05/2013

INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 5 - 2013

WAARBORGEN CONTINUÏTEIT SAAS-INFORMATIESYSTEMEN

DDOS - SMASHING THE BUSINESS FOR FUN AND PROFIT

WOMEN IN CYBER SECURITY: NUT OF NOODZAAK?

LOGIN, LOGOUT, WAAR GAAT HET FOUT?

CYBERCRIME, MAG EEN BEETJE PREVENTIE OOK?

TSTC – de Security Opleider van Nederland

- Diginotar, Facebook, KPN gehackt!
Bent u de volgende?

- En wat is dan uw reputatie- en/of financiële schade?
- Vormt uw Blackberry of iPhone een security risico?
Herkent u bovenstaande vragen?

Deze tijd vraagt om oplossingen en kennis van zaken.

Zorg dat u goed getraind bent, kijk gauw op
www.tstc.nl/training/security

Een greep uit onze security certificeringen:

Certified Ethical Hacker (CEH)
Computer Hacking Forensic Investigator (CHFI)
Certified Security Analyst (ECSA)
Licensed Penetration Tester (LPT)
Certified Information Systems Security Professional (CISSP)
Certified Information Security Manager (CISM)
Certified Information Systems Auditor (CISA)
Cloud Security Audit and Compliance (CSAC)
Certified Risk Manager ISO 27005/31000

TSTC - 6e jaar op rij de beste EC-Council Security Opleider Europa!

TSTC TSHUKUDU TECHNOLOGY COLLEGE

Want security start bij mensen!!

WWW.TSTC.NL

VOORWOORD

Recentelijk zijn er twee zaken groots in het nieuws geweest: de zoektocht naar de broertjes Ruben en Julian en het afluisterproject PRISM. Beiden gaan over het vinden van informatie in de zee van gegevens die tegenwoordig beschikbaar zijn. In 2010 sprak ik al over dit onderwerp met Bruce Schneier [1]. Hij zei hier toen over:
"Sociale netwerken maken het internet zeker minder anoniem. Echter, anonimiteit op het internet bestaat nog steeds. Dit lijkt een paradox, maar het is echt waar. Als je dat wilt, kun je volledig anoniem zijn op het web. Kwaadwillende gebruikers passen dit toe, maar ook diegenen die verborgen willen blijven voor kwaadaardige entiteiten."
"In het dagelijks leven is privacy in overvloed aanwezig. Het delen van informatie is binnen de fysieke context inefficiënt. Zelfs als je informatie deelt in een publieke setting, dan is de gedeelde informatie niet meteen publiek bekend. Op het internet is dat net andersom. Publiekelijk delen van informatie is eenvoudig. Je hoeft maar een blog te beginnen of lid te worden van Facebook of Twitter en je gedeelde informatie is publiek bekend. En alle context is weg. Je kunt niet langer informatie delen in de juiste context. Als je je hier niet van bewust bent, kun je van een koude kermis thuiskomen. Privacy is op het internet heel moeilijk te krijgen."
We hebben in beide nieuwsstromen de waarheid gezien die in deze opmerkingen opgesloten ligt.
Ruben en Julian konden maar moeilijk gevonden worden, ook al was er een massale zoektocht aan de gang. Waarom? Er waren heel veel surveillance-gegevens beschikbaar, maar er waren nog veel meer auto's op de weg geweest. Het bleef zoeken naar een naald in een hooiberg. Zeker als je al geen beperkt gebied hebt waarbinnen je kunt zoeken. Toen de broertjes gevonden waren, was het een stuk eenvoudiger om sporen te verifiëren, want toen wisten we waar we naar aan het zoeken waren. Hetzelfde moet gelden voor PRISM. Ook al is dit een gigantische zee van privacygevoelige gegevens (om het maar vriendelijk te zeggen), het moet toch moeilijk zijn daarin net die stukken te vinden die je helpen een aanslag te verijdelen. Hier is meer informatie de vijand van veel informatie, zeker als je je wilt verbergen. Zelfs met nieuwe "big data" ontwikkelingen verwacht ik niet dat hier veel nuttige zaken uit naar boven komen. Maar op het moment dat je een gerichte vraag hebt en dus een filter kunt toepassen, verandert het. Reken maar dat er dan veel informatie boven kan komen, die dan gebruikt wordt ter verificatie van wat dan ook. En dát maakt het zo eng, want je weet niet wie welk filter gaat toepassen voor welke verificatie. ●

Lex Borger, hoofdredacteur

Links

[1] IB5 2010, Bruce Schneier over privacy en meer: https://www.pvib.nl/download/?id=16673090

INHOUDSOPGAVE

Foto omslag: Study of a Cloudy Sky – John Constable

WAARBORGEN CONTINUÏTEIT SAAS-INFORMATIESYSTEMEN

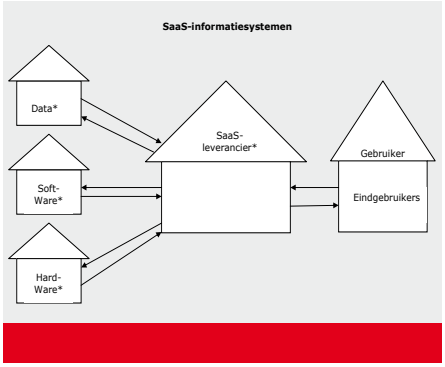
BRONCODE-ESCROW ALLEEN IS NIET VOLDOENDE

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

Onlangs is in dit blad vanuit Software Borg een publicatie verschenen waarin wordt gepleit voor een multidisciplinaire aanpak bij het verzorgen van de continuïteit van softwaregebruikers[1]. In dat artikel wordt mede gewezen op het belang van een sterke rechtspositie: de softwaregebruiker moet naast technische, ook de juridische middelen hebben om zijn continuïteit af te dwingen. Betoogd wordt, dat zulks met name geldt voor een broncode-escrowregeling. In dit artikel wordt aan de bespreking van het onderwerp broncode-escrow een vervolg gegeven. De nadruk ligt daarbij op de bespreking van de continuïteitsrisico's van de gebruiker van Software as a Service (SaaS) en met name op de manier waarop die risico's kunnen worden beperkt.

De karakteristieken van SaaS: complexer en meer divers dan on premises oplossingen

Net als dat bij on premises oplossingen het geval is, krijgt de gebruiker van SaaS tegen betaling een recht op het gebruik van de software. Verschil met 'traditionele' licenties is echter, dat de softwaregebruiker ook de toestemming moet hebben om gebruik te maken van de hardware en infrastructuur op afstand, waarmee de toegang tot de software feitelijk aan hem geleverd wordt. De SaaS-gebruiker krijgt geen objectcode-exemplaar, maar met de inloggegevens die zijn leverancier hem heeft verstrekt, kan hij zich via het internet toegang tot de software en de daarmee verwerkte gegevens verschaffen. Het toegankelijk en beschikbaar houden van die toegang gebeurt onder de verantwoordelijkheid van de leverancier, die daarbij vaak derde-partijen inschakelt.



De leverancier stuurt als hoofdaannemer de door hem ingehuurde derde-partijen aan. Een (eenvoudig en bekend) voorbeeld: de leverancier ontwikkelt en onderhoudt de software, maar een hostingprovider verzorgt de beschikbaarheid van de programmatuur en data. De gebruiker heeft niet in beeld door wie en hoe het totale SaaS-systeem functionerend wordt gehouden. De taken rondom het verzorgen van het beheer en de bereikbaarheid van de software en de gegevens kunnen dus onder meerdere, in een keten verbonden, partijen zijn verdeeld. Het wegvallen van één van die partijen kan het gebruik van de software en de toegang tot de data al frustreren. Omwille van de omvang, wordt in dit artikel uitgegaan van de situatie waarin de SaaS-leverancier wegvalt.

> De SaaS-gebruiker is eerstverantwoordelijke voor de continuïteit van zijn eigen bedrijfsvoering

De SaaS-gebruiker: wel verantwoordelijk, maar geen beschikkingsmacht

Van tijd tot tijd is er in de literatuur aandacht voor de risico's die de gebruiker van SaaS loopt. Dan gaat het bijvoorbeeld om vragen als: hoe zit het bijvoorbeeld met de af- en bescherming van de data (risico van onvoldoende informatiebeveiliging)? Worden de gegevens in een overdraagbaar formaat opgeslagen (risico van vendor lock-in)? Welke (overheids)instanties kunnen de op afstand verwerkte persoonsgegevens inzien (risico van niet voldoen aan wettelijke plichten)?

De SaaS-gebruiker is eerstverantwoordelijke voor de continuïteit van zijn eigen bedrijfsvoering. Wanneer die continuïteit mede wordt bepaald door de continuïteit van het onderhoud en gebruik van een computerprogramma en de daarmee verwerkte gegevens, eist zijn verantwoordelijkheid dat hij dat onderhoud en gebruik veiligstelt. De middelen die daarvoor nodig zijn, vallen echter niet onder zijn beschikkingsmacht. Dat is bij on premises software het geval, maar des te meer bij SaaS. In het eerste geval kan de gebruiker immers terugvallen op een werkend objectcode-exemplaar dat hij op eigen hardware heeft geïnstalleerd, terwijl daar bij SaaS niet op kan worden gerekend. Bovendien geeft hij naast de controle over de hardware en de software, de beschikkingsmacht over de data die met de SaaS-applicatie worden verwerkt uit handen.

Dit alles klinkt negatief, maar uiteraard moet niet uit het oog worden verloren dat het buitenshuis laten beheren van

IT hem grote (kosten)voordelen kan bieden [2]. De SaaS-gebruiker geeft met andere woorden meer weg, maar hij mag er wel wat terug voor verwachten. SaaS is dan ook een succesvol businessmodel, al betekent dit dus niet dat de SaaS-gebruiker minder (eind) verantwoordelijkheid heeft voor de continuïteit van zijn informatiesysteem. Bovendien moet hij meer doen om die verantwoordelijkheid goed in te vullen: hij moet meer beschikkingsmacht (terug) zien te krijgen.

Broncode-escrow: oplossing voor continuïteitsrisico's SaaS-gebruiker?

Het voldoen aan de verantwoordelijkheid voor het verzorgen van de continuïteit van bedrijfskritische software, is voor de softwaregebruiker zonder medewerking van zijn leverancier niet eenvoudig. Die medewerking kan tot uiting komen doordat de leverancier kiest voor het opzetten van een broncode-escrowregeling, waarbij de softwaregebruiker in het geval van een calamiteit toegang krijgt tot de broncode van de software en de daarbij horende technische documentatie. Het doel van broncode-escrow is het loskoppelen van de software-continuïteit van het voortbestaan van de leverancier.

Broncode-escrow alleen is, mits technisch en juridisch goed geregeld, voor de gebruiker van een on premises informatiesysteem dat door hemzelf draaiend wordt gehouden, voldoende. Met de toegang tot de broncode kan hij op de lange termijn voorzien in het onderhoud en de doorontwikkeling van de software. Met de veiligstelling van een (curator-proof) gebruiksrecht op de software is hij ook op de korte termijn verzekerd van het onafgebroken gebruik van de software: hij heeft immers reeds een werkend objectcode-exemplaar ervan in huis. Ook de gegevens die met de software worden verwerkt, zijn intern en op eigen gegevensdragers vastgelegd.

Voor de gebruiker van SaaS is broncode-escrow onvoldoende. Dat komt met name omdat het onafgebroken gebruik van de software niet meer kan worden bewerkstelligd met een stevig gebruiksrecht en een werkend exemplaar van de objectcode. De gebruiker kan immers niet terugvallen op een draaiend informatiesysteem: daar is de inzet van de leverancier voor nodig. De leverancier zorgt voor het dagelijkse beheer van de door hem aangeboden SaaS-oplossing. Voorts is hij degene die de voor de levering van de software ingeschakelde derde-partijen aanstuurt en hen betaalt voor hun diensten. Deze derde-partijen hebben geen verplichtingen tegenover de SaaS-gebruiker, waardoor zij hun dienstverlening zouden kunnen staken op het moment dat de leverancier hen niet meer betaalt. Leveranciersonafhankelijke softwarecontinuïteit is bij SaaS daarom lastiger te bewerkstelligen dan bij on premises programmatuur.

Continuïteit SaaS-informatiesysteem bij faillissement leverancier?

Ook het verzorgen van de continuïteit van SaaS-oplossingen is een multidisciplinaire aangelegenheid. De gebruiker moet niet alleen over de technische middelen (broncode, documentatie, data etc.) beschikken die voor het verzorgen van zijn continuïteit noodzakelijk zijn (de technische beschikkingsmacht), hij moet ook het recht hebben om die zaken te gebruiken (de juridische beschikkingsmacht). Het is de vraag of de rechten die hem in de SaaS-overeenkomst zijn toegekend, voldoende zijn. Allereerst zit het gebruiksrecht alleen op een draaiend exemplaar van de objectcode van de applicatie dat niet op de apparatuur van de gebruiker is geïnstalleerd. De gebruiker kan met enkel de SaaS-overeenkomst in de hand geen aanspraak maken op de broncode. Datzelfde kan ook gelden voor de data, waarvan de gebruiker niet zonder meer eigenaar is op het moment dat daaromtrent geen afspraken gemaakt zijn.

Die vraag wordt extra relevant op het moment dat de leverancier wegvalt, omdat hij in staat van faillissement is gesteld, vooral vanwege het door de Hoge Raad gewezen Nebula-arrest[3]. Een curator kan beslissen om SaaS- en continuïteitsregelingen die niet tegen die beslissing bestand zijn gemaakt, te wanpresteren. De curator heeft dus goede mogelijkheden om de continuïteit van een SaaS-oplossing en de beschikbaarheid van de daarmee verwerkte data, te frustreren.

De curator dient immers niet het belang van de SaaS-gebruiker, maar zijn handelen is erop gericht om de vorderingen van de schuldeisers op de failliete boedel zoveel mogelijk te voldoen. Hij heeft daarbij veel vrijheid. Hij kan ervoor kiezen om mee te werken aan een continuïteitsregeling of om de SaaS-dienstverlening onder dezelfde

Een té beperkt begrip

Escrow is een begrip dat in beginsel moet worden gebruikt voor het verschijnsel waarin een partij ten behoeve van zijn wederpartij een goed in bewaring geeft aan een betrouwbare derde. Bij broncode-escrow betreft dat goed een softwarebroncode. Zoals in deze publicatie wordt betoogd, is broncode-escrow slechts een klein onderdeel van het verzorgen van de continuïteit van SaaS-informatiesystemen. De escrowdienstverlener is niet meer de partij die slechts een DVD in bewaring neemt en aan de gebruikers overhandigt in het geval van een calamiteit. Hij moet daarentegen de middelen en know how hebben om onder andere SaaS-ketens en de omvang van de continuïteitsrisico's voor de SaaS-gebruiker in kaart te brengen, de contractuele huishouding van een continuïteitsregeling samen te stellen en de taken van een weggevallen SaaS-dienstverlener of ketendienstverlener over te nemen.

SaaS-escrow

voorwaarden voort te zetten. Denkbaar is daarentegen dat de curator de uitvoering van de continuïteitsregeling stil legt en de gebruikers laat bieden voor de toegang tot de software en/of de data. Dat een curator in het ene faillissement niet tegenwerkt, zegt niets over zijn rol in een ander geval.

De gebruiker is niet zonder meer eigenaar van de data

Kortom de curator is een onvoorspelbare factor die in een continuïteitsregeling voor SaaS-informatiesystemen moet worden geneutraliseerd. De exclusieve technische en juridische beschikkingsmacht over de middelen waarmee de continuïteit van de softwaregebruiker kan worden verzorgd, moet in de regeling aan een potentiële curator worden ontrokken. De SaaS-gebruiker moet in het geval van een calamiteit bij zijn leverancier, met de continuïteitsregeling er zeker van zijn dat ook hij die beschikkingsmacht krijgt.

Verzorgen continuïteit SaaS-informatiesysteem: algemene aandachtspunten

Die beschikkingsmacht ziet op de componenten van het SaaS-informatiesysteem die door de gebruiker uit handen zijn gegeven. Het gaat in de hoofdzaak om de software, hardware, data en het operationele beheer. In een continuïteitsregeling zal dus in ieder geval aan deze specifieke zaken aandacht moeten worden besteed. In de komende paragrafen zal hierop worden ingegaan, naast het feit dat ook de volgende algemene aandachtspunten een rol spelen bij het verzorgen van de continuïteit van SaaS.

Allereerst moet rekening worden gehouden met het feit dat de regeling, zowel op de korte als op de lange termijn, continuïteit moet bieden. Bij het wegvallen van de SaaS-leverancier betekent dat ten aanzien van de korte termijn dat het onafgebroken gebruik van de applicatie en de onafgebroken beschikbaarheid van de data worden veiliggesteld. Voor de lange termijn betekent dit onder andere dat de oplossing moet kunnen worden onderhouden en doorontwikkeld. De gebruiker moet dus de middelen krijgen die hem in staat stellen om de SaaS-oplossing te laten aanpassen en beheren door een partij of partijen die de weggevallen leverancier op dat punt vervangt respectievelijk vervangen. Een (kostbare) migratie van het SaaS-informatiesysteem en/of de overstap naar nieuwe programmatuur moeten liefst niet noodzakelijk zijn voor continuïteit.

Een algemeen aandachtspunt is tevens het feit dat het opzetten van een continuïteitsregeling maatwerk betreft, omdat SaaS-informatiesystemen en de daarachter liggende ketenstructuren van geval tot geval verschillen. Dit betekent dat het pas duidelijk is welke continuïteitsmaatregelen moeten worden genomen, op het moment dat deze zaken in kaart zijn gebracht. Bovendien is dit een multidisciplinaire aangelegenheid. Een gedegen technisch en juridisch vooronderzoek is dus noodzakelijk.

Bij het opzetten van de regeling spelen voorts de kosten van continuïteit een rol. Er mag geen afbreuk worden gedaan aan de economische voordelen die voor de gebruiker juist de beweegreden zijn geweest om op SaaS over te stappen. Dat betekent dat er altijd een afweging is tussen de kosten van een continuïteitsmaatregel enerzijds en de omvang van het af te dekken risico anderzijds.

De SaaS-gebruiker moet de beschikkingsmacht over de applicatie en de gegevens behouden

In het algemeen kan ten slotte gesteld worden dat het verloop van een calamiteit bij de leverancier en de afwikkeling daarvan van te voren moeilijk te voorspellen is. Een faillissement bijvoorbeeld, kan het einde van de leverancier betekenen, maar een curator kan ook bijvoorbeeld proberen om een doorstart te organiseren. En een curator is niet de enige onzekere factor. Ook van de noodzakelijke medewerking van de partijen die onderdeel zijn van de SaaS-keten, mag niet vanzelfsprekend worden uitgegaan. Een escrowdienstverlener dient dus in het belang van de gebruiker zoveel mogelijk uit te gaan van een worst case scenario.

Verzorgen continuïteit SaaS-informatiesysteem: software en hardware

Bij het verzorgen van de continuïteit van een SaaS-informatiesysteem moet allereerst de component software worden veiliggesteld. Voor de continuïteit op de korte termijn is nodig dat de software onafgebroken kan worden blijven gebruikt. Hiervoor zal het allereerst zo moeten zijn dat de software te gebruiken is wanneer de SaaS-leverancier wegvalt. De gebruiker moet gerechtigd zijn om de applicatie in het geval van een calamiteit bij zijn leverancier te blijven gebruiken: zijn softwarelicentie moet in stand blijven. Voorts moet bij een calamiteit de feitelijke beschikbaarheid van de software en dus de beschikbaarheid van de hardware waarop de software draait, worden verzorgd. De partijen die binnen een SaaS-keten daarvoor verantwoordelijk zijn, moeten daartoe dus technisch en juridisch in staat zijn. Bovendien moeten zij zich tegenover de gebruiker met zekerheid committeren, maar er ook op kunnen vertrouwen dat zij voor hun dienstverlening worden betaald.

Voor continuïteit van de software op de lange termijn, dient gebruik te worden gemaakt van solide broncode-escrow. Uitgangspunt is dat alle broncode, technische documentatie, beheersinformatie, hulpsoftware en de overige zaken die noodzakelijk zijn voor het kunnen beheren, reconstrueren en onderhouden van het SaaS-informatiesysteem, gedeponeerd zijn bij de escrowdienstverlener.

Dit depotobject moet werkzaam en actueel zijn, iets waarbij de specifieke kenmerken van SaaS een belangrijke

rol spelen. Zo moet rekening worden gehouden met het feit dat veel SaaS-oplossingen zeer frequent worden geupdate, en de broncode ervan dus snel veroudert. Een mogelijke oplossing voor dit probleem is om met behulp van een koppeling aan het versie managementsysteem van de leverancier, ervoor te zorgen dat de escrowdienstverlener bij totstandkoming van een nieuwe versie van de broncode daarover meteen de beschikking krijgt.

In het geval van een calamiteit bij de SaaS-leverancier, wordt het depotobject aan de gebruiker afgegeven. Hij moet daarbij kunnen rekenen op ondersteuning bij het aanwenden van het depotobject voor continuïteit. Zo moet de escrowdienstverlener in staat zijn om het dagelijkse beheer van het SaaS-informatiesysteem over te nemen.

Verzorgen continuïteit SaaS-informatiesysteem: data en operationeel beheer

Bij het opzetten van een continuïteitsregeling verdienen de data specifieke aandacht. Ten eerste moeten zij beschikbaar blijven bij het wegvallen van de leverancier, iets wat net als bij de beschikbaarheid van de software gekoppeld is aan de beschikbaarheid van de hardware. De hosting van de data moet kortom gegarandeerd zijn, omdat de gebruiker niet de feitelijke beschikkingsmacht heeft over de gegevens, althans in verwerkbare vorm. Daarbij komt echter, dat de SaaS-gebruiker zonder nadere afspraken niet zonder meer eigenaar van de data is. In het kader van de continuïteitsregeling zullen daarom de (intellectuele) eigendomsrechten die op de data rusten, moeten worden overgedragen aan de gebruiker. De data moeten ten slotte in een voldoende overdraagbaar formaat zijn opgeslagen. Dit opdat de gebruiker, indien hij gewenst, over kan stappen naar een andere applicatie op het moment dat zijn SaaS-leverancier wegvalt.

Daarnaast dient de escrowdienstverlener bij het opzetten van de continuïteitsregeling vast te stellen welke organisatorische maatregelen moeten worden genomen: welke partijen moeten wat doen in het geval van een calamiteit bij de leverancier? Moeten werknemers van de weggevallen leverancier betrokken worden bij de voortzetting van het beheer van het informatiesysteem? De afspraken die worden gemaakt, zullen in een contract moeten worden gegoten, zodat de verplichtingen afdwingbaar zijn. De escrowdienstverlener zorgt ervoor dat de rol van de weggevallen SaaS-leverancier wordt uitgevoerd en dat op operationeel niveau het roer wordt overgenomen. Hij kan dat zelf doen, maar deze taak kan (op termijn) tevens worden uitgevoerd door een andere partij die daartoe bekwaam is. De escrowdienstverlener heeft ten slotte de functie van coördinator: hij verzorgt de aansturing van de ketendienstverleners die de SaaS-applicatie draaiend moeten houden. ●

> Een escrowdienstverlener dient uit te gaan van een worst case scenario

Links

[1] *H.J.J. Hensen en J.W. Oordt, 'Recht en Informatiebeveiliging: samen sterk', Informatiebeveiliging 2013/1.*

[2] *W.S. Chung, 'Informatiebeveiliging versus SaaS, Compact 2008/4.*

[3] *Zie voor een meer uitvoerige bespreking van dit arrest ook link [1].*

[4] *Software Borg Stichting: http://www.softwareborg.nl*

Software Borg Stichting en IT-notaris

De SaaS-continuiteitsregeling van Software Borg [4] gaat voor een belangrijk deel uit van de noodzaak van gedegen vooronderzoek en maatwerkoplossingen. Dat komt uiteraard doordat de techniek en organisatie van de dienstverleners-keten achter een SaaS-oplossing van geval tot geval verschilt. Zo kan het inschakelen van een hostingback-up noodzakelijk zijn, wanneer de software-leverancier zelf de applicatie en de data host. Een andere oorzaak is de contractenketen die de basis vormt voor de verplichtingen van de partijen die bij de SaaS-oplossingen betrokken zijn. De softwareleverancier hoeft bijvoorbeeld niet de houder van de auteursrechten op de applicatie te zijn.

Software Borg inventariseert en verzamelt de middelen en kennis die noodzakelijk zijn voor het voortzetten van de SaaS-oplossing bij het wegvallen van de leverancier. Deze worden gecontroleerd op werkzaamheid en actualiteit. Vervolgens worden deze zaken in een (digitale) kluis van de IT-notaris opgeslagen.

Voorts voorziet de continuïteitsregeling in de doorbetaling van de partijen die de SaaS-oplossing in stand moeten houden op het moment dat de softwareleverancier is weggevallen. Daartoe wordt gebruik gemaakt van een derdengeldenrekening. De gebruikers maken naar die rekening een bedrag over op het moment dat een calamiteit zich voordoet. De IT-notaris verzorgd aansluitende de doorbetaling.

Als tegenprestatie voor de zekerheid van de doorbetaling van hun dienstverlening, verplichten de ketendienstverleners zich tot het in de lucht houden van de SaaS-oplossing gedurende een bepaalde periode. Zo kan de SaaS-applicatie ook bij een calamiteit voor een bepaalde periode onafgebroken worden gebruikt en is het mogelijk om voor de lange termijn een oplossing te vinden met de broncode en de andere technische middelen die aan de IT-notaris zijn toevertrouwd.

DDOS - SMASHING THE BUSINESS FOR FUN AND PROFIT

by Maciej Ogórkiewicz. Maciej Ogórkiewicz is Deputy Director of ING's Global Security Operating Centre. He can be reached at Maciej.Ogorkiewicz@ing.nl.

The fourth quarter of 2012, and the months of 2013 up to now exhibit high levels of activity from Distributed Denial of Service (DDoS) attackers against many companies and institutions across the globe. Recent press headlines have informed of many attacks against large financial services in the US and Europe.

Not only financial companies are under attack. Recent information and reports indicate that the e-commerce sector and software-as-a-service (SaaS) organisations have been attacked by DDoS during the last few months. The security world is evolving now and advanced persistent threats (APTs) are a top concern for operators and enterprises now. Organisations are more concerned and focused on dealing with 'botted' and compromised machines (by malware), industrial espionage, data exfiltration and malicious insiders. DDoS attacks are seen as one of the most important security threats nowadays. Why is DDoS so painful for the organisation? There are a few answers to this basic question:

No one is safe

Even the largest and most powerful organisations in the world are unable to defend themselves on their own (without cooperation with 3rd parties such as service providers, cloud providers and/or Anti-DDoS Services providers) – no one is safe.

The means and the tools

Perpetrators are well equipped with DDoS toolkits (i.e. isokandnoproblemobro toolkit aka BroDoS toolkit have been identified recently) and large networks of 'botted' workstations and mobile devices – attackers have the means and the tools.

Attacks harder to overcome

DDoS attacks are getting more and more sophisticated and advanced since malware is highly involved in DDoS attacks. Evolution and improvements in the existing toolkits and techniques are observed by Anti-DDoS Service Providers such as Arbor, Prolexic or Akamai. These organisations are reporting more multi-vector DDoS attacks mostly against Web-based services.

> DDoS attacks are seen as one of the most important security threats

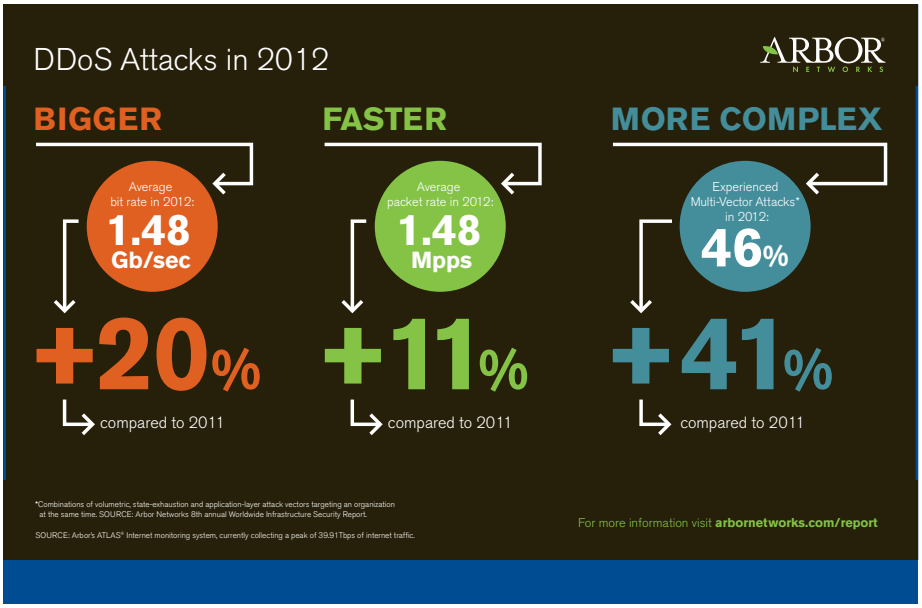
Multi-vector attacks employ combinations of volumetric, state-exhaustion and application-layer attack vectors targeting an organisation at the same time. Multi-vector attacks can be challenging to mitigate and generally require layered solutions across the data centre and the cloud for successful mitigation – which is why they are an attractive approach for hackers looking to cause the most damage – the DDoS attacks are harder to overcome.

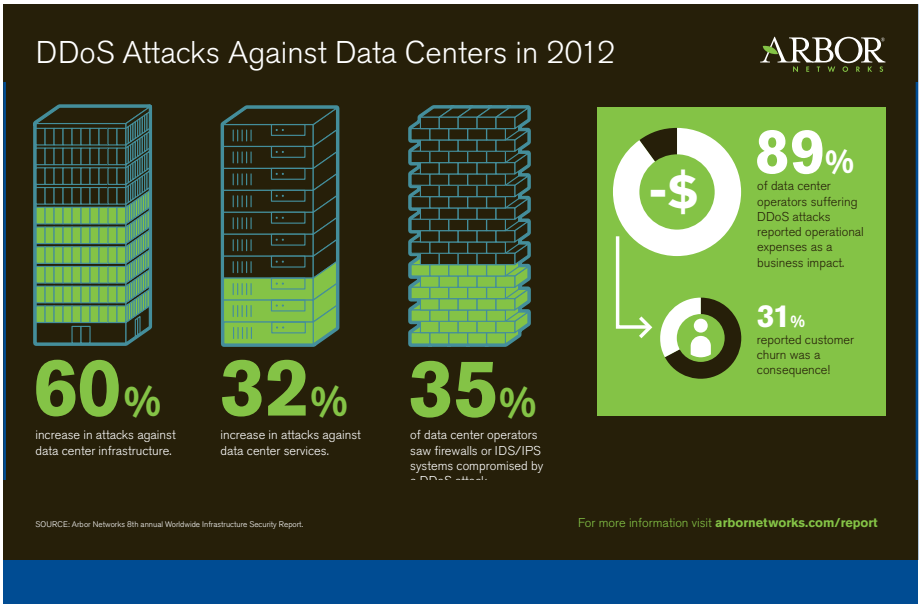
Anyone can be a victim

The 'Bring Your Own Device' (BYOD) trend and an increasing number of mobile devices (increasing LTE technology, more bandwidth available for mobile devices) in relation with a lack of detective and preventive measures at reactive rather than preventive mobile service providers cause a threat to unprotected organisations. Perpetrators have an area to create large botnets ready to launch attacks – anyone can be a victim and a tool in perpetrators' hands.

Unprotected communication channels

Domain Name Service (DNS) infrastructure is still vulnerable to DDoS and organisations are starting to consider DNS as a problem but still there are a lot of DNS servers allowing anyone to do recursive queries [3]. Also unsecured IPv6 deployments in production environments could





expose organisations to the risk. Many organisations are switching from IPv4 to IPv6 due to exhaustion of available IPv4 addresses. Having full IPv6 implementation or so-called 'dual stack' (concurrent implementation of IPv4 and IPv6 protocols in the same network) is normal practice nowadays, especially in the operator's network and DC's service providers. Unfortunately, many organisations have not endeavoured to have the IPv6 world well protected and IPv6 security is not perceived as a serious problem by many of them. Although DDoS in IPv6 is possible, attacks are rarely observed. It will change in the coming months and years – there are still unprotected communication channels.

Undetected perpetrators

Readiness and awareness have increased over the last few years, especially in large organisations concerned by DDoS and other APTs. This is good but law enforcement is not effective. Just over a half of responders surveyed by Arbor Networks still do not refer security incidents to law enforcement. Confidence in the efficiency of law enforcement is low and the reasoning behind that could be reflected by the fact that the real perpetrator usually remains undetected. Many types of DDoS enable the attacker to use spoofing and to be evasive – the real perpetrator could remain undetected and DDoS attacks could be relatively easy to render.

In 2011 Arbor Technologies stated, for the first time, the motivations for DDoS attacks. The top three most common perceived motivations are as follows:

- Political and/or ideological (i.e., hacktivism)
- Online gaming (not gambling)
- Vandalism and/or nihilism
- These are largely personally motivated acts done in reaction to real or perceived offences.

DDoS – What's going on?

The taxonomy of the attack

A Distributed Denial of Service attack is, in fact, a keyword describing a set of attacks aiming for the same goal: to make a machine or network

DDoS attacks at a glance (Y2012)

Bigger: Average bit rate in 2012: 1,48 Gb/s (+20% compared to 2011)
Faster: Average packet rate in 2012: 1,48 Mpps (+11% compared to 2011)
More Complex: Experienced Multi-Vector Attacks in 2012: 46% (+41% compared to 2011)

Source: Arbor Network 8th Annual Worldwide Infrastructure [6]

DDoS attacks against data centres (Y2012)

60% increase in attacks against data centre infrastructure
32% increase in attacks against data centre services
35% of data centre operators saw firewalls or IDS/IPS systems compromised by a DDoS attack
89% of data centre operators suffering DDoS attacks reported operational expenses as a business impact
31% reported customer churn was a consequence!

Source: Arbor Network 8th Annual Worldwide Infrastructure[7]

resource unavailable to its intended, legitimate users. The main difference between Denial of Service attack and its 'distributed' variety is the source of the attack. Usually DoS has one source while DDoS attackers use many, multiple sources of attacks at the same time. DDoS attacks could be differentiated from many angles but there are three main approaches to distinguish them. Accordingly to Arbor technologies, DDOS Attack vectors tend to fall into one of three broad categories:

- Volumetric Attacks: These attacks attempt to consume the bandwidth either within the target network/ service, or between the target network/service and the rest of the Internet. These attacks are simply about causing congestion.
- TCP State Exhaustion Attacks: These attempt to consume the connection state tables that are present in many infrastructure components, such as load balancers, firewalls and the application servers themselves. Even high-capacity devices capable of maintaining state on millions of connections can be taken down by these attacks.
- Application Layer Attacks: These target some aspect of an application or service at Layer 7. They are the most sophisticated, stealthy attacks because they can be very effective with as few as one attacking machine generating a low traffic rate. This makes these attacks very difficult to proactively detect and mitigate.
- Another vendor of Anti-DDoS solutions – RioRey proposes a different taxonomy of DDoS attacks [5]:
- TCP Based Attacks (SYN Flood, SYN-ACK Flood, ACK & PUSH ACK Flood, Fragmented ACK, RST or FIN Flood, Synonymous IP, Fake Session, Session Attack, Misused Application)
- TCP HTTP Based Attacks (HTTP Fragmentation, Excessive VERB Excessive VERB Single Session, Multiple VERB Single Request, Recursive GET, Random Recursive GET, Faulty Application)
- UDP Based (UDP Flood, Fragmentation, DNS Flood, VoIP Flood, Media Data Flood, Non-Spoofed UDP Flood)
- ICMP Based (ICMP Flood, Fragmentation, Ping Flood)

Prolexic – Anti-DDoS service provider – distinguishes the DDoS Attacks from a 'layer' perspective in reference to the IOS/OSI network model. This is a combination of those two from above:

- Infrastructure – Layer 3 & 4 (ICMP, TCP Fragment, SYN PUSH, DNS, UDP Fragment, ACK, RST, UDP, SYN)
- Application – Layer 7 (SSL GET, PUSH, HTTP POST, SSL POST, HTTP GET)

Accordingly to "Prolexic Quarterly Global DDoS Attack Report Q4 2012" [1], throughout Q4 2012, the majority of observed attacks were focused on network infrastructure (75%,05%). 24,95% of the attacks were being led in the application layer. The most common infrastructure (Layer 3) attack types made use of SYN floods and UDP floods. The majority of SYN floods are suspected to have originated from botnets consisting of infected workstations or mobile devices. The UDP floods primarily originated from the use of web server booter shell scripts such as that mentioned previously, the itsoknoproblemobro attack suite (BroDoS).

Malware is highly involved in DDoS attacks

Application Layer 7 attacks, the majority of flood traffic, came in the form of GET floods and POST floods targeted against web services. A combination of both booter shell scripts (malware installed on a server/zombie intended to initiate a DDoS attack) and traditional botnet infrastructures were responsible for the bulk of Layer 7 attack traffic observed by the Prolexic Security Emergency Response Team.

Interesting information can also be found in the "Worldwide Infrastructure Security Report" by Arbor Network, Inc [2]. Arbor's responders, surveyed for application-layer attacks, see the increasingly common role of application-layer attacks over the past few years (86% of them report application-layer attacks targeting high-profile web services). The proportion of reported application-layer attacks has not changed significantly over the years and the Top Five of them are as follows: HTTP, DNS, HTTPS , SMTP, SIP/VoIP. The role of HTTPS is proportionally increasing, which indicates that e-Banking applications and e-Commerce applications are a target of attacks more than in the past.

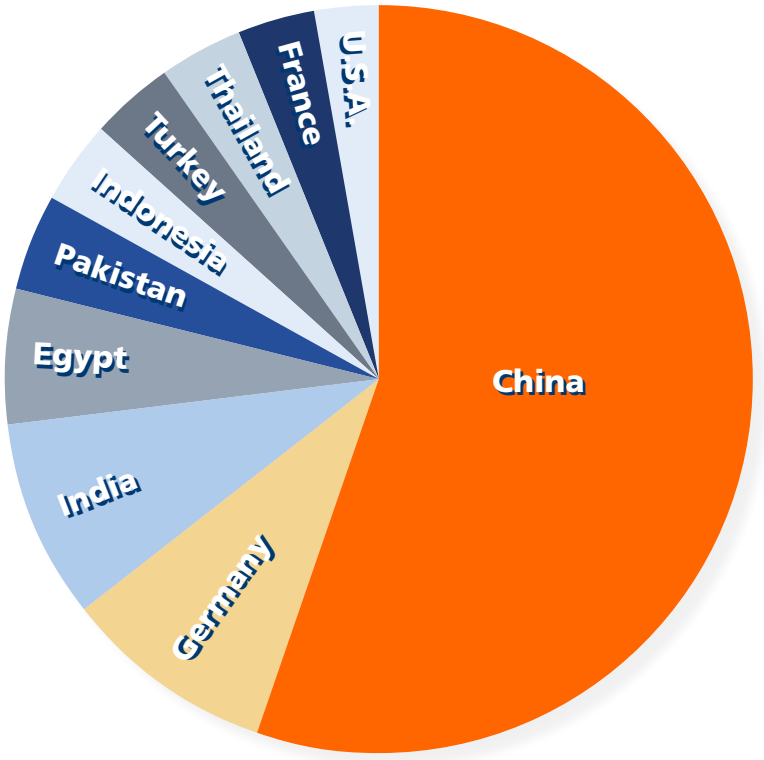
Know your enemy

Operators and service providers regularly publish data about sources of DDoS attacks per country or per AS number (AS – autonomous system – unique identifier assigned to operator/ provider in the Internet network; AS is being used by Border Gateway Protocol – BGP, to route IP packets between source and destination).

The latest "Prolexic Quarterly Global DDoS Attack Report Q4 2012" [1] depicts interesting data regarding the sources of DDoS attacks, presented by country and AS. According to that information, providers from China (over 55%) have taken the lead in the ranking exhibiting the top originators of DDoS attacks against organisations worldwide. This trend has not changed for the last two quarters. It is believed that China is at the top due to a large number of vulnerable servers and workstations that exist in the country. The majority of the remaining attack traffic originated from botnets or machines compromised by malware within Europe and Asia (see: chart on the next page).

Arbor: Confidence in the efficiency of law enforcement is low

Q4 2012 was active in comparison to previous quarters. The total number of attacks increased by 27,5%, the total amount of infrastructure attacks increased by 17,4 per cent and the total



Top Ten Originators of DDoS attacks in Q4 2012 per country

China: 55,44%, Germany: 9,07%, India: 8,77%, Egypt: 5,73%, Pakistan: 4,26%, Indonesia: 3,61%, Turkey: 3,58%, Thailand: 3,52%, France: 3,31%, U.S.A.: 2,71%.

number of application layer attacks increased by 72,2%. The average attack duration rose by 67% from 19,2 hours to 32,2 hours. Additionally, the average bandwidth was up 20 per cent, rising from 4,9 Gb/s to 5,9 Gb/s this quarter. That data was presented by Prolexic, although other Anti-DDoS Service Providers presented different values (Arbor measured the average DDoS attacks as 1,48 Gb/s) but they claim that there is an increase in DDoS activity in terms of amount of attacks and volumes. The bandwidth used by DDoS attack perpetrators is a hot topic, especially for Internet Service Providers and DC Operators. The largest observed attacks by Arbor in 2011 and 2012 exceeded 100 Gb/s, but attacks at the level of 60–80 Gb/s are not unusual nowadays. These values are a problem even for large service providers because inter-operator links and backbone networks do not have infinite capacity enabling them to absorb and process such a big amount of traffic. Big players on the service provider market are capable technically to increase the bandwidth on their links but it costs and money spent on that cannot be easily reflected in customer invoices (those investments are not justified by market demand).

Are we defenceless?

The truth is no one can feel safe but there are countermeasures available on the market to defend organisations from DDoS attacks. The potential consequences of DDoS attacks cannot be mitigated by the installation of 'yet another magic security box' which prevents DDoS attacks 100%. The only organisations which have Anti-DDoS holistic architectures implemented, processes that work in case of an attack, and tested procedures, can survive DDoS attacks and remain in relatively good condition. The solution lies in the organisation's IT system or processes. The risk of DDoS cannot be mitigated with good cooperation with well-prepared Internet Service Providers and/or Anti-DDoS Service Providers capable of dealing with the traffic affected by DDoS perpetrators.

China (over 55%) is the top originator of DDoS attacks worldwide

So, what can organisations do to defend services and customers from attacks? The items listed on the next page are a set of keywords describing several techniques that could be used and/or the concepts that could be considered as a countermeasure in the Anti-DDoS architecture:

Sufficient capacity of network links, network devices and IT equipment hosting applications and databases: the links and equipment on the path between the Internet and the application should have the capacity to process the traffic and number of sessions bigger than usually processed in normal conditions. It is worth mentioning that replacing the links toward the Internet or replacing the device in the path with a device of a bigger capacity, will result in a bottleneck somewhere in the path. Usually, equipment such as: firewalls, IPS, application firewalls, have less capacity than the speed of their network interfaces. During the process design of a new architecture the capacity and performance of every element has to be assessed. As previously mentioned, trends indicate that the role of application-layer attacks will increase in the coming years, therefore especially key devices, processing application-layer traffic (i.e. load balancers, SSL accelerators, web servers etc.) need to be evaluated. It is worth mentioning that application-layer DDoS attacks conducted in vital communication channels used by online applications (i.e. HTTP, HTTPS) are the most difficult to mitigate. When attacks happen, analysts try to find a pattern describing the DDoS traffic and with that they recommend actions aiming to eliminate those packets from the bandwidth. The most painful situation is when such a pattern cannot

be determined, for instance: the HTTP request is directed to a web application, and those requests originate from many countries (it is difficult to determine which flow is an attack and which is not). Cases and scenarios like that have to be considered during the process design of Anti-DDoS architecture.

Sufficient capacity of the service providers: The Internet Service Providers and DC Operators need to be prepared and capable to mitigate the consequences of DDoS attacks directed towards their customers. The selected provider or operator has to have Anti-DDoS measures implemented, processes and knowledgeable personnel in place and has to be fitted with devices and links of sufficient capacity (please note that the providers' infrastructure is shared among customers).

Attacks at the level of 60–80 Gb/s are not unusual nowadays

Anti-DDoS Services / Scrubbing Centres: During a DDoS attack, traffic is redirected to a scrubbing centre. Usually it is a cloud-based, high-performance infrastructure connected to the biggest, global Internet Service Providers' carriers (i.e. 800 Gb/s capacity). Scrubbing centres are fitted with DDoS filtering techniques, advanced routing, and anti-DoS hardware devices that remove DDoS traffic close to the source of botnet activity. Clean traffic is then routed back to the customer's network. It is recommended to have more than one scrubbing centre available in the providers' network to switch or double them in case of a very severe and large attack.

Blackholing: This technique enables the organisation to trigger remotely the directing of traffic generated by botnets to a non-existing IP address or null interface of the providers' routers (in practice it means that the traffic is dropped). Two types of blackholing can be distinguished: source based remote triggered blackholing (S-RTBH) and destination based remote triggered blackholing (D-RTHB). The main difference between these two is that the first type drops traffic described by the source pattern while the second one drops traffic based on its destination. This technique can be used effectively to mitigate the infrastructure-layer attack mostly in the case when a pattern in the traffic can be determined to trigger blackholing. For application-layer attacks the scrubbing centres are more effective (because the scrubbing centre is trying to 'heal' the traffic) while blackholing means in practice dropping the traffic coming to/from a particular country or provider. Blackholing could be used as an additional mitigating control in the case of the most severe attacks when a scrubbing centre is unable to remove DDoS packets from the bandwidth, but this is a 'last resort' countermeasure.

No one can feel safe from attacks but there are countermeasures available

DDoS threats are one of the biggest concerns for organisations and institutions using the Internet to render services for their customers. Based on trend analysis, the main conclusion is that DDoS attacks will increase in the coming years and attacks will be more sophisticated and advanced. organisations willing to have the ability to provide undisrupted online services need to be prepared for DDoS attacks by implementing anti-DDoS measures, crisis procedures and being able to respond to attacks smoothly. That is another battle in the security field that needs to be fought.

IT Cloud Services: External IT cloud service providers could be used as an additional mitigating control in designed anti-DDoS architecture. Some parts of applications or web-based services could be installed outside the primary network, in the external cloud. This is relevant mostly to static main web pages, pictures and everything that is not directly related with vital online applications but is related to the organisation's presence on the Internet. In the case of a DDoS attack, requests for the main page, pictures and everything which might adversely affect bandwidth stressed by DDoS (especially in an upstream direction), can be served from the external IT Cloud preserving the resources and the bandwidth for application-related requests and traffic.

DNS Protection: As presented, trends indicate DDoS attacks against Domain Name Service infrastructure. This is a vital infrastructural component which ensures that the organisation is visible in the

network under the company's domain name and a brand, and the organisation's services are visible in the network.
Hitting the DNS servers with a DDoS attack could result in the unavailability of online services because clients would be unable to resolve the domain name into an IP address to establish a connection.
DNS infrastructure should be protected against DDoS and this protection must be an important element of Anti-DDoS architecture. The most common technique used for that is to use the concept of primary and secondary DNS servers hosting domains. The domain should be hosted by the secondary DNS servers residing in the provider's network outside the network that can be hit by DDoS. This ensures the availability of the DNS services in case of an attack and full saturation of the bandwidth causing the company network to respond slowly or become inaccessible.
Although this paragraph describes DNS protection, it is worth mentioning that other protocols, ensuring the network and systems are working properly, need to be well protected. For example BGP sessions should be preserved and properly maintained in case of a DDoS attack.
A broken BGP session would result in the unavailability of the company's IP address pools in the global Internet network and other anti-DDoS techniques would help. BGP should be operational by secondary network links toward a provider enabling the organisation to advertise its address pools even under attack. ●

Links

[1] *Prolexic Quarterly Global DDoS Attack Report Q4 2012 - http://www.prolexic.com/knowledge-center-ddos-attack-report–2012-q4.html*

[2] *Worldwide Infrastructure Security Report 2012 (Arbor Networks, Inc.) - http://www.arbornetworks.com/research/infrastructure-security-report*

[3] *Distributed Reflection Denial of Service (DDoS) Attacks (Prolexic) - http://www.prolexic.com/knowledge-center-white-paper-series-dns-reflection-amplification-drdos-attacks-ddos.html*

[4] *Cisco Systems Documentation, for instance http://www.cisco.com/en/US/tech/tk59/technologies_white_paper09186a0080174a5b.shtml*

[5] *Taxonomy of DDoS Attacks (RioRey) - http://www.riorey.com/x-resources/2011/RioRey_Taxonomy_DDoS_Attacks_2.2_2011.pdf*

[6] *DDoS Attacks in 2012 (Arbor Networks, Inc.) - http://pages.arbornetworks.com/rs/arbor/images/DDoS%20Attacks%20in%202012.pdf*

[7] *DDoS Attacks Against Data Centers in 2012 (Arbor Networks, Inc.) - http://pages.arbornetworks.com/rs/arbor/images/DDoS%20Attacks%20Against%20Data%20Centers%20in%202012.pdf*

COLUMN

WAT JE NIET HEBT, KAN JE NIET ONTNOMEN WORDEN

Toen ik een paar jaar geleden begon met het schrijven van deze column, deed ik een oproep voor zelfcensuur. Ik doe het nu nogmaals, maar dan wat breder. Als het gaat om data, in welke vorm dan ook, bedenk je dan eerst: wat ik niet heb of een ander niet heeft, kan niet ontnomen worden. Ik besef me dat dit geen zaligmakend adagium is, maar meer een pleidooi om wat zuiniger te zijn (dat zou ons Hollanders toch moeten aanspreken, nietwaar?).

Nog niet zo heel lang geleden liep een ISO bij me binnen. Dat 'men' graag gratis Wifi wil aanbieden en dat 'men' daarbij bedacht had dat het handig was om gebruikers te laten inloggen met zelfgekozen naam en wachtwoord. Daarnaast zouden separaat de IP-adressen gelogd worden. Ik snap de wens voor naam en wachtwoord, je helpt de Wifi-gebruiker te voorkomen dat hij makkelijk prooi wordt voor een man-in-the-middle. De ISO maakte zich druk over de privacy van gebruikers, maar ook over aansprakelijkheid van het bedrijf in die gevallen dat gebruikers 'onkuise' dingen zouden doen via de Wifi. En wat nu als de overheid zou willen vorderen, we hebben immers de data van gebruikers en ook IP-adressen? Ik gaf hem twee zaken mee: 1) verbied gebruikers in te loggen met een emailadres, laat ze zelf iets geks verzinnen waarmee ze hun identiteit niet prijsgeven. Zo help je gebruikers hun privacy te bewaken, en; 2) willen we echt de IP-adressen loggen? Want, wat je niet hebt, kan ook niet gevorderd worden.

Ik keek op mijn telefoon, zag dat er een grote hoeveelheid ongelezen Whatsapp-berichten op stonden, waaronder ook een aantal met een foto. Leuk! Ik keek eens naar mijn fotoalbum en moest constateren dat daar eigenlijk een schrikbarende hoeveelheid foto's en filmpjes in stonden. Waaronder ook een heel aantal die anderen mij gezonden hadden. Daar ben ik dan toch wel mooi mede-verantwoordelijk voor geworden… Hoeveel foto's en filmpjes staan er eigenlijk op uw telefoon? En hoeveel daarvan zouden beter niet in het publieke domein terecht komen? Mij ontglipte onlangs nog het woord "held" toen ik aan een heerschap vroeg of hij dat ene filmpje nog had en hij antwoorde: "dat soort dingen wis ik hoor, dat is veel te gevaarlijk om op een telefoon te laten staan! Je weet maar nooit." Wat je niet hebt, kan je niet ontnomen worden.

Wist u trouwens dat – in het slechtste geval – een datalek een bedrijf 200 dollar per record kost? Symantec heeft dat laatst berekend en woog daarin mee: de kosten die nodig zijn voor het ontdekken van het lek, de kosten voor het herstel, het op de hoogte brengen van de slachtoffers en de kosten die gemoeid zijn met het schadeloos stellen. Vraag u nu nog eens af: heb ik echt al die data nodig? Wat je niet hebt, kun je niet verliezen en verliezen kost geld.

Is dit nu nieuw? Welnee. Dat heet: Dataminimalisatie. In de late jaren 70 was dit al een van de kernwoorden in de zogenaamde OESO-privacy-principles. Principes waarop vele wetgevers hun privacywetgeving hebben geënt. Ook onze huidige Wet bescherming persoonsgegevens is doorspekt van regels die geïnspireerd zijn op het beginsel van dataminimalisatie. Gegevens dienen "behoorlijk en zorgvuldig" verwerkt te worden, zij moeten "ter zake dienend en niet bovenmatig" zijn. Hetgeen erop neerkomt dat zo min mogelijk gegevens verwerkt moeten worden om het doel dat u voor ogen staat te realiseren. Gegevens mogen ook niet verder verwerkt worden als dat "onverenigbaar is met het doel waarvoor ze verkregen zijn". Wat je hebt, mag je dus niet zomaar naar een andere context overhevelen om het daaraan toe te voegen (en wellicht zelfs van betekenis te doen veranderen). Daarnaast mogen gegevens "niet langer bewaard worden dan noodzakelijk voor de vervulling van het doel". Wat je niet meer nodig hebt, moet je verwijderen. En als je het niet meer hebt, kan het je ook niet meer ontnomen worden.

Ik hoor u bijna denken: "Gaat ze het nu nog over PRISM hebben?" Nee, dat ga ik niet doen. U weet namelijk net zo goed als ik dat wat u niet heeft en zij niet hebben, u ook niet ontnomen kan worden. ●

Mr. Rachel Marbus, @rachelmarbus op Twitter

WOMEN IN CYBER SECURITY: NUT OF NOODZAAK?

Mary-Jo van de Velde, werkzaam bij NCSC, zij is te bereiken via Mary-Jo.vandeVelde@ncsc.nl

Women in Cyber Security (WiCS) is in december 2012 opgericht door Iowa Carels, Anouk Vos en Mary-Jo van de Velde. Drie dames die elkaar kennen doordat zij (al dan niet als externe medewerker) werkzaam zijn bij het Nationaal Cyber Security Centrum (NCSC). Een cybernetwerk voor vrouwen: nut of noodzaak?

"In december kwamen wij met het idee bij elkaar om een platform te creëren voor vrouwen met het doel kennisuitwisseling op het gebied van cyber(security)," zegt Anouk Vos. "Wij werken nou eenmaal in een mannenwereld en daar is niets mis mee. Maar op een gegeven moment kom je zo weinig vrouwen tegen, waardoor je bijna denkt dat je een 'misfit' in het domein bent. We wilden daarom onderzoeken of andere cybervrouwen dat ook zo ervaren. Dat wij voorzien in een behoefte bleek daags na de oprichting en het bekend maken van de groep op LinkedIn. In no time groeiden we uit tot meer dan 120 leden en daarmee bleken we, in één klap, het grootste vrouwennetwerk op het gebied van cybersecurity van de wereld te zijn."

Mary-Jo van de Velde: "Het voornaamste doel van Women in Cyber Security is het stimuleren van contacten tussen de schaars vertegenwoordigde vrouwen in verschillende cybersecuritydomeinen (onderzoek, beleid, architectuur, beheer, design, management, communicatie et cetera). Hiertoe is dus het netwerk gecreëerd van vrouwen die dezelfde cybersecurity-interesses en -ambities delen, dezelfde conferenties bezoeken en die dezelfde kansen en belemmeringen in hun cybersecurity-carrières ervaren. Het is prettig om te kunnen klankborden. Zo heb ik bijvoorbeeld meegemaakt dat iemand mij iets ging uitleggen: er was een heel boos netwerk (Zeus). En die verspreidde niet zulke aardige internetbacteriën (Dorifel). Maar omdat het boze netwerk goed (en anoniem) verstopt was (TOR-netwerk) kon het boze netwerk niet worden opgerold (NTD). Echt gebeurd! En dat ik de koffie niet haal, dat is inmiddels iedereen wel duidelijk".

"Women in Cyber Security is een dynamische en snel groeiende gemeenschap," vervolgt Iowa Carels. "De eerste offline bijeenkomst was binnen een dag vol: een ontbijt met Europarlementariër Marietje Schaake (D66). Tijdens dit ontbijt, waar ook delegaties uit het buitenland vertegenwoordigd waren zoals de FBI, hebben we voor eerst naar elkaar uitgesproken wat wij uit het netwerk willen "halen". Uiteraard is er ook gesproken over wat je "meebrengt". Wat dat betreft zijn vrouwen wellicht iets bescheidener, want de vraag of iedereen zijn toegevoegde waarde wilde schetsen, werd wel heel voorzichtig beantwoord. Dat terwijl de top (van het bedrijfsleven en de overheid) in dit unieke netwerk zijn vertegenwoordigd. Ik noem als voorbeeld een Chief Information Officer van een Telecomprovider, dat wordt je niet zo maar en daar mag je dan best trotst op zijn. Of je nou vrouw bent of niet."

Anouk Vos: "De afgelopen maanden hebben de Women in Cyber Security elkaar meermalen getroffen tijdens verschillende offline evenementen waarbij iedere keer een ander cybersecurity-thema werd verkend. Voor deze bijeenkomsten krijgen wij regelmatig ondersteuning, onder andere vanuit het NCSC, Fox-IT, Policy Research Corporation en de Nationale Politie. De offline bijeenkomsten hebben er in korte tijd voor gezorgd dat het netwerk op de kaart is gezet. Recentelijk hebben wij deelgenomen aan Operation Cyberpaint: blackhat down! waar wij overigens een verdienstelijke tweede plaats haalden. Inmiddels worden WiCS-leden veelvuldig voor Cyber Security en IT-evenementen uitgenodigd en zijn zij, in ieder geval voor het nationale debat, verworden tot een 'force to reckon with'. Dus Women in Cyber Security: nut of noodzaak? Ik zou zeggen: beiden!" ●

Meedoen aan Women in Cyber Security?

Er zijn twee manieren om deel te nemen aan Women in Cyber Security.

1. Meld je aan op de professionele Linkedin groep van Women in Cyber Security. We posten vacatures, initiatieven tot samenwerking, evenementen, nieuwe publicaties en forumdiscussies met betrekking tot alle Cyber Security gerelateerde onderwerpen;
2. Neem deel aan de Women in Cyber Security evenementen. Naast het delen van kennis (bijv. door lezingen) bieden deze bijeenkomsten ook de mogelijkheid tot informeel netwerken. Aanmelden kan via de e-mail aanmelden@womenincybersecurity.nl

FOX IT

for a more secure society

FOX-IT voorkomt, onderzoekt en beperkt de meest serieuze cyberdreigingen met innovatieve oplossingen voor overheid, defensie, politie, vitale infrastructuur, banken en grote bedrijven wereldwijd. Onze aanpak combineert slimme ideeën met technologie om hiermee innovatieve oplossingen te bieden die zorgen voor een veilige maatschappij. We ontwikkelen producten en maatwerkoplossingen om de beveiliging van gevoelige overheidssystemen te garanderen, industriële netwerken te beschermen, online bankiersystemen te verdedigen en strikt vertrouwelijke data te beveiligen.

FOX-IT.COM

Fox zoekt nieuwe Foxers

FOX-IT groeit en bloeit. Om deze reden zijn wij over de volle breedte van ons werk op zoek naar hackers, Forensic Experts, Pentesters, Developers (Python / C++), Hardware Engineers en Fraude analisten. Een Foxer is nieuwsgierig, kritisch en talentvol.
Je draagt bij aan de missie van FOX-IT: having fun in making technical and innovative contributions for a more secure society

Interesse om bij ons te komen werken?
Bel of mail Walter Doorduin 06 41901011 of doorduin@fox-it.com.

LOGIN, LOGOUT, WAAR GAAT HET FOUT?

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

Toegang is de sleutel tot uw bedrijfsinformatie en vormt de basis voor al uw beveiligingsmaatregelen. Toch hebben (ex)medewerkers in de praktijk regelmatig méér rechten dan noodzakelijk, ondanks de gecentraliseerde, gekoppelde en complexe alles-in-één Identity & Access Management systemen. Toezichthouders, zoals DNB en OPTA, eisen daarom om controle op de werkelijke autorisaties, maar is security - zonder budget en mandaat - nog te onvolwassen om deze verantwoordelijkheid te nemen.

Het is voor IT/EDP-auditors een bekend probleem, zie het kader "Top-10 Typical IT-audit Findings". Uit punten 3, 4, 7 en 9 in dit kader blijkt dat de typische organisaties het toegangsvraagstuk structureel niet onder controle hebben.

Autorisaties worden door de lijnmanager aangevraagd en/of ingetrokken via een gestandaardiseerde procedure en IT zorgt voor een geautomatiseerde koppeling of voert deze aanvragen 1-op-1 uit via een ticketsysteem. Dit proces wordt periodiek door de auditor gecontroleerd en vaak goed bevonden. Echter, gezien de bovenstaande lijst met top tien typische IT-audit bevindingen, kan je concluderen dat dit slechts een halve controle is.

Top-10

1. Inability to find or produce an inventory of assets and associated classifications.
2. Evidence of change management on material systems cannot be found.
3. *Administrator accounts are not tied to specific individuals.*
4. *It is not possible to determine each user's privileges or to determine that each user has appropriate and appropriately approved privileges.*
5. Activity logs are not being collected and analyzed.
6. The enterprise is unable to control segregation of duties in ERP systems.
7. *Physical access permissions are not documented and unknown. Unauthorized access is achievable.*
8. Business continuity plans and disaster recovery plans are not available and current. Evidence of periodic updating and review of such plans is not available.
9. *Agreements with third-party service providers and business partners do not specifically address data protection requirements.*
10. Security education is not provided to employees. Knowledge and understanding of data protection responsibilities of employees is not tested and documented.

Bron: Maxi-pedia.com [1]

Typical IT-audit Findings

De meeste organisaties hebben het uitgangspunt toegang op een 'need-to-know'-basis in hun beleid opgenomen. In de praktijk komt het geregeld voor dat een werknemer die een andere functie krijgt, toch zijn oude autorisaties onnodig behoudt. Ook zijn er voorbeelden van ex-medewerkers die toegangsrechten behouden tot diverse cloud-diensten van het bedrijf. Een cloud-dienst waar een IT-afdeling geen weet van heeft en dus ook geen autorisatie-beheer doet. Of een ex-medewerker bij de leverancier, die toegang heeft tot beheerfuncties van uw bedrijfs-applicaties die niet tijdig worden ingetrokken. Kortom, bedrijven lopen nog steeds een groot risico, ondanks de SOX- en audit-verklaringen van accountancy bureaus (denk aan debacle Diginotar met PWC als auditor).

> Het is voor IT/EDP-auditors een bekend probleem

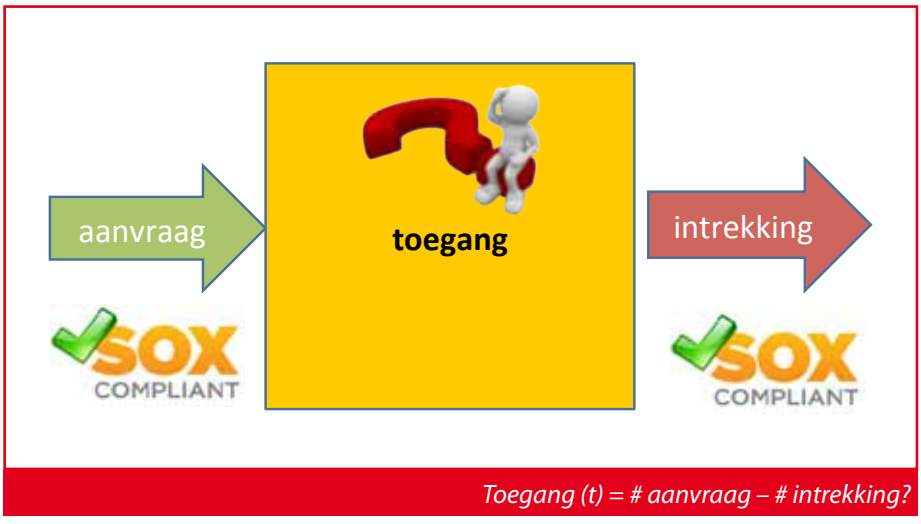
Misbruik van autorisaties kan leiden tot aanzienlijke schade. Daarbij is er dikwijls sprake van imagoschade, fraude, inbreuk op privacy, schending van vertrouwelijkheid of het niet naleven van wetten en regels. Iedere bestuurder is daarvoor eindverantwoordelijk en is zich terdege bewust van de bedrijfsrisico's. Echter, de bestuurder waant zich veilig met de verklaring van externe auditors dat processen lopen zoals ze gedocumenteerd zijn. Hun risico van aansprakelijkheid is daarmee voor hen voldoende afgedicht. Daarentegen wordt naast zo'n accountancyverklaring vaak alleen in de "side-letter" de verbeterpunten rondom onterechte autorisaties in bedrijfskritische systemen genoemd. Niet verwonderlijk, want hoe goed je autorisatieprocedure ook is, en hoe netjes die ook op papier staat, het kan heel lastig zijn om voortdurend bij

te houden hoe het werkelijk geregeld is. De vraag is hoe dat komt?

Ik vergelijk de problematiek rondom autorisaties wel eens met het voorraadbeheer in een supermarktwinkel. Als je 100 goederen inkoopt en er vervolgens 60 verkoopt, dan is de winkelvoorraad 40. Een auditor zal de inkoopbon van 100 stuks vergelijken met de 60 verkopen en toetsen of de winkelvoorraad 40 stuks is. In het begin klopt de administratie 100% met de werkelijkheid. Echter, in de praktijk gebeuren er allerlei "onverwachte" dingen die ervoor zorgen dat de papieren telling niet overeen komt met de werkelijkheid. De verschillen moet je kunnen verklaren en/of administratief aanpassen. Een telling over de chips, zegt nog niks over de voorraad van de koffie. Met andere woorden, je zal zo nu en dan een telling moeten doen over de gehele voorraad om te toetsen of het basisproces op orde is en de werkelijkheid overeenkomt met het administratieve voorraadbeheersysteem. Zo is het ook met het uitgeven en intrekken van autorisaties over verschillende bedrijfssystemen.
Het centrale IAM systeem en/of ticketsysteem is de administratieve weergave wat het zou moeten zijn (SOLL).
De werkelijke voorraad staat symbool voor de werkelijke toestand van alle autorisaties in de keten (IST). Mijn stelling is dat je beide toestanden structureel in kaart moete hebben om te bepalen of je primaire beveiligingsproces effectief is.

Onze traditionele oplossing is om het beheer over autorisaties te standaardiseren, centraliseren en automatiseren met een IAM implementatie. Deze top-down gedachte maakt het management van autorisaties efficiënter (goed in het kader van return on investment en efficiency), maar niet per definitie veiliger, om drie redenen:

1. Autorisaties buiten de scope van de ICT-afdeling worden vaak buiten beschouwing gelaten (bijvoorbeeld cloud-diensten, fysieke toegang, leveranciers/partners).
2. De werkelijkheid gaat op den duur afwijken, doordat informatie over gewijzigde toegangsrechten niet (tijdig) op de juiste plek terecht komt. Bijvoorbeeld voor iemand die met pensioen gaat en actief in de systemen blijft, omdat hij op de loonlijst staat. Of door legacy systemen die niet centraal gekoppeld kunnen worden aan het centrale systeem. Of door een medewerker die een nieuwe functie/rol in de organsiatie krijgt en alleen autorisaties erbij krijgt. Of door lokale admin rechten die het centrale IAM-systeem omzeilen. Of door de nieuwe manager die nooit een overzicht krijgt waar zijn medewerkers integraal toegang toe hebben. Of door de constante verandering in de organisatie. Of door outsourcing. Etc.
3. Non Personal Accounts (NPA) en shared accounts blijven mogelijk, waardoor het in sommige situaties onmogelijk is geworden om te bepalen wie wat gedaan heeft aan de hand van logfiles.

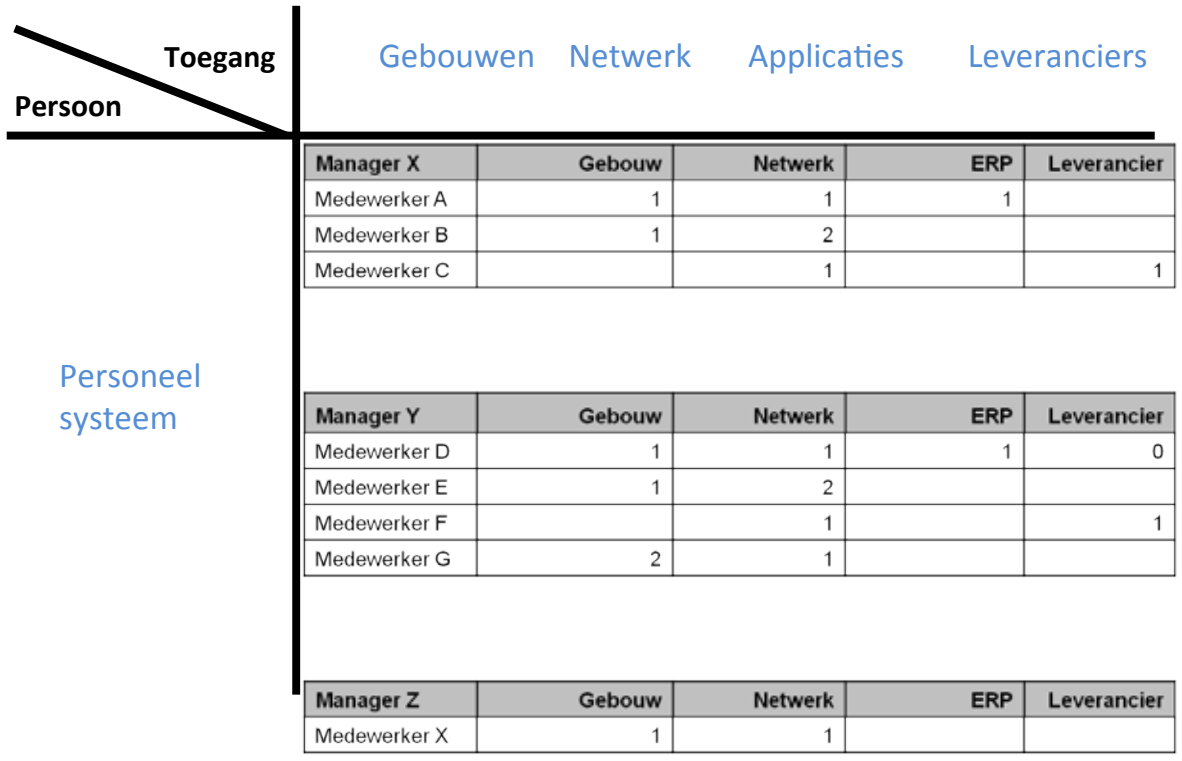


Toegang (t) = # aanvraag – # intrekking?

Informatie over toegangrechten is - steeds meer - gefragmenteerd over verschillende (keten)organisaties, afdelingen en systemen, waardoor de informatie soms niet (tijdig) op de juiste plek is. Omdat niemand zich eindverantwoordelijk voelt voor dit probleem, kan Security hierin een prominente rol in krijgen door een brug te slaan tussen business en IT. Een intelligent mechanisme te bouwen waarmee de "business" eenvoudig en integraal per medewerker kan controleren of de toegangsrechten nog steeds op een need-to-know-basis zijn. Deze intelligente tussenlaag is een uitgelezen kans voor de security afdeling om haar toegevoegde waarde aan te tonen. De verantwoordelijkheid is namelijk nu niet belegd binnen de huidige organisatiestructuur van IT, HR, Finance/Inkoop(leverancier, cloud) en Facilitaire Dienst.

> In de praktijk gebeuren er allerlei dingen die ervoor zorgen dat de telling niet overeen komt

De beoogde systematiek voor dit mechanisme is niet nieuw; in de cloud geeft wieowie.nl als gespecialiseerde zoekmachine een overzicht per individu welke sociale media deze persoon 'gebruikt' (zoals LinkedIn, Facebook, Hyves). Nu is het een kleine denkstap om dit te idee te vertalen naar gebruikers van bedrijfskritische applicaties, cloud-oplossingen en fysieke toegangssystemen binnen organisaties. Met zo'n gespecialiseerde zoekmachine, de CHECK-functie, weet je als organisatie tenminste waar een medewerker toegang toe heeft als je gevraagd wordt alle autorisaties – dus cloud, IT en fysiek - direct in te trekken, zonder het hem zelf te moeten



Manager X	Gebouw	Netwerk	ERP	Leverancier
Medewerker A	1	1	1	
Medewerker B	1	2		
Medewerker C		1		1

Manager Y	Gebouw	Netwerk	ERP	Leverancier
Medewerker D	1	1	1	0
Medewerker E	1	2		
Medewerker F		1		1
Medewerker G	2	1		

Manager Z	Gebouw	Netwerk	ERP	Leverancier
Medewerker X	1	1		

Toezicht op werkelijke autorisaties

vragen. En voor de financiële afdeling heeft dit nog het voordeel dat auditkosten worden bespaard door te laten zien dat dit controleproces op autorisaties bestaat en effectief uitgevoerd wordt. Met het product "Identity eQ"[2] is het integraal toezicht op toegangsrechten al bij een drietal grote organisatie in kaart gebracht en dit heeft zeer verhelderende inzichten gegeven.

Omdat de meeste security professionals deze materie nog moeten omdenken, wil ik de belangrijkste denkstap nog benadrukken: de betrokkenheid en input van de business is cruciaal. IT kan niet zelfstandig beoordelen of de huidige toegangsrechten nog noodzakelijk zijn door een overzicht te creëeren. De business wil ook niet in rigide 'veilige' rol gestopt worden.

Met zo'n zoekmachine weet je als organisatie waar een medewerker toegang toe heeft

De bedrijfsbehoefte is granulair, tijdig en flexibel de juiste rechten hebben die nodig zijn om het werk uit te kunnen voeren. In dit betoog behoudt daarom de lijnmanager het proces voor het aanvragen en intrekken van autorisaties, maar krijgt de lijnmanager ook een regie-functie middels een overzicht van de werkelijke gebruiker-accounts per medewerker. De praktijk leert dat naast lijnmanager, medewerkers zelf ook unieke aanvullende informatie hebben over hun toegangsrechten. Op basis van een overzicht van autorisaties worden medewerkers getriggerd om onnodige rechten te laten intrekken. Hiermee wordt toezicht op de autorisaties gefaciliteerd en beheerd door IT, maar gecontroleerd door de business. Vandaar dat er in dit artikel wordt gesproken worden over een brugfunctie.

Kortom, een security afdeling heeft met een CHECK-functie op de werkelijke autorisaties over de gehele keten – bestaande uit cloud, IT en fysieke toegang - een grote toegevoegde waarde. Toezichthouders, zoals de DNB en OPTA, eisen deze controle zelfs, waarbij opgemerkt moet worden dat de scope van toegangsrechten zich hoofdzakelijk beperkt tot financiële systemen. Security bekijkt de toegang-problematiek integraal en risico gedreven vanuit de medewerker, creëert een brugfunctie tussen business en IT en vormt een belangrijke key performance indicator (KPI) voor de veiligheid van bedrijfsinformatie. Met dit verhaal moet een security officer budget en mandaat kunnen regelen. ●

Links

[1] *Top-10 typical IT audit-findings: http://www.maxi-pedia.com/IT+security+audit+findings*

[2] *Identity eQ: http://www.trustinpeople.com/home/identity-access*

SECURITY NAAR DE BOARDROOM

Theo Arts, werkzaam bij Enterprise Architect Rijkswaterstaat,
http://nl.linkedin.com/in/theoarts/nl
Ben Elsinga, werkzaam bij Enterprise Architect Capgemini,
http://nl.linkedin.com/pub/ben-elsinga/4/4ab/869

Vaak is het moeilijk om vanuit de IT-organisatie security op een aansprekende wijze bij de boardroom op de agenda te krijgen. Om meer inzicht te krijgen in wat we nu eigenlijk "fout" doen, is tijdens de bijeenkomst van het Nationale Architectuur Forum (NAF) op 30 mei 2013 één van de tafels aan dit onderwerp gewijd. Tijdens vier sessies hebben 30 deelnemers, vanuit de financiële, overheids- en private sectoren, hun inzichten gedeeld over het fenomeen "security in de boardroom". Dit is niet zozeer een verslag wat er aan iedere tafel is gezegd, alswel een synthese van alle verschillende ideeën over de wijze waarop security op de boardroom agenda betekenisvol kan zijn. Onze dank gaat daarom uit naar Daan Rijsenbrij en alle 30 NAF-deelnemers, omdat wij juist door hun inbreng dit verhaal hebben kunnen optekenen.

Wat verstaan we onder de boardroom?

Er bestaan verschillen van inzicht wat we eigenlijk onder de board verstaan. In de wat meer beperkte zin zien we de board als de beslissers aan de IT-kant waar besluiten genomen worden over de opbouw van security maatregelen. In de bredere zin wordt de board beleefd als de top management-laag (CxO's) van het bedrijf waar de strategie bepaald wordt en waar IT als een, belangrijke maar toch, ondersteunende dienst gezien wordt. Details over de IT-dienstverlening, zoals security maatregelen, worden door die managementlaag gezien als een tactische uitwerking en binnen dat kader niet van belang voor de agenda van de board. Toch is iedereen ervan overtuigd dat security dusdanig belangrijk is dat de top van het bedrijf hierin betrokken moet zijn. Vraag is: Op welke manier?

De board en security

Misschien ligt de oorzaak van onze problemen aan de wijze waarop we zelf naar security kijken. De eerste spraakverwarring begint al bij het woord security! Bedoelen we informatiebeveiliging of bedoelen we meer de bedrijfsbeveiliging in algemene zin. Voeg daar nog aan toe dat, door onze dagelijkse verbondenheid met het Internet, de termen security, "Cyber Security" en informatiebeveiliging praktisch gezien synoniemen zijn geworden.
Zodra we praten over informatie-beveiliging (of de synoniemen) komen al snel kreten naar boven als DDos aanval, hackers, "intrusion detection", "identity theft", etc. Soms, als we wat meer functioneel denkende mensen vragen, komen kreten naar voren als beschikbaarheid, continuïteit, fout-gevoeligheid enzovoort. Wat moet de Board hiermee? In de beleving van de board zijn dit allemaal tactische en operationele zaken (of bedreigingen), waarvoor de IT-organisatie aan de lat staat.
Waar is de board dan wel in geïnteresseerd? Risico's die te maken hebben met het voortbestaan van de organisatie en het kunnen realiseren van de organisatiedoelstellingen!
De vraag die daarbij hoort is: Wat zijn de kroonjuwelen van het bedrijf? Voorbeelden over het voortbestaan kunnen we voldoende vinden: Valse certificaten (Diginotar ging eraan failliet), aandelenprijzen die kelderen als gevolg van reputatieschade doordat een bedrijf gevoelige informatie kwijt raakt, verlies van vertrouwen als bekend wordt dat een bank creditcard gegevens, rekeninggegevens of zelfs geld kwijtraakt door malafide activiteiten en voor veel bedrijven belangrijk; bedrijfsspionage naar klantgegevens en/of intellectuele eigendommen. Voor overheden komt daar nog politieke schade bij, maar dat kan ook gezien worden als een vorm van reputatieschade.
Of de board geïnteresseerd is in security issues hangt dus niet zozeer af van taalgebruik of van de hoeveelheden geld die ermee gemoeid zijn, maar wordt bepaald door het niveau waarop de issues spelen; strategisch, tactisch en operationeel. En een board is vrijwel alleen bezig met strategische en relationele vraagstukken.
Toch kan de board binnenkort niet helemaal om de tactische en operationele aspecten van informatie-beveiliging heen. Door de komst van Europese wetgeving, waardoor het mogelijk wordt om boetes op te leggen tot een hoogte van 2% van de totale omzet, wordt de impact van falende informatiebeveiliging wel degelijk naar een hoger niveau getild. Ook de nieuwe Nederlandse wetgeving, die bedrijven verplicht om verlies/diefstal van persoonsgegevens te melden aan de overheid en aan de personen wier gegevens het

betreft, zal van invloed zijn op het informatiebeveiligingsbeleid, omdat de mogelijkheid van reputatieschade aanzienlijk toeneemt.
Praktisch gezien zal de board zich moeten uitspreken over de informatiebeveiligingskaders en de tolerantie van de onderneming voor inbreuken op de informatiebeveiliging (te vertalen naar de "risk appetite" van de onderneming). De Chief Information Officer (CIO) en de aangestelde functionaris voor beveiliging zijn, binnen hun lijnverantwoordelijkheid, vervolgens "accountable" om de vertaling te laten maken naar beleid en maatregelen. De IT- en Business organisatie zijn vervolgens "responsible" voor het uitvoeren van de maatregelen. Wij gebruiken hierbij bewust de Engelse termen "accountable" en "responsible" omdat het Nederlandse begrip "verantwoordelijk" niet het exacte verschil aangeeft.
Samengevat: Informatiebeveiliging is voor de individuele boardmembers dus iets anders als voor de board als geheel.

Informatiebeveiliging in de business
De meeste praktijkproblemen waar we met informatiebeveiliging tegen aan lopen, hebben niet te maken met de board, maar met de tactische leiding van de business. Daar bestaat nog vaak het probleem dat de bewustwording voor informatiebeveiliging volstrekt onvoldoende is in relatie tot de risico's die gelopen worden. Op dit niveau kan veel directer met betrokkenen gecommuniceerd worden en kunnen velerlei vormen gekozen worden om problemen bespreekbaar te maken. Alle vormen hebben echter één ding gemeen, vermijd vakjargon en vermijd de focus op maatregelen. Business is net als de board voornamelijk geïnteresseerd in risico's en de hoeveelheid geld die gemoeid is met het beperken van die risico's. Dit kan naar voren gebracht worden door over uitkomsten van maatregelen te praten en niet over de maatregelen zelf. Dus kosten versus baten c.q. vermindering van de risico's. Daarnaast kan voor de business inzichtelijk gemaakt worden dat informatiebeveiligingsmaatregelen vaak leiden tot procesverbeteringen en daarmee de doelstellingen van de business zelf ondersteund ("what's in it for me?").

Informatiebeveiliging en verandering
Iedere verandering brengt nieuwe risico's met zich mee. Op welk niveau deze veranderende risico's afgehandeld moeten worden, zal moeten blijken uit een impactanalyse waar de business zelf "accountable" voor is en waarvoor de "responsibility" bij zowel de business als de IT ligt. Samenwerken en processen hebben die hiervoor bedoeld zijn maken zelfs van informatiebeveiliging een "business as usual".

Informatiebeveiliging in culturele context
In het bijzonder voor internationaal georiënteerde bedrijven, maar ook bij overheden, speelt er nog een belangrijk aspect mee dat van invloed is op security assessments. Cultuur! "Risk appetite" is zeer cultuurgebonden. Wat voor een overheid onacceptabel is, daar lacht het bedrijfsleven om, maar omgekeerd zijn de voorbeelden ook te noemen. Denk ook eens aan China; intellectueel eigendom heeft daar minder betekenis dan hier en internationale wetgeving heeft daar duidelijk geen invloed op. Het heeft dus geen zin om aan deze kant een miljoen te investeren in beveiliging, terwijl aan de andere kant van de wereld de informatie gewoon verspreid wordt. Omdat organisaties steeds verder globaliseren, kan een lokaal en cultuurgebonden risico afweging toch niet het juiste effect hebben op het geheel.

Aanvliegroute voor informatiebeveiliging
Informatiebeveiliging begint met het inzichtelijk krijgen van wat er beschermd moet worden en waartegen. Kroonjuwelen worden beter beschermd dan een diamant van 0,01 crt. Goede beveiliging kost wat en mag ook wat kosten, maar er moet wel vooraf duidelijk zijn dat absolute veiligheid niet bestaat. Er is dus *altijd* een restrisico. Hoeveel restrisico er binnen een onderneming acceptabel is, is een wezenlijke vraag waarover de board waarschijnlijk wel een uitspraak wenst te doen. Vervolgens wordt er tegen de business gezegd: regel het. ●

HANDS-ON INNOVATIE IN HET NIEUWE CYBER SECURITY LAB VAN TNO

Ir. Richard Kerkdijk studeerde Technische Natuurkunde aan de Universiteit Twente en werkte van 1997 tot 2002 bij KPN Research als onderzoeker en adviseur op het gebied van informatiebeveiliging. Begin 2003 maakte hij de overstap naar TNO. Vanuit zijn rol als senior security consultant vervult hij een strategische adviesrol voor diverse bedrijven en overheden. Dhr. Kerkdijk maakt binnen TNO deel uit van het kernteam Cyber Security en coördineert op dit onderwerp onder meer onderzoeksopdrachten voor telecomaanbieders en de Cyber Security Raad.

Ing. Roy Mente MSc is werkzaam als Senior Business Consultant (Cyber) Security bij TNO. Als projectmanager heeft hij leiding gegeven aan het opzetten van het Cyber Security Lab. Als security innovator heeft Roy zijn sporen verdient bij de politie en Koninklijke Marechaussee (w.o. winnaar politie innovatie prijs). Om de essentiële verbinding tussen de wetenschap en de operatie te behouden is hij reservist (Majoor) bij de KMar.

Op 21 mei 2013 opende TNO de deuren van haar nieuwe Cyber Security Lab. Wat gebeurt daar nou eigenlijk en hoe past dat in de rol die TNO op het gebied van Cyber Security speelt? Aan het woord Richard Kerkdijk en Roy Mente van TNO.

Cyber Security en TNO

Cybercrime, cyberactivisme en cyber e-spionage zijn actuele en snel groeiende fenomenen waarover welhaast dagelijks berichtgeving in de media verschijnt. Ook Nederlandse ondernemingen kampen met deze problematiek. Onlangs werd bijvoorbeeld het betalingsverkeer verstoord door een golf van Distributed Denial of Service (DDoS) aanvallen op Nederlandse banken. Eerder dwong de Diginotar affaire de Nederlandse overheid ertoe om op grote schaal haar digitale certificaten te vervangen. TNO innoveert en adviseert voor een veilige cyberspace die innovatie, de economie èn de nationale veiligheid bevordert. Mente: "Wij benaderen het fenomeen Cyber Security niet zozeer als bedreiging, maar juist als *enabler* voor digitaal gedreven innovaties. Multidisciplinariteit is daarbij een sleutelwoord. We richten ons niet louter op techniek, maar hebben ook nadrukkelijk aandacht voor de mens, processen, organisatie en besturing." TNO richt zich met haar onderzoek en advisering op een drietal primaire doelgroepen:

1. De overheid als beleidsmaker en regelgever. In dit verband levert TNO onder meer een bijdrage aan de Nationale Cyber Security Strategie.
2. Gebruikers en aanbieders van cyberinfrastructuur. Kerkdijk: "Voor deze doelgroep adviseren wij bijvoorbeeld over inrichting en optimalisatie van incident monitoring en response voorzieningen."
3. Defensie en opsporingsdiensten. Defensie wordt bijvoorbeeld ondersteund bij het optimaliseren van haar *cyber operations*.

Ten grondslag aan deze werkzaamheden ligt diverse kennisgebieden, variërend van technieken en processen om de kwetsbaarheid voor cyberaanvallen

De aanwezigen in het TNO Cyber Security Lab

Dick Schoof, NCTV, bij de opening

te reduceren tot modellen om de effecten van dergelijke aanvallen te voorspellen. Op deze onderwerpen wordt ook nadrukkelijk samenwerking nagestreefd met kennisinstellingen en industriële partners.

Het Cyber Security Lab

Om tot een "secure cyberspace" te komen is veel onderzoek en innovatie nodig. Mente: "zeker voor een onderwerp als cybersecurity is een labvoorziening essentieel om al experimenterend tot volwassen oplossingen te komen. Het TNO Cyber Security Lab (hierna CSL), gevestigd op TNO locatie Den Haag, is daarvoor een *dedicated facility*."

Waar een ander lab voorziet in reageerbuisjes, veiligheidsbrillen, ovens, centrifuges en microscopen, biedt het TNO CSL de basisvoorzieningen voor het cybersecurity werk. De *technische infrastructuur* (hard- en software) voor cybersecurityprojecten omvat onder meer gescheiden netwerksegmenten en servers, 'vuil' (ongefilterd) internetverkeer, systemen voor network traffic generation, Security Information & Event Management (SIEM) systemen en verschillende soorten target systemen (inclusief mobiles) waarop aanvallen kunnen worden verricht. Elk project zal weer nieuwe voorzieningen toevoegen en in één lab is dit beter te beheren en kan hier meer rendement uit worden behaald dan op verschillende projectlocaties. "Het is ook fysieke werkruimte waar cyber onderzoekers elkaar kunnen ontmoeten en een demonstratieruimte met *proof of concepts* en demo's van cyberprojecten voor onze klanten. Dit zorgt voor kruisbestuiving tussen projecten. *Seeing is believing,* aldus Roy Mente."

Het CSL moet uiteindelijk ook een 'pleisterplaats' worden waar je onderweg naar een secure cyberspace even halt houdt om te experimenteren, om nieuwe kennis tot je te nemen en om andere specialisten en belanghebbenden te ontmoeten. Want het is ook een plek waar we, samen met partijen uit de gouden driehoek van overheid, bedrijfsleven en kennisinstituten, projecten ondernemen.

Bij de opening op 21 mei debatteerden relaties uit overheid, kennisinstellingen en bedrijfsleven over het realiseren een 'secure cyberspace' en wat daarvoor nodig is. De opening werd in het bijzijn van Nationaal Coördinator Terrorisme en Veiligheid Dick Schoof, verricht door Jan Willem Kelder, lid van de TNO Raad van Bestuur. De openingshandeling bestond uit een symbolische 'hack' door twee jongens van 9 jaar. Bezoekers kregen vervolgens verscheidene cybersecurity demo's en presentaties voorgeschoteld, onder meer op het gebied van aanvalsdetectie , DDoS en *typosquatting*.

Eerste projecten

Inmiddels zijn de eerste projecten binnen het CSL van start gegaan. In het kader van The Hague Security Delta is bijvoorbeeld het project *Cyber Incident Experience* opgestart, een samenwerking tussen TNO en Fox-IT. Kerkdijk hierover: "We willen organisaties de mogelijkheid gaan bieden om een cyberincident dat werkelijk heeft plaatsgevonden op een later moment in al zijn facetten opnieuw te beleven. Het leereffect dat hier van uitgaat, moet organisaties in staat stellen om hun weerbaarheid tegen cyberaanvallen te verbeteren".

Van een technischer karakter is het project *Cyber Attack Detector* (TNO, UVA, TU Twente en Fox-IT), dat zich richt op nieuwe algoritmes om grote, complexe cyberaanvallen (zogeheten Advanced Persistent Threats, APT's) snel en accuraat te kunnen detecteren. Deze gerichte aanvallen worden typisch niet, of onvoldoende, opgemerkt door reguliere ICT-beveiligingssoftware. Overigens wordt samen met bedrijven als IBM en HP ook gekeken naar mogelijkheden om state-of-the-art detectie- en monitoringsystemen zodanig door te ontwikkelen dat nieuwe aanvalssoorten beter worden geweerd. Mente: "De problemen en oplossingen van morgen en overmorgen willen we aan gaan pakken in een gezamenlijk onderzoeksprogramma met de TU Twente, TU Delft en de Haagse Hogeschool, waar ook stagiaires, afstudeerders en AIO's uit verschillende disciplines kunnen werken aan taaie cybervraagstukken."

Meer informatie

Bent u geïnteresseerd in TNO en het Cyber Security Lab? Kijk op www.tno.nl/cybersecurity voor meer informatie of om contact op te nemen. ●

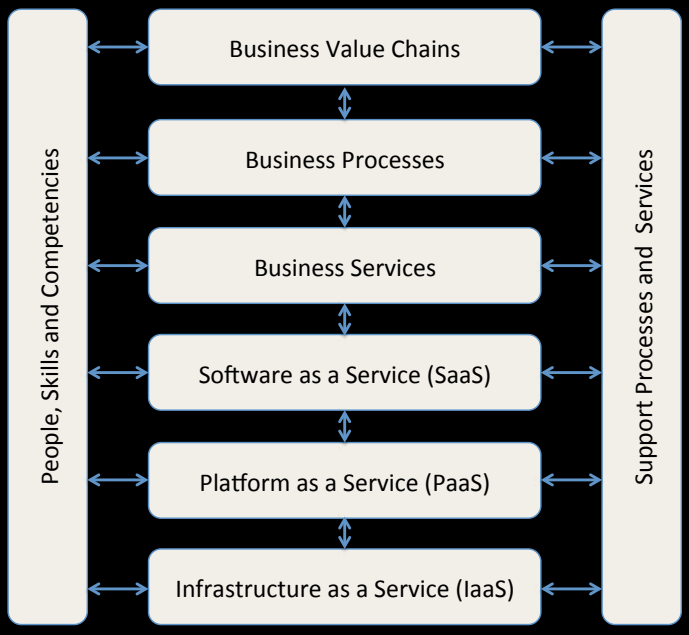
Foto's bij dit artikel zijn welwillend door TNO ter beschikking gesteld.

COLUMN

SUPPORTABLE

This Business Attribute from the SABSA Business Attributes Taxonomy is one that deserves a great deal of attention with respect to every solution architecture. First let's establish a conceptual framework within which business solutions are constructed. The essential goal of any such solution is to create 'business value' through what we call 'value chains'. Supporting this goal we build a 'business stack' – a layered view of what it takes to create value. So immediately we introduce the concept of 'support' – each layer supporting the one above it.

The diagram shows a high level conceptual view of such a stack. Notice that it is a combination of people, process and technology – you cannot do this with technology alone. The people are supportive of every layer in the stack and are therefore aligned at all levels. Similarly there are a number of support processes and services also aligned at every level. The type of support service and the type people skills and competencies will, of course, vary from layer to layer. To meet the requirements of the attribute 'supportable' we must consider all of these aspects of support.



So, having set the scene for support as a concept, we shall now take a very focused case study to reveal some of the complexities that can arise. We shall consider what it means to support a specific technical product that forms part of an integrated business solution. In the case of a vendor product one of the questions we would ask during the buying process would be about the type of support that the vendor would provide and what the cost of this support would be. Then we find that two different vendor products are to be interfaced together as part of the system integration. Now it starts to get tricky unless the interface is clearly defined and the vendors are both clear about which side of the interface is their responsibility. The important thing here is to ensure that there are no gaps between the vendor domains of responsibility where there would be no support. It is also necessary that the interface is clean enough to prevent the vendors from claiming that the other is responsible and for this mutual face-off to create a deadlock in resolving support issues.

So far, so good: vendor products, out of the box, clean interfaces, clear domains of support responsibility.
What happens next in so many cases is what destroys the capability to support the integrated system into the future. The system owner starts to customize it. New code is written locally and added to the vendor products to make them a better fit. This code does not have vendor support – it will be supported in-house, and requires the same type of rigorous support that we can expect form a reputable vendor. It is hard to replicate that with our own people, but it can be done. What should not happen is to leave it to the imperative of the moment to 'get it working' and then move on the next emergency. Support documentation should be of high quality, because people move on, change jobs, and new ones replace them. When it comes to the point where we need to support this customized component, there should be no dependence on those who knew how it worked, the documentation should be enough to instruct the new people.

What do we do when we fail to achieve this: we call the vendor. The vendor will recommend that we first clean up the product and make it once again 'out-of-the box', otherwise any third party interfaces will not work. That is a big risk and a huge investment. So, supporting a product yourself is a costly option at best.

The lesson from this discussion is that whilst altering the internal functionality of a vendor product may be acceptable, provided that you really support it, once you change the external interfaces of the product you really will be in trouble at some future point. The cost of this can be very punishing. SABSA Business Attribute Profiling is all about getting a balance between a wide range of attributes that cannot be treated in silos, otherwise the results can be catastrophic. ●

The Attributer

CYBERCRIME, MAG EEN BEETJE PREVENTIE OOK?

Arjen Kamphuis is werkzaam als CTO bij Gendo B.V. Hij is te bereiken via arjen@gendo.nl

Cybercrime is op dit moment de hippe termen om als overheid extra middelen en mogelijkheden te verwerven. Als men cybercrime kan combineren met de distributie van kinderporno is het helemaal prijsschieten. Dan mag en kan bijna alles. Toch willen de meeste Nederlanders liever geen politie-staat naar Noord-Koreaans model.

Op OHM2013 gaan 3000 hackers, programmeurs, activisten, kunstenaars en technologen elkaar bijpraten over de nieuwste ontwikkelingen op het gebied van informatiebeveiliging, privacy, spionage, netwerktechnologie, wetenschap, wetgeving, opensource, 3D printen en vele andere zaken. Iedereen is welkom om te komen luisteren en deel te nemen aan discussies, workshops en projecten. Voor meer info zie www.ohm2013.org.

OHM2013

Maar wat in alle discussies over toelaatbare opsporingsmethoden, (cr)(h)ackende KLPD-ers en crime-fightende politici totaal ontbreekt, is de vraag waarom cybercrime zo enorm gegroeid is. Het feit dat we veel meer en complexere IT gebruiken, zal daar zeker aan hebben bijgedragen. Belangrijke andere factoren zijn de enorme digitale ongeletterdheid onder verreweg de meeste burgers en een extreme technische monocultuur van Windows, waarmee burgers online diensten benaderen. Afgezien van wat voorlichtingscampagnes doet de overheid er opvallend weinig aan burgers echte kennis en volwassenheid bij te brengen. Een paranoïde persoon zou haast gaan denken dat de privacy van burgers geen prioriteit is.

Als je al wat langer online zit is het lastig je voor te stellen dat veel internetgebruikers van vandaag helemaal niet weten hoe een URL in elkaar zit. Met de browsers van vandaag is dat ook niet meer zo nodig. Vaak zie ik mensen een naam van een site in Google intikken en daarna doorklikken. En dus voert men ook zonder blikken of blozen bankgegevens in op helpdesk.br.ru/ING, of iets dergelijks. Want het logo stond in de mail en het is toch de helpdesk van de ING? Als mensen het verschil zouden snappen tussen een top level domein en de rest van de URL, kunnen ze zelf bedenken dat ING bank niet in Rusland huist.

Het succes van cybercrime is mede te danken aan de diepe onwetendheid van de meeste computergebruikers. Deze onwetendheid wordt mede veroorzaakt doordat men in het onderwijs gewoon Windows & Office leert, zonder inzicht in wat een computer doet of hoe netwerken functioneren. Een set minimale inzichten (zoals het kunnen 'lezen' van een URL) zou al veel leed kunnen voorkomen. Mensen die het een beetje begrijpen ontwikkelen zich vaak ook zelfstandig verder. Een samenleving waarin competentie 'cool' is, in plaats van één waar incompetentie regelmatig als legitiem excuus wordt opgevoerd, is een stuk weerbaarder tegen allerlei risico's.

Daarnaast blijft de enorme monocultuur van computersystemen een groot probleem dat de overheid nog steeds actief groter maakt. Zo is het in Nederland vrijwel onmogelijk de middelbare school af te maken zonder gebruik van Windows en Office. Studeren aan diverse universiteiten is zonder Google-account onmogelijk geworden en bij andere instellingen is een Facebook-account verplicht. De buitenlandse spionage op je volledige leven krijg je er gratis bij.

De rol van IT voor het van seconde tot seconde functioneren van onze samenleving is de afgelopen jaren echter sterk toegenomen. Ziekenhuizen, havens, vliegvelden, scholen, politiebureaus, sluizen en ambulance dispatchers... Allemaal hebben ze pc's met internetverbinding nodig. En die pc's missen vaak de laatste updates. Criminelen of buitenlandse cyberlegers die deze systemen kunnen overnemen of uitschakelen hebben onze samenleving in een wurggreep.

Als cybercrime echt zo belangrijk is, zou het logisch zijn als de overheid een begin maakt met computeronderwijs dat ook echt onderwijst, het zo snel mogelijk afbouwen van onze software-monocultuur en het reduceren van de hoge afhankelijkheid van buitenlandse dienstverleners die ons bespioneren. Op deze gebieden echte stappen zetten heeft meer zin dan nog meer macht geven aan een overheidsapparaat dat daardoor steeds meer totalitaire trekjes krijgt, terwijl de competentie ervan terecht nog zeer ter discussie staat. ●

VERSLAG

INFORMATIEBEVEILIGERS MAKEN WERK VAN PROFESSIONALISERING

Marcel Spruit, lector Cyber security & safety aan de Haagse Hogeschool en senior consultant bij Het Expertise Centrum.
Fred van Noord, voorzitter van het Platform voor Informatiebeveiliging (PvIB) en zelfstandig Adviseur Informatieveiligheid.

Op 30 mei jongstleden is bij VNO-NCW in Den Haag een werkconferentie gehouden over kwalificatie van informatiebeveiligers. Op deze werkconferentie lichte het Platform voor Informatiebeveiliging (PvIB) de plannen voor een kwalificatiestelsel toe en presenteerde ze het convenant voor kwalificatie van informatiebeveiligers. Door het convenant te ondertekenen, geven organisaties aan dat zij achter het beoogde kwalificatiestelsel staan en het willen gebruiken voor werving en selectie. Acht grote organisaties beten de spits af en ondertekenden het convenant publiekelijk.

In de huidige samenleving neemt het economische en maatschappelijke belang van informatie steeds verder toe. Toenemende digitalisering van producten en diensten, zowel bij overheid als bedrijfsleven, vraagt om vertrouwen in deze producten en diensten. Ook communicatie en ketensamenwerking vereist vertrouwen in de onderliggende informatiesystemen. De betrouwbaarheid van deze systemen moet buiten kijf staan. Maar betrouwbaarheid is geen vanzelfsprekendheid. Door de toenemende complexiteit van de informatiesystemen, hun onderlinge verwevenheid en een steeds complexer dreigingenbeeld, is het borgen van de betrouwbaarheid van de informatiesystemen een uitdaging van formaat geworden. Dit stelt hoge eisen aan de informatiebeveiliging. Recente incidenten, zoals DDoS-aanvallen, ICT-verstoringen, datalekken en identiteitsfraude, illustreren de noodzaak om informatiebeveiliging te professionaliseren. Daarvoor zijn goede informatiebeveiligers nodig.

Iedereen kan zich informatiebeveiliger noemen, maar niet iedereen is een goede informatiebeveiliger. Hoe herken je een goede informatiebeveiliger? Steeds vaker laten organisaties horen dat dat onvoldoende mogelijk is aan de hand van de bestaande kwalificaties op het gebied van informatiebeveiliging. In de afgelopen jaren is een chaotische situatie ontstaan met grote aantallen onderling onvergelijkbare certificaten en titels. Allerlei instanties in binnen- en buitenland geven certificaten en titels uit, die soms op cursussen/opleidingen zijn gestoeld, soms op beroepservaring en soms op beide. Een aantal willekeurig gekozen voorbeelden van acroniemen die men als titel voor of achter zijn naam mag plaatsen: CEH, CIPP, CISA, CISM, CISSP, CRISC, CSSLP, FBCI, ISMAS, ISMES, ISSAP, ISSEP, ISSMP, MBCP, MISM, MSIT, OPSA, OPST, QiCA, RE, RIB, RO, RSE, SSCP.

Het grote aanbod aan titulatuur biedt weliswaar mogelijkheden voor degene die zijn naam wil opleuken met een reeks interessant ogende titels, maar informatiebeveiligers kunnen met dergelijke titels en de bijbehorende certificaten niet meer duidelijk maken welke kennis en ervaring zij hebben. Werkgevers kunnen niet zien wanneer zij een goede informatiebeveiliger voor zich hebben, of de betreffende informatiebeveiliger wellicht bijscholing nodig heeft en welke opleiding daar dan voor in aanmerking zou komen. En opleidingsinstellingen krabben zich met dit woud van certificaten en titels nog wel een keer achter de oren alvorens te investeren in nieuwe opleidingen op het gebied van informatiebeveiliging.

Het Platform voor Informatiebeveiliging (PvIB), de Nederlandse beroepsvereniging voor informatiebeveiligers, vond deze onoverzichtelijke en weinig transparante situatie op het gebied van kwalificatie onacceptabel. Daarom heeft zij, in samenwerking met organisaties in de publieke en private sector en brancheorganisaties, stappen genomen om een uniform kwalificatiestelsel voor informatiebeveiligers voor te bereiden. Een dergelijk kwalificatiestelsel beschrijft de kennis en ervaring die gekwalificeerde informatiebeveiligers moeten bezitten. Dit geeft de gekwalificeerde informatiebeveiliger de mogelijkheid zich op uniforme en transparante wijze te profileren. Het biedt werkgevers beter inzicht in de capaciteiten van informatiebeveiligers die ze in dienst hebben of willen nemen. Bovendien biedt het opleidingsinstellingen handvatten voor het inrichten van opleidingen en bijscholingsprogramma's op het gebied van informatiebeveiliging en het stroomlijnen van de doorstroming tussen aansluitende opleidingen.

Fred van Noord (midden) en Marcel Spruit (rechts) met dagvoorzitter mevrouw Marjolijn Bonthuis van ECP

De ondertekenaars van het eerste uur met beide organisatoren

Het beoogde kwalificatiestelsel voor informatiebeveiligers moet aan een aantal criteria voldoen. Enkele vermeldenswaardige niet-vakinhoudelijke criteria zijn:

- Het stelsel wordt vastgelegd, beheerd en ondersteund door een onafhankelijke organisatie zonder winstoogmerk.
- Het stelsel sluit aan op de Europese standaard voor kwalificatie, het e-Competence Framework (e-CF).
- Het stelsel biedt kwalificaties op verschillende opleiding-/denk-/werkniveaus.
- Het stelsel omvat kenniscomponenten (body of knowledge), ervaringscomponenten en onderhoud van kennis en ervaring.
- Het stelsel biedt informatiebeveiligers de mogelijkheid om eerder verworven certificaten en ervaring om te laten zetten in equivalente kwalificaties binnen het nieuwe stelsel.

Het kwalificatiestelsel wordt op nationaal niveau uitgewerkt en ingevoerd, maar is met het e-CF gebaseerd op een internationale standaard voor kwalificatie. Daarmee kan het nationale kwalificatiestelsel in een later stadium een internationale status krijgen door internationale erkenning van dit kwalificatiestelsel, of door dit stelsel aan te laten sluiten op een buitenlands kwalificatiestelsel. Op dit moment is er nog geen buitenlands kwalificatiestelsel beschikbaar dat aansluit op het e-CF en toegepast kan worden in Nederland.

Een uniform kwalificatiestelsel voor informatiebeveiligers is een maatregel waarmee de huidige kwalificatieproblematiek op orde kan worden gebracht. Daarmee wordt werving en selectie van informatiebeveiligers beter ondersteund en kunnen aanbieders van opleidingen gerichter informatiebeveiligingsopleidingen inrichten.
Om effectief te kunnen zijn, moet het uniforme kwalificatiestelsel breed worden geaccepteerd en toegepast. Om een breed draagvlak te creëren en zichtbaar te maken, stelde het PvIB, in samenwerking met organisaties in de publieke en private sector en brancheorganisaties, een convenant op voor kwalificatie van informatiebeveiligers.

Op 30 mei jongstleden organiseerden het PvIB, ECP en CIO Platform Nederland bij VNO-NCW in Den Haag een werkconferentie over kwalificatie van informatiebeveiligers. Tijdens deze werkconferentie presenteerde het PvIB het convenant. Acht grote organisaties uit de private en publieke sector tekenden het convenant onder het oog van publiek en pers. In alfabetische volgorde: ABN AMRO, AkzoNobel, Alliander, ENECO, Equens SE, ING, Rabobank en UWV.
Met de ondertekening geven deze organisaties aan dat niet iedereen zich zo maar informatiebeveiliger kan noemen, maar dat er vraag is naar gekwalificeerde informatiebeveiligers die kunnen aantonen dat ze voldoen aan de gestelde eisen voor kennis en ervaring. En dat daarvoor het beoogde uniforme kwalificatiestelsel nodig is dat ingezet kan worden voor werving en selectie. Ook het NCSC, BZK/DGOBR/ICCIO, ECP, CIO-Platform Nederland en de Cybersecurity Raad hebben aangegeven het initiatief te ondersteunen.

Het ligt in de verwachting dat nog meer organisaties zich achter het convenant zullen scharen en het beoogde kwalificatiestelsel toe gaan passen bij werving en selectie. Daarmee wordt een belangrijke impuls gegeven aan de professionalisering van informatiebeveiliging en het veiliger maken van de (digitale) maatschappij.

Het uitwerken van het uniforme kwalificatiestelsel voor informatiebeveiligers is nog geen gelopen race. Vooral de financiering is een heikel punt. Het gaat dan vooral om het traject om te komen tot het kwalificatiestelsel. De exploitatie ervan wordt namelijk kostendekkend. Dit laatste kan gerealiseerd worden door voor het uitreiken van kwalificaties een kostendekkende vergoeding te vragen. Om een beeld te vormen van de kosten die gemoeid zijn met het opzetten van het beoogde kwalificatiestelsel, is gekeken naar andere beroepsgroepen waar een dergelijk stelsel al gebruikt wordt, zoals accountants, juristen, IT-auditors en artsen.

Het traject om te komen tot een kwalificatiestelsel voor informatiebeveiligers zal gefinancierd worden met sponsorbijdragen. Gestreefd wordt naar een groep sponsoren met een 50-50 procent verdeling publiek-privaat. Het traject wordt gefaseerd uitgevoerd. Voor de eerstvolgende fase, met een lengte van één jaar, worden nog meer sponsoren gezocht. De toegevoegde waarde voor de sponsoren is dat ze kunnen meebeslissen over het vormgeven van een informatieveilig Nederland.

In de werkconferentie is besloten dat het traject aangestuurd gaat worden door een stuurgroep, met een brede achterban. Vooralsnog hebben de brancheorganisatie PvIB, een aantal koepelorganisaties en de belangrijkste sponsoren zitting genomen in de stuurgroep. De heer Wim Hafkamp, CISO van de Rabobank, is benoemd tot voorzitter. ●

ACHTER HET NIEUWS

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

PRISM. Tot voor kort dacht ik bij het horen van de term terug aan mijn lessen natuurkunde. De buigzaamheid van lichtstralen was fascinerend. Maar begin juni viel deze associatie toch even in het niet bij de wijze waarop de Amerikaanse veiligheidsdiensten de terrorisme wetgeving omgebogen lijken te hebben naar een grootschalig internetspionagesysteem. Als we de verhalen moeten geloven, werken Amerikaanse service providers mee aan het massaal verzamelen van informatie over internetters die hun diensten gebruiken. Zelf ontkennen de serviceproviders in alle toonaarden dat ze inlichtingendiensten directe servertoegang verschaffen. Ook de Amerikaanse overheid meldt dat de berichtgeving niet klopt. Over toegang tot data via netwerkverkeer of via handige interfaces hoor je vooralsnog niemand. De Amerikaanse overheid start ondertussen wel een onderzoek naar het lek en brengt haastig naar buiten dat er zeker geen informatie over Amerikanen wordt verzameld. De rest van de wereld doet er in het land blijkbaar minder toe.

Hoe lezen onze redacteuren dit nieuws? Moeten we ons zorgen maken? Of zouden we juist blij moeten zijn dat onze "bondgenoot" ook ons helpt beschermen tegen de boze buitenwereld?

André Koot

Ik ben zo blij dat PRISM naar buiten is gekomen! Beter een vijand die je kent dan één die je niet kent, maar waarvan je het bestaan vermoedt. Dat PRISM zou komen, was natuurlijk allang duidelijk. Sterker, ik heb er vorig jaar al de nodige tweets aan gewijd. Ik ben in september vorig jaar net zo erg geschrokken als de rest van de wereld deze weken. Vorig jaar was ik aanwezig bij een presentatie van Caspar Bowden, de voormalig Privacy officer van Microsoft, tijdens het EMEA congres van de Cloud Security Alliance in Amsterdam [1]. Boeiende conferentie en volgens mij heb ik al eens gemeld dat de eerste vraag uit het publiek bij de eerste lezing ging over de Patriot Act [2]. Na de lezing van Bowden heb ik maar gemeld dat de Patriot Act kinderspel is, vergeleken met FISA-A-A1881.
De boodschap van Bowden was feitelijk dat afzonderlijke staten bezwaar moeten maken op de inbreuk op hun autonomiteit door die Amerikaanse wetgeving. En voor ons betekent dat: Laat de EU in het geweer komen tegen deze inbreuken.

Helaas. Niets van dat alles is tot nog toe gebeurd. Onze minister van BZK doet nog niets en onze minister van V&J vindt privacy sowieso al te veel geld kosten [3].

Mensen, we moeten er maar mee leren leven. We kennen onze 'vijand', laten we ons ervan bewust zijn.

Lex Dunn

PRISM: de 29-jarige Edward Snowdon heeft gegevens laten lekken over het programma van de Amerikaanse NSA om op grote schaal internetgebruikers te volgen (in elk geval via hun gedrag op Google, Facebook en Yahoo, maar ga er maar van uit dat ze alle verkeersstromen bekijken). Is dat nieuws? Nou nee, want de ouderen onder ons herinneren zich vast nog wel Echelon. Destijds vooral gericht op het verzamelen van informatie via radio- en satellietverbindingen (er was toen nog geen internet). En wat heeft dat "aangericht"? Gevoelige informatie over de ontwerpen van Airbus bleken bij Boeing te zijn opgedoken. Dat geeft al aan dat de US of A slechts haar eigen (economische) belangen voorop stelt: we kunnen dan wel gezellig thee drinken met ze in Brussel onder het mom van de Noord-Atlantische Verdrags Organisatie, maar achter je rug om jatten ze het recept van de thee ;-) Ik vertrouwde de Amerikanen al niet, en na het horen over PRISM nog veel minder.

Reactie Maarten Hartsuijker

Terwijl ik in het nieuws lees hoe Amerikaanse functionarissen creatief met woorden spelen om zonder te liegen de berichtgeving als onjuist te kunnen bestempelen, vraag ik mij af waar we als samenleving meer van te vrezen hebben. Traditioneel terrorisme, of informatiesystemen die specifieke machthebbers in staat stellen om alles en iedereen naar eigen criteria in hokjes te stoppen. Makkelijk is het antwoord op deze vraag niet. Ik ben er namelijk van overtuigd dat veel parlementsleden en overheidsfunctionarissen oprecht en met goede bedoelingen naar oplossingen zoeken om onze huidige manier van leven te beschermen. Maar het is ook een interessante vraag hoe je op termijn de controle houdt over dit soort machtsmiddelen.

Goed opgezette datamining technologie is immers veel breder

inzetbaar dan tegen enkel het "terrorisme". Denk aan het vroegtijdig signaleren dat een jongere aan het ontsporen of radicaliseren is en op internet op zoek gaat naar wapens. Dit zou een hoop schietpartijen op school kunnen voorkomen. En zou het ook niet mooi zijn om in te kunnen grijpen bij online geuite vroege vormen van pyromanie of pedofilie? Wellicht zouden we deze mensen dan tijdig een behandeling kunnen aanbieden om daarmee escalatie van hun problemen te voorkomen. Als we dan toch druk aan het profileren zijn, kunnen we wellicht ook meteen de communicatie met buitenlandse banken analyseren om zwartspaarders te ontdekken, we kunnen auteursrechtenschenders beboeten, mensen die teveel junkfood laten bezorgen een zorgkostentoeslag laten betalen en potentiële asielzoekers die overwegen naar Nederland te komen alvast in het land van herkomst in hechtenis laten nemen. Worden we daar niet met z'n allen uiteindelijk alleen maar beter van?

Als je naar spelden zoekt, heb je een hooiberg nodig. Op basis van dit principe is het niet vreemd dat veiligheidsdiensten toegang tot steeds meer data proberen te krijgen. Maar zijn wij als samenleving wel in staat om te voorkomen dat dit soort dataverzamelingen en analysemogelijkheden op termijn gebruikt gaan worden voor doeleinden waarvoor we ze eigenlijk niet hadden willen ontwikkelen? Als we daar niet zeker van zijn, zou dit middel op termijn wel eens erger kunnen zijn dan de kwaal.

Lex Borger

Wat mij het meest verbaasd is de publieke verbazing dat PRISM bestaat. De Verenigde Staten hebben de middelen, het motief en de gelegenheid om dit te doen. Waarom zouden ze het dan niet doen? De Chinese overheid doet het; en let maar op: Europa doet het vast ook.

Onduidelijker is wát ze vastleggen. Ik ga er altijd van uit dat alles wat over het internet gaat te lezen is. En ik denk niet dat het gaat om alle expliciete verzoeken die gedaan zijn aan Facebook en Microsoft. Bedenk ook dat er een gigantische aggregatie van gegevens mogelijk is. Nummerplaten, mobieltjes, gezichtsherkenning, email versturen/ ontvangen, surfen. Alles kan met elkaar in verband gebracht worden. En als het kan ... gebeurt het ook.

De onderste steen is nog lang niet boven...

Ronald van Erven

PRISM gezien vanuit een stukje e-discovery, datamanagement, IT-forensics en business intelligence gezien is briljant. Denk alleen maar aan die gigantische hoeveelheden data die via filters doorzocht worden en dan nog met enige snelheid. Tenminste ik hoop dat de Amerikaanse overheid het niet handmatig doet, alhoewel het is wel een goede werkgever. Maar realiseer je de technologieën die er achter zitten, state-of-the-art. Een search engine van google is hierbij een joke. En deze technologieën zullen in de tijd doorsijpelen naar bedrijfstoepassingen. Er komen enorme kansen aan voor de digitale marketeers. Dat hierom heen een heleboel ruis is omtrent privacy.... ach dat waait wel weer over. Immers wij weten al heel lang dat dergelijke activiteiten gaande zijn. Jawel, uw eigen gekozen politici in Den Haag en Brussel hebben ingestemd met verregaande inzage in financiële transacties en reisinformatie - u bent een bekende Nederlander! Kortom er komt een mooie toekomst aan voor degene die nu hun internet-recht, digitaal marketeer en Digitaal-bewust-politicus diploma aan het halen zijn. En zeker op deze laatste zitten we met smart te wachten - ook mijn digitale belangen moeten goed behartigd worden in binnen- en buitenland. ●

Links

[1] *Presentatie Casper Bowden: http://www.slate.com/blogs/future_tense/2013/01/08/fisa_renewal_report_suggests_spy_law_allows_mass_surveillance_of_european.html*

[2] *Tweet van @meneer: https://twitter.com/meneer/statuses/250940081857241088*

[3] *Bericht Webwereld: http://webwereld.nl/beveiliging/78052-opstelten-vindt-bescherming-persoonsgegevens--te-duur-*

COLOFON

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

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

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

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

Vormgeving en druk
VdR druk & print, Nijkerk
www.vdr.nl

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

Abonnementen 2013
De abonnementsprijs bedraagt 115 euro per jaar (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

COLUMN

INTERNETJES WEL OF INTERNETJES NIET

In 1969 werd het ARPANET (een van oorsprong militair netwerk) omgebouwd en geschikt gemaakt voor burgerlijke initiatieven. Deze initiatieven begonnen eigenlijk pas echt van de grond te komen in 1994 en als je dat dan beziet, betekent het dat internet nog geen twintig jaar bestaat. Internet heeft de wereld veranderd en zal de wereld blijven veranderen en niet altijd kun je deze veranderingen positief noemen. Ik ben altijd bijzonder enthousiast geweest over het internet en behoorde tot de early adapters. Het eerste negatieve wat mij opviel, was het uitsterven van de fotozaken. Vroeger was op iedere hoek van de straat wel een fotowinkel te vinden die gespecialiseerd was om jouw rolletje binnen 3 uur te ontwikkelen en af te drukken.

Kijk nu naar de binnensteden en kijk naar de winkelstraten die eigenlijk alleen nog maar uit winkelketens bestaan. De HEMA's, de Blokker's, de C&A, de Free Record Shops, de ECI's (o nee, de laatste twee bestaan ook niet meer). De kleine zelfstandige winkels zijn eigenlijk allemaal weg. De bankgebouwen staan allemaal leeg, omdat we nu zelf onze betalingen regelen op de telefoon of thuis achter de computer. PostNL weet ook niet meer welk verdienmodel te hanteren, omdat brieven eigenlijk niet meer verzonden worden. Onze postbode komt altijd met een paar brieven, de rest is folders. Telefonie is in deze column ook vaak besproken, maar het aantal mensen met een vaste lijn is ook niet meer vergelijkbaar met vroeger.
Videotheken (een winkeltje waar je video's, DVD's of CD's kunt huren) zijn er niet meer en de te verhuren content wordt ook al niet meer verkocht. Dat downloaden we allemaal van internet. Trouwens wat moet je met een DVD als je hem één of twee keer hebt gezien. Ik heb al mijn eigen muziek en films digitaal en heb nog een paar kasten volstaan met oude DVD's en CD's.
Internet is makkelijk, heel makkelijk. Niet alleen de goedwillende gebruikers hebben er veel lol aan, maar zeker ook de gebruikers die op een illegale wijze hun geld ermee verdienen. In deze columns heb ik vaak de bedreigingen beschreven, maar mijn oog viel laatst op een artikel waarin een adverteerder op marktplaats werd vrijgesproken ondanks het feit dat hij willens en wetens gelden had ontvangen van kopers van producten die hij niet eens had, laat staan wilde uitleveren.
Het is toch wonderlijk dat een technologische ontwikkeling het hele maatschappelijke leven verandert en dat er zich ineens een beroepsgroep heeft ontwikkeld waarin oplichting, hacking, diefstal van gegevens en andere criminele ontwikkelingen ontstaan. Natuurlijk, als er geld te verdienen is, trekt dit ook mensen aan die we liever niet zouden zien.
Internet is ook nooit gemaakt en ontwikkeld om er betalingen op te verrichten of om als portaal te dienen naar je spaarrekening. Is nooit bedoeld geweest om je declaraties te verzenden naar je zorgverzekeraar. Natuurlijk bedenken we met zijn allen maatregelen om het veiliger te maken of in ieder geval de indruk te wekken dat alles veilig is. Beveiligingsbedrijven zijn ontstaan, ontwikkelaars die de mooiste sites maken, beroepsgroepen die twintig jaar geleden nog niet bestonden, verdienen er nu een goede boterham aan, inclusief ikzelf.
De mannen (sorry, is echt veruit de grootste groep) die in de bedrijven rondlopen en vrijblijvende dan wel dwingende adviezen geven om activiteiten op een andere wijze uit te voeren. De bedrijven die zich hebben gespecialiseerd in het uitvoeren van penetratietesten.
Is Berry weer vreselijk negatief? Verlangt hij weer terug naar de tijd van de kroontjespen en paard en wagen?
Nee, beslist niet. Iedere gadget die in de winkel te krijgen is, kan bij mij thuis geprobeerd worden. Ik vind het heerlijk om dagelijks met mijn telefoon en tablet te spelen en te werken. De ongekende mogelijkheden verbazen mij nog steeds en ik word er heel blij van. Natuurlijk maak ik ook gebruik van de mogelijkheden van de toestellen, ook ik betaal via mijn telefoon, maar ik denk er wel bij na. Mijn kinderen en echtgenoot kunnen iedere minuut van de dag zien waar ik uithang en wanneer mijn biertje opengemaakt kan worden. Natuurlijk weet ik dat de fabrikant van mijn telefoon ook weet waar ik zit, maar daar maak ik me geen zorgen over. Ik maak me veel meer zorgen over mijn creditcard gegevens die ze ook hebben. Natuurlijk weet ik dat mijn mail dagelijks doorzocht wordt door mijn mail provider en dat te pas en te onpas advertorials worden getoond van de onderwerpen waar ik in geïnteresseerd ben.
Als we ons er maar bewust van blijven, blijven internet en de technologische ontwikkelingen geweldig. ●

Berry

Data Leakage

Bring Your Own Device

Security As A Service

Compliance & Auditing

SECURITY

geen keuze, maar noodzaak!

De toepassingsmogelijkheden van Bring Your Own Device, Security As A Service, Data Leakage en Compliance & Auditing ontwikkelen zich in hoog tempo. Daarmee nemen ook bedreigingen toe in de vorm van Cybercrime, Hacking en Identiteitsfraude. Ook worden deze bedreigingen steeds geavanceerder. Adequate beveiliging van werkomgevingen, data en identiteitsgevens zijn inmiddels geen keuze, maar noodzaak geworden. Security vereist nu ervaren, betrouwbare en loyale partners. CRYPSYS is toonaangevend op het gebied van security analyse, advies en installatie bij overheden, semi-overheden, gemeenten, grote bedrijven en organisaties.

CRYPSYS
secure computing

CRYPSYS Data Security BV Edisonweg 4 4207 HG Gorinchem **tel** +31 (0)183 62 44 44 **fax** +31 (0)183 62 28 48 **mail** sales@crypsys.nl **web** www.crypsys.nl

CRYPSYS is officieel distributeur van: Sophos. Lumension. Norman. Cryptzone. Cryptshare. Adyton. Tenable. Kanguru