bevoegdheid tot het afgeven van een Notice-and-Take-Down-bevel er moet komen

In dit artikel wordt uitgebreid ingegaan op de belangrijkste punten uit het wetsvoorstel, namelijk het NTD-bevel, de bepaling voor heling van gegevens en het overnemen van gegevens uit een niet-openbaar werk. Uiteindelijk wordt antwoord gegeven op de vraag of het wetsvoorstel moet worden toegejuicht of nog aanpassing behoeft.

NTD-bevel officier van justitie

Notice-and-Take-Down houdt in dat de aanbieder van informatie in kennis wordt gesteld (de 'notice') van illegaal of onrechtmatig materiaal, en een verzoek wordt gedaan het materiaal te verwijderen (de 'take down'). Iedereen, inclusief opsporingsambtenaren, kunnen in de huidige situatie een beroep doen op de zogenaamde 'Notice-and-Take-Down-gedragscode'[2]. Onder deze gedragscode bepaalt uiteindelijk de beheerder van informatie, of de dienstaanbieder, of het verzoek 'onmiskenbaar onrechtmatige informatie' betreft en verwijderd moet worden. Onmiskenbaar onrechtmatige informatie is bijvoorbeeld prepuberale kinderpornografie. Twijfel kan bestaan over de onrechtmatigheid van informatie dat te maken heeft met delicten als smaad, haatzaaiing en het oproepen tot het plegen van misdrijven of geweld. Degene die de beschikkingsmacht heeft over de informatie bepaalt uiteindelijk of de informatie wordt verwijderd.

Op basis van artikel 54a van het Wetboek van Strafrecht (hierna: Sr) zou een officier van justitie, na machtiging van een rechter-commissaris, de bevoegdheid hebben een bevel tot Notice-and-Take-Down te geven. Let op! Het gaat hier om een *bevel* en niet om een verzoek waar vrijwillig aan kan worden voldaan. De formulering van het artikel is echter zó belabberd, dat het bevel niet rechtmatig is. Uit literatuur blijkt dat aan artikel 54a Sr zoveel tekstuele, wethistorische, wetsystematische en rechtsbescherming bezwaren kleven, dat het niet rechtmatig kan worden toegepast[3]. Dit is in de praktijk ook gebleken, want in twee zaken (bij de Rechtbank Assen op 22 juli 2008 en het gerechtshof Leeuwarden op 20 april 2009) weigerde een rechter-commissaris toestemming te geven voor een NTD-bevel op grond van artikel 54a Sr.

Gedragscode.

De huidige situatie, dat in de praktijk alleen een beroep op de NTD-gedragscode kan worden gedaan, wil de regering veranderen. In het conceptwetsvoorstel Computercriminaliteit III wordt in artikel 125p van het Wetboek van Strafvordering voorgesteld een gespecialiseerde officier van justitie de bevoegdheid te geven tot het afgeven van een bevel tot Notice-and-Take-Down. Het bevel om de gegevens ontoegankelijk te maken zou moeten gelden voor *elk* misdrijf en kan wor-

den afgedwongen met een last onder dwangsom (een boete die elke dag oploopt indien niet wordt voldaan aan het bevel). Het begrip 'ontoegankelijkmaking' ziet toe op het offline halen van informatie met behoud van een kopie ten behoeve van een eventueel strafproces. Belangrijk is dat volgens de Memorie van Toelichting de ontoegankelijkheidsmaking ook kan bestaan uit het *filteren of blokkeren* van

Computercriminaliteit bij Nieuwsuur.

gegevens bij een aanbieder van een communicatiedienst. Het bevel tot de ontoegankelijkheidsmaking van gegevens kan namelijk ook worden gegeven voor nieuwe strafbare feiten. Filteren is een methode om ontoegankelijkheidsmaking van nieuwe strafbare feiten te bewerkstelligen. De regering sluit niet uit dat de filterverplichting wordt gebruikt ter bestrijding van de schending van auteursrechten op internet[4]. Eerst zal echter nog de Tweede Kamer en Eerste Kamer moeten worden overtuigd van de noodzaak van zo'n vergaande maatregel. Aan de artikelen die te maken hebben met Notice-and-Take-Down is echter nog meer aan te merken.

Ten eerste vervalt in het voorgestelde artikel de machtiging van de rechtercommissaris. Dat betekent dat er geen onafhankelijke rechterlijke macht meer controleert of het NTD-bevel wel terecht is afgegeven. De machtiging van de rechter-commissaris heeft een belangrijke functie want het verwijderen van bepaalde informatie op internet staat in spanning met het recht op de vrijheid van meningsuiting, zoals onder andere neergelegd in artikel 7 Grondwet. In de Memorie van Toelichting op het conceptwetsvoorstel wordt aangegeven dat het NTD-bevel juist in die gevallen wordt toegepast waar de gedragscode niet toereikend is. Oftewel, in die gevallen waar twijfel bestaat of het om *onmiskenbaar* onrechtmatige informatie gaat. Zoals eerder is aangegeven gaat het hierbij in de praktijk vooral om delicten zoals smaad en haatzaaiing. De regering onderkent dat voor de beoordeling van uitingsdelicten een 'diepgaande juridische expertise' vereist is. Als oplossing wil zij een bepaalde groep officieren van justitie een opleiding geven om beter de afweging te kunnen maken of het materiaal van het internet verwijderd moet worden of niet. Ik ben niet overtuigd van deze waarborg en geloof dat het beter is het vereiste van de machtiging van een rechter bij de NTD-bevoegdheid terug te laten komen[5].

> De argumentatie van de minister is flinterdun en behoeft meer toelichting

Ten tweede wordt nergens in het artikel of in de toelichting op het conceptwetsvoorstel gesproken van een melding aan de informatieaanbieder dat de informatie van de desbetreffende server ontoegankelijk wordt gemaakt. De internetaanbieder wordt ook niet verplicht een klant in kennis te stellen van de verwijdering van de informatie. Het 'slachtoffer' van de take down, moet er dus zelf achter komen of de informatie is verwijderd en moet dan zelf bedenken dat hij naar de raadkamer kan stappen om zijn recht van beklag (op grond van artikel 552a Sv) uit te oefenen[6]. De vraag is of dat in de praktijk wel gebeurt en een notificatieplicht is daarom wellicht wenselijk. Wel brengt het een extra administratieve werklast voor justitie met zich mee.

Ten derde is de dwangsombevoegdheid in het voorgestelde artikel 125q Sv curieus. Een last onder dwangsom is een handhavingsmaatregel uit het bestuursrecht. Het Openbaar Ministerie kan al langer een bestuurlijke boete opleggen (denk aan de boete bij het rijden door rood licht). Bij een dwangsom wordt de betrokkene echter verplicht een boete te betalen zolang niet wordt voldaan aan het bevel tot herstel van de rechtmatige situatie. Het is echter maar de vraag of het opleggen van een last onder dwangsom door een officier van justitie rechtmatig is. De argumentatie van de toenmalige minister van Justitie voor de bevoegdheid is flinterdun en behoeft meer toelichting[7]. De vergaande maatregel is bovendien een vermenging van het bestuursrecht en strafrecht, iets waarover erg goed moet worden nagedacht[8].

Tóch denk ik dat de bevoegdheid tot het afgeven van een Notice-and-Take-Down-bevel er moet komen. Er zijn zeker situaties te bedenken waarin een afdwingbaar NTD-bevel wenselijk is. Bijvoorbeeld wanneer kinderpornografie wordt gehost, een botnet wordt aangestuurd of spam wordt verstuurd, bij een 'bulletproof hosting provider' in Nederland. Bij dit soort dienstaanbieders is het een onderdeel van hun business model niet mee werken met

politie en justitie. Het bevel tot Notice-and-Take-Down moet natuurlijk niet te snel worden afgegeven, omdat daarmee ook interessante monitoring-mogelijkheden verloren gaan waarmee wellicht het criminele netwerk achter de strafbare activiteiten kan worden achterhaald. Maar, bij een zorgvuldig afgewogen beslissing, na machtiging van de rechter-commissaris (eventueel mondeling gegeven wegens tijds-gebrek), kan ik mij een afdwingbaar NTD-bevel bij dit soort delicten goed voorstellen. Het voordeel van een bevoegdheid tot NTD in plaats van een beroep op de gedragscode is dat het bevel tot Notice-and-Take-Down kan worden afgedwongen en het OM niet afhankelijk is van de willekeur van de communicatieaanbieder.

Actief waarschuwen geïnfecteerde gebruikers.

Naast het NTD-bevel worden in de nieuwe Wet Computercriminaliteit wellicht een aantal belangrijke veranderingen doorgevoerd in het Wetboek van Strafrecht. Hier wordt in de volgende paragraaf op ingegaan.

Heling van gegevens

De Manon Thomas-zaak is een katalysator geweest voor de strafbaarstelling van het overnemen van gegevens uit een niet-openbaar werk en het beschikbaar stellen van die gegevens (heling van gegevens). In deze zaak werd een 'privéfilmpje' waarop de presentatrice naakt was te zien en naaktfoto's van de computer van Manon Thomas gestolen. Via YouTube en het chatprogramma MSN Messenger werd het beeldmateriaal verder verspreid. Door het Hof Leeuwarden werd schending van het portretrecht en auteursrecht van de presentatrice bewezen geacht en de verdachte veroordeeld tot werkstraf van 30 uur en een boete van €250,-. Daarnaast moest de verdachte €3000,- aan immateriële schadevergoeding betalen[9].

In deze zaak kon de dader niet strafrechtelijk worden vervolgd, omdat computervredebreuk niet kon worden bewezen. Het verder verspreiden van gegevens kon bovendien niet onder de normale helingbepaling worden geplaatst, omdat gegevens binnen het strafrecht in principe geen 'goed' zijn. Naar aanleiding van deze zaak zijn Kamervragen gesteld en heeft de regering besloten dat het wenselijk is het wederrechtelijk overnemen van gegevens uit een niet-openbaar werk strafbaar te stellen in artikel 139c Sr.

> Het toont aan waarom het Openbaar Ministerie de verantwoordelijkheid niet alleen zou moeten dragen

Als voorbeeld wordt de situatie genoemd dat een werknemer zonder toestemming bedrijfsinformatie kopieert met de bedoeling deze voor zichzelf of een ander te gebruiken. Het beschikbaar stellen van die gegevens, oftewel 'heling van gegevens', wordt in het conceptwetsvoorstel in artikel 139e Strafbaar gesteld.

Koops heeft uitvoerig commentaar geleverd op de artikelen. Hij merkt op dat wellicht nog expliciet een rechtvaardigingsgrond in de Memorie van Toelichting moet worden gezet, omdat klokkenluiders soms om hele goede redenen informatie 'stelen' en verder verspreiden. Ook stelt hij, mijns inziens terecht, dat het vreemd is dat heling niet van toepassing zou zijn als gegevens zijn verkregen door diefstal of afpersing van een laptop. Ten slotte geeft de auteur aan dat de clausule 'ten tijde van' in de helingbepaling ontbreekt. Als dit niet wordt gerepareerd in het artikel dan zou degene die de gegevens heeft verkregen ook strafbaar zijn als hij pas achteraf kennis krijgt van de strafrechtelijke afkomst van de gegevens[10].

> De bereidheid bij de regering is er om auteursrechtschending op internet beter te handhaven

Als laatste noemenswaardige artikel wordt in het conceptwetsvoorstel ook het heimelijk opnemen van communicatie strafbaar gesteld. Wellicht verrassend is echter de mogelijke *last-minute* wijziging van het mogelijk maken van hacken als opsporingsmethode.

Hacken als opsporingsmethode

Op 25 oktober 2010 heeft minister van Veiligheid en Justitie, Opstelten naar aanleiding van Kamervragen van PvdA-

kamerlid Recourt toegezegd voorstellen te doen om hacken als opsporingsbevoegdheid in de wet vast te leggen. De Kamervragen werden gesteld naar aanleiding van een uitzending van Nieuwsuur waarin officier van justitie Lodewijk van Zwieten pleitte voor het mogelijk maken van 'terughacken'[11]. Het vastleggen van hacken als opsporingsbevoegdheid in de wet is echter geen eenvoudige opgave.

Het zal waarschijnlijk niet gaan om één opsporingsbevoegdheid, maar meerdere. Hacken kan namelijk allerlei toepassingen hebben in een opsporingsonderzoek. Het kan gaan om het hacken van computers teneinde 'rond te kijken' of bestanden te kopiëren voor bewijsmateriaal. Verder kan overwogen worden dat het bij 'terughacken' gaat om het uitschakelen van een geautomatiseerd werk (bijvoorbeeld een computer of server) op afstand. Elk van deze toepassingen leveren echter verschillende inbreuken op de persoonlijke levenssfeer - en wellicht nog andere grondrechten - van de betrokkene. Naar mijn mening moeten voor toepassing van de opsporingsmethode daarom zware waarborgen gelden. Onduidelijk is welke waarborgen dat moeten zijn.

> De Manon Thomas-zaak is een belangrijke katalysator geweest om heling van gegevens strafbaar te stellen

Op deze en andere vragen moeten nog antwoorden komen. Bovendien is het maar de vraag in hoeverre 'grensoverschrijdend' hacken juridisch mogelijk is, aangezien opsporingsbevoegdheden in principe maar tot de Nederlandse grens mogen worden toegepast. Voor de toepassing van opsporingsbevoegdheden in het buitenland moet eerst een rechtshulpverzoek worden gedaan.
Indien hacken als opsporingsbevoegdheid in de Wet Computercriminaliteit III wordt vastgelegd levert dat in elk geval een andere dimensie aan het wetsvoorstel. Wellicht zal de discussie verschuiven van voornamelijk de NTD-bevoegdheid naar de vergaande opsporingsbevoegdheid tot hacken.

Conclusie

Met het wetsvoorstel zal het voor het Openbaar Ministerie gemakkelijker worden illegaal materiaal van internet te halen. Door het als een opsporingsbevoegdheid aan te merken kan het NTD-bevel bovendien worden afgedwongen en dat is in sommige situaties zeer wenselijk. Wel is het artikel in haar huidige formulering naar mijn mening te vergaand, omdat het om 'elk misdrijf' kan gaan, geen toestemming van de rechter-commissaris meer is vereist en het een filterverplichting kan betreffen. De machtiging van de rechter-commissaris moet daarom wat mij betreft terugkomen in het artikel. Ten slotte is de dwangsombevoegdheid slecht beargumenteerd en het artikel over heling van gegevens slordig geformuleerd. Op deze punten is het conceptwetsvoorstel slordig te noemen. Toch leveren de voorgestelde maatregelen wellicht een bijdrage aan een effectievere vervolging van computer gerelateerde delicten.

> De grensoverschrijdende toepassing van opsporingsbevoegdheden is juridisch gezien nog erg beperkt

Nu moet worden afgewacht in welke vorm het wetsvoorstel naar de Tweede Kamer wordt gestuurd. Zal de machtiging van de rechter-commissaris terugkomen en houdt Opstelten zich aan zijn toezegging hacken als opsporingsmethode mogelijk te maken?
Het zal spannend worden om te zien wat er van het wetsvoorstel overblijft na debat in zowel de Tweede Kamer als de Eerste Kamer.

Eindnoten

Het conceptwetsvoorstel, de Memorie van Toelichting en de reacties zijn te vinden op:

http://internetconsultatie.nl/wetsvoorstel_versterking_bestrijding_computercriminaliteit. (Archived at www.webcitation.org/5yGLdr99m).

[2] De gedragscode is te downloaden via:

URL: www.samentegencybercrime.nl/UserFiles/File/,DanaInfo=ex01tp+NTD_Gedragscode_Opmaak.pdf. Accessed: 2011-04-27. (Archived at www.webcitation.org/5yGKGDEXv).

[3] M.H.M. Schellekens, B.J. Koops & W.G. Teepe, Wat niet weg is, is gezien. Een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime, Universiteit van Tilburg 2007, p. 42. Beschikbaar op: www.cycris.nl/uploads/NTD-54a_rapport_--_30_november_2007.PDF. (Archived at www.webcitation.org/5yGJb3ODX).

[4] Zie Memorie van Toelichting conceptwetsvoorstel versterking bestrijding computercriminaliteit, p. 13 en de brief van 11 april 2011 van staatssecretaris Teeven aan de Kamer over het beleid met betrekking tot auteursrechten. De regering is voornemens downloaden uit illegale bron te verbieden en als maatregel een filterverplichting mogelijk te maken.

[5] Ik ben niet de enige die hier zo over denkt. Op 15 september 2010 hebben twintig (!) hoogleraren en belangenorganisaties een 'brandbrief' gestuurd naar de toenmalige demissionaire Minister van Justitie. Een belangrijk punt is dat in de brief wordt gepleit voor de terugkeer van de machtiging van de rechter-commissaris bij het NTD-bevel wegens het spanningsveld met de vrijheid van meningsuiting. De brief is beschikbaar op: https://www.bof.nl/live/wp-content/uploads/brandbrief.pdf. (Archived at www.webcitation.org/5yGKU5a0R).

[6] Zie ook B.J. Koops, 'Tijd voor Computercriminaliteit III', NJB 2010, afl. 38, p. 2463.

7 Zie uitgebreid: J.J. Oerlemans, 'Het conceptwetsvoorstel versterking bestrijding computercriminaliteit nader bezien', Tijdschrift voor Internetrecht 2010, nr. 5, p. 148-152. Beschikbaar op: http://weblog.leidenuniv.nl/media/blogs/106178/J.J._Oerlemans_-_Tijdschrift_voor_Internet_recht_-_conceptwetsvoorstel_nader_bezien.pdf. (Archived at www.webcitation.org/5yGKdhtq9).

[8] Zie ook B.J. Koops, 'Tijd voor Computercriminaliteit III', NJB 2010, afl. 38, p. 2464.

[9] Hof Leeuwarden 4 mei 2010, LJN BM3169.

[10] B.J. Koops, 'Tijd voor Computercriminaliteit III', NJB 2010, afl. 38, p. 2465.

[11] Het fragment is beschikbaar via: http://nieuwsuur.nl/video/193776-de-strijd-tegen-cybercrime.html. (Archived at www.webcitation.org/5yGKpeW7H). De uitspraak werd gedaan naar aanleiding van het ontmantelen van botnets van computers die besmet waren met Bredolab-malware.

ANDROID-GEBRUIKER KWETSBAAR DOOR TRAAG DOORGEVOERDE UPDATES

Maarten Hartsuijker is security consultant bij Classity Informatiebeveiliging. Hij helpt organisaties met security management, security audits en website penetratietesten. Volg Maarten via @classityinfosec.

Beveiligingskwetsbaarheden in software zijn aan de orde van de dag. Microsoft patcht ze maandelijks, Oracle elk kwartaal en ook Apple ontkomt er niet aan om de software zo nu en dan van een pleister te voorzien. Waar het de PC betreft zijn softwareleveranciers redelijk op beveiligingsupdates ingespeeld. Waar het onze telefoon betreft, hebben sommige leveranciers nog een lange weg te gaan.

Begin dit jaar werd bekend dat de hackertool Metasploit een functie heeft toegevoegd om automatisch misbruik te maken van een kwetsbaarheid in Android-telefoons. Via de functie kan een gebruiker van de Metasploit tool automatisch gegevens van een telefoon kopiëren. Hiervoor hoeft hij de gebruiker van de telefoon alleen over te halen om zijn website te bezoeken. Om misbruik van de kwetsbaarheid te kunnen maken dient een aanvaller wel de naam van het bestand te kennen dat hij dient te stelen. Maar doordat veel bestanden (zoals bijvoorbeeld de met de camera genomen foto's) eenvoudig te raden namen hebben, vormt dat niet de allergrootste drempel.

Hardware fabrikanten veel te laat met Android updates

Een kwetsbaarheid als deze is op zichzelf verre van schokkend. De kwetsbaarheid werd in november ontdekt, netjes gemeld en door Google weggenomen in Android 2.3. Om gebruikers te beschermen werden de details achtergehouden tot medio januari. Wat echter wel schokkend is, is dat de overgrote meerderheid van de Android-gebruikers zich met geen mogelijkheid tijdig tegen de kwetsbaarheid kan beschermen.

Android is niet Android

Hoewel we omkomen in Android-telefoons en telecomproviders zelfs klagen over het grote aantal producten met vergelijkbare specificaties, is geen Android-telefoon functioneel exact hetzelfde. Bijna elke fabrikant voorziet Android van een eigen grafische schil en eigen apps of modules. Doordat elke fabrikant Android een klein beetje aanpast, moet ook elke fabrikant moeite doen om updates van Google te verwerken in hun eigen Android-versie. Niet elke fabrikant is hier even happig op, wat er toe leidt dat wij als eindgebruikers blijven zitten met een telefoon die door hackers eenvoudig misbruikt kan worden.

Mogelijke gevolgen

We zetten onze telefoon steeds breder in. Niet alleen bevatten smartphones steeds vaker vertrouwelijke informatie, met misbruik van de telefoon zelf kan ook veel geld worden verdiend. Met een botnet aan telefoons kan een internetcrimineel natuurlijk traditionele internetaanvallen uitvoeren. Maar het is wellicht nog interessanter om de telefoons te laten bellen of sms'en naar dure betaalnummers. Of om op de telefoon een TAN-code aan te vragen om mee te internetbankieren. Of indien de telefoon een functie als digitale portemonnee krijgt, misbruik te maken van de betaalfunctie. 'Gelukkig' beperkt deze 'cross-zone'-kwetsbaarheid zich tot het stelen van gevoelige informatie van een Android-telefoon, maar net als met Windows, Linux en Mac is het natuurlijk slechts een kwestie van tijd tot er een zeer ernstige kwetsbaarheid wordt onthuld waarop de leveranciers geen (of een heel laat) antwoord hebben.

Goede bescherming vereist continu updaten.

Eindgebruiker niet serieus genomen

Het lijkt er op dat de telefoonfabrikanten de eindgebruiker vooralsnog niet erg serieus nemen. Google neemt weliswaar de verantwoordelijkheid om de kwetsbaarheden weg te nemen uit de Android 'core', maar na Google dienen ook de fabrikanten en telecomoperators mee te werken. En die lijken vooralsnog niet te springen om hun klanten te beschermen. De updates voorzien de klanten vaak ook van nieuwe features. En die nieuwe features zijn nou juist vaak de aanzet tot het kopen van een nieuwe telefoon. Daarnaast is het verwerken van de updates voor alle modellen gewoon erg prijzig. Men moet in dat licht wellicht nog wennen aan het feit dat men door

de keuze Android-maatwerk te leveren ook de verantwoordelijkheden van een volwaardige softwareleverancier heeft gekregen.
Daarnaast bevatten nieuwe Android-versies nieuwe functionaliteit. En nieuwe functies zijn nou juist het best business model om consumenten over te halen tot het kopen van een nieuwe telefoon.

Op een verzoek voor een update voor een HTC desire, reageerde de fabrikant als volgt:
"We kunnen op dit moment geen verdere informatie verschaffen over de mogelijkheid van deze update. Mocht hierover verdere informatie beschikbaar komen, dan kunt u deze vinden op onze website, (htc.com) en onze Facebook- en Twitter pagina's. Gelieve deze kanalen in het oog te houden voor verder informatie."
Voor een eindgebruiker is een dergelijke reactie uiteraard uitzichtloos. Begin mei (vele maanden nadat Google de updates beschikbaar stelde) start HTC eindelijk met de uitrol van de updates, maar slechts voor een beperkt aantal toesteltypen.

Op welke support hebben we eigenlijk recht?
Microsoft onderhoudt een oude Windowsversie als XP tot ruim 12 jaar na de releasedatum. Apparatuur waarop de software is geleverd is daardoor een ruime tijd bruikbaar. Maar hoe zit dit eigenlijk met onze telefoon? Of met onze tablets? Hoe snel dwingen fabrikanten ons straks tot vervanging doordat onze apparatuur niet meer van beveiligingsupdates wordt voorzien?

Gebruikers machteloos

Door de uitzichtloze situatie waarmee fabrikanten als Samsung, Motorola en HTC ons confronteren, reist de vraag waar we als eindgebruikers eigenlijk recht op hebben. Terwijl Google begin december Android 2.3 lanceerde worden telefoons zoals de HTC Desire/ Wildfire, de Samsung Galaxy S en de Motorola DEFY maanden later nog steeds uitgeleverd met Android 2.2 of 2.1. Als mainstream toestellen als de DEFY, de Desire en de Galaxy S, al zo slecht worden onderhouden op het moment dat ze nog volop in de verkoop zijn… hoe zal het onderhoud van deze modellen dan zijn op het moment dat er een nieuwe versie op de markt is gekomen? Motorola is hier op haar website duidelijk over. Het geeft aan nauw samen te werken met Google en haar telecompartners om haar klanten een zo optimaal mogelijke gebruikerservaring te bieden, maar zal het merendeel van haar telefoons (zoals te lezen op: https://supportforums.motorola.com/community/manager/softwareupgrades) helaas niet meer van een nieuwe Android-versie voorzien.

Om een smartphone zo goed mogelijk te kunnen onderhouden is het verstandig om gebruik te maken van een toestel dat zo dicht mogelijk op de eigenlijke softwareontwikkelaar zit. Google maakt vooral gebruik van de hardware van derden (OEM's) om Android aan de man te brengen. De wijze waarop deze partijen met hun firmware omgaan maakt het lastig om updates van Google snel op de telefoon te krijgen. Daarnaast hebben ook veel telecomproviders specifieke wensen ten aanzien van de telefoons die ze uitleveren. De lange keten tussen de ontwikkelaar en de eindgebruiker maakt het snel uitbrengen van beveiligingsupdates complex.

Wil je een zo veilig mogelijke telefoon? Overweeg dan om in plaats van een HTC, Motorola of Samsung Android-telefoon een Google Nexus, Apple iPhone of een Blackberry aan te schaffen. Al deze telefoons staan onder directe controle van de bouwers van de software. Ook Microsoft probeert vanaf Windows Phone 7 haar gebruikers gedeeltelijk rechtstreeks van updates te voorzien. Hierdoor kun je als eindgebruiker sneller beschikken over de

HTC: doodstil rondom beveiligingsupdates

updates die in reactie op beveiligingskwetsbaarheden zijn uitgebracht.

Ondertussen doen Google, de OEM-fabrikanten en telecomproviders er goed aan om de basis van een Android-telefoon los te koppelen van de modules en grafische schil die ze zelf mee willen leveren. Gelet op telefoonspecifieke hardware zal dit niet altijd eenvoudig zijn. Maar alleen indien gebruikers belangrijke Android (beveiligings) updates direct van Google kunnen

Updates Android core afsplitsen van updates fabrikanten

krijgen, zullen Google, de leveranciers en de telecomproviders in staat zijn om hun gebruikers snel en passend te beschermen. Slagen ze hier niet in, dan zijn hun eindgebruikers vogelvrij op het moment dat op mobieltjes gerichte virussen en aanvallen echt vorm beginnen te krijgen.

INFORMATIEBEVEILIGING: PEOPLEWARE (3)

Hans Labruyere is directeur en mede-eigenaar van LBVD informatiebeveiligers.
Hij is te bereiken via hans.labruyere@lbvd.nl

In een serie van drie artikelen over informatiebeveiliging en het (on)bewustzijn met betrekking tot dit onderwerp zet de schrijver een keten methoden uiteen die elkaar kunnen versterken. De keten bestaat globaal gezien uit analyseren, informeren, kanaliseren en toetsen. In dit derde deel wordt de waarde van toetsen uiteengezet.

Een bruikbaar voorbeeld van bewust onbekwaam gedrag wordt wellicht gegeven door het 100 km/uur bord langs de snelweg. De schrijver bezit een rijbewijs, en neem van me aan dat ik weet wat er bedoeld wordt met dat bord. Toch heb ik er mijn beweegredenen voor om wel eens anders met die aanwijzing om te gaan. Zodra ik echter door de Hermandad wordt gevat, kunnen we met de overhandiging van mijn rijbewijs de discussie overslaan of ik weet wat met het bord werd bedoeld.

(Te snel) rijden met rijbewijs.

Zo kan het met informatiebeveiliging ook gaan. Indien alle medewerkers een theorietoets over informatiebeveiliging binnen hun bedrijfsproces met positief gevolg zouden hebben afgelegd, garandeert dat absoluut nog geen juist gedrag. Maar het brengt de medewerkers wel voorbij het punt van persoonlijke evaluatie, voorbij attitude, tot aan intentie in fig. 1. Oftewel, het confronteert ze met de vraag: "Wíl ik?"

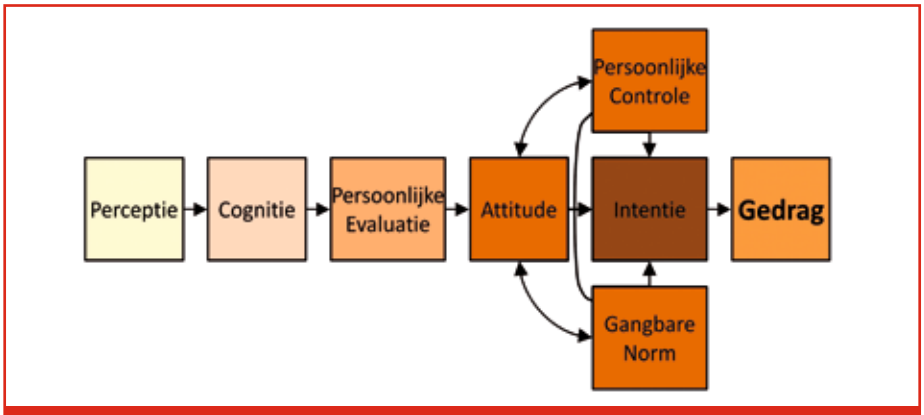
Als en wanneer een medewerker ervoor kiest een regel toch niet te volgen (net zoals de auteur bij het 100 km/uur bord) dan is dat naar verwachting een weloverwogen beslissing, die te verdedigen is, en waarop die medewerker door anderen kan worden aangesproken. Het omgekeerde geldt ook. Een medewerker die door middel van het voldoende afleggen van een toets 'bewijst' dat hij of zij weet welke regel waar past, is zich meer bewust, leert zich zaken aan, is eerder in staat om anderen aan te spreken op gedrag en zal zich eerder voegen naar de gangbare norm.

Indien alle medewerkers een theorietoets hebben afgelegd, garandeert dat nog geen juist gedrag

Toetsmodellen

De markt levert een groot aantal bruikbare toetsmodellen. De meeste modellen zijn echter vrij specifiek van aard. Ze testen de kennis die is opgedaan in een voorafgaand programma met een specifiek leerdoel. Daarbij is het voor de (security) verantwoordelijke van belang te beoordelen WAT er wordt getest. Wil je dat respondenten voldoende kennis van het onderwerp hebben, of wil je testen of ze de leerstof goed hebben begrepen? Het een is niet noodzakelijkerwijze beter dan het andere, maar het geeft wel een bepaald ander beeld!

Vraag aan iemand die net zijn theorierijbewijs heeft gehaald wat voornoemd bord (rode rand, 100 er in) betekent, en hij zal wellicht goed antwoorden. Zet hem een paar jaar later bij nacht, met een volle blaas, in een auto op een vierbaans weg met datzelfde bord langs de weg, en je hebt een heel andere situatie...



Model: beïnvloeding van gedrag volgens de sociale psychologie.

Dus: 'WAT wil je testen' is een minstens zo belangrijke vraag als 'HOE gaan we dat doen?'

Generiek

Bij voorkeur gebruik je bovendien een zo generiek mogelijk toetsmodel. Hierbij is de inhoud van de te stellen vragen niet afhankelijk van eerder aangeleverde CBT of e-learning content. Bij een generiek model kun je voor elk bedrijfsproces, voor elke situatie een andere set vragen aanbieden. Denk aan onderwerpen als ORM, IRM, BHV, Solvacy, informatiebeveiliging, ISO 27000, fysieke veiligheid, GBA, SUWINet, BAG, NEN7510, enzovoorts. Voor een aantal niveaus binnen een organisatie (parttimers, leidinggevenden, leden van de Raad van Bestuur) wil je bovendien bepaalde verschillende niveaus van vragen kunnen stellen.

Bij een generiek model kun je voor elke situatie een andere set vragen aanbieden

Bij een generiek model zijn vragen gedurende jaren naar believen aan te passen om op die manier optimaal aan te sluiten bij de volwassenheid van de organisatie en de veiligheidssituatie ter plaatse. Door met zekere regelmaat een toets af te nemen, wordt bovendien het onderwerp informatiebeveiliging (of fysieke veiligheid of integriteit of privacy of welk onderwerp men er ook maar in wil opnemen) telkens opnieuw aangeboden waardoor er bij medewerkers (alle medewerkers) een meetbare toename van kennis zal zijn te constateren.

Die kennis kan worden beloond. Hetzij met weggevertjes of met bonussen, hetzij met communicatievormen aangaande incidentenlogs, hetzij negatief beloond (als je het niet hebt gehaald). Een en ander is vanzelfsprekend sterk afhankelijk van de cultuur van de organisatie.

Groepseffect

Testen en examens hebben ook een positieve werking op groepen. Mensen acteren als kuddedieren. Men wil niet graag achterblijven als collega's de toets reeds hebben behaald. Met 'collega's' wordt in dit verband gedoeld op gelijkgestemden in een bepaald relevant proces. Alle medewerkers van HRM willen dat er zorgvuldig met personeelsdossiers wordt omgegaan. Voor ICT is dit een dusdanige vanzelfsprekendheid, dat ze er veelal verder niet over nadenken. Alle opdrachtgevers aan externe datacenters willen dat er zorgvuldig met hun data wordt omgegaan, en hebben soms zelf SLA' s afgesproken. De gebruikers van die data zal dat tot op zekere hoogte veelal een zorg zijn...

Als er één HRM-medewerker aanvullende kennis op het gebied van privacy heeft opgedaan, is dat voor veel HRM-collega's een reden die cursus ook te volgen (voor niet-HRM'ers blijft dit onderwerp een non-issue). Nu er opdrachtgevers zijn (voornamelijk overheden) die eisen stellen aan de informatiebeveiliging van datacenters in de vorm van ISO27000-certificatie, zie je dat die eisen steeds vaker worden gesteld. Je wilt als gelijkgestemde niet graag achterblijven in jouw specifieke groep. Dat heeft met eigenwaarde en zelfreflectie te maken en dat geldt, zoals gezegd, voor medewerkers binnen één proces, maar zeker ook voor managers onderling.

Je wilt als gelijkgestemde niet graag achterblijven in jouw specifieke groep

Prof-check in een vluchtsimulator.

Een generieke toets is daarin derhalve nuttig. Hij kan met regelmaat opnieuw worden aangeboden. In de luchtvaart is een zogenaamde prof-check, die periodiek wordt afgenomen, heel gebruikelijk. Artsen kennen een bijscholingsplicht. Brandweerlieden moeten met regelmaat oefenen en EHBO-houders dienen jaarlijks op een terugkomdag te bewijzen dat ze nog weten waar het over gaat.

Een toets moet ook regelmatig worden aangeboden omwille van de geldigheid, omwille van de herhaling, omwille van de gewoonte en omwille van bij te blijven met de gewijzigde inhoud.

Ideaal is dan als je een toetsmodel kunt vinden dat zowel met regelmaat kan worden aangeboden, alsook voor verschillende onderwerpen generiek is uitgevoerd. Op die manier herkennen de betrokken medewerkers de modus operandi, zullen ze minder weerstand ontwikkelen, en derhalve een beter resultaat behalen met minder moeite.

LBVD heeft een eigen toetsmodel ontwikkeld dat aan bovenstaande eisen voldoet. Het is generiek, kan voor alle onderwerpen worden ingezet, en kan een onbeperkt aantal differentiaties aan in kaders van doelgroepen, locaties, processen, enz. Het door ons ontwikkelde model vult de vraag tot borging in. Een respondent die voldoende vragen goed heeft beantwoord komt op een accreditatielijst en kan via de tool een certificaat van de behaalde kennis verkrijgen. Op die manier is voldaan aan de belangrijkste criteria aangaande toetsen: hou de toets specifiek voor die bepaalde deelnemer en zorg dat de respondent er zelf iets aan heeft.

VAN SAS70 NAAR ISAE 3402

Menno Arentsen RE is sinds 2008 werkzaam als IT auditor bij de Outsourcing practice van Capgemini Nederland B.V. Hij is verantwoordelijk voor het uitvoeren van interne en begeleiden van externe audits en is betrokken bij de uitvoering van de SAS70- en ISAE3402-audit. Menno Arentsen is te bereiken via e-mail: menno.arentsen@capgemini.com .

Dit jaar wordt de SAS70-standaard vervangen door een nieuwe internationale standaard de ISAE3402. Wat betekent deze vernieuwing voor de serviceauditor, de serviceorganisatie en de klant? Hoe gaat een outsourcing-organisatie als Capgemini hiermee om?

Bedrijven besteden al jaren (het beheer van) hun IT-omgeving(en) en diensten uit aan serviceorganisaties. De organisatie kan zich dan meer richten op haar primaire proces.
Daarnaast zijn serviceorganisaties, door schaalgrootte, vaak in staat het beheer efficiënter en effectiever uit te voeren.
Een aspect dat bij het uitbesteden van diensten speelt is dat men dan wel zekerheid wil verkrijgen over de wijze waarop de serviceorganisatie deze diensten levert. Naast de diverse rapportages en certificaten wordt hiervoor ook gebruikgemaakt van onderzoekrapportages. Daar waar het gaat om het verkrijgen van zekerheid over de betrouwbaarheid van de (financiële) gegevensverwerking bestaat al sinds de jaren 90 de mogelijkheid tot het verkrijgen van een SAS70-verklaring van de serviceorganisatie. Hierbij voert een onafhankelijke service auditor een onderzoek uit bij de serviceorganisatie en geeft over de uitkomsten van het onderzoek een verklaring af. Het onderzoek richt zich op de opzet en het bestaan van bepaalde controlemaatregelen,Type I-verklaring, en desgewenst ook over de werking van de maatregelen, Type II-verklaring (kader 1).
Vooral de laatste jaren is het verkrijgen van een dergelijke verklaring enorm in populariteit toegenomen. Dit wordt veroorzaakt door nieuwe wet- en regelgeving welke specifieke eisen stelt aan de gegevensverwerking van bedrijven. Tegelijk is daardoor de beperkte toepasselijkheid van de SAS70-standaard steeds zichtbaarder geworden. Immers, de SAS70 diende van oorsprong een specifiek doel: de jaarrekeningcontrole waarbij dienstverlening is uitbesteed aan een derde partij. Minder wordt rekening gehouden met aspecten als offshoring (kader 2) en eisen uit specifieke wet- en regelgeving.
Tijd voor het inrichten van een nieuwe standaard die flexibeler inspringt op de eisen van de markt. In 2008 is hiervoor een nieuwe conceptstandaard opgesteld, de ISAE 3402. Deze standaard is in januari 2010 geaccordeerd en zal de SAS70-standaard vervangen voor alle verklaringen die betrekking hebben op een auditperiode waar 15 juni 2011 binnenvalt (fig. 1).
De SAS70 bood al een (aanvullende) controle op informatiebeveiligingsaspecten, de ISAE 3402 kan hier nog beter op aansluiten.

In dit artikel wordt ingegaan op de overeenkomsten en verschillen tussen de twee standaarden en de veranderingen die dit teweegbrengt voor de verschillende betrokken partijen.
Daarna wordt ingegaan op de kansen die de ISAE 3402 biedt voor informatiebeveiliging. Ten slotte wordt de implementatie bij Capgemini kort geschetst.

De overeenkomsten tussen SAS70 en de ISAE 3402 samengevat
Er zijn belangrijke verschillen te onderkennen tussen de SAS70- en de ISAE 3402-standaard. De grote lijnen zijn echter hetzelfde gebleven.

Doel van de standaard
De SAS70 en de ISAE 3402 zijn beide standaarden die richtlijnen bieden voor een onafhankelijke auditor (de service auditor) om een opinie te geven over de beschrijving en uitvoering van beheersingsmaatregelen van de serviceorganisatie.

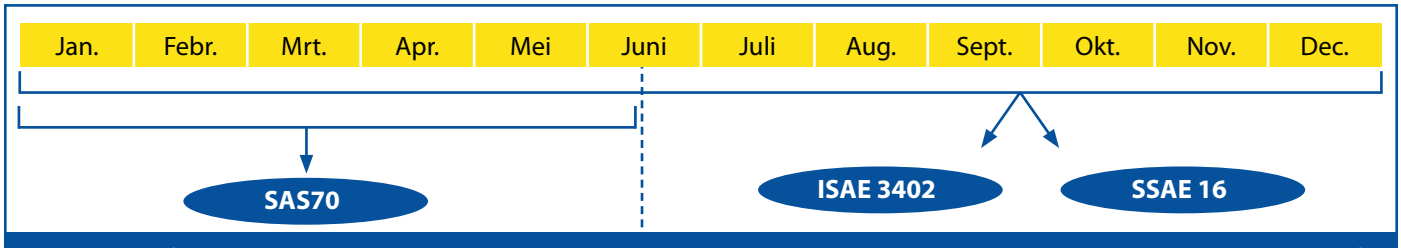


Fig. 1. Vanaf 15 juni 2011 vervalt de SAS 70-standaard en wordt deze vervangen door de ISAE 3402-standaard (inter-national) of de SSAE16 (VS). Dat wil zeggen dat een verklaring over een auditperiode voor 15 juni 2011 mag bestaan uit een SAS 70-verklaring. Valt echter de datum 15 juni 2011 binnen de auditperiode dan zal moeten worden gekozen voor de ISAE 3402- of de SSAE16-standaard.

Opzet, bestaan en werking
Een auditor toetst controlemaatregelen tegen de opzet, het bestaan en de werking, maar wat wordt daarmee bedoeld?

De opzet
Bij de opzet wordt beoordeeld of een ontwerp van de maatregel aanwezig is, bijvoorbeeld binnen een beleidstuk of een (project)plan.

Het bestaan
Bij het bestaan wordt beoordeeld of de opzet vertaald is naar procedures, activiteiten en concrete maatregelen/gedrag in de praktijk, bijvoorbeeld in de vorm van rapportages, wijzigingsregistraties, testdocumentatie.

De werking
Bij de werking wordt beoordeeld of de maatregelen feitelijk voor een vastgestelde periode zijn uitgevoerd. Bij de ISAE 3402 is dit een periode van ten minste zes maanden.

Kader 1. Opzet, bestaan en werking.

Doelgroep van de standaard
De doelgroep van het onderzoek blijft gelijk: de gebruikersorganisatie en haar accountant.

Scope van het onderzoek
De SAS70 en de ISAE 3402 richten zich beide in de basis op de betrouwbaarheid van de financiële gegevensverwerking. Deze wordt getoetst aan de hand van een raamwerk van beheersdoelstellingen en maatregelen die zich richt op de financiële gegevensverwerking. De toereikendheid van dit raamwerk wordt getoetst door de service auditor. Bij deze toetsing wordt niet alleen gekeken naar de juiste dekking van aspecten als juistheid, volledigheid, tijdigheid en validiteit van de gegevensverwerking, maar ook naar toegangsbeveiliging.

Objecten van onderzoek
De objecten van onderzoek worden bij beide standaarden bepaald door de klant en zijn accountant. Deze stellen de kritische (financieel materiële) processen vast en vervolgens de applicaties die deze processen ondersteunen. Daarna kan worden vastgesteld welke applicaties, databases, systemen en platformen in beheer bij de serviceorganisatie de objecten van het onderzoek zijn.

Rapportagevorm
Beide standaarden kennen twee rapportagevormen, resultanten van een type I- of type II-onderzoek. Bij een type I-onderzoek wordt opzet en het bestaan van de controlemaatregelen beoordeeld (lees de borging in het beleid, de procesbeschrijvingen, de procedures en de werkinstructies).

Bij het type II-onderzoek wordt aanvullend aan de opzet en het bestaan ook onderzoek gedaan naar de werking van de maatregelen gedurende een bepaalde periode.

Onderzoeksperiode
Bij beide onderzoeken geldt dat het type II-onderzoek een periode van ten minste zes maanden moet beslaan.

> Tijd voor het inrichten van een nieuwe standaard die flexibeler inspringt op de eisen uit de markt

Opzet van de auditrapportage
In grote lijnen is de opzet van het ISAE 3402-rapport gelijk aan het SAS70-rapport. Beide rapporten bevatten de conclusie van de service auditor, een beschrijving van de serviceorganisatie en de uitkomsten van het onderzoek naar de controlemaatregelen. Er zijn echter ook belangrijke verschillen tussen de nieuwe en de oude standaard te onderkennen.

De belangrijkste verschillen samengevat
Al in eerdere artikelen zijn de verschillen tussen de ISAE 3402- en de SAS70-standaard aangeduid. In deze paragraaf worden ze nog eens samengevat. De aanpassingen zorgen ervoor dat de verklaring beter past in de tijdsgeest. De uitkomsten sluiten beter aan op de bestaande wet- en regelgeving, met name de Sarbanes Oxley Act (SOx). Bovendien biedt de nieuwe standaard meer flexibiliteit voor de klant om zekerheid te verkrijgen over aspecten die de SAS70-standaard niet dekt.

Managementverklaring
SAS 70 is een auditingstandaard. De ISAE 3402 is een 'assurance' of 'attestation' standaard. Belangrijk daarbij is dat het management een verklaring in het rapport moet opnemen. Deze verklaring gaat in op de doelgroep van het rapport en geeft aan dat de beschrijvingen in het rapport juist zijn ten aanzien van de beheeromgeving, het risicobeheerproces, informatie, communicatie en de beheersingsactiviteiten. Ook dient het management aan te geven dat de beheermaatregelen adequaat zijn ontworpen en hebben gewerkt. Hiermee wordt, net als bij SOx, de verantwoordelijkheid van het management voor het vaststellen van het stelsel van beheersingsmaatregelen benadrukt.

Suitable Criteria
In de ISAE 3402 is de minimale set van onderzoekscriteria (Suitable Criteria) opgenomen op basis waarvan het management en de auditor de interne beheersing beoordelen. Het betreft criteria ten aanzien van:
de getrouwheid van de beschrijving (Fairness of Presentation);
de mate waarin de maatregel passend

is voor de beheersingsdoelstelling (Suitability of Design);
de mate waarin de maatregel effectief werkt (Operating Effectiveness).
Het controleraamwerk van de serviceorganisatie moet ten minste aan deze criteria voldoen.

Subserviceorganisaties
Als door de serviceorganisatie een deel van de relevante processen is uitbesteed aan een derde partij (de subserviceorganisatie) dan moeten ook de beheersingsmaatregelen die zij hanteert en die waarmee zij vaststelt dat de beheersingsmaatregelen van de subserviceorganisatie effectief werken, in het rapport worden opgenomen. Dit zou bijvoorbeeld aan de hand van een auditrapport van de subserviceorganisatie kunnen worden vastgesteld. Het feit dat wordt gesteund op deze auditrapportage moet dan worden opgenomen in de verklaring.

Gebruik interne auditafdeling
In de ISAE 3402-rapportage moet de service auditor, indien van toepassing, specifiek de werkzaamheden vermelden die door de interne auditafdeling zijn uitgevoerd.

Risicoanalyse
De ISAE 3402-standaard geeft aan dat de gehanteerde beheerdoelstellingen en -maatregelen moeten zijn gebaseerd op een risicoanalyse.

Compliance
De ISAE 3402 biedt de mogelijkheid om de reikwijdte van het rapport te verbreden. Nog steeds is de financiële gegevensverwerking de basis voor het onderzoek en de verklaring.
Echter, er kunnen nu ook beheersingmaatregelen worden toegevoegd om te voldoen aan relevante wet- en regelgeving.
De hierboven benoemde verschillen leiden ertoe dat voor de verschillende betrokkenen een aantal zaken anders zal moeten worden aangepakt.
Er zal vooral in dit overgangsjaar extra

Fig. 2. Verandering van richting (bron: isae3402.com.

aandacht en communicatie moeten zijn. Hieronder wordt geschetst welke aspecten van belang zijn voor de service auditor, de serviceorganisatie en de klant.

Veranderingen vanuit service auditorperspectief
Het werk van de service auditor zal door invoering van de nieuwe standaard niet drastisch veranderen.

Suitable Criteria
Wel is voor de service auditor duidelijker op welke wijze hij zijn beoordeling moet uitvoeren doordat nu een minimale set van criteria is benoemd die hij dient toe te passen bij zijn beoordeling.

Raamwerk van beheersingsmaatregelen
De service auditor weet wat de basis is geweest bij het opstellen van het raamwerk van de beheersingsdoelstellingen en -maatregelen door de serviceorganisatie. Immers de serviceorganisatie dient dit nu in een managementverklaring te beschrijven.
De service auditor moet aan de hand hiervan beoordelen of de basis van dit raamwerk klopt. Gevolg is dat de juistheid en volledigheid van dit raamwerk door de service auditor eenduidiger is vast te stellen.

De service auditor zal met de serviceorganisatie in dit aanloopjaar extra tijd kwijt zijn om een gedegen raamwerk van beheersingsdoelstellingen en -maatregelen op te zetten en vast te stellen.
Na deze fase zal hij niet veel meer tijd kwijt zijn aan het uitvoeren van de audit aan de hand van de ISAE 3402-standaard dan bij de SAS70-standaard het geval was.

Uniformiteit
Laatste verandering voor de service auditor is dat de formele Nederlandse vertaling van de standaard haar duidelijke handvatten geeft voor het opstellen van de verklaring. Dit maakt de rapportage eenvoudiger en draagt bij aan een uniforme verklaring.

Veranderingen vanuit serviceorganisatieperspectief
Voor de serviceorganisatie zijn een aantal verschillen tussen de SAS70- en de ISAE 3402-standaard zeer relevant.

Raamwerk van beheersingsmaatregelen
Belangrijkste verandering is dat het management van de serviceorganisatie een formele verklaring dient op te nemen in het rapport. Hiermee is het management formeel verantwoordelijk voor de kwaliteit en de werking van het stelsel van beheersingsmaatregelen.
Tegelijk dient het raamwerk van beheersdoelstellingen en -maatregelen gebaseerd te zijn op een risicoanalyse en dienen de maatregelen te voldoen aan een minimale set van onderzoekscriteria.
Deze aanpassing geeft de serviceorganisatie gelegenheid om samen met haar management het controleraamwerk te actualiseren. Hiermee kunnen verouderde raamwerken passend worden gemaakt op de huidige manier van werken. Denk daarbij aan nieuwe technieken die de laatste jaren zijn ingevoerd en die op een andere manier risico's afdekken of juist introduceren zoals centrale opslag, redundantie en virtualisatie.

Gelijk moet worden gekeken welke wet- en regelgeving voor haar klantportfolio relevant is. Denk bijvoorbeeld aan SOx, privacywetgeving, belastingwetgeving, enz. Bepaald moet worden welke aspecten hiervan in het raamwerk kunnen worden opgenomen.

Een gewijzigd raamwerk met gewijzigde of nieuwe beheersingsmaatregelen betekent ook dat deze maatregelen aantoonbaar moeten worden uitgevoerd.

Met andere woorden, de service auditor moet bewijsstukken hebben waaruit blijkt dat de maatregelen worden uitgevoerd. Bovengenoemde aanpassingen kunnen daarmee leiden tot noodzakelijke aanpassingen in de processen, procedures en rapportages binnen de serviceorganisatie.

Subserviceorganisaties
Ander relevant aspect is de manier waarop de serviceorganisatie de beheersing binnen haar subserviceorganisaties bewaakt. Dit zal aantoonbaar en meetbaar moeten zijn.

Communicatie
Ten slotte zal de serviceorganisatie alle interne en externe betrokkenen van de veranderingen op de hoogte moeten stellen. Denk hierbij aan de verkoopafdeling en aan de relevante klanten.

Veranderingen vanuit klantperspectief
In eerste instantie lijkt er voor de klant van de serviceorganisatie weinig te veranderen. Zij zal nog steeds een verklaring ontvangen van een onafhankelijke service auditor over de opzet, het bestaan en (bij Type II) de werking van de beheersingmaatregelen bij de serviceorganisatie.

Raamwerk van beheersingsmaatregelen
De kans dat door de serviceorganisatie dit jaar het raamwerk van beheersingsdoelstellingen en -maatregelen wordt bijgewerkt is vrij groot. Voor de klant is het van belang om zoveel mogelijk bij dit proces aangesloten te zijn.

De klant doet er verstandig aan met zijn accountant te bespreken in welke mate het huidige en het nieuwe (concept) beheersingsraamwerk voldoende zekerheid geeft in zijn specifieke situatie. Daarbij kan weer worden gekeken naar de financiële gegevensverwerking en de daaraan gerelateerde wet- en regelgeving. Hoe eerder in het proces deze analyse plaatsvindt hoe groter de kans dat specifieke aspecten door de serviceorganisatie en de service auditor kunnen worden meegenomen in de veranderingen die de serviceorganisatie ondergaat.

Toegevoegde waarde van de verandering voor informatiebeveiliging
Ook de security officer (binnen de serviceorganisatie, maar ook bij de klant) heeft er belang bij om aan te sluiten bij ontwikkelingen waar de nieuwe standaard toe leidt.
Alle beveiligingsaspecten die te relateren zijn aan risicovolle financiële gegevensverwerking zouden meegenomen kunnen worden in het raamwerk van beheersingsmaatregelen.

SAS 70 is een auditingstandaard, de ISAE 3402 is een 'assurance' of 'attestation' standaard

Beveiligingsmaatregelen in het raamwerk
Borging van deze beveiligingsaspecten in het raamwerk van beheersingsmaatregelen is het beste te realiseren door, waar van toepassing, te verwijzen naar de relevante informatiebeveiligingsdocumentatie, zoals het beleid, statement of applicability, procedures en baselines. Om dit zo effectief mogelijk plaats te laten vinden zou de security officer en/of manager aangehaakt moeten zijn in het verandertraject.
Toegevoegde waarde is dat een aantal basis informatiebeveiligingsmaatregelen bij een type II onderzoek gedurende een periode van ten minste zes maanden wordt beoordeeld en daarmee bewaakt.

Aanpak van de implementatie bij Capgemini Outsourcing
Capgemini Outsourcing biedt sinds 2007 haar klanten de mogelijkheid om een SAS70-verklaring te verkrijgen. De basis van de SAS70-verklaring was een globaal controleraamwerk dat in details specifiek aansloot op de Nederlandse werkwijze. De onderzoeksperiode was telkens zes maanden (van juli tot en met december van elk jaar). Deze periode geeft aan dat 2011 voor Capgemini Outsourcing de ISAE3402 van toepassing is (fig. 1).

Sinds 2007 is er veel veranderd:

Meer zekerheid
Steeds meer klanten willen zekerheid over de uitbestede dienstverlening op diverse vlakken. Vooral is de vraag naar continuïteitsmaatregelen en privacyaspecten toegenomen. Het SAS70-raamwerk biedt dit slechts beperkt. Daarnaast wil de klant ook steeds vaker zekerheid verkrijgen over de gehele periode. Met andere woorden, de SAS70-verklaring moet het hele jaar dekken.

Techniek
Daarnaast is de technische infrastructuur in de laatste jaren snel veranderd. Met name virtualisatie van omgevingen en netwerken spelen hier een grote rol.

Offshoring
Techniek en marktontwikkelingen, vooral op het vlak van kwaliteit/prijs-

Offshoring
Uitbesteden naar het buitenland kan in verschillende vormen: nearshoring (uitbesteden in de nabijheid, bijvoorbeeld vanuit Nederland naar Polen of Hongarije) en offshore outsourcing (uitbesteden naar een overzees continent). Offshoring naar lagelonenlanden is de nieuwste trend in het begin van de 21e eeuw, met als voornamelijk argument het besparen van kosten. India is een populair land voor offshore outsourcing. Werknemers hebben een goed opleidingsniveau, zijn de Engelse taal goed machtig, maar werken wel tegen lagere kosten dan in de westerse landen (bron Wikipedia).

Kader 2. Offshoring.

Carve out method (uitsluitingsmethode)
Een methode van omgaan met de diensten die worden verleend door een subserviceorganisatie. Hierbij omvat de beschrijving van de serviceorganisatie van haar systeem de aard van de diensten die door een subserviceorganisatie worden verleend. De relevante interne beheersingsdoelstellingen en de daarmee verband houdende interne beheersingsmaatregelen van de subserviceorganisatie zijn echter uitgesloten van de beschrijving van de serviceorganisatie van haar systeem en van de reikwijdte van de opdracht van de auditor van de serviceorganisatie.
De beschrijving van de serviceorganisatie van haar systeem en de reikwijdte van de opdracht van de auditor van de serviceorganisatie bevatten interne beheersingsmaatregelen van de serviceorganisatie die de effectiviteit van de interne beheersingsmaatregelen van een subserviceorganisatie monitort, wat kan inhouden dat de serviceorganisatie een assurancerapport (bijvoorbeeld ook een ISAE3402-rapport) betreffende de interne beheersingsmaatregelen van de subserviceorganisatie beoordeelt.
Als de interne beheersingsdoelstellingen en -maatregelen van de subserviceorganisatie wel binnen het onderzoek vallen wordt gesproken over de inclusive methode (opnamemethode).

Kader 3. Carve out method (uitsluitingsmethode)

verhouding, heeft ertoe geleid dat steeds meer van de dienstverlening van Capgemini uit een derde land komt. Veel taken en activiteiten vinden nu plaats in landen als India en Polen. Dit leidt ook tot een andere wijze van aansturing en interne rapportage.
Dit alles heeft ertoe geleid dat Capgemini deze verandering aangrijpt als kans om een aantal verbeteringen uit te voeren. De volgende stappen worden in het eerste kwartaal 2011 uitgevoerd.

1. *Opstellen risicobeoordeling* - De risicobeoordeling bij het tot stand komen van het beheersingsraamwerk en de rol van het management daarin wordt formeel uitgewerkt en afgestemd met de service auditor.
2. *Verbeteren van raamwerk van beheersingsmaatregelen* - Het raamwerk dat wordt gebruikt voor de SAS70-audits is een global raamwerk. De beheersingsmaatregelen worden wel daar waar nodig landelijk specifiek gemaakt afhankelijk van de exacte geleverde diensten. De maatregelen worden op basis van bovengenoemde risicoanalyse nauwkeuriger aangesloten op de processen en de techniek. Specifiek spelen hier zaken als invoering van nieuw ingevoerde best practices (zoals ASL), tooling (zoals authenticatietools) en techniek (zoals het gebruik van redundante omgevingen).
3. *Aansluiten op assurance subserviceorganisaties* - Ten aanzien van de subserviceorganisaties zal Capgemini Outsourcing kiezen voor de carve out-methodiek (kader 3), waarbij wordt gesteund op de eigen ISAE 3402-verklaringen van deze onderdelen van Capgemini.
4. *Communicatie intern en extern* - Bij dit alles moet intensieve communicatie plaatsvinden.
Intern vindt communicatie plaats met het algemeen management, service delivery management, security management, risk management, sales en de quality managementafdelingen van de subserviceorganisaties. Extern met de service auditor en de klant. De uitkomsten van de interne auditwerkzaamheden worden opgenomen in interne auditrapportages waarbij gelijk een 'mapping' wordt gemaakt met de relevante beveiligingsmaatregelen, als opgenomen in de Statement of Applicability van Capgemini.
5. *Verlengen auditperiode* - Besloten is om ook aan de klantwens te voldoen om de auditperiode te verlengen naar een jaar. Een en ander betekent dat er nu aanpassingen plaatsvinden die van invloed zijn op het auditproces over de huidige periode. Gekozen is daarom om de veranderingen in het eerste kwartaal af te ronden en op basis van de nieuwe standaard met het nieuwe beheersingsraamwerk de beoordeling per 1 april over het eerste kwartaal uit te voeren. Naast de veranderingen die worden doorgevoerd wordt gewerkt aan het opstellen van de vereiste managementverklaring en de overige rapportageonderdelen.

Samenvattend
Hoewel het binnen de SAS70-standaard ook altijd mogelijk was om verbeteringen door te voeren, zorgt de invoering van de nieuwe ISAE 3402-standaard voor extra motivatie om dit te doen. Dit wordt vooral veroorzaakt door het feit dat er nu sowieso aanpassingen moeten plaatsvinden voor de nieuwe standaard. Met name het feit dat de risicobenadering van de serviceorganisatie binnen de standaard moet worden geformaliseerd door de serviceorganisatie en getoetst door de service auditor speelt een grote rol. Een en ander leidt tot een intensivering van communicatie over en weer waardoor een effectievere en efficiëntere auditstructuur kan ontstaan voor de serviceorganisatie en haar klanten. Beide partijen hebben er belang bij om dit in stand te houden.

Literatuur
NOREA Richtijn 3402 www.norea.nl (Nederlandse vertaling van de standaard).
René Ewalls, ISAE 3402: een nieuw hoofdstuk voor de IT-Auditor, de IT-Auditor: nummer 3 2010.
Dennis Houtekamer en Remco de Graaf, ISAE3402 einde van SAS70 in zicht? De EDP Auditor: nummer 1 2009.
Dennis Houtekamer en Ad Buckens, Ontwikkelingen in Third Party Reporting, Informatiebeveiliging december 2008.

CYBERSECURITY ALS DRIVER VOOR ANDERE AANPAK RISICOMANAGEMENT

VERANTWOORDELIJKHEID NEMEN IN EEN BESTUURLIJK VERSNIPPERDE WERELD

Andre Smulders is senior consultant security bij TNO. Hij is bereikbaar op andre.smulders@tno.nl

Op 9 februari 2011 werd de 19e meeting van het Informatie Beveiligings Overleg (IBO) gehouden in Amsterdam. Met de plannen voor de Nationale Cyber Security Strategie (NCSS) als context gaf de auteur zijn beeld op de ontwikkelingen die in de nabije toekomst een rol spelen om verantwoordelijkheid te kunnen blijven nemen voor risico's en assurance bij cybersecurity. Dit artikel is een verdere uitwerking van de achtergrond bij die presentatie.

'De betrouwbaarheid van de dienstverlening in kritieke infrastructuren is (nog) niet significant aangetast, ondanks de paradoxale situatie dat kritieke infrastructuren in toenemende mate technisch vervlochten raken, terwijl het management van deze systemen juist fragmenteert.' [Bruijne, 2006]

Wat voorheen centraal gestuurde ketens waren, is een samenwerkingsverband geworden tussen bestuurlijk gefragmenteerde onderdelen. Een blik op de energiesector maakt deze ontwikkeling duidelijk. Waar voorheen de productie, transport en levering onder de verantwoordelijkheid van een partij viel, de overheid, is dit nu verdeeld over verschillende organisaties. De energiesector is hierin niet uniek. Ook andere (vitale) sectoren hebben dezelfde transformatie ondergaan. Voorbeelden hiervan zijn de telecomsector en de spoorwegen. Wie denkt dat dit een ontwikkeling is die alleen het bedrijfsleven treft, komt bedrogen uit. Ook de overheid zelf ondergaat die transformatie. De overheid consolideert immers activiteiten waarvan vervolgens grote onderdelen worden uitbesteed bij private partijen. Het gevolg hiervan is dat de verantwoordelijkheden voor onderdelen van de keten op verschillende plaatsen komt te liggen en de verantwoordelijkheid voor de integrale keten als geheel door geen enkele partij wordt opgepakt.

Het 'bestuurlijk fragmenteren' van ketens in onderdelen is niet noodzakelijk een slechte ontwikkeling. Het grote voordeel hiervan is dat grote efficiency winsten te behalen zijn. In tegenstelling tot de vroegere situatie hoeft een ketenverantwoordelijke immers niet langer alle onderdelen van die keten zelf in stand te houden. In plaats daarvan maakt hij gebruik van diensten of producten die derden aanbieden (verder zal in dit artikel gebruik worden gemaakt van de term 'diensten' waarmee zowel diensten als producten worden bedoeld). Doordat zo'n dienstaanbieder zich alleen focust op zijn dienst, kan hij deze dienstverlening heel goed optimaliseren. Een consequentie van deze optimalisatie binnen onderdelen in de keten, is echter wel dat de 'rek' in de gehele keten steeds verder afneemt. Immers, het exclusief focussen op de eigen dienstverlening impliceert dat er minder aandacht is voor andere partijen in de keten. Ontwerpkeuzes die goed zijn voor (de efficiency van) de eigen dienstverlening, kunnen dan risico's introduceren voor andere ketenpartijen die aan de aandacht ontsnappen. De dienstverlener zal zelf ook risico's over het hoofd kunnen zien die worden veroorzaakt door de wijze waarop andere partijen in de keten hun dienstverlening hebben geïmplementeerd.

Fragmentatie van verantwoordelijkheid

De fragmentatie van verantwoordelijkheid in de keten is slechts een tussenstap naar het denken in services. Een service is te vergelijken met een dienst, met als belangrijkste verschil dat hoe de dienst geleverd wordt, een 'black box' is voor de afnemer. Dat dit geen toekomstmuziek is en dat een service niet alleen iets technisch is, kunnen we zien in alledaagse voorbeelden. Waar voorheen alle benodigde expertise en middelen voor het leveren van energie onder directe verantwoordelijkheid van de overheid viel, wordt deze in toenemende mate belegd bij private partijen. Ook deze partijen maken weer gebruik van diensten die door derden geleverd worden. Denk bijvoorbeeld aan onderhoudspersoneel en telecommunicatiediensten. De aanschaf van benodigde middelen, onderhoud en training van personeel die hiervoor nodig zijn, vallen niet langer onder de eigen verantwoordelijkheid maar worden verzorgd door de partijen die deze dienst leveren. Hoe zij dat doen is

feitelijk niet van belang voor de afnemer. In gevallen waarin helemaal niet inzichtelijk is hoe een functionaliteit wordt geleverd, spreken we van een service.

Intuïtief voelen we wel aan dat niet zomaar een willekeurige partij zal worden ingeschakeld om kritische services te leveren. De reden hiervoor is dat naast de functionaliteit (de 'wat'-vraag) die geleverd wordt, eisen worden gesteld aan de betrouwbaarheid van die functionaliteit. Deze aanvullende eisen noemen we assurance-eisen.
In de klassieke centraal gestuurde ketens is de assurance (vaak impliciet) geregeld vanuit het inzicht in de wijze waarop een service tot stand komt (de 'hoe'-vraag), of door een specifieke partij (met een goed 'track record') hiervoor in te schakelen. Vaak worden assurance-eisen dus impliciet of in een aantal gevallen helemaal niet gesteld. Als we een dienstenketen willen zien als een keten van 'bestuurlijk versnipperde' services, waarin elke dienst voor de anderen een 'black box' is, dan dringt zich de vraag op wat de gevolgen hiervan zijn voor de huidige aanpak van security governance?

Om de bovenstaande vraag te kunnen beantwoorden kijken we eerst naar de huidige structuur van security governance. Dit illustreren we hier door de ontwikkelingen van keten denken naar denken in services schematisch weer te geven. Fig. 1 illustreert een traditionele keten op twee manieren. Links staat de oude vorm, waarbij alle onderdelen (A t/m D) die nodig zijn om een dienst te leveren onder dezelfde bestuurlijke verantwoordelijkheid vallen. De huidige situatie wordt in deze figuur rechts weergegeven. Hier zien we dat delen van die keten door anderen (C en D) geleverd worden.
In de huidige situatie worden niet alleen eisen gesteld aan de organisatie die een bepaald ketenonderdeel (C) levert, maar heeft de verantwoordelijke voor het eindproduct ook een grote mate van inzicht in de samenhang van de keten als geheel. Dit gaat ook op als andere delen (D) daarvan door (C) ergens anders zijn ondergebracht. De assurance in deze situatie leunt zwaar op de mate van inzicht in de wijze waarop C en D de dienst leveren. In enkele gevallen schrijft de dienstverantwoordelijke zelfs voor hoe en met welke middelen C en D hun onderdelen moeten leveren. Het meest in het oog springende is dat onze huidige benadering van security governance hoofdzakelijk nog gebaseerd is op het denken in ketens.

Van centraal naar decentraal

De ontwikkelingen gaan echter nog verder dan wat in het voorgaande voorbeeld is geschetst. Meer en meer komen we in een paradoxale situatie dat bestuurlijke verantwoordelijkheid steeds verder wordt opgedeeld terwijl de onderlinge afhankelijkheden steeds meer toenemen. In fig. 2 is de situatie geschetst van een samenstel van services, ook wel web van services, die als geheel dezelfde dienst leveren als in de voorgaande voorbeelden. Een eigenaar die overzicht wil houden wordt dan ook met steeds meer (en steeds kleinere) services geconfronteerd die door steeds meer en verschillende partijen worden geregeld en onderlinge afhankelijkheden (kunnen) vertonen. Overzicht houden wordt 'tot de derde macht' moeilijker, omdat (1) met steeds meer partijen moet worden afgestemd, (2) dit steeds kleinere functionaliteiten betreft en het dus meer detailwerk wordt en (3) de mogelijkheden voor afhankelijkheden tussen services kwadratisch toeneemt met het aantal services. Het moge duidelijk zijn dat dit type complexiteit (exponentieel) aan het toenemen is en tot onwerkbare situaties leidt dan wel gaat leiden.

Bestuurlijk gezien is de leverancier van een eindproduct of dienst verantwoordelijk voor zijn product of dienst. Op hoofdlijnen zijn er twee opties om deze verantwoordelijkheid te nemen. Bij de eerste optie (de 'crystal box'-optie) zorgt de verantwoordelijke ervoor dat zij integraal inzicht heeft in de invulling en samenhang van services waarmee het eindproduct (of dienst)

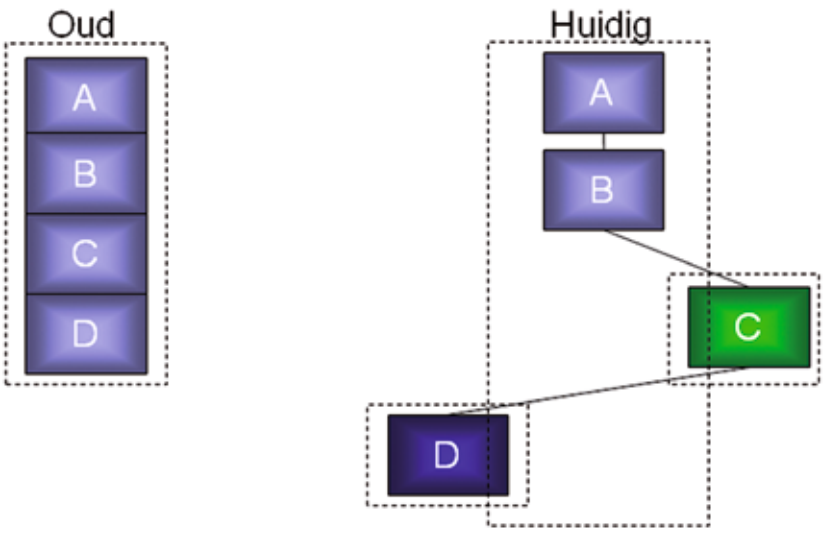


Fig. 1. Oude versus huidige aanpak.

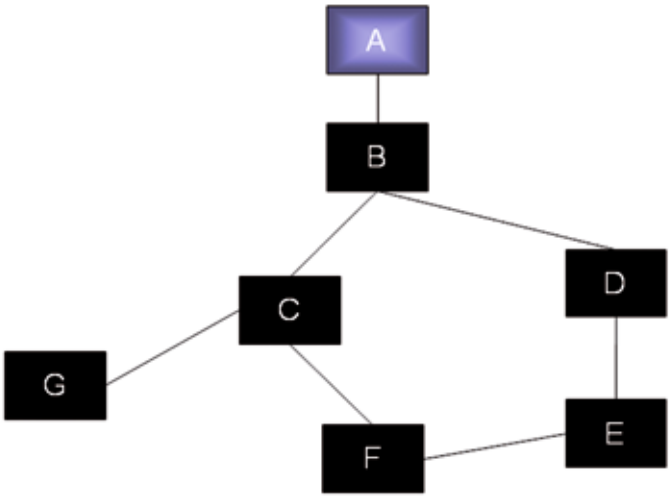


Fig. 2. Toekomstige situatie.

tot stand komt en sturing daaraan geeft. Een tweede optie (de 'black box'-optie) is dat zij op het raakvlak van de dienst(en) die zij afneemt voldoende informatie verkrijgt om de risico's voor haar eigen product of dienst te beheersen. Uiteraard kan men ook voor een laissez-faire aanpak kiezen maar omdat daarmee feitelijk niets geregeld wordt, is dat geen valide governance aanpak.

Het grote nadeel van de eerste optie is dat dit afbreuk doet aan de efficiency winst die het denken in services belooft. De tweede optie benut deze potentiële efficiency winst wel, ook waar het gaat om security governance. In plaats van governance over de gehele keten te voeren, richt een verantwoordelijke zich op de raakvlakken met de service(s) die zij nodig heeft om haar dienst(en) te kunnen leveren. Op zo'n raakvlak moeten dan twee hoofdvragen expliciet worden beantwoord. De eerste is de 'wat'-vraag. Dat wil zeggen, welke functionaliteit wordt geleverd door zo'n raakvlak?
De tweede, vaak veel lastigere vraag is de assurance-vraag. Oftewel, met welke zekerheden moet de service geleverd worden en welke risico's loopt de dienst als hier niet aan wordt voldaan?

Crystal box versus black box

Het invullen van de tweede optie vraagt om een fundamenteel andere benadering van security-vraagstukken en de manier waarop de governance hierover wordt ingericht. De belangrijkste noodzakelijke verandering is de manier waarop afspraken in samenwerkingsverbanden tot stand komen. Er kan niet langer worden gestuurd op het uitgangspunt dat de hele keten onder controle is van de eindverantwoordelijke of dat deze eisen op kan leggen hoe onderdelen hun werk moeten doen. Om een efficiënte samenwerking vorm te kunnen geven waarbij ook de veiligheid goed geborgd is, zal moeten worden omgekeken naar een nieuwe vorm van security governance, waarbij de sturing en assurance op het raakvlak tussen services is ingericht.

De hierboven geschetste ontwikkeling is samen te vatten in twee tegengestelde bewegingen. Enerzijds de beweging dat bestuurlijke verantwoordelijkheid steeds verder wordt opgedeeld terwijl anderzijds de onderlinge technische afhankelijkheid toeneemt. De focus hierbij ligt op de grote voordelen namelijk, beter grip op de functionaliteit en een betere kostenefficiency. De keerzijde is echter dat er minder grip is op assurance van deze samenhangende services. Dit effect wordt versterkt door de toenemende verwevenheid en dynamiek van samenhang tussen de services.

Het bewustzijn hierover neemt toe, hetgeen ook een fundamentele driver is voor de aandacht die er op dit moment is voor het onderwerp cybersecurity. TNO definieert cybersecurity als: *het krijgen van grip op dreigingen en risico's die samenhangen met de toenemende verwevenheid van ICT terwijl tegelijkertijd de opdeling van bestuurlijke verantwoordelijkheid toeneemt.*

Literatuur:

Bruijne, Mark de: Proefschrift 'Networked Reliability', 2006

VERSLAG

SURFCERT & SURFIBO BEVEILIGINGSCONFERENTIE 2011

Rogier Spoor, SURFnet. Rogier is te bereiken via rogier.spoor@surfnet.nl

'Er moet een eigen cloud komen voor het hoger onderwijs en onderzoek. Dat is veiliger dan de publieke cloud.' Dit was een verrassende conclusie tijdens het debat met politici en bestuurders uit het hoger onderwijs en onderzoek over Cloud Computing, gehouden tijdens een gezamenlijke conferentie van SURFcert & SURFibo.

Het platform voor informatiebeveiligers in het onderwijs (SURFibo) en het incident response team van SURFnet (SURFcert) organiseerden op 10 en 11 februari 2011 voor de vierde keer een gezamenlijke conferentie die in het teken stond van beveiliging in het hoger onderwijs en onderzoek. De conferentie werd gehouden in het Museum van Communicatie in Den Haag. Het was zeer succesvol en compleet volgeboekt met 150 bezoekers. Aan bod kwamen onderwerpen zoals actuele ontwikkelingen op het gebied van informatiebeveiliging en het spanningsveld tussen privacy enerzijds en de mogelijkheden om allerlei gegevens op te slaan, te analyseren en uit te wisselen anderzijds. Ook werd er aandacht besteed aan de risico's van het afnemen van diensten in een cloudomgeving en werd uitgelegd hoe (on)veilig het gsm- en dect-telefonienetwerk is. Ten slotte presenteerden SURFcert en SURFibo de resultaten van 2010 en de innovatieve ontwikkelingen die voor 2011 op het programma staan.

SURFcert Security Award 2011 voor Team Cymru

Op de conferentie heeft Team Cymru de SURFcert Security Award in ontvangst genomen. Tijdens de eerste dag van de SURFcert/SURFibo beveiligingsconferentie reikte Ot van Daalen van Bits of Freedom, winnaar in 2010, de Award uit aan Ian Cook van Team Cymru. Team Cymru doet onderzoek naar beveiligingsincidenten op internet en ondersteunt organisaties bij het oplossen van beveiligingsproblemen. Team Cymru is al meer dan tien jaar van grote waarde voor het collectieve niveau van beveiliging op internet. Vanwege het ontbreken van winstoogmerk en het zeer concreet aanbieden van operationele ondersteuning aan CERT's (Computer Emergency Response Teams) wereldwijd is Team Cymru een belangrijke partner voor niet-commerciële organisaties zoals SURFcert en zijn aangesloten instellingen.

> Er liggen kansen voor het hoger onderwijs om een gezamenlijke 'community cloud' te ontwikkelen

De SURFcert Security Award is bestemd voor een persoon, initiatief, organisatie, oplossing of implementatie met een substantiële bijdrage aan het (collectieve) beveiligingsniveau van SURFnet-gebruikers. De jury van de Award heeft uit zes nominaties gekozen voor Team Cymru, dat hiermee een geldbedrag ontvangt van 3000 euro.

Debat

Wegens een inspirerend en hoog gewaardeerd debat in 2010 op vlak van privacy, was er dit jaar een debat met als thema 'Cloud computing in het hoger onderwijs en onderzoek'. Deelnemers aan dit debat waren: Amandus Lundqvist (voorzitter van het algemeen bestuur van SURF), Brigitte van der Burg (Tweede Kamerlid VVD), Michiel Leenaars (directeur ISOC, directeur stichting NLnet) en Johannes van der Vos (HBO raad). Het debat stond onder leiding van Leo Plugge (SURF).

Het thema was cloud computing en ICT-dienstverlening binnen het hoger onderwijs, met daarbij uiteraard bespreekpunten als de beleidsmatige aspecten rondom organisatie, verantwoordelijkheid, security en financiën.

Conclusie was dat er voor het hoger onderwijs kansen liggen om een gezamenlijke 'community cloud' te ontwikkelen. Dit is op tal van punten veiliger dan een publieke cloud. Het is dan namelijk bekend waar de data komt te staan (in Nederland), de wetgeving is helder, de beheerpartner wordt gezamenlijk geselecteerd en kan gecontroleerd/geaudit worden. Er kan gezamenlijk aan standaardisering worden gewerkt in deze cloud en een community cloud biedt een platform waarin gezamenlijk kan worden geïnnoveerd.

Ten slotte is het een efficiëntieslag en zal hardware en personeel efficiënter ingezet kunnen worden wat tot CO_2- en kostenreductie leidt.

Hoogtepunten in presentaties

Michiel Leenaars is tegenstander van het in de publieke cloud afnemen van e-mail/storage en andere basisdiensten door het hoger onderwijs. Volgens Michiel is het belangrijk om binnen het hoger onderwijs zelf innovatie te doen aan clouds en een eigen ho&o community cloud op te zetten. Als het hoger onderwijs essentiële diensten in de publieke cloud doet, dan geeft het onderwijs z'n kroonjuwelen weg. De vraag is wie dan nog in de toekomst de cloud innoveert, als het onderwijs de kennis/ervaring niet meer opdoet.

Herbert Bos liet zien hoe het Android-besturingssysteem beter beveiligd kan worden door een geavanceerde inbraakdetectie. Mobieltjes zijn tegenwoordig ultra-krachtig in vergelijking met een paar jaar geleden. Het zijn minicomputers geworden. De verwachting is dat gehackte en besmette mobieltjes een sterke opmars gaan maken.

Reden hiervoor is een stijgend gebruik van deze mobieltjes, het ontbreken van beveiligingssoftware en een slecht update management van de operating system software.

Remy Chavannes had als advocaat een interessante kijk op de rol die internet-providers spelen bij het bewaren van gegevens en het meehelpen aan het aftappen van het verkeer. Hij vergeleek hun rol met die van de wegbeheerder en vroeg zich af of het normaal is dat Rijkswaterstaat auto's controleert op illegale spullen.

Nico Dijkshoorn vormde het sluitstuk van de conferentie, met enkele pittige uitspraken zoals: "Ik ben hier nog geen vijf minuten binnen en ik hoor dat iedere willekeurige nerd in bus 33 nog geen vijf seconden zijn kruis tegen mij aan hoeft te drukken om in mijn telefoon te zitten."

Uitreiking Security Award 2011 door Ot van Daalen (R) aan Ian Cook (L).

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.

(ON)TERECHT INFORMATIE DELEN?

Pete Warden en Alasdair Allan waren aan het zoeken in bestanden op de iPhone en vonden een log van locatiegegevens. Dit brachten ze op 20 april in het nieuws, en de hele week, totdat Apple zelf een verklaring naar buiten bracht, stonden deze ontdekking en verdere ontknopingen hiervan pontificaal in het nieuws. We zijn er nauwelijks aan gewend dat gratis diensten onze gegevens opslaan, maar het gaat hier om betaalde diensten. Na uitleg kun je een positieve kijk hebben: er is waarschijnlijk niets fouts aan de hand en Apple gaat nóg zorgvuldiger met onze informatie omspringen. Of je hebt de negatieve kijk: er had van alles mis kunnen gaan, dit is nooit duidelijk uitgelegd aan de gebruiker en welke informatie is er nog meer waar we Apple, Google en Microsoft ongevraagd of half gevraagd aan helpen? Het heeft in ieder geval een nieuwe draai gegeven aan de privacy-discussies. Een panel van onze redactieleden doet ook een duit in het zakje.

Maarten Hartsuijker:
Toen ik een aantal jaren geleden met de voor-voor-voorloper van mijn huidige PDA door Brussel moest navigeren, was het apparaat al snel het spoor bijster. De hoge gebouwen, vele tunnels en smalle straatjes stelden de ingebouwde GPS niet in staat om zijn positie vast te houden. Dat dit slimmer kan, bewijzen de huidige smartphones. En als consument moet ik eerlijk zijn: betere locatiebepaling is een ontwikkeling waar ik écht op zat te wachten. Ik wil in een vreemde omgeving snel kunnen weten waar ik ben en als ik mij voortbeweeg verwacht ik van mijn smartphone dat hij mij bij kan houden.
Waar ik als informatiebeveiliger ook van houd is van controle over mijn eigen gegevens. En helaas bewijst het iPhone- en Android-nieuws dat deze twee zaken nog niet altijd goed samengaan. Apple en Google ontwikkelen geweldige nieuwe diensten op basis van publiek beschikbare gegevens. Maar het zou de bedrijven sieren als ze gebruikers niet alleen in de kleine lettertjes op de gevolgen van hun keuzes wijzen, maar tevens de controle zouden geven over de uitgewisselde data. Waarom moet er van locatiegegevens historie worden bewaard? En waarom kunnen gebruikers niet kiezen of zij de historie al dan niet willen bewaren voor toekomstig gebruik?
Op dit moment worden deze keuzes voor ons gemaakt en worden we regelmatig onaangenaam verrast door de privacy-consequenties hiervan. Als wij als gebruikers zelf kunnen kiezen welke gegevens wij willen uitwisselen en deze gegevens achteraf ook kunnen inzien en verwijderen, dan ziet het plaatje er ineens heel anders uit.

Aart Jochem:
Apple, Google en Microsoft verzamelen informatie over jou. Het is wel schrikken. Die o-zo-sexy digitale vriendin, die je overal meeneemt, alles toevertrouwt en waar je dagelijks mee naar bed gaat en mee opstaat, blijkt achter je rug om loslippiger te zijn dan je denkt. Het wordt pijnlijk duidelijk, als je de kaarten met locaties ziet. Er is geen geheim meer. Maar laten we eerlijk zijn. Eigenlijk wist je allang dat ze niet te vertrouwen was. Je was gevallen voor haar uiterlijk en de kunstjes die ze kon. Verandert dat, nu iedereen het weet? Ik denk het niet, we laten ons graag verleiden.
Het is toch ook prachtig? Op maat gesneden informatie en aanwijzingen, altijd op tijd en to-the-point. Ik droomde ervan toen ik met collega's bij Rijkswaterstaat een toekomstbeeld voor me zag over de manier waarop in 2027 reisinformatie wordt gewonnen en bij reizigers terechtkomt (www.scribd.com/doc/44875051). Dat was in 1998. Al 15 jaar later blijken deze dromen een accurate werkelijkheid te zijn. Er is één verschil. In 1998 was Googles motto nog 'Don't be evil'. Met het nieuws van afgelopen weken ontvouwt zich een schema van heimelijk ingewonnen data, waarop eindgebruikers geen invloed meer hebben behalve dan terug te keren naar het simpele Nokiaatje. Leveranciers van mobiele platforms, telecomproviders, handhavers van de wet, ze weten je allemaal te vinden. Er

is inderdaad een markt voor positie-informatie ontstaan van vele miljarden in omvang. Laten we er nu naar streven die markt open te maken en inzichtelijk te maken voor jou en mij. Misschien met een mogelijkheid voor opt-out, al is het maar voor even? Een digitaal boudoir, een plekje om me terug te trekken. Maar niet zonder m'n iPhone.

André Koot:
56% van de smartphone-bezitters kent de mogelijkheden van de GPS-functie in hun mobiel en 39% gebruikt die ook. Anderen doen dat niet, 33% van de bezitters maakt geen gebruik van GPS-functies uit privacy-overwegingen. De rest heeft nog geen reden gevonden om GPS te gebruiken. Zomaar een paar gegevens uit een recent White Horse-onderzoek onder smartphone-gebruikers.
Ik ben zelf ook een foursquare gebruiker en check regelmatig in. Maar ik ben wel selectief. Een deel van mijn gedrag wil ik wel delen met de wereld, maar niet alles. Net zoals ik een deel van mijn identiteit wel openbaar maak en een ander deel niet. Lastig is wel dat ik steeds na moet denken over welk stuk van mijn privacy ik prijsgeef. En daar wringt de schoen. Ik wil graag zelf bepalen wat ik met wie dan ook deel. De discussie die de afgelopen weken ontstond gaat nu juist dáárover. Ben je zelf 'in control' of denk je dat alleen maar? Het probleem is dat je zelf blijkbaar onvoldoende in staat bent om te bepalen welk deel van je privacy je prijsgeeft als leveranciers van jouw spullen buiten jouw wil om in staat zijn om jouw privacy prijs te geven. Natuurlijk weten we dat ze heel veel van ons weten. Daar maken we ook volop zelf gebruik van. Cloud apps zijn voordelig, want er wordt op een andere manier geld aan je verdiend. Als je er willens en wetens gebruik van maakt, dan moet je ook leven met de gevolgen. Dat geldt ook voor GPS. Als je willens en wetens gebruikmaakt van locatiediensten: jouw probleem. Maar als daarin de transparantie ontbreekt is er geen sprake van een eerlijke verhouding.

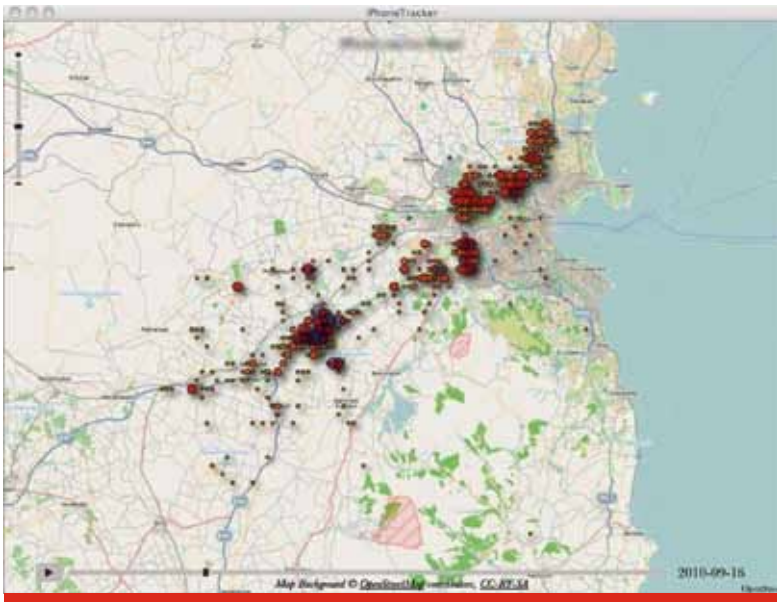
Lex Dunn:
Locatiegegevens zijn wat mij betreft privacygerelateerde gegevens. Het gaat niemand wat aan waar jij je op enig moment van de dag bevindt (zolang je tenminste niet van een misdrijf wordt verdacht). Dus het verzamelen van locatiegegevens via mobiele telefoons is ook onderhevig aan de WBP. Dat houdt in dat je als bedrijf vóóraf je klanten moet informeren dat je dit doet, waarom je het doet, en hoe lang je de verzamelde gegevens bewaard.
Voor zover ik de berichtgeving rondom de Apple iPhone, Google's Android en ook Microsofts Windows Phone 7 heb kunnen volgen, hebben deze allen verzuimd hun gebruikers ook maar iets te vertellen over de verzamelde locatiegegevens, of dat zover weggestopt in de gebruikersvoorwaarden dat zelfs een jurist het over het hoofd ziet. Dat mag dan misschien in de US of A wel zo gebruikelijk zijn maar hier in Europa denken we er toch anders over. Het vervelende voor de gebruiker is dat je totaal geen mogelijkheid hebt om na te gaan wat je mobiele telefoon of smartphone allemaal de ether in slingert.
Weet je nog, de ophef rondom het overmatige datagebruik op de eerste Windows Phone 7-toestellen? De gebruikers kwamen daar pas achter toen hun databundel op was, zonder dat ze zelf wat gedaan hadden met e-mail, Twitter of andere apps. Het helpt daarbij natuurlijk niet dat de besturingssystemen van de nieuwe generatie smartphones door de leveranciers volkomen dicht zijn gezet, zodat je alleen door hen goedgekeurde apps kunt installeren, en ook niet meer in het geheugen van JOUW smartphone kunt komen. Moet je jezelf hier druk over maken? Misschien wel, maar weet dat jouw locatiegegevens aan de hand van de GSM-signaalinformatie via de masten al jaren door de telecom providers wordt vastgelegd.

Links

upyours-internetmarketing.nl/blog/ook-windows-phone-en-android-slaan-locatiegegevens-op/

www.nrc.nl/nieuws/2011/04/20/iphone-slaat-in-het-geheim-je-locatie-op/

www.apple.com/pr/library/2011/04/27location_qa.html



Voorbeeld van een locatielog uit de iPhone (Ierland).

PRIJSUITREIKING ARTIKEL VAN HET JAAR 2010

Leo van Koppen is lid van de jury voor de verkiezing artikel van het jaar.
Hij is bereikbaar op l.c.m.vankappen@hhs.nl.

Op 19 april is tussen de PvIB-ledenvergadering en de workshop 'Social Engineering' in Rotterdam de prijs voor het artikel van het jaar uitgereikt. Voorafgaande aan de prijsuitreiking had columnist Berry van het redactielid André Koot al een eervolle vermelding in ontvangst genomen voor zijn trouwe bijdrage als columnist, al meerdere jaren. De fotograaf heeft hierbij helaas niet goed opgelet. Berry gaat schuil achter een pilaar…

Kees (L) reikt de 1e prijs uit aan Jan de Boer (R).

Kees Hintzbergen presenteerde namens de jury het verslag van de jury, inclusief het juryrapport, wat hierbij volledig is afgedrukt. Een leuke toevallige bijkomstigheid was dat de organisator van de workshop, Jan de Boer, ook de winnaar was van het artikel van het jaar.

Verslag van de jury

Ook dit jaar werden we als jury weer verrast met een longlist van negen genomineerden. Verrast omdat er toch altijd weer onderwerpen naar voren worden gebracht die op zijn zachts gezegd *bijzonder* zijn. Voor de derde keer alweer een verkiezing van het beste artikel in Informatiebeveiliging. Het is goed om nog even de winnaars van de voorgaande jaren in het zonnetje te zetten.

WINNAARS VAN VORIGE JAREN

2008
Wolter Pieters met *De monsterlijke trekjes van beveiligingsproblemen*

2009
Saïd El Aoufi met *De rol van audits (in beveiliging en architectuur raamwerken)*

Kees Hintzbergen presenteert het Juryrapport.

De jury bestaande uit de volgende drie personen, John Rudolph, Kees Hintzbergen en ondergetekende, heeft zich weer met enthousiasme over de artikelen gebogen en op basis van de door de redactie aangeleverde criteria een beoordeling opgemaakt. Dat hebben we eerst afzonderlijk gedaan en vervolgens, na een dit jaar korte discussie, hebben we een top drie samengesteld van beste artikelen. Hierbij onze bevindingen.

Het juryrapport

Op de 3e plaats is geëindigd het artikel van *J.M.T Wijnberg* over *Paspoortwet brengt burgers in gevaar*.
De jury is van mening dat de auteur in dit artikel een maatschappelijke kwestie aan de orde stelt die een zeer brede doelgroep benaderd. Het is een ook zeer actueel onderwerp en zal zeker ook daarom door informatiebeveiligers (die zich aangesproken moeten voelen) ter harte moeten worden genomen. Weliswaar is de basis van het artikel gelegd door organisatie Vrijbit en in het bijzonder ook de student Aaron Sjors Boudewijn die daar zijn inzet voor heeft getoond. Tegelijkertijd dus ook een soort postuum eerbetoon.
Op de 2e plaats heeft de jury het artikel van *Cor Rosielle* geplaatst dat gaat over *Trust audits*. Van vertrouwen weten we allemaal dat het te voet komt en te paard gaat, maar de auteur is er in geslaagd daar een heel andere dimensie aan te geven. Vertrouwen blijkt heel goed te kwantificeren te zijn en dat is verassend. We hebben nog niet eerder gezien dat emoties ook kwantificeerbaar zijn. In de huidige trend van het 'business like maken van informatiebeveiliging' past een dergelijk artikel natuurlijk uitstekend. Vlot geschreven en zeer actueel bovendien.
Op de 1e plaats is geëindigd het artikel van *Jan de Boer*, met de titel *De misleider te werk*. In dit artikel neemt de auteur ons mee naar de gewone wereld en hij probeert parallellen te trekken tussen de gewone wereld en het vakgebied van informatiebeveiliging. Hij maakt duidelijk hoe kwetsbaar we zijn als gewone mensen en daarmee ook als organisatie. Het artikel leest erg gemakkelijk en is voor informatiebeveiligers verplichte kost, omdat het op een uitstekende wijze illustreert dat het aandachtspunt van de inrichting van informatiebeveiliging zich zou moeten richten op de mens. In voorgaande afleveringen heeft Jan ons er al meermalen op gewezen dat mensen eenvoudig te verleiden zijn. Hieruit mag worden afgeleid dat de eerste plaats tegelijkertijd ook een soort van oeuvre prijs is.
Ook dit jaar is de jury van mening dat er een extra vermelding op zijn plaats is. Het artikel *In marketing shoes* van Wendy Goucher maakt op een zeer humoristische wijze duidelijk waar het allemaal om draait. Hoe verkoop ik informatiebeveiliging eigenlijk? Na het lezen van dit artikel kom je tot de conclusie dat je dat in het vervolg toch anders moet aanpakken. De gedachte 'security needs sex to sell' komt hierbij toch heel dicht in buurt. 'Wie de schoen past trekke hem aan' is het Nederlandse spreekwoord, maar geen van de juryleden wist echter raad met de 'high

Nieuw jurylid gezocht

Zoals Leo in zijn afsluiting aangeeft, zoeken we een jurylid. Hierbij doe ik het verzoek aan allen om een nieuw jurylid voor te dragen. John Rudolph bezette de 'auteurszetel' in de jury. We gaan dus op zoek naar een auteur als vervanging voor John. Eenieder die in de afgelopen drie jaar een artikel gepubliceerd heeft in Informatiebeveiliging kan genomineerd worden. Uit de nominaties kiest de redactie een nieuw jurylid. Stuur je nominatie binnen 30 dagen na verschijning van dit blad naar ibmagazine@pvib.nl.

Lex Borger, hoofdredacteur

Uitreiking eervolle vermelding door André Koot (L) aan Berry (R).

heels size 4'. Is dat nu de hoogte (4") of de maat van de schoen? In beide gevallen past het ons niet, maar de essentie van het verhaal hebben we zeker begrepen.

Alles overziend kan je zeggen dat alle vier artikelen vooral aandacht besteden aan het feit hoe Informatiebeveiliging toegankelijker kan worden gemaakt. IB dichter bij de dagelijkse gang van zaken brengen dat is klaarblijkelijk de boodschap waar we gezamenlijk voor staan.
We deden het weer met erg veel genoegen en mede namens Kees Hintzbergen danken we John Rudolph voor zijn inzet gedurende de afgelopen drie jaar, volgens reglement dient de jury nu ververst te worden.
We zijn benieuwd wie ons komt versterken.

Genomineerde artikelen (in chronologische volgorde):

Jaap van der Veen. De opbouw van IB-patronen. *Informatiebeveiliging 1,* 11

Peter Hoogendoorn en Jean-Pierre Vincent. Het business oriented autorisation model. *Informatiebeveiliging 2,* 11

Wendy Goucher. In marketing's Shoes. *Informatiebeveiliging 3,* 4

Erno Duinhoven. Een iPhone van de zaak. *Informatiebeveiliging 3,* 12

Leon Kuunders. Identity management en privacy. *Informatiebeveiliging 4,* 25

J. M. T. Wijnberg. Paspoortwet brengt burgers in gevaar. *Informatiebeveiliging 4,* 38

Ella Broos. Nederland is niet immuun voor autoritaire tendensen. *Informatiebeveiliging 4,* 43

Cor. Trust Audits. *Informatiebeveiliging 7,* 19

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)
Maarten Hartsuijker (ANWB)
Aart Jochem (GOVCERT.NL)
André Koot (Univé-VGZ-IZA-Trias)
Rachel Marbus (KPMG, IT Advisory)
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

Tenzij anders vermeld valt de inhoud van dit tijdschrift onder een Creative Commons Naamsvermelding-GelijkDelen 3.0 Nederland licentie (CC BY-SA 3.0).

creative commons

ISSN 1569-1063

CRISIS? WHAT CRISIS!

In de afgelopen periode hebben de kranten vol gestaan over wantoestanden bij financiële instellingen, banken, pensioenfondsen en andere instellingen waar de bestuurders de zakken vullen en hoge bonussen krijgen wanneer ze in staat zijn hoge rendementen te realiseren. Of de gerealiseerde rendementen een aantal maanden worden omgezet in zware verliezen zal de ontvanger van de bonus een zorg zijn. Investeren in Griekse fondsen leverde hoge rendementen op maar zijn helaas nu helemaal niets meer waard. En wie wordt de dupe van dit alles? Juist, de klant. Waarom gaan ze dan niet naar een andere financiële instelling? Dat komt deels omdat de overstap zorgt voor het nemen van grote verliezen of het wordt dermate moeilijk gemaakt dat je er echt niet aan wilt beginnen. Het grootste probleem is echter dat als je overstapt, je bij een andere club zakkenvullers terechtkomt.

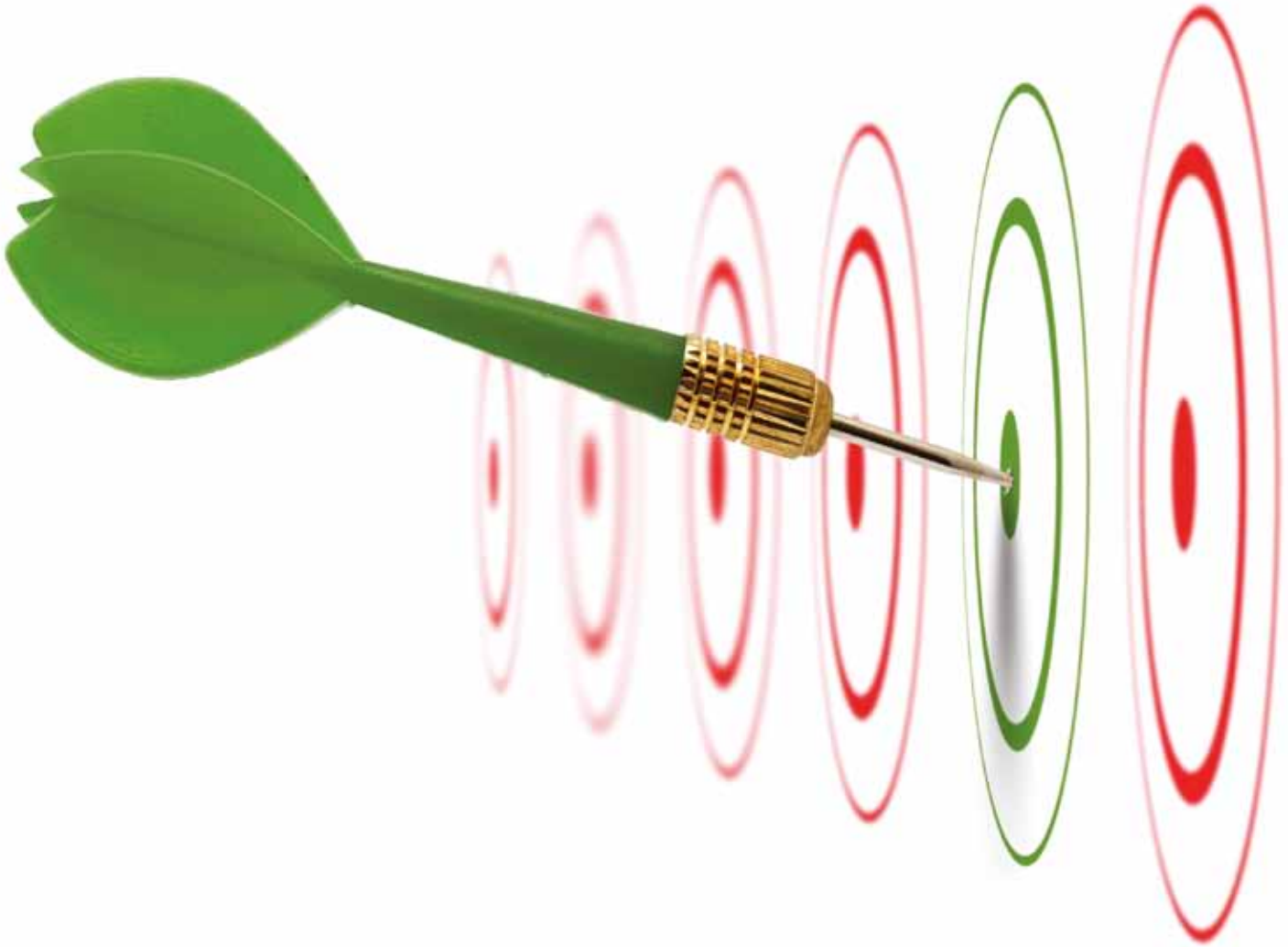
Als ik dit zo opschrijf bedenk ik me dat er nog een bedrijfstak bij hoort namelijk, de internetproviders. Ook dan is heel veel moed vereist om vrijwillig over te stappen. Ter illustratie een relaas van mijn gedwongen overstap naar een andere internetprovider. 'Gedwongen' omdat mijn provider werd overgenomen door deze grote provider. Ik zal het kort houden want alleen de gedachte aan deze ellende maakt mij al weer een beetje boos terwijl de dokter mij heeft aangegeven dat ik er veel over moet praten.
Mijn nieuwe modem komt aan, aansluiten en testen. Ik zie dat de processor continu op meer dan 95% belasting staat. Dat is niet goed en ik bel de helpdesk. "Dit gesprek kost 50 cent per minuut tot een maximum van 25 euro". Ik dacht dat het wel mee zou vallen want mijn modem is gewoon stuk. De man aan de andere kant van de lijn wilde allerlei testjes doen en toen ik uiteindelijk op één been stond, modem in de linkerhand en mijn rechterhand naar boven deed het ding het nog niet. "Tuut, tuut, tuut", zei mijn telefoon. Verbijsterd kijk ik naar het display en zie 50 minuten en 2 seconden staan. De verbinding was verbroken en ik moest opnieuw bellen. Na nogmaals voor zeven euro te hebben gebeld komt de man aan de andere kant van de lijn met het verlossende antwoord: "Meneer, uw modem is stuk. Ik stuur u een nieuwe". Drie seconden later was het modem echt stuk en de spiegel in de gang ook. Ik bespaar u het verdere verhaal omdat mijn vingers wederom beginnen te trillen.

Waarom internetproviders in het rijtje van banken en pensioenfondsen thuishoort moge duidelijk zijn. De heren maken zich zorgen om de smartphone. Na eerst deze telefoons zwaar te hebben gepromoot en daar een fijn datapakketje bij te hebben verkocht blijkt dat er inkomsten weglekken naar allerlei handige apps. Er zijn inmiddels allerlei goede alternatieven voor de peperdure diensten die de providers leveren. Tegenwoordig sms je niet meer, nee je pingt elkaar. Gratis en voor niets. Datzelfde kun je doen met bellen. Niet meer via de provider maar over VOIP die op je mobiele telefoon uitstekend functioneert. Dat was natuurlijk niet de bedoeling van onze providers. Nadat wetgeving had bepaald dat er vanuit het buitenland slechts een normaal bedrag voor een sms betaald hoeft te worden en de gesprekken goedkoper gaan worden zullen ongetwijfeld ook de datakosten in het buitenland onder handen worden genomen. En al die verloren inkomsten moeten natuurlijk terugkomen. Mijn eigen internetprovider staat nu al het 'tetheren' niet toe. Tetheren is het fenomeen dat ik mijn telefoon laat fungeren als modem voor mijn tablet. Nee, dat mag niet, maar ze kunnen niet uitleggen waarom. Dan moet je gewoon een tweede data-abonnement nemen op je tablet. Ik heb een poging gedaan mijn provider te overtuigen via het call center van die club (die overigens na de publiciteit van Youp van 't Hek nu wel goed functioneert) dat mijn datagebruik niet afneemt als ik twee 'abbo's' heb. Niet te overtuigen en (ondanks het feit dat ik het eerder beloofde nooit meer te zullen doen) heb ik op internet een app gedownload die ervoor zorgde dat ik met mijn tablet via mijn telefoon het internet op kan.

Ik durf één voorspelling te doen. Wie geproefd heeft van het gratis sms-verkeer en gratis IP-telefonie zal nooit meer anders willen en zal zich gedwongen voelen in de donkere hoeken van ons internet te zoeken naar alternatieven. Heren providers, wij betalen voor onze internetverbinding. Bemoei je er niet mee wat we ermee doen.

Groetjes,
Berry

CronLab's hosted web- en emailfilter missen hun doel nooit!



CronLab cloud security
Cronlab hosted email- en webfilter missen hun doel nooit! Met deze hosted filters is beveiliging makkelijker dan ooit. Ervaar hetzelf en probeer CronLab 30 dagen gratis. Surf naar www.crypsys.nl.

SC Magazine gaf CronLab pro 2000 antispam maar liefst 5 sterren! Met name het gebruiksgemak en de bijzonder goede spam detectie van maar liefst 99,1% maakten indruk op deze experts!

CRYPSYS Data Security is de expert op het gebied van security oplossingen en distributeur van o.a. CronLab. Neem contact met ons op via sales@crypsys.nl of via 018 362 44 44 om 30 dagen gratis gebruik van CronLab te kunnen maken! Kijk voor meer informatie op www.crypsys.nl.