iB

INFORMATIEBEVEILIGING

jaargang 15 - 2015

#4

Detectie en risicoclassificatie van typosquatting

Logging- niet Dat, maar Wat en Hoe

Advanced Business Impact Analysis

Drie boeken over IB besproken

Partnership EXIN en Security Academy

Partnership

EXIN en de Security Academy zijn een partnership aangegaan om een volledig portfolio van onafhankelijke security certificeringen te ontwikkelen. De certificeringen zijn gebaseerd op de Security Academy opleidingen en sluiten aan op het e-Competence Framework (e-CF).

Met de wereldwijde release van dit nieuwe examenprogramma versterken EXIN en Security Academy hun partnership in de voortdurende ontwikkeling op het gebied van Security en Cyber-programma's.

Alle examen programma's binnen EXIN's Security en Cyber Portfolio zijn vendor-neutral, onafhankelijk gevalideerd en beschikbaar voor alle partijen. De examens zijn wereldwijd verkrijgbaar, in meerdere talen en via meerdere examenkanalen.

De reeds beschikbare certificeringen zijn:

- Secure Programming Foundation
- Ethical Hacking Foundation

Dit jaar zullen veder ontwikkeld worden:

- Data Privacy
- Business Continuity
- Cyber Crime Essentials

Secure Programming Foundation

In deze opleiding worden de basisprincipes geleerd van het veilig programmeren. De opleiding is bedoeld voor iedere programmeur of softwareontwikkelaar die (web)applicaties ontwikkelt. De cursus bereidt u voor op het internationale Secure Programming Foundation examen van het Exin.
De cursusprijs bedraagt €1.100,- euro exclusief BTW. Dit is inclusief cursusmateriaal en catering maar exclusief het EXIN examen.

Ethical Hacking Foundation

U heeft het misschien wel voorbij zien komen, termen als SQL Injections en Cross-Site Scripting. Maar wat betekenen deze termen eigenlijk? Tijdens deze basistraining kruipt u in de huid van een hacker en leert u de basisstappen van veel voorkomende digitale inbraken. Deze cursus is uitermate geschikt voor personen die over weinig technische kennis bezitten en nieuw zijn in het vakgebied van het ethisch hacken.

De cursus bereidt u voor op het internationale Ethical Hacking Foundation examen van het Exin.

De cursusprijs bedraagt €1.100,- euro exclusief BTW. Dit is inclusief cursusmateriaal en catering maar exclusief het EXIN examen.

BEL ONS +31(0)348-408061

WWW.SECURITYACADEMY.NL
INFO@SECURITYACADEMY.NL

DE STARBUCKS HACK DIE GEEN HACK WAS

"Wij zijn niet gehackt" riep Starbucks. Dit als reactie op berichten dat verschillende klanten last hadden gehad van onbekende transacties op hun Starbucks account, leidend tot behoorlijke onkosten voor de klant.
We luisteren mee op kantoor van Starbucks, waar de boze berichten binnenkomen van klanten, wiens geld verdwenen is. Marketing vraagt IT: "Wat ging er fout?" IT antwoordt: "Niets, alles heeft volgens specificaties gewerkt. We vinden niets in onze logs wat er op wijst dat er inlogfouten zijn geweest of een ander soort aanvallen op de accounts. Er is gewoon correct ingelogd. En als dat niet de klant was, dan was dat een ander die met zijn wachtwoord inlogde." Marketing concludeert: "De klant is dus slordig geweest met zijn wachtwoord." Marketing weet ook allang waardoor er per klant veel meer geld weg is dan in het account zat. Zij waren degenen die IT de opdracht hadden gegeven. "Bouw het zo dat de klant maar een keer zijn bankrekening hoeft in te stellen. Opwaarderen moet snel en transparant kunnen gaan. De klant moet nooit hoeven nadenken of hij de koffie wel kán betalen." Gelijk hebben ze, op beide punten. Maar wil je dat gelijk ook halen bij je klant? Dat moet je je niet pas afvragen bij het incident, maar al bij de BIA (business impact analyse). Ik stel me voor dat het als volgt had kunnen gaan. De analist brengt in: "Impact van accountproblemen: de klant zal voelen dat het 'zijn' account is. Sterker nog, wij zullen direct toegang hebben tot één van zijn rekeningen. Als hier iets mis gaat, hoe erg is dat?" Marketing manager: "De klant mag niet aan de financiële last denken als hij koffie besteld." "Goed, maar wat als het nou mis gaat?" werpt de analist tegen. De marketing manager denkt na en zegt: "We moeten zorgen dat de kans dat dat mis gaat klein is, want hier zit een flinke mogelijkheid tot imagoschade achter. Reken maar dat wanneer het mis gaat we al dat geld moeten vergoeden en een imagoherstelcampagne moeten opzetten."
Met deze BIA vooraf zou het wellicht anders gelopen zijn. IT zou in de risicoanalyse tot twee-factor authenticatie gekomen zijn, of een out-of-band verificatie van het opwaarderen. Misschien zou IT een regel gemaakt hebben dat één keer opwaarderen per dag de limiet is. Of dat je jezelf moet legitimeren om cadeaukaarten te mogen kopen met jouw kaart. Dat is toch een transactietype met een hoger frauderisico...
Dan hadden ze niet naar buiten hoeven komen met een verklaring dat het de stomme fout was van de klant, maar dan hadden ze de klant kunnen aanspreken vanuit een respect-positie. "Zelfs een missertje van de klant heeft maar beperkte gevolgen gehad, dankzij onze voorzorgen."

Lex Borger, hoofdredacteur

In dit nummer

DETECTIE EN RISICOCLASSIFICATIE VAN TYPOSQUATTING

Typosquatting, ook wel domeinkaping genoemd, is het registreren van een domeinnaam die sterk lijkt op een bestaande domeinnaam. Een groeiend probleem dat vraagt om een oplossing. Ondanks dat het al een meer dan vijftien jaar oud concept is, wordt het nog steeds actief gebruikt, zoals blijkt uit onder meer een recente studie van de Universiteit van Leuven. TNO ontwikkelde een tool waarmee snel en eenvoudig inzicht en grip kan worden verkregen op de situatie.

Een voorbeeld van domeinkaping is bijvoorbeeld het registreren van belasingdienst.nl als variant van belastingdienst.nl – een van de vele varianten van de belastingdienst.nl die actief zijn. Door het maken van een eenvoudige typefout in een webadres of e-mailadres komt de gebruiker uit bij deze typosquat-website of wordt de e-mail naar de typosquat-mailserver verstuurd. In het voorbeeld van www.belasingdienst.nl, krijgt de bezoeker een advertentiesite te zien, waar een link naar de belastingtelefoon te vinden is, deze leidt echter naar http://nl-contact.nl/klantenservice/belastingdienst en het nummer dat we hier vinden is een betaald 0900-nummer, terwijl de belastingtelefoon een gratis nummer is. Uiteindelijk zien we dat de eigenaar van www.belasingdienst.nl verdient aan de advertenties die op de website staan. En dat een advertentie-aanbieder verdient op het betaalde belastingtelefoonnummer, dat doorgestuurd wordt naar de oorspronkelijke belastingtelefoon.

Er zijn verschillende toepassingsvormen van typosquatting te onderkennen. In veel gevallen wordt de persoon die de typo maakt naar een website geleid die voornamelijk reclame bevat, om zo inkomsten te genereren – niet zelden reclame voor de site van de originele domeineigenaar of daaraan gerelateerde diensten. Ook wordt het gebruikt om de persoon te leiden naar een website van de concurrent van de originele site. Een andere belangrijke vorm van misbruik is het afvangen van e-mail verkeer met de betreffende typefout er in.

Sommige vormen van typosquatting zijn legitiem en lijken vaak toevallig zo te zijn ontstaan. Zo herleidt het domein www.un.nl naar het Utrechts Nieuwsblad, dat onderdeel van het AD is. Terwijl un.nl een variant van nu.nl is die als typefout niet ondenkbaar is. Hoewel een typosquat-domein van nu.nl hierbij direct herleidt tot de concurrent, is er hier geen aanleiding om aan te nemen dat hier 'kwade opzet' in het spel is.

Ten behoeve van phishingdoeleinden (zie ook phishtank.org) door de website erg te laten lijken op de originele site en zo bijvoorbeeld inloggegevens af te vangen, wordt de gebruikte domeinnaam in de praktijk niet meegenomen. Dat komt waarschijnlijk omdat op phishingsites regelmatig snel wordt geacteerd, en de betreffende sites worden verwijderd, waarbij gebruik gemaakt wordt van het overnemen van een bestaande website en contentmanagement-systeem onafhankelijk van gebruikte domeinnaam.

Er is inmiddels al veel onderzoek naar typosquatting gedaan, maar toch is er nog geen efficiënte oplossing gevonden voor het probleem. Vaak is het advies om veel typosquat-domeinen zelf te registreren voordat iemand anders hier misbruik van maakt. Het aantal mogelijke typosquat-domeinen is echter zo hoog dat dit vaak niet realistisch is.

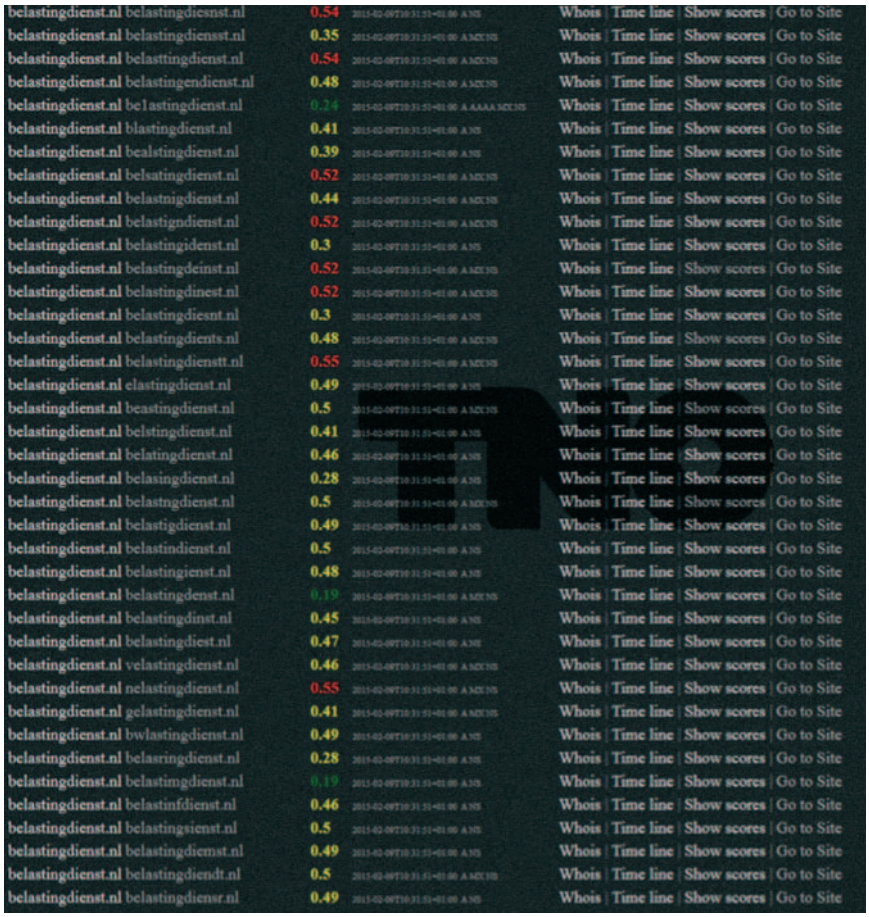
Onderzoek typosquatting

Hoewel er verschillende onderzoeken zijn die zich richten op het gevaar van typosquatting, zijn er voor zover bekend weinig onderzoeken die zich richten op het beter kunnen detecteren en inschatten van typosquat-risico's.

Daarom heeft TNO een uitgebreid onderzoek uitgevoerd dat gericht is op het vaststellen of typosquatting daadwerkelijk een risico vormt. TNO heeft daartoe vierendertig domeinnamen geregistreerd die varianten zijn van in totaal achttien verschillende overheidsdomeinen. Voor deze vierendertig varianten heeft TNO een mailserver ingericht die alle e-mails die gericht zijn aan deze domeinen afvangt. In een periode van circa zes maanden zijn op deze mailboxen ongeveer vijfduizend berichten binnen gekomen van in totaal ruim negenhonderd megabyte. Naast dat dit veroorzaakt wordt door typo's in e-mailadressen, is er nog een ander belangrijk effect dat bijdraagt aan de omvang. Indien de e-mailberichten adressen bevatten met een typefout er in, inclusief in de cc-velden worden deze automatisch overgenomen bij de actie "beantwoord allen". Hiermee zijn hele mailuitwisselingen te volgen zonder dat de deelnemers zelf typefouten maken. In sommige e-mails was ook zeer vertrouwelijke informatie te vinden, omdat het soms communicatie betrof die gewoon intern in een organisatie uitgewisseld werd. Een ander opvallend detail is ook dat een deel van de berichten uit spam bestaat – wat aangeeft dat de typovarianten van de e-mailadressen zeer waarschijnlijk al langere tijd in gebruik zijn.

Uit dit onderzoek is gebleken dat het tamelijk eenvoudig is om een typosquat-domein te claimen, en hier e-mail-communicatie op af te vangen. Bovendien bleek dat

Gerben Broenink heeft informatica gestudeerd aan de Universiteit Twente, waarna hij in 2008 voor TNO is gaan werken als information security researcher. Hij is gespecialiseerd in smartphone security, netwerk security en smartphone security.



Een groeiend probleem, dat vraagt om een oplossing

Typosquat-domeinen van www.belastingdienst.nl en hun typosquat-scores

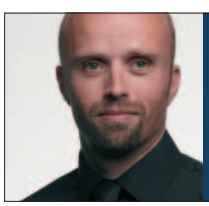
zodoende een aanzienlijke hoeveelheid gevoelige data verkregen kon worden. Naar aanleiding van dit onderzoek heeft TNO in een typosquat-detectietool ontwikkeld om typosquat-domeinen geautomatiseerd te herkennen en te analyseren.

Typosquat-detectie

TNO heeft een experimentele tool gemaakt waarmee snel kan worden gescand welke varianten van een domeinnaam actief zijn en op basis van de geselecteerde kenmerken deze varianten classificeert. Daarbij kan snel een overzicht gekregen worden tegen welke sites (juridisch) actie moet worden ondernomen. In Figuur 1 is een weergave van deze tool gegeven, waarin een deel van de gevonden typosquat-domeinen van belastingdienst.nl weergegeven worden, met daarnaast hun scores. Deze score is het resultaat van de detectie-algoritmen. Daarbij geldt dat scores dicht bij de nul legitieme sites lijken te zijn, terwijl scores dicht bij de één duiden op mogelijk misbruik door de betreffende site.

Het detecteren van deze domeinnamen gebeurt in enkele stappen:

1. Het genereren van typosquat-varianten van een legitiem domein. Dit wordt gedaan door veel voorkomende typefouten 'na' te doen. Bijvoorbeeld het omdraaien van twee letters (zoals www.raobbank.nl of www.bealstingdienst.nl) of het verwijderen van één letter (b.v. www.beastingdienst.nl). Hiervoor worden enkele tientallen algoritmes voor gebruikt, onder andere op basis



Harm Schotanus heeft informatica gestudeerd aan de Universiteit Twente, waarna hij in 2000 voor TNO is gaan werken als information security researcher. Hij is gespecialiseerd in de beveiliging van web technologieën, toegangsbeveiligingsystemen en de detectie van targeted en advanced persistent attacks.

Domain	Variation	RR Type	RR value
abnamro.nl	abnameo.nl	A	95.211.117.206
abnamro.nl	abnamero.nl	A	95.211.117.206
apple.com	aplple.com	A	95.211.117.206
apple.com	appile.com	A	95.211.117.206
paypal.com	apypal.com	A	95.211.117.206
belastingdienst.nl	bealstingdienst.nl	A	95.211.117.206
belastingdienst.nl	belasingdienst.nl	A	95.211.117.206
belastingdienst.nl	belastingsdienst.nl	A	95.211.117.206
belastingdienst.nl	belstingdienst.nl	A	95.211.117.206
belastingdienst.nl	blastingdienst.nl	A	95.211.117.206
google.com	gboogle.com	A	95.211.117.206
google.com	geoogle.com	A	95.211.117.206
google.com	gmoogle.com	A	95.211.117.206
google.com	go0ogle.com	A	95.211.117.206
google.com	goeogle.com	A	95.211.117.206
google.com	goigle.com	A	95.211.117.206
google.com	golgle.com	A	95.211.117.206
google.com	googlenet.com	A	95.211.117.206
google.com	goopgle.com	A	95.211.117.206
google.com	goougle.com	A	95.211.117.206
google.com	gqoogle.com	A	95.211.117.206
paypal.com	papypal.com	A	95.211.117.206
paypal.com	paqypal.com	A	95.211.117.206
paypal.com	patpal.com	A	95.211.117.206
paypal.com	paydpal.com	A	95.211.117.206
paypal.com	paygpal.com	A	95.211.117.206
paypal.com	payoal.com	A	95.211.117.206
paypal.com	payopal.com	A	95.211.117.206
politie.nl	plitie.nl	A	95.211.117.206
politie.nl	ploitie.nl	A	95.211.117.206
politie.nl	politei.nl	A	95.211.117.206
politie.nl	poltie.nl	A	95.211.117.206
google.com	sgoogle.com	A	95.211.117.206
snsbank.nl	snabank.nl	A	95.211.117.206
apple.com	spple.com	A	95.211.117.206

Meerdere typosquat-domeinen gehost op dezelfde server

van taalkundige aspecten van de domeinnaam. Uiteindelijk worden er van een legitieme website zo'n honderd tot duizend typosquat-varianten gemaakt.

2. Controleren of de typosquat-varianten geregistreerd zijn. Van iedere variant worden vervolgens de dns-records opgevraagd. Als dit dns-record niet bestaat, kan er geconcludeerd worden dat dit domein niet gebruikt wordt. Als het dns-record wel bestaat, betekent het dat hier mogelijk sprake is van typosquatting.
3. Onderzoeken van de gevonden varianten, om te verkennen of deze ook een webserver en/of mailserver hosten. Deze test houdt effectief in dat er gecontroleerd wordt of de gevonden variant ook daadwerkelijk gebruikt wordt. Of dat het wellicht een variant is die niet (meer) gebruik wordt, of misschien een door de oorspronkelijke eigenaar geclaimd domein is om misbruik te voorkomen. Hierbij wordt primair gekeken of er een webserver of een mailserver actief is op het betreffende domein.
4. Kwalificeren van het typosquat-domein. Alle varianten die nu nog over zijn, zijn potentiële typosquat-domeinen. In de ontwikkelde tool wordt geautomatiseerd een kwalificatie gegeven aan deze domeinen. Deze kwalificatie is gebaseerd op kenmerken van de typosquat-domeinen.

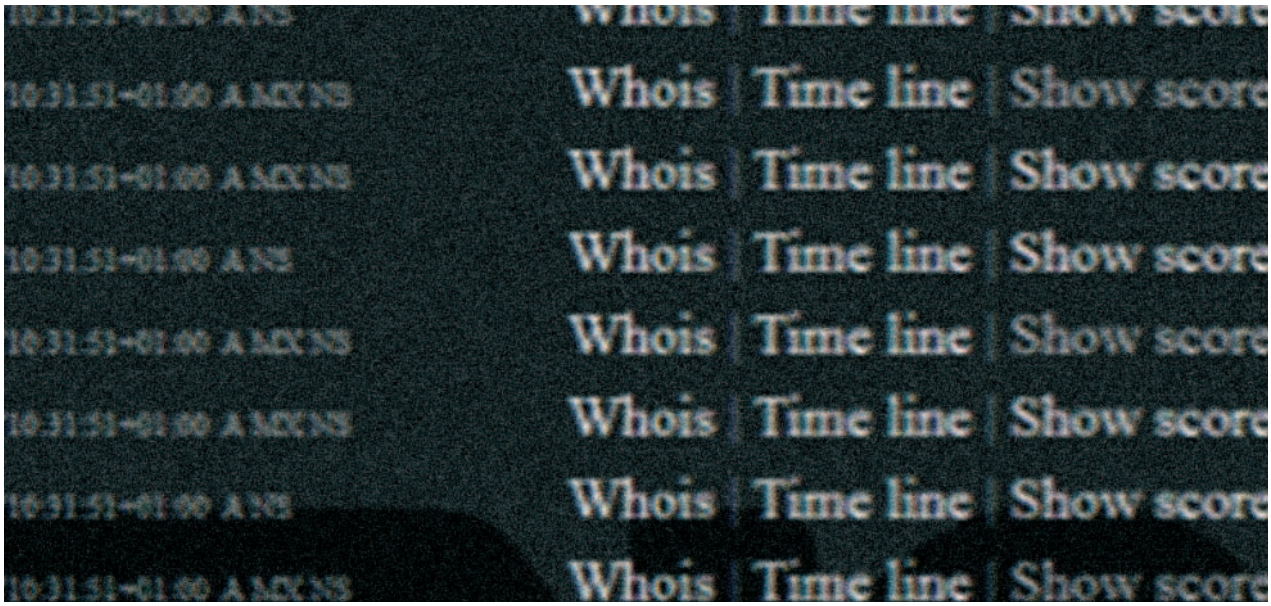
Een opvallend fenomeen is dat diverse typosquat-domeinen van verschillende originele domeinen op één systeem, met één IP-adres worden gehost. Daarnaast zijn een aantal varianten vrijwel standaard geregistreerd, zoals beginnend met www, bijv. wwwbelastingdienst.nl. Een aantal grote partijen heeft inmiddels ook massaal varianten van hun eigen domeinnamen geclaimd, zoals Google en Apple.

Kwalificeren typosquat-domeinen

Per gevonden typosquatdomein wordt gekeken welk type typosquat-domein het betreft aan de hand van onder meer de volgende kenmerken die duiden op een site die misbruik maakt van typosquatting:

- Bevat de website advertenties en in het bijzonder Google-ads?
- Known IP-address (wordt het domein gehost op een IP-adres dat ook heel veel andere verdachte domeinnamen hosten).
- Wordt de website geredirect en niet naar de originele websites.
- Is er sprake van dat de domeinnaam te koop wordt aangeboden.
- Maakt de website gebruik van een zogenaamd affliate-programma, waarbij de aanbieder van dat programma de website-eigenaar betaalt als de bezoeker bijvoorbeeld een dienst afneemt bij de aanbieder van het affiliate-programma.
- Output van diverse reputatie-sites, zoals web of trust, safebrowsing en alexa kunnen heel nuttig zijn.

Daarnaast zijn er ook indicaties die juist duiden op het niet misbruiken van typosquatting. Zoals een redirect naar de echte domeinnaam of een zelfde eigenaar van het domein als de echte domeinnaam op basis van who-is-gegevens. Zo zijn er diverse qualifiers te definiëren waar relatief eenvoudig op gecontroleerd kan worden. Van deze qualifiers wordt een gewogen gemiddelde berekend en wanneer deze boven een bepaalde waarde uitkomt, wordt dit beschouwd als een misbruikte variant. In de praktijk blijkt dit gewogen gemiddelde van qualifiers heel effectief te zijn om vast te stellen of een website misbruik maakt van domeinkaping.



De schade van typosquat-domeinen lijkt op dit moment geaccepteerd te zijn

Typosquat-profielen

Er zijn verschillende mogelijkheden om misbruik te maken van getyposquate domeinnamen. Een advertentiesite zal een webserver aanbieden, die naast advertenties ook content aanbiedt die verleidt tot het klikken op een van de aangeboden links. Een mail-catcher zal geen webserver inrichten maar alleen een mailserver aanbieden. De verschillende kenmerken kunnen op verschillende manieren meegewogen worden om tot een bepaald profiel van misbruik te komen. Het is dan ook mogelijk om verschillende profielen te maken van deze verschillende mogelijkheden om misbruik te maken van getyposquate domeinnamen.

In de huidige TNO typosquat-detectietool is er momenteel één profiel gemaakt dat de advertentiesites filtert. Dit profiel hecht dus een grote waarde aan de aanwezigheid van advertenties op de sites, maar ook is gebleken dat het zoeken naar 'bekende' IP-adressen een erg goede indicatie is. Dit betekent dat veel advertentiesites uiteindelijk op de zelfde server gehost worden. En dus dat een site die ook op deze servers gehost wordt, hoogstwaarschijnlijk een advertentiesite is. Andere profielen zijn relatief eenvoudig toe te voegen, door de weging van de kenmerken aan te passen. Er is echter vervolgonderzoek nodig om te achterhalen welke profielen nuttig zijn en welke weging van de kenmerken hiervoor gebruikt moet worden.

Conclusies

In de praktijk blijkt dat typosquatting vooral gebruikt wordt om snel geld te verdienen door middel van advertenties en affiliate-programma's. Een ander voorbeeld zoals phishing wordt eigenlijk slechts zelden toegepast. In dat geval wordt er veel meer gebruik gemaakt van gehackte CMS'en.
Voor populaire domeinen (Alexa top 10 – google.com, apple.com) zijn vele typosquat-varianten al bezet. Deels door de eigenaar van het originele domein, maar lang niet allemaal. Veel van deze domeinen worden ook gebruikt voor bijvoorbeeld affiliate-programs en advertentiesites. Voor een andere vorm van misbruik van typosquat-domeinen, het afvangen van e-mailverkeer, zijn op dit moment geen bruikbare cijfers bekend. Maar wel is onderzocht dat op deze manier eenvoudig veel vertrouwde informatie verkregen kan worden.

De schade van typosquat-domeinen lijkt op dit moment geaccepteerd te zijn. Maar er zijn nieuwe TLD's op komst, en wanneer domeinnamen geïnternationaliseerd worden, neemt het aantal mogelijke typosquat-domeinen alleen maar toe. De traditionele maatregelen van het zelf registreren van alle typosquat-domeinen wordt daarmee alleen maar minder realistisch. Dit leidt ons naar de conclusie dat typosquatting een groeiend probleem is en dat de door TNO ontwikkelde tool een eerste hulpmiddel is om grip te krijgen op de omvang van het probleem.

PECUNIA NON OLET?

Na vele jaren in privacyland rondgelopen te hebben, kan ik nog steeds verbaasd worden. U begrijpt, ik hou van mijn vak. Het is nooit saai. Mijn verbazing werd gewekt door een Nederlands artikel dat suggereerde dat je wel gek zou zijn als je voor privacy zou betalen. Amerikanen, bang voor onze aanstaande strenge privacywetgeving en het op de schop gaan van Safe Harbor, brachten uitermate stellig een rapport uit waarin ze beweren dat Europese gezinnen 1000 euro per jaar gaan inleveren als Safe Harbor daadwerkelijk de nek omgedraaid wordt (hetgeen overigens zeer in de lijn der verwachting ligt).

Nu hoor ik u denken: "Maar Rachel, verbaas jij je nog over de Amerikanen?". Nee, natuurlijk niet. Een land dat niet eens een volwaardig grondrecht op privacy heeft, daarvan kun je niet verwachten dat die serieus over privacy denken (aldus schreef zij ietwat snobistisch). Wat mij verbaasde is de gedachte achter de stellingname en de portee van het artikel. Betalen voor een grondrecht. Deze gedachte wordt voorondersteld zonder dat zij ter discussie wordt gesteld. Sterker nog, je bent een mafkees als je ervoor wilt betalen. En dat dan niet omdat je ten principale tegen het feit bent dat je voor een grondrecht moet betalen, maar omdat je "toch geen privacy hebt en je daarom een mafkees bent als je ervoor zou betalen".

De gedachte om te betalen voor privacy is niet nieuw, het is meermalen geopperd in zowel populaire pers als wetenschappelijke publicaties. Ook ontwikkelaars van allerhande privacytools zien privacy als business waarmee geld te verdienen valt. Begrijp me niet verkeerd, ik zou zeker niet willen beweren dat bedrijven hun producten dan maar moeten weggeven. Waar het mij om gaat is de basis van de discussie; daar is iets wat ten zeerste stinkt.

Een grondrecht is het hoogste recht wat een burger toekomt. Het beschermt tegen ongewenst indringen door de overheid en in bepaalde mate ook tegen het indringen door bedrijven. Indringen in dat grondrecht is verboden tenzij de wet regelt dat dit in specifieke omstandigheden geoorloofd is. De overheid behoort ervoor zorg te dragen dat burgers hun grondrechten kunnen genieten door er geen inbreuk op te maken. Sommige auteurs gaan (wetenschappelijk onderbouwd) nog een stap verder en stellen dat de overheid actief moet handelen om schending te voorkomen; ook bij schending door bedrijven.

Het grondrecht op privacy is van oudsher klassiek (alhoewel sommigen inmiddels menen dat het dus ook sociaal is en de overheid een actieve taak heeft het grondrecht te garanderen). Daarnaast is het een onvervreemdbaar recht. Het is het bezit van de burger, een recht dat hem niet ontnomen kan worden. Ik zou daar graag een schepje bovenop doen. Het grondrecht op privacy is een recht dat je hebt, waar niet in getreden mag worden en waar je bovendien niet voor hoeft te betalen.

Mr. Rachel Marbus
@rachelmarbus op Twitter

LOGGING

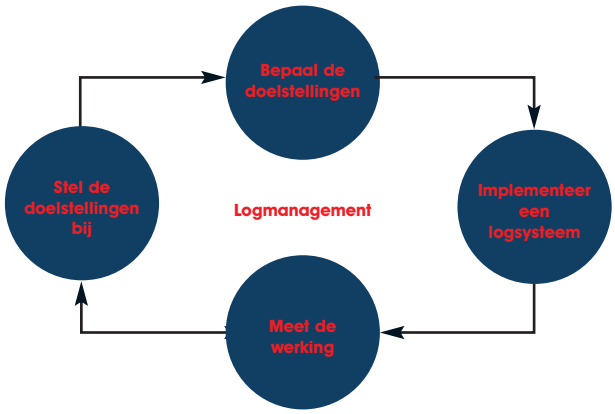
niet Dat, maar Wat en Hoe

In IB2 van 2015 verscheen het eerste artikel uit een reeks van twee over logging-management. Het eerste artikel beschreef wat gelogd moet worden en waarom. In dit deel beschrijft Jean hoe dat in zijn werk gaat.

De redactie

Hoe

Zoals bij veel bedrijfsactiviteiten is het verstandig om een procesmatige aanpak te kiezen voor het opzetten en onderhouden van logging; i.c. logmanagement. De stappen die doorlopen worden, vormen dan samen een geheel (cf. de bekende Deming-cirkel) en worden door eenieder begrepen en zijn eenvoudig toe te passen.



Logmanagement bestaat uit vier fasen:

1. **Bepaal de doelstellingen**
   Voordat een logsysteem succesvol geïmplementeerd kan worden, is het van belang dat de doelstellingen duidelijk zijn. Welke gebeurtenissen zijn interessant om te loggen, waar wordt de logging bewaard, hoe snel moeten logging beschikbaar zijn en wordt de logging regulier of incidenteel gecontroleerd?
2. **Implementeer een logsysteem**
   Welke opties zijn mogelijk voor de inrichting van een logsysteem en hoe gaat het gebruik en beheer ervan uitzien?
3. **Meet de werking**
   De effectiviteit van logmanagement kan alleen vastgesteld worden als de prestaties regelmatig worden gemeten tegen de vooraf bepaalde KPI's.
4. **Stel de doelstellingen bij**
   Formuleer nieuwe eisen naar aanleiding van de gemeten performance van logmanagement.

1. Bepaal de doelstellingen

Zoals vaak bij nieuwe toepassingen en activiteiten, is het van belang om de organisatie te helpen bij het opzetten van een gestructureerde aanpak. Zo ook bij logging. Dit kan gebeuren door tijdens plenaire sessies of workshops met verantwoordelijken van de verschillende bedrijfsafdelingen de noodzaak, de mogelijkheden en zeker de toegevoegde waarde van logging toe te lichten. Vervolgens wordt tijdens deze sessies een inventarisatie gemaakt van de behoeften, wensen en eisen. Dit is niet altijd eenvoudig, omdat het onderwerp vaak nieuw en relatief abstract is.
Een alternatieve aanpak kan zijn dat er een concept voor de inrichting van logging wordt gebruikt als voorstel. Dit maakt het onderwerp concreter en er zullen sneller reacties volgen, die gebruikt kunnen worden om het inrichtingsvoorstel te verbeteren. In deze bottom-up-aanpak schuilt het gevaar dat het voorstel minder draagvlak krijgt bij de verantwoordelijken van de verschillende bedrijfsafdelingen, omdat hun input en invloed als beperkt kan worden ervaren.
De snelste en meest effectieve aanpak is de combinatie van beide. Tijdens een workshop wordt gebruik gemaakt van een concept voorstel, dat tijdens de plenaire sessies meteen zal worden aangepast. Zo is er ruimte voor toelichting, voldoende input vanuit de verantwoordelijken van de verschillende bedrijfsafdelingen en komt er snel een concreet voorstel voor de inrichting en het gebruik van logging.
Om te komen tot behoeften, eisen en wensen is het handig om antwoorden te zoeken op de volgende vragen. Gebruik deze bij het voorbereiden van een concept voorstel en ook als leidraad voor een plenaire workshop.

- Wie is de afnemer van de informatie uit de logging?
- Welke informatie moet er geleverd worden, waar is behoefte aan?
- In welke situatie moeten loggegevens ondersteuning bieden?
- Hoe lang moeten loggegevens beschikbaar blijven (retentieperiode)?
- Worden de loggegevens integraal of steekproefsgewijs gecontroleerd?
- Worden loggegevens regulier of incidenteel beoordeeld?
- Welke afwijkingen zijn relevant?
- Wie moet zich verantwoorden met behulp van logging?
  - de organisatie;
  - een afdeling;
  - een medewerker.
- Welke informatiesystemen bevatten welke gegevens / informatie?
- Is er behoefte aan rapportages, alerts, meldingen en/of dashboards?

Vier specifieke aspecten kunnen helpen bij het maken van de juiste keuzes als het gaat om de inrichting van een logsysteem

Jean Coenen is security consultant bij Saganto. Hij is per de e-mail bereikbaar via Jean.Coenen@saganto.nl

en het logmanagement-proces. Zo is het van belang om vooraf te bepalen welke loggegevens van belang zijn, in dit geval de inhoud van de logging. Daarnaast zal de verzamelplaats en de tijdsfactor het mogelijke gebruik van logging bepalen.

I. Inhoud van de logging

Met de antwoorden op de eerder genoemde vragen wordt bepaald welke gebeurtenissen van belang zijn om te loggen en of we te maken hebben met technische logging uit ICT-apparatuur (denk bijvoorbeeld aan syslogs) of logging in applicaties. Bij logging in applicaties is vervolgens weer een onderscheid te maken naar beheertooling en bedrijfsapplicaties. Bij deze twee soorten informatiesystemen (ICT-apparatuur en applicaties) kan het van belang zijn om vast te stellen hoe gebruikers welke informatie hebben gebruikt. Gebeurtenissen die we gaan loggen worden voornamelijk gekozen op basis van de wijze waarop ze gebruikt worden voor de verantwoording. We kennen hiervoor een aantal categorieën van gebeurtenissen:

- **Operationele gebeurtenissen**
  Dit zijn gebeurtenissen die voortvloeien uit het normale gebruik van een informatiesysteem. Van alle pakketjes die door een router worden ontvangen en verstuurd, ieder gebruik van beheertools tot alle activiteiten van een eindgebruiker in een bedrijfsapplicatie. Het invoeren, wijzigen, verwijderen en raadplegen van gegevens zijn reguliere gebeurtenissen in een applicatie.
- **Bijzondere gebeurtenissen**
  Hieronder vallen bijvoorbeeld uitzonderingen op reguliere gebeurtenissen. Afwijkende bewerkingen in een applicatie en afwijkende waarden van gegevens in de database. Financiële bedragen die bovengemiddeld hoog zijn, nieuwe of buitenlandse bankrekeningnummers of mutaties buiten kantoortijd. Gegevensbewerkingen die buiten de standaard applicatiefunctionaliteiten om rechtstreeks in de database zijn doorgevoerd.
- **Toegangsbeheer gebeurtenissen**
  Zowel de toegang tot computersystemen als ook de toegang tot informatiesystemen leveren veelal relevante logging. Foutieve inlogpogingen, toegangspogingen op afwijkende tijdstippen en simultane toegang tot dezelfde systemen. Het aanmaken, wijzigen en verwijderen van (de rechten van) gebruikers, groepen, profielen en rollen.
- **Logging gebeurtenissen**
  Hieronder valt het in- en uitschakelen van logging . Tevens het aanpassen van de rechten voor de toegang tot logging en het wijzigen en verwijderen van loggegevens.

Bij alle categorieën van gebeurtenissen worden kennisregels vastgesteld die bepalen of gebeurtenissen wel of niet worden gelogd. Met andere woorden nemen we een white-list of een black-list als uitgangspunt voor een te loggen gebeurtenis. De systeemeigenaar (de applicatie-eigenaar of bijvoorbeeld de beheerder) bepaalt welke bekende of onbekende gebeurtenissen gelogd moeten worden.
Om de gewenste actie voor een gebeurtenis te bepalen, wordt het niveau van de gebeurtenis vastgesteld. Hiermee wordt bedoeld dat vooraf bekend moet zijn welke impact een gebeurtenis op de bedrijfsvoering zal hebben. Het is uiteindelijk van belang om te bepalen wanneer en hoe snel loggegevens beschikbaar moeten zijn en tot een vervolgactie moeten leiden. Daarom is het goed om een gebeurtenis in te delen in een van de volgende impactniveaus en de daarbij passende acties te definiëren.

Niveau gebeurtenis	**Impact voor de organisatie**
Noodgeval	Dit soort gebeurtenissen bedreigt direct het voortbestaan van de organisatie of het leven en/of de gezondheid van personen loopt direct gevaar.
Waarschuwing	Het betreft een gebeurtenis die de operatie van de organisatie of het welzijn van personen ernstig in gevaar kan brengen.
Kritisch	De gebeurtenis werkt verstorend op de bedrijfsvoering van de organisatie of de bedrijfsprocessen. Misbruik van gegevens, personen en/of middelen en fraude kan aan de orde zijn.
Fout	De uitvoering van de bedrijfsprocessen is niet correct en dient, na een eventuele datacorrectie, aangepast te worden. De operatie van de organisatie wordt niet verstoord, maar verloopt niet conform gestelde eisen, regels en voorschriften.
Notificatie	De gebeurtenis is niet verstorend voor de organisatie en de organisatie hoeft zich over deze gebeurtenis niet te verantwoorden.
Informatief	Deze gebeurtenis dient nader onderzocht te worden om vast te stellen of er een noodzaak is tot corrigerende maatregelen. Er is geen aanwijsbare impact voor de organisatie.
Debugging	Gebeurtenissen in niet-productionele systemen die worden gebruikt voor de ontwikkeling of verbetering van informatiesystemen en/of bedrijfsprocessen.

De categorie van de gebeurtenis in combinatie met het impactniveau bepaalt of en op welke wijze gegevens gelogd moeten worden en hoe en hoe snel de opvolging dient plaats

te vinden. Tevens kan een inschatting worden gemaakt van de hoeveelheid logging die bewaard dienen te worden, in welke systemen de logging gegenereerd worden en welke verwerkingssnelheid noodzakelijk is.

II. Verzamelplaats van logging

Veelal hebben informatiesystemen de mogelijkheid om zelf logging bij te houden en op te slaan. Soms is het ook mogelijk om binnen het informatiesysteemrapportages te genereren op basis van opgeslagen logging.
Het kan verstandig of voldoende zijn om logging vorm te geven in een informatiesysteem. Indien het vastleggen van de gewenste en noodzakelijke logging mogelijk is en de rapportages voorzien in voldoende rapportages, dan is deze optie zeker het overwegen waard.
Daarnaast bestaat de mogelijkheid om gebruik te maken van een dedicated logsysteem, separaat van de informatiesystemen waarin de logging worden gegenereerd. Gecentraliseerde opslag en verwerking van de loggegevens gebeurt dan in een SIEM-tool; i.c. Security-Information-and-Event-Management-tool.
Daar waar blijkt dat alleen een centraal logsysteem voldoet of waar een volgend niveau van logmanagement nodig is, kan een SIEM-tool ingezet worden. De functionele en technische mogelijkheden van een SIEM-tool zijn uitgebreider en er zijn weinig beperkingen ten aanzien van de hoeveelheid te verwerken logging . De verwerkingssnelheden van een SIEM-tool zijn, vanwege de vaak eigen DBMS en de geoptimaliseerde opslag, zeer hoog.

III. Tijdsfactor van logging

Zoals reeds eerder aangeduid bestaan er - afhankelijk van de bedrijfsbehoefte - diverse mogelijkheden tot verwerking, presentatie en gebruik van logging of afwijkingen uit logging . Dit kan variëren van real-time alerts in een dashboard, rapportages die op afgesproken momenten worden gegenereerd tot specifieke rapportages die inzicht moeten geven bij het optreden van een gesignaleerde afwijking c.q. bij incidenten. Bij de keuze uit deze opties is het van belang om onderscheid te maken naar monitoring, waarbij real-time bewaking van events plaatsvindt en logging waarbij gegevens worden opgeslagen voor analyse achteraf.
Voor iedere behoefte dient nagegaan te worden hoe lang na het vastleggen van loggegevens er behoefte is aan informatie. Bedenk hierbij dat alleen een SIEM tool goed in staat is om alerts real-time te verwerken en deze zichtbaar kan maken in een grafisch dashboard. Een alert kan ook een melding zijn die real-time aan een ander systeem of zelfs aan een gebruiker wordt aangeboden.

IV. Gebruik van logging

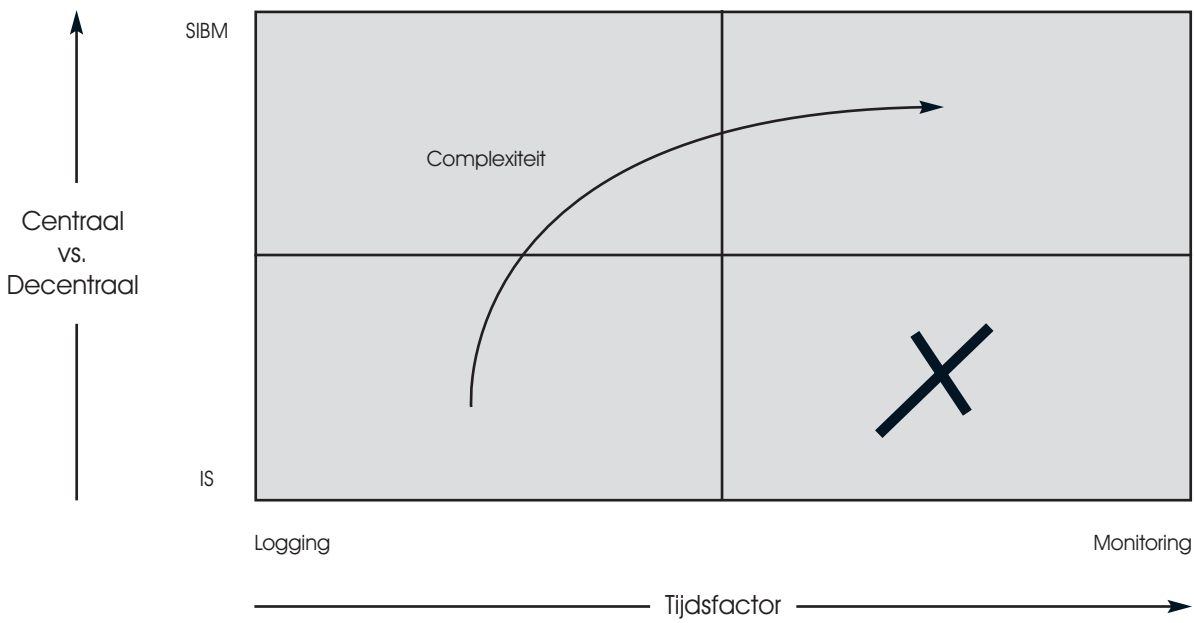
Logging kan op een aantal manieren door een organisatie gebruikt worden. Om de juiste logging te activeren is het van belang dat vooraf het mogelijke gebruik van logging bepaald is. Veel loggingparameters activeren of alle gebeurtenissen loggen betekent niet dat deze logging bruikbaar is op de manier waarop een organisatie daar behoefte aan heeft. Bedenk daarom goed welke behoefte een organisatie heeft of eventueel zou kunnen hebben en bepaal daarmee welke gegevens gelogd dienen te worden en realiseer daarbij de juiste rapportages, alerts of dashboards.
Veelal wordt logging gebruikt voor het uitvoeren van reguliere controles, die aanvullend zijn op interne controles die in een informatiesysteem zijn ingebouwd. Omdat deze reguliere controles vaak duidelijk te benoemen zijn, is het vervolgens ook goed mogelijk om te bepalen welke gebeurtenissen er gelogd moeten worden. Voor deze reguliere controles worden rapportages gebouwd die voor de reguliere bedrijfsvoering (bijv. dagelijks, wekelijks, …) gebruikt worden.
Vaak bestaat er een specifieke aanleiding voor een nader onderzoek van loggegevens. Dit komt meestal voort uit een incident of op verzoek uit de organisatie. Om dit soort incidentele controles mogelijk te maken is het van belang om na te denken over de noodzakelijke loggegevens. Lang niet altijd is het mogelijk om voor deze controles vooraf alle behoeften te voorzien en kan het noodzakelijk zijn om op een later moment nieuwe logging te introduceren. Bij forensisch onderzoek is bijvoorbeeld vooraf niet bekend naar welke informatie gezocht zal worden of welke afwijkingen naar een oplossing leiden en welke behoeften ontstaan tijdens het onderzoek.
Gelogde gebeurtenissen kunnen real-time worden vergeleken met vooraf bepaalde grenswaarden. Indien gebeurtenissen boven of beneden een vooraf bepaalde grenswaarde komen, kunnen deze afwijkingen worden opgeslagen of meteen tot een actie leiden. Door middel van alerts en/of automatische meldingen worden de afwijkingen getoond in rapportages, automatische meldingen of via grafische dashboards. Deze vorm van logging wordt veelal monitoring genoemd, omdat afwijkende gebeurtenissen (excepties) direct opgevolgd kunnen worden.
Logging kan heel nuttig zijn om trendanalyses uit te voeren. Zonder dat vooraf bepaald is welke vervolgacties noodzakelijk zijn, kunnen gelogde gebeurtenissen worden geanalyseerd. Het gedrag, gebruik en de performance van mensen, informatie en ICT-middelen kunnen gedurende een bepaalde periode veranderen en aanleiding zijn tot het nemen van maatregelen. Trends kunnen handig zijn voor het analyseren van de effectiviteit en efficiëntie van bedrijfsprocessen, het gebruik van ICT-middelen en het gedrag van mensen.

2. Implementeer een logsysteem

Bepaal of gebruik van beschikbare loggingfunctionaliteiten in een informatiesysteem voldoende is om invulling te geven aan

uw loggingbehoeften. Wellicht betreft het een eerste kennismaking of implementatie van logmanagement. Ook dan is het aantrekkelijk om op deze eenvoudige wijze kennis te maken met de mogelijkheden en het actieve gebruik van logging.
Uiteraard betreft dit de 'goedkopere' versie van logmanagement. Het betreft immers een geïntegreerde en standaardfunctionaliteit van een informatiesysteem en er zijn meestal geen extra modules of licenties noodzakelijk. Het opzetten kan relatief eenvoudig en snel en de voordelen voor de organisatie zijn direct zichtbaar. Diegene die verantwoordelijk wordt voor logmanagement kan samen met de organisatie de eerste serieuze stappen zetten in de richting van een volwassen logmanagement en op een eenvoudige manier leren en ervaring op doen.
Voor een uitgebreid logsysteem of een logsysteem dat data uit meerdere informatiesystemen moet combineren, wordt gebruik gemaakt van aparte tooling; een zogenaamd SIEM-tool. Een SIEM-tool wordt separaat van informatiesystemen geïnstalleerd en zal daardoor geen invloed hebben op de prestaties van de informatiesystemen; de opslag- en de verwerkingscapaciteit gaat niet ten koste van applicatiesystemen. SIEM-tooling kent, in tegenstelling tot logfunctionaliteiten die ingebouwd zijn in een informatiesysteem, de mogelijkheid om gegevens te normaliseren en te verrijken door meerdere bronnen te combineren en te correleren. De database van een SIEM-tool is ontworpen voor de verwerking van zeer veel gegevens en kent een snelle verwerking van loggegevens. Daarnaast zijn de rapportagemogelijkheden van een SIEM-tool uitgebreider en beschikt een SIEM-tool meestal over grafische dashboards en heeft een SIEM-tool vaak al veel kennisregels aan boord. Met dit soort dashboards is het mogelijk dat afwijkingen real-time worden weergegeven op het moment dat een afwijking zich voordoet (monitoring-functie). De toegang tot logging is specifiek afgeschermd door een specifieke inrichting van autorisaties.
In het speelveld van logsystemen staat een mogelijke groeistrategie, die bepaald wordt door de benodigde complexiteit. Het is duidelijk dat met een implementatie van logging in een decentraal IS (informatiesysteem) geen real-time-monitoring mogelijk is.

SIEM is de afkorting voor Security Information and Event Management en is een combinatie van Security Information Management (SIM) en Security Event Management (SEM). Het onderscheid tussen SIM en SEM komt voort uit hun respectievelijke oorspronkelijke functionaliteiten.
Een SIM is bedoeld voor het opslaan van loggegevens uit een informatiesysteem of veelal bedrijfsapplicatie. Het collecteert gegevens, analyseert deze en rapporteert hierover. Een veelgebruikt doel is om interne bedreigingen te beheersen aan de hand van rapportages, die bij wijze van evidence, de compliance van een organisatie aantonen. Het heeft de mogelijkheid om via toegangsbeheer de loggegevens alleen voor bevoegden beschikbaar te maken. Een SIM is niet in staat om real-time acties uit te voeren.
Een SEM kent een meer technische oorsprong en is bedoeld om loggegevens uit security- en netwerk-apparatuur en beheersystemen te ondersteunen. Het voorziet in real-time-security-monitoring en kan loggegevens real-time correleren. Daarnaast kent een SEM veel incidentmanagement-functionaliteiten.



Maak, om logging succesvol te implementeren, iemand binnen de organisatie eindverantwoordelijk voor de uitvoering en het onderhoud van logmanagement

In een modern SIEM-tool zijn de functionaliteiten van SIM en SEM gecombineerd, waardoor een SIEM-tool voor bijna alle logging toepassingen inzetbaar is. Er zijn tientallen aanbieders van SIEM-tools, die in meer of mindere mate beschikken over genoemde functionaliteiten.

De aanpak

Om op een optimale wijze gebruik te maken van logging is het noodzakelijk om logmanagement als een proces in te richten. Hiertoe is het noodzakelijk om iemand te benoemen die verantwoordelijk is voor het logmanagement. Dit is dan de proceseigenaar en tevens de beheerder van het logsysteem. Binnen logmanagement worden logging, lograpportages en dashboards ontwikkeld, onderhouden, beheerd en voor aanvragers ter beschikking gesteld. Daarnaast wordt het toegangsbeheer van het logsysteem ingericht en onderhouden. Gebruikers van het logsysteem worden door de beheerder geautoriseerd, onder de verantwoordelijkheid van de systeemeigenaar. Aanvragen voor het beschikbaar stellen van logging en lograpportages worden behandeld door de beheerder of door geautoriseerde gebruikers.
In een (eenvoudig) SLA worden afspraken over het gebruik en het beheer van logmanagement en het logsysteem vastgelegd. Het betreft afspraken zoals:

- de tijdsduur waarbinnen een verzoek moeten worden uitgevoerd;
- het leveren van 'ad-hoc'-rapportages;
- het leveren van reguliere en structurele rapportages;
- change-procedure voor het realiseren van nieuwe rapportages;
- gebruikers ondersteuning;
- geheimhouding.

Bedenk hierbij dat deze afspraken een overeenkomst betreft van logmanagement met de gebruikersorganisatie.

3. Meet de werking

Omdat in de SLA is vastgelegd welke logging op welk moment beschikbaar moet zijn en aan welke voorwaarden logmanagement moet voldoen, is het mogelijk om de werking van logmanagement te meten. Twee voor de hand liggende KPI's die hiervoor gebruikt kunnen worden zijn:

- MTD: voor een logging is te meten wat de gemiddelde tijd van detectie is (MTD = Mean Time to Detect)
- MTR: het is mogelijk om de gemiddelde tijd van herstel te meten (MTR = Mean Time to Remediate)

Samen met de gebruikersorganisatie kan een evaluatie plaatsvinden van de effectiviteit van de rapportages en de efficiëntie van het logmanagement-proces. Door de vertegenwoordigers van de verschillende afdelingen kan de gebleken bijdrage van rapportages (c.q. logmanagement) worden vastgesteld. Tevens kan aan de hand van het daadwerkelijke gebruik van rapportages en logging in het algemeen de bijdrage aan de bedrijfsvoering worden vastgesteld.

Voor de afhandeling van incidenten en verzoeken voor logging rapportages is het van belang om te evalueren hoe eenvoudig het is om 'ad-hoc'-rapportages op te stellen en beschikbaar te stellen. Zeker bij incidenten is deze snelheid van belang om zorg te dragen voor een adequate (re)actie.

4. Stel de doelstellingen bij

Dit betreft de belangrijke laatste stap van een procesmatige aanpak, die de mogelijkheid biedt om verbeteringen door te voeren aan het logsysteem en het logmanagement-proces. Alleen als de meetgegevens over de werking van het 'logsysteem' verwerkt worden in het 'logsysteem' zullen de resultaten en de toegevoegde waarde ervan toenemen. De inspanning voor het gebruik van logging zal afnemen en de snelheid waarmee de juiste en bruikbare informatie beschikbaar komt op de noodzakelijke momenten neemt toe.

Maak, om logging succesvol te implementeren, iemand binnen de organisatie eindverantwoordelijk voor de uitvoering en het onderhoud van logmanagement. Hiermee wordt geborgd dat de laatste stap van logmanagement niet wordt overgeslagen en de gewenste bijdrage aan uw bedrijfsvoering zal leveren.

Kortom

Om ervoor te zorgen dat logging er daadwerkelijk komt en wordt ingericht op een manier die de organisatie van dienst zal zijn, is het van belang om het hoe en het wat te bepalen. Wat moet gelogd worden, hoe kunnen we logging effectief en efficiënt gebruiken en welke faciliteiten hebben we hiervoor nodig. Het geschetste proces voor logmanagement helpt bij de invulling van de 'hoe' vraag. De LogCycle helpt bij de beantwoording van de 'wat' vraag. Want 'dat' we moeten loggen staat al jarenlang als een paal boven water; en nu aan de slag.

ADVANCED BUSINESS IMPACT ANALYSIS

Verbeterd risico-management door gerichte impactbepaling

Alle bedrijven lopen risico's, waardoor er een kans bestaat dat bedrijven hun verplichtingen naar hun stakeholders - zoals klanten of aandeelhouders - niet meer kunnen nakomen en daardoor zelf schade leiden. Het is dus van vitaal belang dat bedrijven de relevante risico's identificeren en vervolgens managen. De stap in het risicomanagementproces waarin de impact van een bepaalde dreiging op het behalen van business doelstellingen wordt bepaald is de Business Impact Analysis (BIA). Aan de BIA zoals die tegenwoordig in de meeste organisaties wordt uitgevoerd kan nog veel verbeterd worden. Dat is de conclusie van een aantal interviews en een expertsessie met verscheidene information-security-consultants met meerjarige ervaring in het ondersteunen van organisaties met het uitvoeren van BIA's. De geconstateerde tekortkomingen resulteren in mogelijk onjuist ingeschatte impacts van cyberdreigingen, met het gevaar dat enerzijds werkelijk relevante risico's over het hoofd worden gezien en anderzijds het risico wordt gelopen om te investeren in onnodige veiligheidsmaatregelen.

In deel 1 van dit artikel benoemen we de geconstateerde onvolkomenheden. In deel 2 zullen we een aantal mogelijke verbeterpunten bespreken voor zowel de korte, als de wat langere termijn.

Business Impact Analyse

Cyberincidenten kunnen een grote impact hebben op bedrijven. In 2013 werd een aantal gerenommeerde banken en bedrijven getroffen door Distributed Denial of Service (DDoS) aanvallen die gedurende enkele dagen het nieuws beheersten en hebben gezorgd voor veel onrust onder klanten. Voor bedrijven kunnen cyberincidenten een directe bedreiging zijn voor het voortbestaan van de onderneming, zoals bij DigiNotar. Bescherming tegen cyberdreiging en het kunnen afslaan van aanvallen is daarom erg belangrijk. Maar het nemen van mitigerende en defensieve maatregelen kost geld en andere resources. Om goed te kunnen onderbouwen welke maatregelen tegen welke risico's het beste genomen kunnen worden – en daarbij de investering waard zijn – moet er inzicht zijn in het effect van cyberincidenten en -dreigingen. Daarbij spelen vragen een rol als: Wat is het gevolg van cyberincidenten voor het bedrijf? Zorgt een veelvuldige DDoS aanval ervoor dat klanten naar de concurrent gaan? Wat doet verlies van klantgegevens met het imago van het bedrijf?
Het bepalen van de impact van een dreiging voor een organisatie, dat wil zeggen de totale schade die een organisatie naar verwachting oploopt als die dreiging ook werkelijk plaats vindt, is van belang omdat die schades altijd betrekking hebben op het niet of onvoldoende verwezenlijken van de - grotere of kleinere - doelstellingen van die organisatie, en dus diens succes mede bepalen.
De activiteit waarbij de (maximaal) te verwachten schades worden ingeschat voor een zekere organisatie met een zeker dreigingsprofiel, heet een Business Impact Analyse (BIA). Op basis van deze inschattingen bepaalt het management welke schade in het geval van optreden onacceptabel groot is en dus actie vereist.
Aan het uitvoeren van de BIA zoals die tegenwoordig in veel organisaties wordt uitgevoerd kan in onze ogen nog veel verbeterd worden.

De context: IT-risicomanagement

Het globale risicomanagement(RM)-proces voor organisaties met IT-systemen staat beschreven in standaarden zoals de ISO 31000:2009 (Risk Management – Principles and Guidelines) en ISO 27005: 2008 (Information Security Risk Management).
Voor de BIA en Risk Assessment (RA) wordt echter nog vaak teruggegrepen op de traditionelere werkwijze - mogelijk omdat die bekend is c.q. al jaren gebruikt wordt - die (nog) terug te vinden is in de NIST SP 800-30. Deze traditionele BIA/RA richt zich op het identificeren van kwetsbaarheden en dreigingen van de IT-infrastructuur die door bedrijven wordt gebruikt om hun verplichtingen na te kunnen komen, en de hoogte van de impact die deze dreigingen zouden veroorzaken in het geval van optreden. Dat is gebaseerd op definities van 'Risk' zoals die staan in de NIST SP 800-30: "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." Hier ontbreekt dus de relatie naar de bedrijfsdoelstellingen zoals die tegenwoordig door ISO wel expliciet wordt gelegd.
Zulke definities leggen naar onze mening een zodanige nadruk op dreigingen en kwetsbaarheden dat het doel waar het allemaal om gaat, namelijk de onzekerheden in het halen van de bedrijfsdoelstellingen tot een acceptabel niveau reduceren, vaak uit het oog wordt verloren. Dit verklaart ook waarom veel Chief Information Security Officers (CISO's) er nog steeds veel moeite mee hebben om security op bestuurlijk niveau aan te kaarten: de directie is doorgaans niet geïnteresseerd in dreigingen en kwetsbaarheden, maar veel meer in wat dit voor de bedrijfsdoelstellingen betekent, welke impact het op bedrijf en bedrijfsvoering heeft, en welke schade ze kunnen veroorzaken. Waar deze link niet of onvoldoende wordt gelegd, zal informatiebeveiliging een ondergeschoven kindje blijven.

Inschatten van Business Impact en Risico's

Hoe goed een organisatie zich tegen risico's heeft gewapend staat of valt met hoe de risicoanalyse wordt uitgevoerd. Een belangrijke stap bij het uitvoeren van een risicoanalyse is het inschatten van de impact en dreigingsrisico's om inzicht te verkrijgen in welke security-incidenten de grootste gevolgen (impact) voor de business kunnen hebben. Omdat men over het algemeen een beperkt budget heeft voor beveiligingsmaatregelen, worden de vervolgstappen van risicoanalyse vaak alleen uitgevoerd voor scenario's die tot hoge schade zullen leiden. Als de impact van bepaalde dreigingen wordt onderschat, zullen er tegen die dreigingen

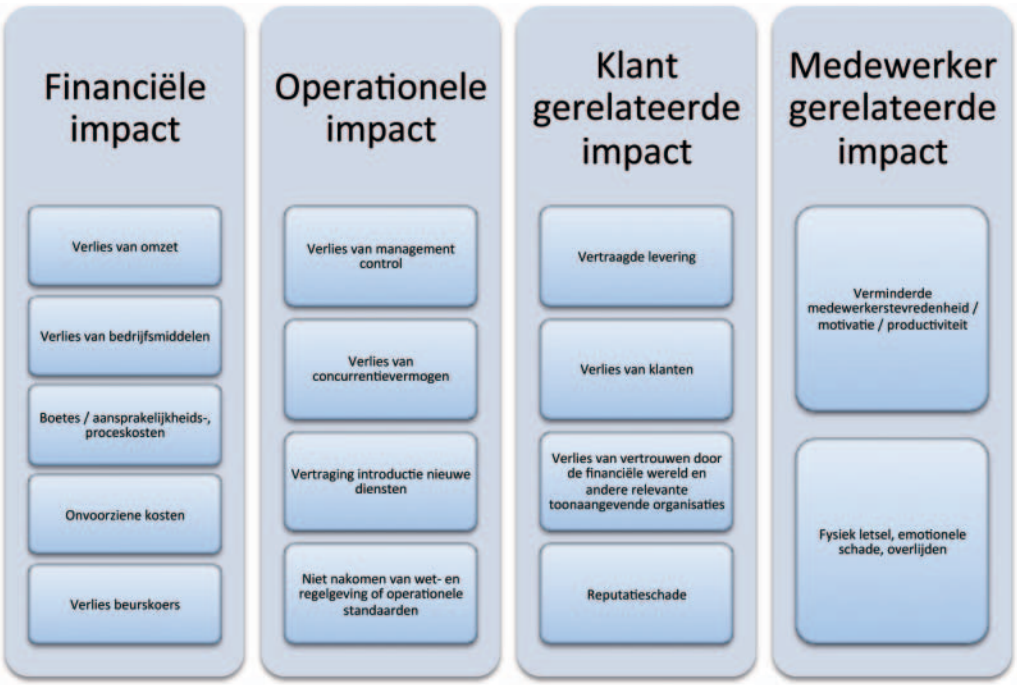
Milena Janic promoveerde aan de Technische Universiteit Delft, op het gebied van performance van informatie- en communicatienetwerken en diensten. Zij werkt als consultant en onderzoekster bij de expertisegroep Information Security van TNO. Haar focus ligt op onderzoek en consultancy op het gebied van risicomanagement, identity- en access-management en privacy gerelateerde vraagstukken.

geen maatregelen getroffen worden, hetgeen kan leiden tot potentieel hoge schade bij het toch optreden ervan. Ook overschatte impact leidt tot inefficiëntie, daar de onnodige maatregelen geïmplementeerd zullen worden en zo onnodige kosten introduceren. Vanwege dit belang zullen we wat dieper ingaan op hoe de impactinschattingen traditioneel worden uitgevoerd.

Gebaseerd op literatuurstudie en gesprekken met experts, concluderen wij dat - binnen de diversiteit aan bestaande methoden - de methodieken voor het uitvoeren van een impact- of risico-inschatting er in hoofdlijnen hetzelfde uitzien. Het doel is om voor een gegeven veiligheidsincident (-scenario) de impact op de business te bepalen. Een veel gebruikt middel om een schatting hiervan te kunnen maken, zijn expertmeningen. Deze worden uitgevraagd in een workshop, interviews, of enquêtes.

Om dit te illustreren gaan we uitgebreider in op de door het Information Security Forum (ISF) voorgestelde methodiek die de bedrijven die lid zijn van ISF gebruiken voor het uitvoeren van risicoanalyses. De Business Impact Analysis Assistant van ISF wordt uitgevoerd voor elke gedefinieerde scope binnen een organisatie. Deze BIA bestaat uit een van tevoren vastgelegde en in Excel gevatte vragenlijst die - meestal in een workshop - door degene die voor die scope verantwoordelijk is beantwoord dient te worden. In deze methodiek worden er voor verschillende processen en bedrijfsmiddelen binnen deze scope verschillende worst-case scenario's geïdentificeerd, die tot compromitteren van vertrouwelijkheid, integriteit of beschikbaarheid van informatie kunnen leiden. Vervolgens wordt er aan de hand van de vastgelegde vragen, behorende tot verschillende categorieën zoals operationeel, financieel, klant, of medewerker-gerelateerd, de impact van het optreden van deze scenario's op de business ingeschat. De vragenlijst is in principe generiek van aard, hoewel de organisaties zelf een versie kunnen opstellen die is aangepast op eigen doelstellingen en behoeftes. Voor scenario's en impact types die hoog en zeer hoog scoren worden workshops gehouden om de dreigingen te identificeren die tot deze scenario's leiden, en de kans van hun optreden in te schatten, zodat de totale risicowaarde bepaald kan worden.

In de ISF methodiek wordt uitgegaan van 15 impactsoorten, Business Impact Types (BIT) genoemd. Deze zijn weergegeven in Figuur 1. Voor elke impactsoort dient van tevoren de norm voor classificatie van impact te worden vastgesteld. Dit betekent dat wordt aangegeven voor welke waarderanges de impact als respectievelijk zeer hoog, hoog, middel, laag en zeer laag gekwalificeerd kan worden. Voor elk van de BITs wordt daarna ingeschat hoe hoog op de schaal van zeer hoog tot zeer laag de impact zou zijn bij het optreden van een geïdentificeerd worst-case scenario.



Figuur 1 - Business Impact Types zoals onderscheiden in de ISF methodiek

Huidige BIA-knelpunten

In een expertsessie met security-consultants met meerjarige ervaring met het uitvoeren van BIA's in het algemeen, en de ISF-methodiek in het bijzonder, zijn de BIA als generieke processtap en de vragenlijst zoals het onderdeel van ISF, onder de loep genomen. Geconcludeerd kan worden dat de BIA zoals die nu wordt uitgevoerd een aantal belangrijke tekortkomingen kent, die we hierna bespreken.

Tekortkomingen in scope-bepaling

Zowel ISO 27001 als ISO 31000 schrijven voor dat aan het begin van het risicomanagement proces een afbakening dient plaats te vinden van het gebied waarbinnen de risico's worden gemanaged: de scopebepaling. Deze standaarden geven echter geen richtlijnen over hoe de scopes bepaald dienen te worden. Het lijkt er overigens op dat in de ISO 27005 die nu wordt gereviseerd, uitdrukkelijk(er) aandacht aan dit probleem geschonken gaat worden, maar vooralsnog wordt impliciet verondersteld dat de meeste organisaties goed weten hoe men deze afbakening moet uitvoeren. De praktijk wijst uit dat er behoefte is aan een betere scope bepaling. Dit uit zich in een aantal aspecten:

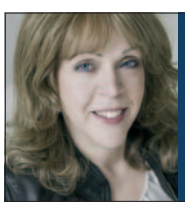
Gebrek aan aansluiting bij de belangen van hogere organisatieniveaus (verticale afhankelijkheden)

De BIA-vragen worden beantwoord door of namens degene die voor een bepaalde scope verantwoordelijk is. In praktijk is dat meestal een dienst- of systeemverantwoordelijke. Niet zelden ontbreekt bij deze persoon echter het inzicht in wat op bestuurlijk niveau als relevante risico's wordt gezien. Op bestuurlijk niveau wordt vaak gesproken in termen van financiële bedrijfscontinuïteit, maar deze doelstellingen en daarmee gepaarde risico's worden vaak niet doorvertaald naar doelstellingen en targets van de scope-verantwoordelijke die de BIA uitvoert. Hierdoor kan het voor komen dat de ernst van het optreden van bepaalde scenario's wordt onderschat, waardoor de daarmee gepaarde risico's ongemitigeerd blijven. Anderzijds kan de impact van scenario's onterecht worden overschat, waardoor onnodige maatregelen getroffen worden voor risico's die er eigenlijk niet zo toe doen. Hierdoor worden onnodige kosten gemaakt. Er is gebrek aan inzicht in de afhankelijkheden tussen scopes (horizontale afhankelijkheden)
Doordat de scope van een BIA meestal beperkt wordt tot bijvoorbeeld een dienst, kan het voorkomen dat het optreden van een bepaald scenario wel enige, maar geen significante impact op de dienst in scope heeft. Daardoor zou zo'n scenario in daar op volgende risicoanalyses buiten beschouwing worden gelaten. Het is echter voorstelbaar dat het optreden van datzelfde scenario ook gevolgen kan hebben op business doelstellingen van andere diensten, doordat bijvoorbeeld hetzelfde systeem wordt getroffen, maar eveneens beperkt qua omvang, waardoor het ook in het resultaat en opvolging van de BIAs van die andere diensten niet wordt opgenomen. Door de scope van de BIA te bepalen zoals het momenteel wordt gedaan, kan het voorkomen dat scenario's over het hoofd worden gezien, en wel die scenario's die op elke individuele dienst beperkte impact hebben, maar door een cumulatief effect wel een significante impact hebben op de bedrijfsvoering van de organisatie als geheel.

Tekortkoming met betrekking tot welke situaties te analyseren

Ambiguïteit ten aanzien van worst-case-scenario.

- Eerder is aangegeven dat de beantwoording van de vragen gedaan wordt voor het geval van het optreden van een worst-case-scenario. Er bestaan echter geen richtlijnen omtrent het definiëren van een worst-case. Dient de BIA te worden gedaan voor een absolute worst-case, waarvan de kans van optreden buitengewoon gering is zoals bijvoorbeeld dat alle systemen niet beschikbaar zijn voor een aanzienlijke tijdsperiode, zoals een week? Of dient de BIA uitgevoerd te worden in de context van een realistische worst-case, bijvoorbeeld op basis van karakteristieken van incidenten die in het verleden plaatsvonden?
- Bij inschatting van impacts wordt een aantal dimensies die de omvang van de impact bepalen niet expliciet aangegeven en meegenomen, zoals bijvoorbeeld de omvang van de incident, tijdsduur en andere karakteristieken van het incident. Zo is bijvoorbeeld de impact op de gezondheid van medewerkers afhankelijk van karakteristieken van incidenten, hoeveel systemen getroffen zijn, de tijdsduur daarvan, maar natuurlijk ook de aard van de mensen zelf. Met name bij de impactbepaling van incidenten die leiden tot verminderde vertrouwelijkheid en integriteit van informatie wordt niet gekeken naar de omvang en de duur van het incident.



Eldine Verweij is als kwantitatief bedrijfseconoom afgestudeerd aan de Erasmus Universiteit Rotterdam en werkt als consultant en onderzoekster bij de expertisegroep Strategic Business Analysis van TNO. Haar focus ligt op onderzoek en consultancy met betrekking tot de economics van cybersecurity en kosteneffectiviteitsafwegingen binnen de informatiebeveiliging.

- Bij de schatting van impact van niet beschikbaarheid van informatie wordt doorgaans wel nagedacht over de duur en de reikwijdte van het incident. Maar helaas wordt deze vraag ook vaak verkeerd geïnterpreteerd. De vraag wordt beantwoord, ervan uitgaande dat de dienst niet beschikbaar is in plaats van de informatie. Stel dat een cyberincident ervoor zorgt dat het facturatiesysteem niet meer werkt, maar dat de informatie om tot facturatie over te gaan, nog wel beschikbaar is. Dan zou ervoor kunnen worden gekozen om de facturatie uit te stellen of om tot handmatige facturatie over te gaan. Er kan nog steeds worden gefactureerd, alleen in een lager tempo. Als de informatie om tot facturatie over te gaan, niet beschikbaar is, kan de impact veel groter zijn. Dan kan er tijdelijk helemaal niet worden gefactureerd.

Positie van een dienst in de product-life-cycle in relatie tot de BIA.

- Huidige BIA-methodieken roepen ook vragen op als het gaat om de impactinschatting voor de diensten die aan beide uiteinden van een product-life-cycle zitten. Voor de diensten die helemaal aan het begin van de life-cycle zitten kan het zijn dat de impact van optreden van incidenten nog zeer beperkt is in absolute zin. Dit kan als gevolg hebben dat er onvoldoende maatregelen worden getroffen om de dienst af te schermen. Veel productmanagers worstelen tijdens het maken van de BIA met de vraag of ze rekening moeten houden met de huidige, of de toekomstige situatie. Moet er worden gekeken naar de impact van het incident op de huidige omzet of op die van de toekomstige verwachte omzet? Dezelfde redenering geldt voor de diensten die aan de

andere kant van het life-cycle-spectrum zitten, die dus in de nabije toekomst uitgefaseerd worden.

Tekortkomingen met betrekking tot beantwoording van de BIA-vragen

Er is beperkte aansluiting van vragen op de doelstellingen en targets van de scope-verantwoordelijke.

- De vragenlijst bevat vaak vragen die eigenlijk betrekking hebben op doelstellingen die relevant zijn voor diverse verschillende organisatieniveaus. Daardoor worden bepaalde vragen door bepaalde scope-verantwoordelijken als "te ver van hun bed" ervaren, waardoor ze niet goed zelfstandig in te vullen zijn. Dit heeft als bijkomend nadeel dat men de betrokkenheid bij de BIA verliest. Zo is het, om een voorbeeld te geven, voor een dienstverantwoordelijke meestal lastig te bepalen of het optreden van één van de scenario's kan leiden tot verlies van aandeelhouderswaarde, en wat de ernst van dit verlies is. De vragen worden daarnaast door verschillende personen verschillend geïnterpreteerd, en verschillend ingevuld. Bijgevolg kunnen sommige impacts worden overschat, terwijl andere juist onderschat blijven.
- Een hiermee samenhangend aspect is dat een aantal BIA-impactfactoren specifiek gericht zijn op commerciële organisaties. Ze hebben geen algemene geldigheid. Voor een overheid zijn bijvoorbeeld verlies van omzet, verlies beurskoers en verlies van concurrentievermogen irrelevant. Ook is de lijst niet voor iedere organisatie compleet. Voor ziekenhuizen is bijvoorbeeld "patiëntveiligheid" verreweg de belangrijkste impactfactor, maar die komt in de lijst van BIA impactfactoren niet voor.
- Tot slot is het voor scope-verantwoordelijken vaak lastig om zich iets concreets voor te stellen bij wat het betekent als vertrouwelijkheid, integriteit of beschikbaarheid van informatie het gecompromitteerd is. Dit zijn vage begrippen, waarbij niet iedereen hetzelfde beeld heeft.

Expertise en middelen om impact te kwantificeren ontbreken.

- Ook voor de vragen die beter in lijn liggen met de doelstellingen en targets van de scope-verantwoordelijke, geldt dat de scope-verantwoordelijken het moeilijk vinden om de impact van verschillende scenario's te kwantificeren. Welk percentage klanten zou weggaan als een scenario optreedt? Wat is de hoogte van onvoorziene kosten die ermee zijn gemoeid?
- Doordat de scope verantwoordelijke onvoldoende kennis of data voorhanden heeft om impact van scenario's te berekenen worden deze vragen meestal op basis van buikgevoel beantwoord. Een voorbeeld is reputatieschade als gevolg van "gelekte" klantgegevens. De gedachte die scope-verantwoordelijken hebben is vaak: "imagoschade door in het nationale nieuws te komen zal wel tot veel schade voor de business leiden". Soms komt dat buikgevoel met de realiteit overeen, maar in vele gevallen ook niet. Vaak wordt vergeten dat de grootte van impact niet statisch is, maar dat de nieuwswaarde van cyberincidenten en daarmee de impact op reputatie in de loop van de tijd afneemt. Ook is er sprake van de zogeheten "beschikbaarheidsheuristiek". Dat wil zeggen dat mensen geneigd zijn om een situatie te beoordelen op basis van gegevens die in hun geheugen beschikbaar zijn. Daardoor laten ze zich gemakkelijk leiden door recente informatie, en laten ze na te zoeken naar oudere of minder vlot beschikbare informatie, of na te denken of de situatie voor hen wel relevant is. Een voorbeeld van het laatste zijn DDoS-aanvallen die in het nieuws komen, waardoor dit als een groot risico wordt gezien, ook door bedrijven die nauwelijks schade zullen ondervinden door een DDoS-aanval.

Samenvatting

Het bepalen van de impact die een bepaalde dreiging kan hebben op de business is een belangrijk onderdeel van risicomanagement. De stap in het risicomanagement-proces waarin deze impact wordt bepaald is de Business Impact Analysis (BIA). Aan de BIA zoals die tegenwoordig in de meeste organisaties wordt uitgevoerd kan nog veel verbeterd worden. Zo is er bij degenen die de BIA uitvoeren vaak te weinig zicht op de belangen van hogere of aanpalende organisatieniveaus, met het gevolg dat belangrijke risicoscenario's over het hoofd worden gezien. Daarnaast worden dimensies als reikwijdte en tijdsduur van een incident vaak achterwege gelaten en leidt het vaststellen van een worst-case-scenario tot ambiguïteit. Tot slot is het bepalen van de impact van incidenten niet eenvoudig. Niet alleen door het ontbreken van data, maar ook door het feit dat er vaak een discrepantie bestaat tussen de scope van de verantwoordelijke persoon en de impactsoort, denk aan een IT-specialist die moet beoordelen wat de impact is van een data-breach op de aandeelhouderswaarde van een onderneming. De geconstateerde tekortkomingen resulteren in mogelijk onjuist ingeschatte impacts van cyberdreigingen, met het gevaar dat enerzijds werkelijk relevante risico's over het hoofd worden gezien en anderzijds loopt men het risico om te investeren in onnodige veiligheidsmaatregelen.

Volgende maand zal in deel 2 van dit artikel worden ingegaan op manieren om de geconstateerde tekortkomingen aan te pakken.

VERSLAG

PRIVACY SECURITY CAFÉ

Volgens de The Hague Security Delta kan Nederland onderscheidend zijn op gebied van privacy- en databescherming. Onze digitale infrastructuur en nieuwe privacywetgeving zijn randvoorwaarden voor een veilige datahaven waar men veilig (internationaal) data kan versturen, bewaren en beschermen. Wat de impact is van onze nieuwe privacywetgeving, is het thema dat werd besproken met drie experts op gebied van privacy bij de Haagse Hoge School, locatie Dutch Innovation Center te Zoetermeer.

Vier maal per jaar organiseert Trust in People het Security Café. De editie van 17 maart 2015 werd bij Haagse Hoge School / Dutch Innovation Factory te Zoetermeer georganiseerd. In het expertpanel: Jeroen Terstegge, partner bij Privacy Management Partners en voorzitter van de commissie Privacy VNO-NCW en MKB Nederland, Rob van der Veer, principal consultant bij Software Improvement Group en Jurgen van der Vlugt, IT auditor bij het Internationaal Strafhof.

Europa, maar Nederland in het bijzonder, staat lijnrecht tegenover privacy wetgeving in Verenigde Staten. Het Safe Harbour convenant tussen VS & Europa repareert die verschillen blijkbaar onvoldoende. De perikelen rondom de NSA in de afgelopen jaren heeft pijnlijk duidelijk gemaakt waar de grenzen worden opgezocht. Onze nieuwe privacywetgeving wordt straks ook ons internationaal speerpunt.

Nederlandse bedrijven worden als eerste met de gevolgen van deze nieuwe wetgeving geconfronteerd. Wanneer deze wetgeving van kracht is, is deze nog niet binnen elk bedrijf geïmplementeerd. Vooral de meldplicht met een boete van 5% van de groepsomzet, zal bij moederbedrijven met decentrale autonome organisaties in de markt angst inboezemen. Daar is voor de toezichthouder namelijk geld en media-aandacht te halen. Vanuit het toezicht is te verwachten dat ziekenhuizen en multinationals de eerste bezoeken kunnen verwachten n.a.v. incidenten die wel in de media staan, maar niet zijn gemeld.

Gerco Kanbier is directeur van Trust in People – the information protection company.

Hij is te bereiken via gerco.kanbier@trustinpeople.com

Een medewerker kan een intern incident melden bij het CBP en eenvoudig een bedrijf te gronde richten

In Nederland zit wel weer een stukje 'buitenland', namelijk het Internationaal Strafhof waar deze nieuwe wetgeving niet van kracht zal zijn. Dat wil niet zeggen dat er geen aandacht is voor privacy. Integendeel, het beschermen van gegevens over getuigen, verblijfplaatsen en beschermingsprogramma's zijn vaak – letterlijk – van levensbelang, aldus Jurgen van der Vlugt. Bij het Internationaal Strafhof is privacy een primair bedrijfsbelang en is het geen papieren tijger of compliance vraagstuk.

Voor het opslaan van persoonsgegevens moet er doelbinding zijn. Vooral doelbinding zoals de klant die ook verwacht. Je kan dus niet zonder toestemming bankgegevens verkopen aan derden voor ander doeleinden dan het beheren van je bankrekening. In de praktijk wordt dit vaak met algemene voorwaarden op gelost, zodat je - juridisch gezien - toestemming hebt gegeven voor andere doeleinden. Zo is Facebook gewoon eigenaar van jouw gegevens. Nu gaat wetgeving in Nederland niks veranderen aan Facebook, maar Europa kan het knap lastig maken voor internationale organisaties met veel persoonsgegevens over Europeanen & Grieken.

Er is overigens in de wetgeving wel een verschil tussen 'gegevens over mij' en 'van mij', aldus Jeroen Terstegge. In beide gevallen kun je als persoon bij een organisatie een verzoek indienen om gegevens over jou op te vragen. Vervolgens kun je ook een verzoek indienen om deze data te vernietigen (m.b.v. formulier Bits Of Freedom). Het vernietigen van data is alleen verplicht als het gegevens betreft 'van mij'. Anders is de organisatie eigenaar van de data en kan deze zelfstandig besluiten of dit verzoek wordt gehonoreerd.

Maar hoe zit dat als je op kleine onderdelen niet voldoet aan die wetgeving? Geldt die boete dan ook? In het MKB is vaak geen privacy-officer aangesteld. Op de back-up staan altijd wel persoonsgegevens die ik formeel moet vernietigen. Een leverancier heeft geen geldige bewerkingsovereenkomst. Een lek is gedicht, maar de mogelijke slachtoffers zijn niet op de hoogte gesteld.

Netwerken en applicaties worden periodiek gemonitord door een onafhankelijke partij. Dat er kwetsbaarheden gevonden worden, wil niet per se zeggen dat je ook een incident hebt gehad. Toch stelt de nieuwe wetgeving voor dat je dit soort kwetsbaarheden ook moet melden omdat er misbruik van gemaakt kan zijn, aldus Jeroen Terstegge.

Over kwetsbaarheden gesproken, een software-foutje is zo gemaakt volgens Rob van der Veer. Hij maakt dagelijks mee dat kwaliteit van software niet een vanzelfsprekendheid is. Afhankelijk van de data die de software beschermt, is dit in meer of mindere mate belangrijk voor de privacybescherming.

Een andere uitdaging is vooral voor overheden die een voorbeeldfunctie hebben eigen wetgeving toe te passen en te handhaven. Een Privacy Impact Analyse brengt natuurlijk die verplichte onderdelen in kaart, maar wat is de risicotolerantie? Iedere afwijking leidt tot een boete? De impact hiervan is nogal verschillend per organisatie, hoeveelheid data en type persoonsgegevens. De maatregelen – privacy by design - vereisen vaak een enorme investering. Ik kan mij voorstellen dat een Internationaal Strafhof privacy toch serieuzer neemt dan de eerste de beste webwinkel.

De overlap tussen 'vertrouwelijkheid' uit informatiebeveiliging en voldoen aan privacywetgeving is vaak in twee aparte functies belegd, te weten de privacy-officer en security-officer. Dat is niet efficiënt en een dubbele belasting voor de organisatie als er analyse en onderzoek gedaan moet worden. Daarom is het verstandig de functie van informatiebeveiliging uit te breiden met het risico niet voldoen aan (privacy-)wetgeving.

Links

Security Cafe: http://www.trustinpeople.com/security-cafe

TIME-TRUSTED

The Attributer and his wife enjoy watching television for relaxation and they often watch 'detective' programmes. Recently one such programme focused on a plot that revolves around knowing what time it really is. It served as a reminder that this aspect of security is as important today as ever it was, even though it's an old and well-known theme. If you can fool someone about what the time is, then you can dupe him or her in so many different ways.

In this television story there was a young man who suspected that his father's alleged suicide was in fact murder and that one of his family was to blame, but he could not determine which one was guilty. He had followed his father's footsteps as a scientific inventor and so he announced that he had invented a time machine that would enable him to travel back in time to investigate what happened when his father died. The machine was literally a lot of 'smoke and mirrors' – blue electric sparks arcing between huge shiny steel balls, dry ice vapours blown around by noisy whirring electric fans, flashing lights, a control panel with banks of switches and dials, and so on. Very theatrical – you get the idea I'm sure.

The family dismissed him as a lunatic, firstly because of his belief that his father had been murdered when there was 'evidence' of suicide, and secondly because of his ridiculous claim to having built a time machine. So, he needed to demonstrate that his machine worked. His demonstration was to travel into the future, not into the past, but if someone could be persuaded that he had succeeded, then maybe it would flush out the culprit, who would then believe that traveling back to the murder scene would be possible.

The house had many clocks in it, and he arranged that the demo would begin at just before twelve noon. When the time came he entered the drawing room to call the family and the amateur detective together in his laboratory. He switched on the time machine, quite frightening them all with the noise and smoke. He emerged from the cloud of smoke with a sealed envelop saying that he had travelled forward in time and had written down the names of the three winning horses in the twelve o'clock race – first, second and third places. He then switched on the radio to listen to the race in real time, and when the winners were announced, he asked the detective to open the envelope. Sure enough, the three winning horses were written on the paper.

Well, it rather spoiled the story for the Attributer because it was such an old trick used in fraud of many kinds, but the Attributer's wife was suitably puzzled. What he had done was to set all the clocks in the house back by enough minutes for him to find out the results of the race, but not so much time as for the others to notice the time difference. The radio was a disguised tape recorder with the race commentary captured from about seven minutes earlier.

Any forensic investigation involves establishing a time line – the logical sequence of events that surround the specific event being investigated. Who was where and when? In what sequence did things happen? Would certain hypotheses fit with this established time line? Trusted time is critical in such investigations. All important transactions and actions in a digital computing world are time/date stamped for exactly this purpose. It is assumed that such time/date stamps are accurate, but if someone tampers with them, or resets the reference clock by which you compare them, then the logical sequence is disrupted in a way that can be exploited by the wrongdoer.

This tells us once again that SABSA Attributes profiling is a powerful tool for setting requirements. If you do not capture all the investigation requirements in detail, then you have little hope of establishing the truth. And yes, the ploy did work – one of the cousins panicked and fled.

The Attributer

PRIJSUITREIKING ARTIKEL VAN HET JAAR OP 21 APRIL 2015

2e prijswinnaar Frans Kersten

3e prijswinnaar Raoul Vernède


Vertrekkend redacteur/ex-hoofdredacteur André Koot

HOE VEILIG IS MIJN '*AANDEEL*'?

Productdetails

Titel: Hoe veilig is mijn 'aandeel'?
Subtitel: Het borgen van reputatie vertrouwen & continuïteit met Maturing Business Information Security (MBIS)
Auteur: Yuri Bobbert
Voorwoord: prof. Dr. Hans Mulder (Antwerp Management School)
Taal: Nederlands
Aantal pagina's: 544
ISBN: 978-90-9028711-9

Het boek is meer een onderzoekmanuscript en reflectie van tien jaar werken en onderzoeken in het werkveld informatiebeveiliging. En dan vooral in het werkveld informatiebeveiliging gezien vanuit de business en de meerwaarde die informatiebeveiliging moet brengen voor die business om succesvol te zijn.

In het boek wordt de actiegerichte onderzoeksmethodiek toegepast en die sprak mij erg aan. Actiegericht onderzoek of 'action research' dient twee doelen. Ten eerste als middel om te komen tot verandering en ten tweede om kennis te genereren. Kortom de opgedane kennis direct in de praktijk brengen om meerwaarde te geven aan het vakgebied.

Omdat informatiebeveiliging geen ICT-zaak is maar een business-zaak, wordt in het boek gepleit om een afdeling databescherming op te richting. Deze afdeling rapporteert op een zelfde manier naar directie en bestuur als de afdeling financiële administratie. Om dit rapporteren mogelijk te maken zijn er kerntallen nodig. Deze kerntallen of Reputatie-Vertrouwen-Continuïteit-score (RVC-score) geeft uitdrukking aan de actuele performance, de mate van volwassenheid, van organisaties op het gebied van hun business-information-security en zal benchmarking mogelijk maken.

Dit boek doet onderzoek om te komen tot deze RVC-score.

Het boek bestaat uit drie, eigenlijk vier delen.

Deel 1 geeft de theoretische grondbeginselen.

Deel 2 brengt de theorie uit deel 1, via diverse casussen bij bedrijven en instituten, in de praktijk.

Deel 3 geeft conclusies naar aanleiding van de theorie die in de praktijk is gebracht en een visie, een richting voor managers, bestuurders en toezichthouders.

Deel 4 bevat de onderzoeksresultaten en bronvermeldingen die de delen 1, 2 en 3 onderbouwen.

In het theoretische deel geeft de auteur zeven aanbevelingen, hoe deze zeven aanbevelingen tot stand komen en waarom ze nodig zijn, onderbouwt de auteur.

Deze zeven aanbevelingen zijn:

1. Identificeren van toepassing zijnde wet- en regelgeving.
2. Uitvoeren van risico- en impactanalyses om de implementatie (en kosten) van maatregelen te verantwoorden.
3. Pas relevante normen (industriestandaarden) toe.
4. Betrek het management direct bij de business impact, in die maatregelen niet worden genomen.
5. Verhoog het alertheidsniveau (bewustwording)
6. Het inrichten en operationaliseren van een "meet-en-bewaak"-cyclus. Dit meten en bewaken moet niet enkel op procesachtige KPI's zijn maar ook op techniek en de factor mens.
7. Onderhouden van kennis en competenties (op alle niveaus in de organisatie)

Ronald van Erven. Ronald is senior (technology) risk manager informatiebeveiliging, bedrijfscontinuïteit en privacy bij Timeos Pensioendiensten en bereikbaar via rvanerven@icloud.com of 06-15584056.

Boekpresentatie

Op 28 november 2014 werd dit boek gepresenteerd in het College Hotel in Amsterdam.

Impressie van de boekpresentatie: https://youtu.be/9uJ_BscuV5I
Interview Prof. Dr. Mulder (schrijver van het voorwoord): https://youtu.be/nlsbAXIfCyo

Deze zeven aanbevelingen of uitgangspunten zijn in het tweede deel in de praktijk gebracht bij financiële instellingen, overheden, gezondheidsinstellingen, woningcorporaties, media- en hotel bedrijven.

Tot slot deel drie: deze kerntallen of Reputatie-Vertrouwen-Continuïteit-score (RVC-score) geeft uitdrukking aan de actuele performance, de mate van volwassenheid, van organisaties op het gebied van hun business-information-security. Het zijn de bovengenoemde zeven aanbevelingen die tot de RVC-score moet leiden. Hier zijn diverse tools al voor op de markt, onder andere de securi-meter. Aan de hand van deze RVC-score in relatie tot toenemende afhankelijkheden van de geautomatiseerde informatievoorziening en cybercrime moeten een bestuur inzicht geven over hun plaats in het "informatie-risico-spectrum" en hun investeringen voor de te nemen informatiebeveiliging maatregelen in te schatten. Daarmee brengt de auteur informatiebeveiliging in de business en de bestuurskamer.

Al met al een interessant boek voor iedereen die meer diepgang wil in informatiebeveiliging vanuit de business, hoe je het in de bestuurskamer brengt en meetbaar kan maken.

We zijn er nog lang niet qua informatiebeveiliging en het is continu een afweging tussen kosten, werkbaarheid en risico's. Maar deze afwegingen worden in de bestuurskamer gemaakt. De informatiebeveiligings-professional moet vooral zin handen uit de mouwen steken, nieuwsgierig, gretig en creatief zijn en blijven.

Onthoud daarbij het volgende:

"Dare to dream, but especially dare to do"
- Mark Vogt

"Stay hungry, be foolish and connect the dots"
- Steve Jobs

Zodra jij als informatiebeveiliging-professional dit verliest, ben jij in dit vak verloren.

Achter Het Nieuws

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

IN-FLIGHT 'ENTERTAINMENT'

Chris Roberts, een beveiligingsonderzoeker, heeft naar eigen zeggen een vliegtuig zijwaarts laten vliegen [1]. Als resultaat is hij van een vlucht gehaald en zijn zijn computers in beslag genomen. Zo op het eerste gezicht lijkt dit een geval van 'shoot the messenger'. Chris wijst de FBI op kwetsbaarheden in vliegtuigen via het in-flight entertainment-systeem. Is Chris een held, of heeft hij zichzelf en zijn medepassagiers in gevaar gebracht door een vliegtuig tijdens een vlucht te hacken? Chris beweert dat de motoren te besturen zijn vanaf het in-flight netwerk. Wat vindt de redactie daarvan?


Lex Borger


Jan Willem Koopman


Maarten Hartsuijker

Maarten Hartsuijker

Ethische hackers vervullen een belangrijke rol in de informatiesamenleving. Ze houden ons scherp en schromen veelal niet om de vinger op de pijnlijke plek te leggen. Ze herinneren organisaties niet zelden aan vergeten onderwerpen en/of aan serieuze kwetsbaarheden die over het hoofd zijn gezien. Vaak is dit waardevol. Je kunt beter over kwetsbaarheden geïnformeerd worden door iemand met goede bedoelingen, dan dat je door een incident met je neus op pijnlijke feiten wordt geduwd. Maar een middel mag natuurlijk nooit erger zijn dan de kwaal. Als het werkelijk zo is dat deze hacker met risico voor de passagiers van de vlucht een punt heeft willen maken, dan is het niet vreemd dat hier wordt ingegrepen.

Toch begrijp ik wel een beetje dat deze beveiligingsspecialist zijn punt heeft willen maken. Iedereen die op veiligheid test weet dat een sprekend voorbeeld makkelijker tot actie leidt dan een theoretisch risico. Zelf ben ik bij tests van connected-car-omgevingen lekken tegengekomen waarmee je bijvoorbeeld vanuit Nederland de auto van een developer al toeterend door Silicon Valley kon laten rijden. Prachtig voor awareness-sessies, maar zo'n grapje is natuurlijk geen ongeluk waard.

Wanneer je als onderzoeker weet dat dit soort kwetsbaarheden bestaan en er geen actie op wordt genomen dan snap ik dat je op een gegeven moment de grenzen opzoekt om de impact van kwetsbaarheden te illustreren. Want hoe zou je je voelen als iemand op een gegeven moment een vliegtuig laat neerstorten door misbruik te maken van kwetsbaarheden die jij 5 jaar eerder al bent tegen gekomen? Maar een lijnvlucht met passagiers op 10km hoogte als demo gebruiken…. Nee, dat lijkt mij niet de plek om de gevolgen van kwetsbaarheden in in-flight-systemen aan te tonen.

Jan Willem Koopman (gastbijdrage)

Jan Willem Koopman is Security Lead Delivery bij Capgemini.
Ik denk dat Chris zichzelf en zijn medepassagiers in gevaar heeft gebracht. Vooropgesteld dat hij inderdaad via het Inflight Entertainment System connectie heeft gemaakt met het Flight Management Control System. Aviation-experts geven in sommige commentaren aan dat deze systemen niet gekoppeld zijn en Chris zelf zegt in het huiszoekingsbevel van de FBI [2] dat hij niet gekoppeld heeft en dat de tweets misleidend waren. Ik denk dat de FBI juist heeft gehandeld. Wel moet gezegd worden dat Chris een punt heeft met betrekking tot de security van IoT in het algemeen en beveiliging van vliegtuigen in het bijzonder. Vliegtuigen worden niet meer mechanisch bestuurd maar middels "flight by wire". Het flight-control-system bestaat eigenlijk uit computers en deze dienen als zodanig beschermt te worden met security-in-depth-maatregelen. Dat Boeing en Airbus niet in het openbaar reageren, geeft te denken. Dit kan betekenen dat Chris gelijk heeft en vliegtuigen hackable zijn met vrij eenvoudige middelen. Beter zou het zijn als zij zich transparanter zouden opstellen. Daarnaast ligt er voor de keurende instanties en overheid een schone taak om cyber-security-normen te ontwikkelen voor vliegtuigen en andere computer-controlled-devices en deze te certificeren.

Lex Borger

Er zitten een paar moeilijke kanten aan dit verhaal. Dit kan aangedikt zijn. De vraag is dan wie het heeft aangedikt. De FBI? Dat zou kunnen duiden op onbegrip bij de inspecteur of het hebben van verborgen motieven om iets anders te verhullen of aan het licht te brengen. Of is het Chris? Heeft hij interessant willen doen in de aanloop naar de RSA-conferentie en is de leugen met hem weggelopen? Dan krijg je zoiets als een gevallen ster. Niet goed voor het imago van de security-onderzoeker in het algemeen…

Echter, als de FBI gelijk heeft, is er een soort Catch-22 patstelling: kan een security-onderzoeker zo stom geweest zijn om tijdens een vlucht zo actief in te grijpen in het verloop van de vlucht? Zelfs passieve verkenning zou blokkering van commando's tot gevolg kunnen hebben, met desastreuze gevolgen. Dit gaat verder dan menig responsible-disclosure-beleid toelaat.

Aan de andere kant is het dan wel belangrijk dat het goed gemeld wordt en er ook serieus op geschakeld wordt. Winn Schwartau dringt hier op aan [3]. Toch zie ik nog geen luchtvaartmaatschappij de in-flight-entertainment stil leggen. United probeert de aandacht af te leiden door hackers voor andere zaken te belonen [4]. Al met al zorgelijk om te denken wat een passagier met zelfmoordneigingen en hackvaardigheid zou kunnen doen.

Links

[1] Link: http://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/
[2] http://aptn.ca/news/wp-content/uploads/sites/4/2015/05/warrant-for-Roberts-electronics.pdf
[3] http://www.phibetaiota.net/2015/05/winn-schwartau-airlines-in-cyber-panic-plus-robert-steele-comment/
[4] http://www.huffingtonpost.com/2015/05/16/united-million-miles-hackers_n_7298292.html

COLOFON

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

PvIB
Platform voor InformatieBeveiliging

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

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

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

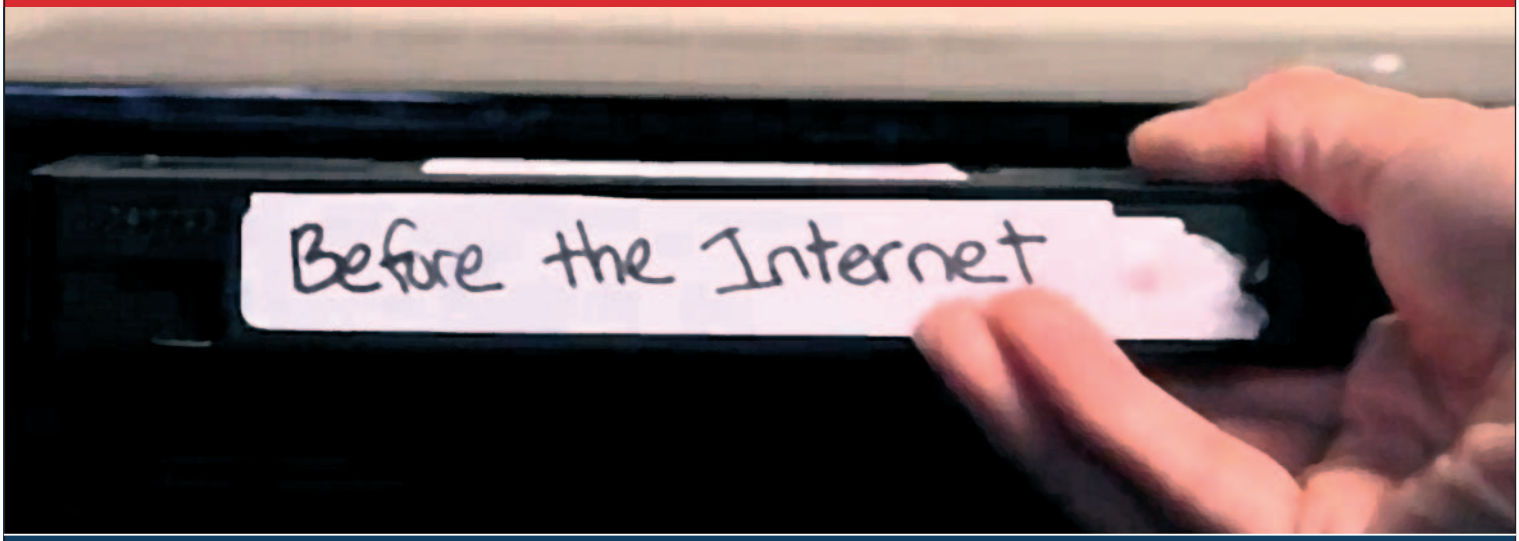
VORMGEVING EN DRUK
VdR druk & print, Nijkerk
www.vdr.nl

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

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

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

ISSN 1569-1063



LEKKER ONHANDIG, DAT INTERNET

Mij werd laatst de vraag gesteld over de pre-internet periode. Je zou denken dat dit een periode is die een paar generaties terug gaat, maar niets is minder waar. Als je in Nederland twintig jaar geleden internet gebruikte dan was je een pionier op dit gebied. In die tijd kreeg ik bijvoorbeeld een instructie van vijfendertig A4-tjes mee om mijn PC voor te bereiden, mijn modem in te stellen en de gegevens van mijn provider in te stellen. Met een beetje geluk kon je toen na twee uurtjes zweten het internet op. Een bijzonder trage verbinding was genoeg om die dingen te bekijken die je wilde bekijken.

Zoeken was een kwestie van creatief zijn want Google was nog in oprichting. Het zoeken was sowieso de beroemde speld in de beruchte hooiberg; er waren nog maar weinig bedrijven met een site. En als ze die al hadden, was het vaak niet meer dan een gedigitaliseerde folder. Interactie met een potentiele klant was niet mogelijk. Met een telefoonnummer en een postadres was het wel klaar.

Ik heb in deze rubriek vaker uitgelegd dat we toentertijd geen enkel vermoeden hadden hoe verstrekkend de gevolgen van deze ontwikkeling zouden zijn en ik wil graag eerlijk zijn: ondanks het feit dat ik beroepsmatig vaak met internet bezig ben, heb ik nog steeds geen idee waar we uiteindelijk terecht zullen komen. De ontwikkeling van internet blijft niet zonder gevolgen. Grote veranderingen bij V&D, de banken en andere voorbeelden heb ik hier wel eens voorbij laten komen. Kijk eens kritisch om je heen en je ziet veel meer voorbeelden van veranderingen die het straatbeeld of je gedrag hebben aangepast. De postbode brengt op de zaterdag alleen nog een bonusfolder van AH, de folderbezorger brengt folders rond met een sticker erop om maar naar folders.nl te gaan om je folders als eerste te lezen. Deze jongen moet binnenkort ook een nieuw baantje zoeken. De bandenboer wil graag dat ik mijn afspraak elektronisch plan en ook bij de huisarts (die zijn winterbanden liet vervangen) ging een lampje branden. "Lijkt mij een strak plan." zei hij en dacht daarbij: "Dit scheelt me weer een assistente."

De belastingdienst stuurt me geen blauwe envelop meer; ik hoef alleen maar een aantal gegevens te accorderen. Niet leuk, wel makkelijk. Het waterbedrijf stuurt de acceptgirokaarten niet meer, maar stuurt je een mail, of je zelf de betaling even wilt regelen. Oh ja, het is wel duurder dan een automatisch incasso. "Waarom eigenlijk?" denk ik dan. Het waterbedrijf hoeft toch niets extra's te doen?

Internet heeft zo veel impact dat de generatie na ons zich afvraagt hoe je vroeger een huisje kon huren. "Belde je ze dan gewoon?" Of: "Waarom heb jij nog een krant, papa?" Allemaal zaken die voor ons vanzelfsprekend waren, maar het nu niet meer zijn. Waarom heb ik eigenlijk nog een krant? Ik heb een paar voorbeelden willen noemen waaruit blijkt dat er niet alleen consequenties zijn op het gebied van werkgelegenheid.

Zo benijd ik de mensen die geen computer hebben, of erg onhandig zijn in het gebruik daarvan niet. Een telefoonnummer zoeken zonder internet? Het boeken van je vliegreis of camping verblijf? Kaartjes voor dat concert? Vergeet het maar zonder computer. Ik wil daarmee aangeven dat je min of meer gedwongen wordt om je zaken op internet te regelen. Dit geldt dus ook voor die groep die er niet handig in is. Hackers vinden met name die laatste groep ideaal want deze groep heeft ongetwijfeld dat eenvoudige wachtwoord, is eenvoudig te overtuigen om inloggegevens af te staan en raakt al snel onder de indruk van je prachtige website die echter niet datgene doet wat de bezoeker verwacht. De bezoeker staat op het punt de wasmachine te bestellen maar zal vervolgens de was nog lang met de hand moeten doen.

Berry

Secure Link
Infrastructure Security Solutions

Gezocht! Security Engineers

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

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

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

Kom jij ons team versterken?

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

Go Secure!

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