07/2012

INFORMATIE BEVEILIGING

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 7 - 2012

INFORMATIEBEVEILIGING OOK ONZE EIGEN ZORG

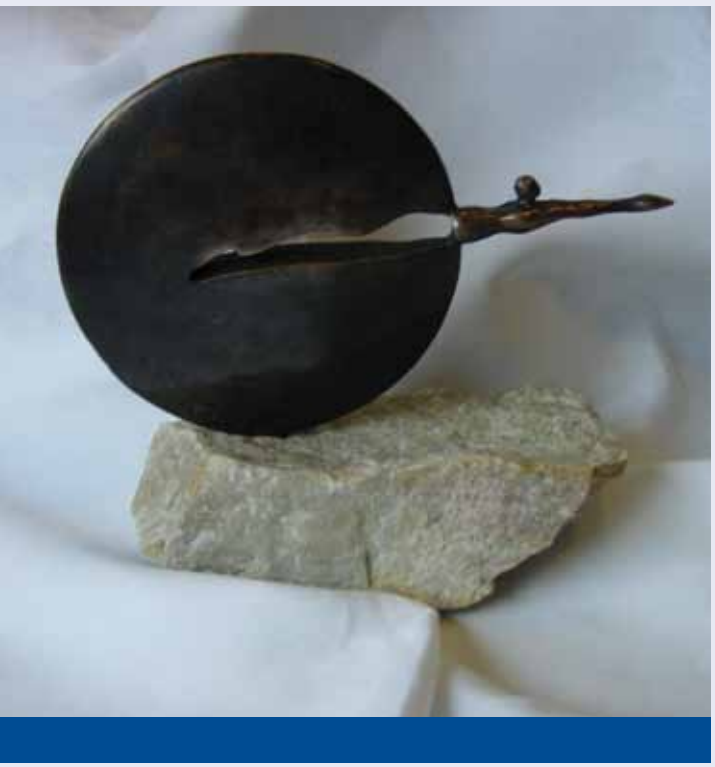
KWANTIFICATIE VAN HERLEIDBAARHEID

WAT IS EEN CERT OF CSIRT?

HOE GOOGLE WEET WAT WIJ NIET VERTELLEN

JOOP BAUTZ INFORMATION SECURITY AWARD 2012

Het PvIB feliciteert Jan Willem Beusink van harte met het winnen van de Joop Bautz Information Security Award. Wij wensen hem veel succes voor de toekomst.



IMF
INTERNATIONAL MANAGEMENT FORUM

Cloud Security (CCSK)

CCSK™ Certificate of Cloud Security Knowledge

De 2-daagse training leidt op voor het wereldwijd erkende Certificate of Cloud Security Knowledge (CCSK) van de Cloud Security Alliance (CSA)

CCSK is de eerste leveranciersonafhankelijke Cloud Security certificering ter wereld. De certificering is ontwikkeld door CSA en ENISA.

CISSP Compact Training

Deze intensieve compacte CISSP training leidt in 5 dagen op voor het officiële CISSP examen van (ISC)2

Deze Engelstalig CISSP Compact Training bestaat uit 5 dagen klassikale training. Ter voorbereiding op deze klassikale training start u met een online studie met volledige Engelstalige mentoring, support en virtual classrooms. Na afloop van de klassikale training krijgt u toegang tot exclusieve web-based testvragen ter voorbereiding op het CISSP examen.

U kunt u ook voorbereiden op het CISSP examen d.m.v. de unieke Nederlandstalige schriftelijke CISSP cursus of de uitgebreide 11-daagse CISSP training.

Meer informatie en inschrijven?
www.imf-online.com/partner/pvib

VOORWOORD

Het is weer die tijd van het jaar: de budgetrondes en de security-shows komen er aan. Over de security-shows hoef ik weinig te vertellen, dat bereikt jullie wel via andere kanalen, inclusief de advertenties in dit blad. Met de budgetrondes zelf mag ik mij niet bemoeien, maar in het vooruitzicht van een nieuwe crisis en wellicht ook een nieuwe regering, voel ik me toch zo vrij om er wat opmerkingen over te maken, vanuit verschillende perspectieven:

Concern: De maatschappij is in rap tempo aan het veranderen. Verwachtingen van medewerkers en klanten verschuiven. Natuurlijk moeten we ons daar niet gek door laten maken, maar we moeten ook niet onze kop in het zand steken. Veel bedrijven hebben nog beleidsraamwerken en risicoinstrumenten die complex zijn om uit te voeren en veel tijd en aandacht vergen. Hoe sneller de samenleving wordt, hoe meer we simpele, effectieve meetinstrumenten nodig hebben om daar effectief mee te kunnen sturen. Cycli worden korter, wie daar niet in mee kan gaan valt buiten de boot. Kijk eens naar het instrumentarium en pas het aan. Het zou ook nog wel eens goedkoper kunnen worden!

Business units: Business-ICT-alignment is cruciaal aan het worden. ICT is al lang niet meer het middel waarmee de back-office effectiever en efficiënter wordt gemaakt, businessketens gebruiken geavanceerde ICT. Investeer in beveiligers die dit begrijpen, hierin kunnen meebewegen en de afstemming met de ICT-leverancier (intern of extern) aan kan gaan. Het is belangrijk inzicht te hebben in de risico's die hiermee aangegaan worden en het eens te zijn dat dit risico's die het waard zijn genomen te worden - en waarom. En valideer alle aannames met metingen - ICT is bezig met security monitoring. Sluit daarop aan en vertaal de uitkomsten naar business belangen.

ICT: De thema's die op de beveiligers afkomen zijn consumerization, BYOD, toepassing van mobiele technologie, cloud. Menig security-event gaat over deze onderwerpen. Ze zijn niet te stoppen, dus geef ze een expliciete plaats in het beveiligingsplan. Reserveer budget voor verkenning van deze thema's - ook als ze nog niet aan de orde zijn. En verken ze risk-based. ICT hoeft niet alle bedreigingen te voorkomen - maar wel die met het grootste risico. Ga dus risk-based te werk. ICT moet ook inzicht kunnen geven en kunnen ingrijpen: Security monitoring en incident response hoort ingericht te zijn en actief geoefend te worden.

Operationele omgeving - de "werkvloer": Hier worden de kosten gemaakt, maar hier wordt het ook mogelijk gemaakt dat er geld verdiend wordt. In de laatste jaren is informatiebeveiliging aardig meegenomen in de kaasschaaf. Het gevolg is dat er minder beveiligingsspecialisten op de werkvloer staan, dat er meer beveiligingswerk direct bij operationele mensen komt te liggen. Deze trend is op zich niet erg, het toont aan dat beveiligingsdenken een commodity wordt. Aan de operationele managers wil ik wel meegeven dat dit dan wel het moment is om te investeren in de kennis en kunde van operationeel personeel op dit gebied.

Budgetaanvraag ingediend? Geniet dan van de security-shows…

Lex Borger, hoofdredacteur

INHOUDSOPGAVE

Foto omslag: CC by Esparta

INFORMATIEBEVEILIGING OOK ONZE EIGEN ZORG

Auteur: Leon van der Krogt is als IT-architect op het gebied van informatiebeveiliging werkzaam bij het UMCG voor de afdeling ICT Beleid. Vanuit wetgeving, landelijke ontwikkelingen en eisen vanuit de business werkt ICT Beleid aan een passende architectuur voor een veilig elektronisch patiëntendossier. Leon is te bereiken via l.van.der.krogt@umcg.nl.

De onderlinge samenwerking en beleidsafstemming tussen de universitair medische centra (UMC's) vindt plaats via de Nederlandse Federatie van Universitair Medische Centra (NFU). De NFU heeft als algemene doelstelling het behartigen van de gezamenlijke belangen van de UMC's. Daartoe ontwikkelt de federatie gemeenschappelijke beleidsvisies en standpunten op alle terreinen die de acht UMC's aangaan. Vrijwel alle algemene ziekenhuizen, alsmede categorale instellingen in Nederland, zoals astmacentra, audiologische centra, kankercentra, radiotherapeutische instituten, revalidatiecentra en dialysecentra zijn verenigd in de Nederlandse Vereniging van Ziekenhuizen (NVZ). De NVZ is primair gericht op de collectieve behartiging van zorginhoudelijke, sociale en economische belangen van de leden. De NVZ streeft ernaar voor de leden zodanige kaders te scheppen dat ziekenhuizen alert en flexibel kunnen inspelen op (veranderingen in) de vraag naar zorg.

In de Nederlandse ziekenhuizen heeft iets heel bijzonders plaatsgevonden. Alle ziekenhuizen in Nederland hebben een audit voor informatiebeveiliging ondergaan tegen dezelfde norm op basis van een vastgesteld kader. Nergens in de wereld is dit eerder zo uitgevoerd. Hiermee dachten we een mooi verhaal te hebben waarbij ziekenhuizen zich goed kunnen vergelijken en van elkaar kunnen leren. Maar de resultaten waren bij nadere bestudering toch onvoldoende vergelijkbaar. In dit artikel zal uiteengezet worden wat hier van de oorzaak is maar ook wat we kunnen doen om wel vergelijkbare resultaten te krijgen. Het CIO-platform heeft een tool ontwikkeld die een goed vergelijkbaar inzicht in uw informatiebeveiliging mogelijk maakt. De methodiek en de tool worden ook hieronder besproken.

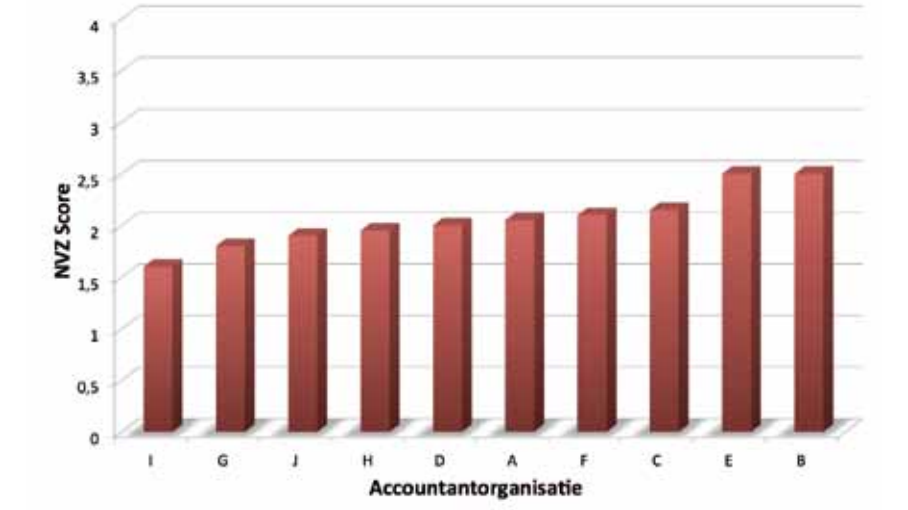
De ene auditpartij scoort gemiddeld altijd hoger dan een andere auditpartij

De leden van het CIO-platform [1] hebben de behoefte om van elkaar te leren op onder andere het gebied van informatiebeveiliging. Om te komen tot vergelijkbare resultaten van informatiebeveiligingsaudits moet er gebruik gemaakt worden van een zelfde referentie en scope. Ondanks het gebruik van dezelfde norm en scope bleken de resultaten niet vergelijkbaar. Dit leidde in 2008 tot de opdracht om met expertise uit het werkveld te werken aan een oplossing. De werkgroep analyseerde de problematiek en constateerde dat de kwaliteit van een audit bepaald wordt door een aantal samenhangende aspecten waaronder het auditproces, de middelen en de auditor. De werkgroep constateerde dat het proces en de middelen vast te leggen zijn en dat de variabele factor bepaald wordt door de auditor. Verder analyserende blijkt dat de norm zo abstract is, dat deze op meerdere manieren te interpreteren is. Ondanks de vakbekwaamheid van auditors blijkt in de praktijk dat elke auditor een eigen vertaling heeft van de(zelfde) norm die gebruikt wordt om een organisatie te toetsen. De aanpak van een audit blijkt niet uniform gestandaardiseerd.

In 2009 is door de inspectie voor de gezondheidszorg gevraagd een integrale audit op basis van de NEN7510 [2] uit te voeren binnen de ziekenhuizen. De reactie daarop was dat het wel erg kostbaar zou worden om de hele NEN7510 te toetsen. Bovendien zegt het niets over het benodigde beveiligingsniveau. In reactie op dit commentaar heeft de Nederlandse Vereniging van Ziekenhuizen(NVZ) een handreiking laten samenstellen van de meest belangrijke beheersmaatregelen uit de norm NEN7510. Deze beheersmaatregelen zijn gebundeld als "toetsingskader NVZ" en beschikbaar gesteld aan de ziekenhuizen.

Met dit toetsingskader heeft elk ziekenhuis een externe audit laten doen. De resultaten zijn door de NVZ anoniem samengevoegd met behoud van de naam van de auditpartij. Deze resultaten toonden aan dat het gebruik van een zelfde vragenlijst toch leidt tot significante verschillen. Ondanks dat het geen wetenschappelijk onderzoek was, zijn de conclusies wel dat de ene auditpartij gemiddeld altijd hoger scoort dan een andere auditpartij. Hierdoor kan een organisatie bewust kiezen voor een bepaalde auditpartij als deze goed zou willen scoren... Dit onderzoek bevestigde dat het hanteren van dezelfde vragenlijst door verschillende personen toch nog leidt tot

verschillende resultaten. Ook een extern onderzoek [3] toont aan dat er kwaliteitsverschillen zijn bij grote accountantsorganisaties. De methodiek en de tooling lost niet alle onvolkomenheden in de auditwereld op maar levert een bijdrage aan de verbetering van de kwaliteit (zie figuur 1).



Figuur 1: Gemiddelde score per accountantorganisatie

Benchmark

De CIO Interest Group Informatie Beveiliging (CIG-IB) is als werkgroep vanuit het CIO Platform Nederland actief met betrekking tot informatiebeveiligingsonderwerpen. Na het succesvol opleveren van de toolkit awareness informatiebeveiliging voor haar leden, is de werkgroep gestart met het onderwerp benchmark informatiebeveiliging. Benchmark is het onderling kunnen vergelijken van de stand van de informatiebeveiliging van de organisaties die lid zijn van het CIO Platform Nederland. Binnen de CIG-IB is de werkgroep Benchmarking samengesteld om een benchmarkmethodiek te ontwikkelen en een bijpassende tool te selecteren.

8 UMC's

Het nut van benchmarken heeft zich bewezen bij de acht academisch medische centra(UMC) die al in 2005 begonnen met het meten van het informatiebeveiligingsniveau en de resultaten met elkaar vergeleken. De rapportage van de benchmark maakt inzichtelijk op welke aspecten de ene UMC verder is dan de andere. Het doel is dan ook dat de organisatie die goed scoorde, de kennis deelt met de organisatie die minder scoorde op het zelfde aspect. Hierdoor wordt niet telkens het wiel opnieuw uitgevonden en ontstaat er een basis van best practices.

Niet telkens het wiel opnieuw uitvinden

Ook op bestuurlijk niveau heeft de benchmark een positief effect. Elke-bestuurder ziet de resultaten van zijn organisatie ten opzichte van de andere UMC's die anoniem zijn weergegeven. Informatiebeveiliging komt hierdoor makkelijker op de bestuursagenda en de rapportage rechtvaardigt het budget voor het uitvoeren van het informatiebeveiligingsplan.

Methodiek en tooling

De ervaring die de UMC's hadden met benchmarking is ingebracht bij de werkgroep CIG-IB en samen met informatiebeveiligers van de leden van het CIO-platform zijn we aan de slag gegaan om de benchmarkmethodiek te verbeteren en vast te stellen zodat er gezamenlijk draagvlak is voor deze methodiek.
De werkgroep heeft voor de benodigde tooling een pakket van eisen opgesteld maar de markt bleek op dat moment nog niet een tool te kunnen bieden die aan de eisen kon voldoen. Via het CIO-platform is een bedrijf met veel belovende Young IT Professionals gezocht die het platform voor benchmarking in een korte tijd konden bouwen. Een van de winnaars van het StrICTly for Business [4] event 2009 heeft de opdracht aangenomen en met zijn bedrijf een platform voor benchmarking neergezet dat voldeed aan de hoge eisen van beveiliging en functionaliteit.

40 Top100-bedrijven

De leden van het CIO-platform hebben toegang tot het benchmark platform en 40 bedrijven zijn aan de slag. De leden hebben zelf direct inzage in hun resultaten ten opzichte van de gemiddelde resultaten van de andere deelnemers.

Omdat de resultaten van de benchmark anoniem zijn, kunnen deze worden gebruikt om algemene conclusies te trekken en deze weer te presenteren binnen het CIO-platform. Zo kan het algemeen gemiddelde informatiebeveiligingsniveau van bedrijven in Nederland worden getoond maar ook de verschillen tussen de branches onderling. Hieruit kunnen heel gericht nieuwe CIO-platformprojecten worden geïnitieerd.

100 Ziekenhuizen

Per 1 mei kunnen ook de leden van de Nederlandse Vereniging voor ziekenhuizen aan de slag. De ziekenhuizen zitten in een eigen branche op het benchmark platform. Speciaal voor de zorg is de norm NEN7510:2011 volgens de benchmark methodiek omgezet en beschikbaar gesteld via het benchmark platform. De zorg heeft nu de beschikking over de ISO27002 en de NEN7510.

CIO-platform methodiek vragenlijsten en antwoorden

Eigenlijk zijn er twee methodieken die gecombineerd het platform voor benchmarken vormen. De eerste methodiek heeft tot doel vragenlijsten en antwoorden te standaardiseren. De tweede methodiek is de vergelijking van deze lijsten en antwoorden en de daaruit voortvloeiende rapportage en beveiligingsstructuur.

Om zo dicht mogelijk tegen de norm te blijven is gesteld dat de beheersmaat-

regel uit de norm ontleed wordt naar deelmaatregelen. En door deze deelmaatregelen in stellingen uit te drukken gaan we uit van de ultieme situatie.
De standaard antwoorden zijn afgestemd op het type beheersmaatregel. Deze antwoorden zijn door COBIT [5] vastgesteld in een matrix die bestaat uit de typeringen:

- Bewustzijn en communicatie
- Beleid, plannen en procedures
- Tools en automatisering
- Vaardigheden en expertise
- Verantwoordelijkheid en verantwoording
- Doelstellingen en resultaatmetingen

Het doel van deze standaard antwoorden is het vinden van het meest passende antwoord en vervolgens het betreffende volwassenheidsniveau te kunnen vaststellen.
In het voorbeeld is letterlijk de beheersmaatregel 12.3.1 weergegeven. De stelling 12.3.1.1 is samengesteld op basis van de hiervoor beschreven methodiek en getypeerd als "Beleid, plannen en procedures" (zie kader 1).

De kracht van de methodiek zit in de eenvoud. De stellingen worden samengesteld met in achtneming van de "aandachtspunten en aanbevelingen voor implementatie" zoals in de norm beschreven. Dankzij de volwassenheidsmethodiek zijn de antwoorden niet meer een simpel "ja of nee" maar vertegenwoordigen de fase waarin de beheersmaatregel is ingevoerd. Hierbij zie je dat de basis ligt in plan, do, check en act (PDCA). Waar het uiteindelijk om gaat is het periodiek controleren of de beheersmaatregel nog afdoende is om het risico te dekken. In de praktijk zie je dan ook dat bij invoer van een nieuw systeem aan alles gedacht wordt maar eenmaal in productie er geen aandacht meer is voor de geldende beheersmaatregelen. Omdat het deelnemen aan het platform voor benchmarking ook een jaarlijkse trigger geeft, blijft de aandacht om periodiek de beheersmaatregelen te (laten) toetsen.

De resultaten van een benchmark worden pseudoniem verwerkt en anoniem gerapporteerd

Uitgangspunten
Binnen de werkgroep CIG-IB is een aantal uitgangspunten benoemd waaraan de methodiek invulling moet geven. Deze aspecten zijn uitgewerkt in de "methodiek voor benchmarking CIO-platform" en ondersteund met de "BMTool, platform voor benchmarking".

Compliancy
Blijf zo dicht als mogelijk bij de norm om te kunnen spreken van "compliant". Om de Compliancy te borgen worden beheersmaatregelen uit de norm ontleed naar deelgebieden. Per deelgebied wordt een stelling neergezet die uitgaat van de optimale situatie. Bij het beantwoorden van de stelling moet aangegeven worden in hoeverre deze optimale situatie benaderd is op het moment van audit. De volledige norm is door experts uit het werkveld ontleed naar deelgebieden en voorzien van stellingen. De stellingen zijn gereviewd en vastgesteld. Het gehele veld gebruikt dezelfde versie. In de tooling wordt versiebeheer geborgd zodat een benchmark alleen kan plaatsvinden met dezelfde stellingensets.

Traceerbaarheid
Zowel het antwoord als de persoon die dit antwoord heeft bepaald, moet traceerbaar zijn om bij een "peer review" de argumentatie te kunnen achterhalen of te onderbouwen.
De traceerbaarheid wordt geregeld door elk antwoord te voorzien van naam, datum en tijd. In de tooling is geregeld dat dit onweerlegbaar wordt vastgelegd.

Volwassenheid beheersmaatregel
De mate van invoering bepaalt de werking van een beheersmaatregel.
Alles maakt een groei door. Dus ook beheersmaatregelen zijn niet van de ene op de andere dag 100% werkend. We noemen dit de volwassenheid van de beheersmaatregel. De antwoorden vertegenwoordigen dan ook de mate van volwassenheid van deze beheersmaatregel.

12.3 Cryptografische beheersmaatregelen

Doelstelling:
Beschermen van de vertrouwelijkheid, authenticiteit of integriteit van informatie met behulp van cryptografische middelen.

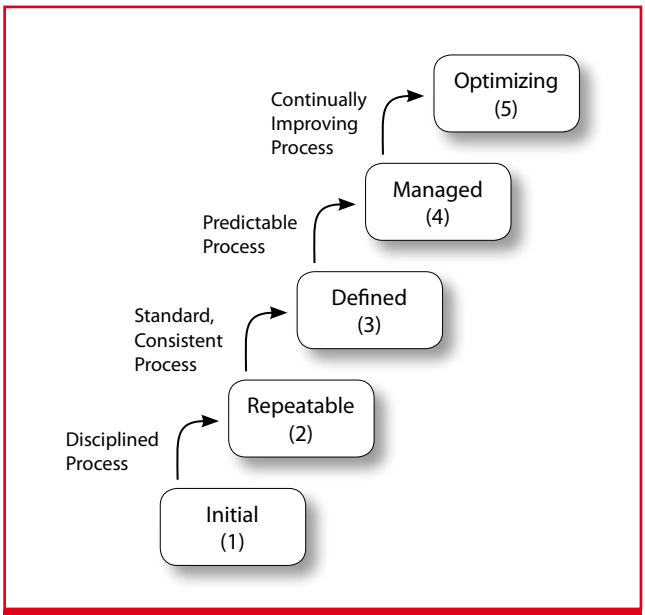
12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen.

Beheersmaatregel
Er behoort **beleid** te worden **ontwikkeld** en **geïmplementeerd** voor het gebruik van **cryptografische** beheersmaatregelen voor de **bescherming van informatie.**

12.3.1.1 Stelling:
Er is beleid ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.

Type: Beleid, plannen en procedures

Kader 1: Voorbeeld beheersmaatregel



Figuur 2: CMM niveaus van COBIT

Figuur 3: Wie ziet wát?

Objectieve antwoorden
De antwoorden moeten gestandaardiseerd zijn.
Hierdoor kan alleen nog discussie ontstaan over de keus van het antwoord. Voor het standaardiseren van de antwoorden is gekozen voor het CapabilityMaturityModel(CMM) van COBIT [6]. Hierin zijn 5 antwoordniveaus gedefinieerd waarbij elk niveau een bepaalde volwassenheid vertegenwoordigt. Zie figuur 2.

Aantoonbaarheid
Elk antwoord moet worden voorzien van argumentatie hoe de auditor tot dit antwoord gekomen is.
De naam, datum, tijd en de argumentatie zijn als één aan elkaar gekoppeld. Binnen de tool is geregeld dat een verwijzing naar documenten opgenomen kan worden. Ook bij een volgende audit kan deze argumentatie weer gebruikt worden om de beheersmaatregel efficiënt te toetsen.

Internationaal erkend
De methodiek moet optimaal gebruik maken van internationale standaarden. De te toetsen norm kan wel een eigen (branche)norm zijn maar de kracht komt voort uit het gebruik van internationale standaard normen. Elke norm is om te zetten naar de benchmark methodiek. Eenmaal omgezet voor deze methodiek kan de norm door iedereen gebruikt worden om te kunnen benchmarken.

Beveiliging
De resultaten van een benchmark worden pseudoniem verwerkt en anoniem gerapporteerd.
De tooling zorgt voor de logistieke en veilige afhandeling van de audit, de rapportage en de samenstelling van de benchmark.

Branches
Voor alle branches geldt dezelfde methodiek. Om ook branches onderling te kunnen vergelijken wordt de methodiek over branches heen hetzelfde toegepast. Alleen zo kunnen vergelijkingen gemaakt worden van dezelfde normen over verschillende branches. De methodiek is bruikbaar voor verschillende normen maar alleen dezelfde normen kunnen vergeleken worden.

De basis ligt in plan, do, check en act

Beveiliging van het benchmarkplatform
De Benchmark tooling is beveiligd volgens de stand van de techniek.
Voor het verwerken van bedrijfsgegevens heb je een betrouwbaar systeem nodig. Binnen de werkgroep is een prototype in Excel gemaakt maar al snel waren de grenzen van beheersmatigheid bereikt. Een toolselectie van bestaande tooling leverde niet het gewenste resultaat. Het CIO-platform heeft de tooling laten bouwen volgens de specificaties.
Vanzelfsprekend is het benchmarkplatform beveiligd op alle niveaus.
De informatie is versleuteld net als de communicatie met het benchmarkplatform. Bij het toevoegen van informatie aan een benchmark of het veranderen van instellingen kan alleen de eigenaar van die informatie met een geldig SMS-token. De verwerkte informatie wordt altijd versleuteld.

CIO-platform methodiekrapportage en beveiligingstructuur
Rapportages worden automatisch gemaakt en zichtbaar zodra een vierde organisatie de resultaten toevoegt aan de benchmark. Rapportages worden alleen gemaakt van de cijfermatige antwoorden. Deze antwoorden worden pseudoniem op het niveau van de branche gebruikt om een benchmark te tonen aan de deelnemende organisatie binnen de branche. Deelnemers zien dus alleen hun eigen resultaten ten opzichte van de benchmark van de deelnemende organisaties.
De uitwerking(argumentatie bij een

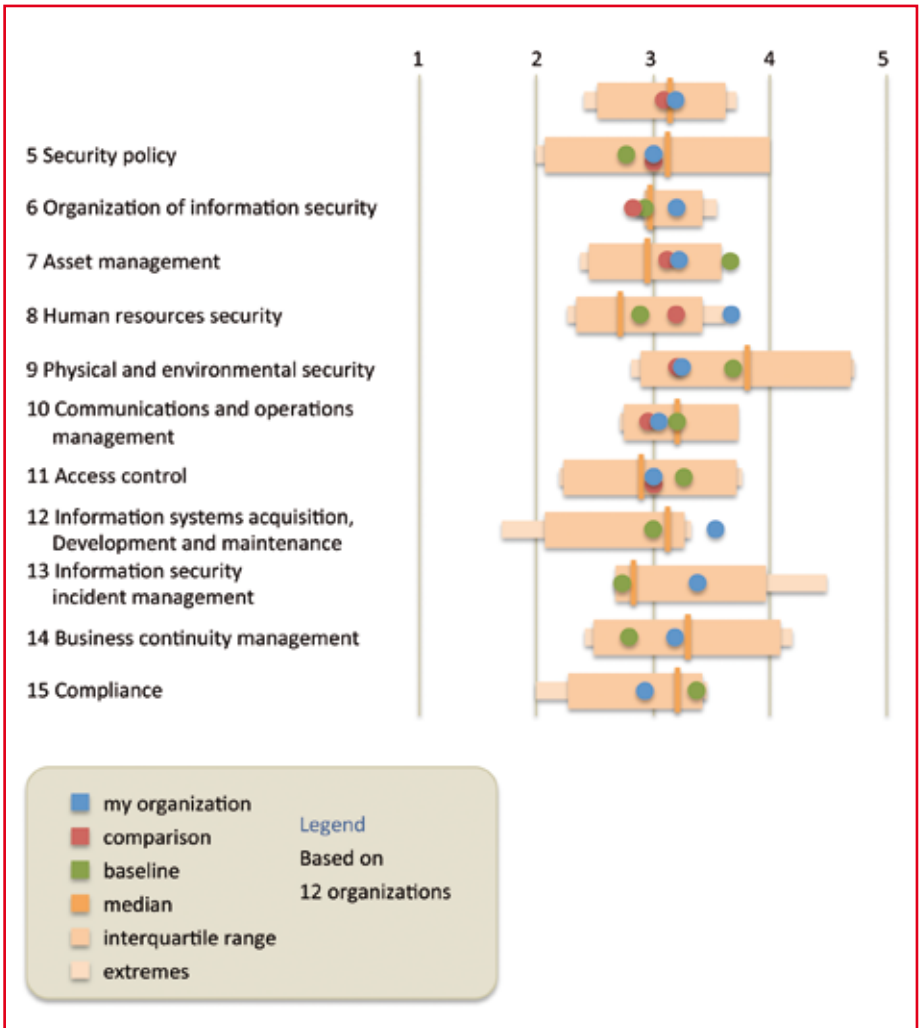
antwoord) is alleen zichtbaar binnen een organisatie. Wil een organisatie de resultaten op inhoud vergelijken met een andere organisatie, dan wordt via de "dating service" via het benchmark platform de beide organisaties met elkaar in contact gebracht. Vergelijking van branches in een benchmark is altijd volledig anoniem (zie figuur 3).

Voorbeeld van een benchmarkrapportage

Figuur 4 toont de resultaten van de benchmark zoals de organisatiemanager deze ziet op het moment dat de resultaten(blauw) zijn toegevoegd. De resultaten zijn zichtbaar ten op zichten van de baseline(groen) en resultaten van een eigen vorige audit(rood). Op de achtergrond zijn de resultaten van de andere organisaties zichtbaar. In dit plaatje zijn het de resultaten van 12 organisaties zichtbaar. De baseline vertegenwoordigt de risicoanalyse, het niveau dat minimaal vereist is om het risico af te dekken. De resultaten in deze benchmark zijn uit de testomgeving en dus volledig willekeurig.

Platform voor benchmarking

De eerste van de BMTool is in vijf maanden gebouwd door een Young IT Professional bedrijf en getest door het veld. Een mooie klus als je bedenkt dat het aanmeldproces volledig is geautomatiseerd en de toegang via SMS-token geregeld wordt. De hosting wordt extern verzorgd via het CIO-platform. Het CIO-platform heeft de hosting uitbesteed aan externe partijen die in opdracht van het CIO-platform natuurlijk geaudit zijn, inclusief een penetratietest en code review. Jaarlijks wordt door de leden bepaald of het platform nog voldoet en welke functionaliteit er bij moet komen. Het platform voor benchmarking is gebouwd voor de leden van het CIO-platform maar ook niet-leden van dit platform kunnen profiteren van benchmarken. Het CIO-platform heeft ook een maatschappelijk doel en heeft bepaald dat het platform voor benchmarking ook buiten de leden om beschikbaar gesteld mag worden, maar dan wel in een gescheiden omgeving. De bouwers van het platform voor benchmarking hebben een eigen platform beschikbaar gemaakt waarbij de resultaten in ieder geval uitwisselbaar zijn.



Figuur 4: Benchmarkrapportage

Eindnoten

[1] *http://www.cio-platform.nl/*

[2] *Norm voor informatiebeveiliging in de Zorg*

[3] *AFM: kwaliteit accountantscontrole Big Four moet fundamenteel beter*

[4] *http://strictlyforbusiness.nl/*

[5] *http://www.securitycn.net/img/uploadimg/20070831/cobit4.0_en.pdf*

[6] *Framework for IT Governance and Control is ontwikkeld door Information Systems Audit and Control Association(WWW.ISACA.ORG)*

Bronvermelding

Normen
http://www.nen.nl

CMM COBIT matrix
http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf

Benchmark tool voor leden van CIO-platform Nederland
http://www.cio-platform.nl/bmtool

Benchmark tool voor niet leden
http://www.bmtool.nl

KWANTIFICATIE VAN HERLEIDBAARHEID

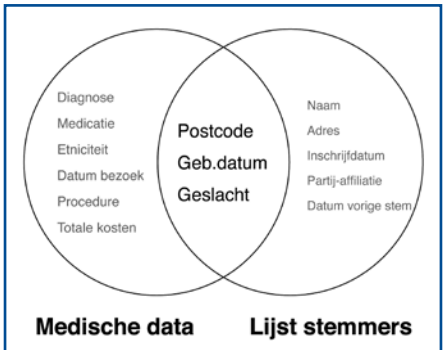
Matthijs R. Koot is als ethisch hacker werkzaam bij Madison Gurkha. Hij is op 27 juni 2012 aan de Universiteit van Amsterdam gepromoveerd op het proefschrift "Measuring and Predicting Anonymity". Dit artikel beschrijft enkele resultaten van dit onderzoek en verscheen eerder in het tijdschrift Privacy & Compliance. Matthijs is inzake dit artikel te bereiken op koot@uva.nl.

Elke ontwerpbeslissing die resulteert in betere bescherming van privacy kan worden aangeduid als Privacy by Design. Daarbij kan het gaan om het ontwerp van IT-systemen, maar ook om de opzet van onderzoek en enquêtes waarbij gegevens over personen worden verwerkt. Privacy by Design kan bijvoorbeeld zijn gebaseerd op het principe van gegevensminimalisatie: verwerk uitsluitend gegevens die noodzakelijk zijn voor het beoogde doel, en geen andere gegevens. De Wet bescherming persoonsgegevens (Wbp) maakt dit principe expliciet.

Het is ook mogelijk om verwerking van 'persoonsgegevens' in juridische betekenis uit te sluiten. De Wbp stelt dat elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon een persoonsgegeven is. Welnu, gegeven een database met gegevens over personen: welke aanpassingen zijn nodig zodat er niet langer sprake is van 'geïdentificeerd' of 'identificeerbaar'? Het verwijderen van persoonsgebonden nummers, namen en adressen uit een bestand leidt waarschijnlijk al snel tot opheffing van 'geïdentificeerd'. Maar wanneer is ook niet langer sprake van 'identificeerbaar'? Eén gedachte is dat gegevens niet langer identificeerbaar worden geacht wanneer deze alleen met *onevenredige inspanning* zijn te herleiden tot personen. Wanneer sprake is van *onevenredige* inspanning, dan is afhankelijk van de aard (medisch, financieel, justitieel, etc.) de misbruikwaarde van de privacygevoelige informatie lager dan de kosten. In een wereld van toenemende gegevensverwerking waarbij gegevens op steeds nieuwe manieren toegankelijk worden, moet worden aangenomen dat wat vandaag onevenredige inspanning kost, in de nabije toekomst mogelijk slechts *evenredige inspanning* gaat kosten. Kortom, dat het voor kwaadwillenden mogelijk rendabel wordt gedeïdentificeerde gegevens tot natuurlijke personen te herleiden. Het fenomeen datalekken en gerelateerde berichtgeving in de media mag worden opgevat als indicatie dat als gevolg van miserabele informatiebeveiliging, de mogelijkheden voor kwaadwillenden om gegevens te kunnen herleiden via gegevensdiefstal toenemen. In zekere zin is de uitspraak "attacks only get worse" van bekende IT-beveiliger Bruce Schneier hier ook van toepassing.

Sweeney en *k*-anonimiteit

Eind jaren '90 heeft de Amerikaanse onderzoekster Latanya Sweeney voor een gedeelte van de populatie van Massachusetts uitgezocht hoe herleidbaar die is via demografische informatie. Sweeney bleek records in een publiek beschikbare geanonimiseerde medische dataset te kunnen herleiden tot natuurlijke personen door de data op bepaalde demografische gegevens te koppelen met een niet-anonieme dataset van stemgerechtigden die zich hadden ingeschreven om te kunnen stemmen (zie figuur 1). De geanonimiseerde gegevens raakten hierdoor 'gedeanonimiseerd'. Gezien de triviale herleidbaarheid van de medische data was in feite in beginsel al geen sprake van anonimiteit, en mag dus eigenlijk niet van 'anonimiseren' worden gesproken. Nauwkeuriger is te spreken van 'de-identificeren' en 'heridentificeren'. Een combinatie van kolommen die tot heridentificatie kan leiden wordt 'Quasi-IDentifier' (*QID*) genoemd.



Figuur 1: Heridentificatie via overlappende kolommen

Als oplossing voor het probleem van heridentificatie bedacht ze '*k*-anonimiteit'. In dat model wordt vereist dat een dataset vóór publicatie een toets doorstaat: elke combinatie van waarden in de QID-kolommen *moet* ten minste *k* keren in de dataset voorkomen. Is dat niet het geval, dan dient de data via 'generalisatie' en 'onderdrukking' te worden aangepast, totdat de toets alsnog wordt doorstaan. Bij generalisatie wordt een gegeven opgehoogd: een geboortedatum wordt bijvoorbeeld vervangen door een leeftijd. Bij onderdrukking wordt een gedeelte van de data in een kolom weggelaten: bij een postcode kan bijvoorbeeld een letter worden weggelaten. Als de toets dan nog niet wordt doorstaan, kunnen beide letters worden weggelaten. Als de toets dan nog niet wordt doorstaan, kan weer worden gekeken naar generalisatie: de postcode vervangen door een plaats- of gemeentenaam, bijvoorbeeld.

Nota bene: Het model van *k*-anonimiteit is niet perfect. Dit heeft geleid tot diverse uitbreidingen op *k*-anonimiteit, elk met eigen voordelen en beperkingen. Een bespreking daarvan valt buiten het blikveld van dit artikel. Het is noodzakelijk dat bij het in praktijk nastreven van onherleidbaarheid rekening wordt gehouden met die verfijningen.

Heridentificeerbaarheid

(Her)Identificeerbaarheid kan worden uitgedrukt in termen van anonimiteit. Een definitie van anonimiteit die in het onderzoeksgebied aan belangstelling wint, luidt [1]:

"Anonimiteit is de onlinkbaarheid van een subject en een voorwerp van belang, gezien vanuit het perspectief van een aanvaller."

In de context van dit artikel vertegenwoordigt 'subject' een persoon waarover gegevens in een database staan geregistreerd; het 'voorwerp van belang' vertegenwoordigt een record over die persoon in de database; en 'aanvaller' vertegenwoordigt een model van een kwaadwillende.

De heilige drie-eenheid bij analyse van anonimiteit is dus:

- subject
- voorwerp van belang
- aanvaller

In deze conceptie heeft een claim over anonimiteit dan ook uitsluitend betekenis als aan al deze begrippen inhoud is gegeven. Een claim als "u bent anoniem" of "deze gegevens zijn anoniem" is dus betekenisloos. Een claim over anonimiteit is gebonden aan één subject, één voorwerp van belang en één kwaadwillende. Strikt genomen is aan elk record in een gedeïdentificeerde database een aparte claim over anonimiteit verbonden. De kwaadwillende wordt gemodelleerd in termen van de gegevens die tot zijn/haar beschikking staan en waarmee gedeïdentificeerde gegevens kunnen worden getracht te worden herleid tot natuurlijke personen.

> Niet identificeerbaar houdt in dat gegevens alleen met *onevenredige inspanning* zijn te herleiden tot personen

Persoonsgegevens zijn onontbeerlijk voor bepaalde terreinen van beleidsonderzoek. Een voorbeeld daarvan is het beleidsonderzoek naar patiëntenzorg in ziekenhuizen. Medio 1960 is de Landelijke Medische Registratie (LMR) opgericht [3]: een centraal archief waar ziekenhuizen kopieën van hun administratie van ziekenhuisontslagen aan verstrekken, bedoeld voor spiegelen van ziekenhuizen onderling, maar ook ten behoeve van verbetering van zorg. Ziekenhuizen kunnen vrijwillig meedoen aan die registratie, en vrijwel alle Nederlandse academische en reguliere ziekenhuizen doen er tegenwoordig aan mee. Ze sturen dan jaarlijks een kopie van hun administratie in. In de resulterende database representeert elke rij één ziekenhuisontslag. Er zijn kolommen voor NAW-gegevens en kolommen voor informatie over de behandelingen, inclusief medische diagnoses (ICD-10 codes). Het CBS beheert een kopie van de LMR-database, en onderzoekers kunnen bij CBS onder bepaalde voorwaarden toegang krijgen tot (gedeeltes van) die data. In de nabije toekomst worden de LMR en een vergelijkbare registratie over ambulante zorg geïntegreerd tot het de Landelijke Basisregistratie Ziekenhuiszorg (LBZ).

> Bij het in praktijk nastreven van onherleidbaarheid moet rekening wordt gehouden met verfijningen op het model van *k*-anonimiteit

Wat nu als een beleidsonderzoeker geen arts is, d.w.z., niet wettelijk gebonden is aan het medische beroepsgeheim? In dat geval is zal de data anoniem moeten worden gemaakt alvorens de beleidsonderzoeker er toegang toe krijgt. Het is evident dat daartoe, zoals eerder genoemd, persoonsgebonden nummers, namen en huisnummers uit de data moeten worden verwijderd. Afhankelijk van de (beleids)onderzoeksvragen zal bepaalde demografische informatie echter beschikbaar moeten blijven, zoals enige indicatie van geslacht, geboortedatum en postcodegebied.

Hoe weten we of de overblijvende demografische informatie niet leidt tot heridentificeerbaarheid? Een mogelijk antwoord hierop is: inventariseer het aantal mogelijke combinaties en tel per combinatie het aantal personen dat dezelfde informatie deelt. Deze personen zitten dan in dezelfde 'anonimiteitsgroep'. In geval van geslacht, geboortedatum en postcode is die telling in Nederland triviaal uitvoerbaar: die gegevens staan in de GBAs. En met dank aan de driejaarlijkse GBA-audit, waarbij steekproefsgewijs de juistheid van GBA-gegevens wordt gecontroleerd, neemt de kwaliteit van GBA-gegevens in principe toe.

Nederland

Recent is de empirische studie van Sweeney in Nederland herhaald met GBA-gegevens [2]. Van 16 gemeenten (zie Tabel 1) is de lijst van geboortedatum, geslacht en postcode van alle

Gemeente	Aantal inwoners
Amsterdam	766656
Rotterdam	591046
Den Haag	487582
Utrecht	305845
Nijmegen	161882
Enschede	156761
Arnhem	147091
Overbetuwe	45548
Geldermalsen	26097
Diemen	24679
Reimerswaal	21457
Enkhuizen	18158
Simpelveld	11019
Millingen a/d Rijn	5915
Terschelling	4751

Tabel 1: onderzoekspopulatie

inwoners verzameld. In totaal omvatte de onderzoekspopulatie 2.7 miljoen burgers.

Van diverse (deel)combinaties van deze GBA-kolommen is geteld hoe vaak dezelfde waarden voor kwamen; dit leverde inzicht in de groottes van anonimiteitsgroepen. Tabel 2a geeft per (deel) combinaties (*Quasi-identifier)* weer:

1. Het aantal verschillende waarden dat in de data voorkomt en een eigen anonimiteitsgroep vormt (*# of sets*)
2. De omvang van de kleinste (anonimiteits)groep (*Min.*)
3. De groepsgrootte waar de 25% kleinste groepen onder vallen (*1st Qu.*; eerste kwartiel)
4. De groepsgrootte waar de 50% kleinste groepen onder vallen (*Median*; tweede kwartiel)
5. De groepsgrootte waar de 75% kleinste groepen onder vallen (*3rd Qu.*; derde kwartiel)
6. De gemiddelde groepsgrootte (*Mean*)
7. De omvang van de grootste groep (*Max.*)

De (deel)combinaties bestaan uit:

- geboortedatum (*DoB*, bijvoorbeeld '1 januari 1970')
- geboortemaand (*MoB*, bijvoorbeeld 'januari')
- geboortejaar (*YoB*, bijvoorbeeld '1970')
- geslacht (*gender*, in de onderzoeksdata uitsluitend 'M' of 'V')
- viercijferige postcode (*PC4,* bijvoorbeeld '1098')
- volledige postcode (*PC6*, bijvoorbeeld '1098 XH')
- plaatsnaam (*town,* bijvoorbeeld 'Amsterdam')
- gemeentenaam (*municipality*, bijvoorbeeld 'Overbetuwe')

Met behulp van kwartielen kunnen uitspraken worden gedaan als: "75% van de anonimiteitsgroepen bestaat uit X of minder personen".

In Tabel 2a zien we bijvoorbeeld bij quasi-identifier *PC6* (dus: alleen de volledige postcode) dat de *Median*-waarde 35 is, dat wil zeggen: 50% van de anonimiteitsgroepen bestaat uit 35 of minder personen. De helft van de 66,883 (*# of sets*) verschillende postcodes is dus zodanig identificerend dat gedeïdentificeerde data dat die postcodes bevat herleidbaar is tot 35 of minder natuurlijke personen. Ook zien we dat de grootste anonimiteitsgroep aanzienlijk groter is: 1322 personen (een postcode in Amsterdam). En de kleinste anonimiteitsgroep is aanzienlijk kleiner: 1 persoon. Voorbeeld van een correct geformuleerde claim over anonimiteit: de anonimiteit van personen (subjecten) ten aanzien van records in een database (voorwerpen van belang) die quasi-identifier *PC6* bevat tegenover iemand die beschikt over een (voldoende volledige en nauwkeurige) database met postcodes en persoonsnamen (aanvaller) loopt uiteen van 1-anonimiteit tot 1322-anonimiteit.

Quasi-identifier:	# of sets	Min.	1st Qu.	Median	Mean	3rd Qu.	Max.
PC4	388	2	3,278	7,090	7,188	10,300	22,330
PC6	66,883	1	24	35	41	50	1,322
PC4+DoB	2,267,700	1	1	1	1	1	42
PC6+DoB	2,759,422	1	1	1	1	1	5
PC4+gender	776	1	1,652	3,536	3,594	5,151	11,730
PC6+gender	133,012	1	11	18	21	25	954
gender+YoB	221	1	5,219	14,570	12,550	19,740	25,580
gender+YoB+MoB	2,699	1	397	1,177	1,028	1,594	2,326
gender+YoB+MoB+PC4	635,679	1	2	3	4	6	40
gender+YoB+MoB+municipality	34,790	1	6	18	80	96	733
gender+DoB	71,318	1	21	40	39	54	571
gender+DoB+PC4	2,488,828	1	1	1	1	1	22
gender+DoB+PC6	2,766,475	1	1	1	1	1	4
town+gender	134	1	222	1116	20,700	3259	347,100
town+YoB	5,642	1	6	29	492	101	14,270
town+YoB+MoB	49,207	1	2	5	56	20	1,262
town+DoB	463,134	1	1	2	6	7	419
town+YoB+gender	10,492	1	4	17	264	60	7,515
town+YoB+MoB+gender	83,172	1	1	3	33	14	695
town+DoB+gender	697,875	1	1	2	4	5	226

Tabel 2a: per quasi-identifier: aantal groepen en verdeling van groepsgroottes

De tabel toont van enkele quasi-identifiers een *Min.-*, *1st Qu.-*, *Median-* en *3rd Qu.*-waarde van 1. Dat betekent dat 75% van de anonimiteitsgroepen omvang 1 heeft; anders gezegd, dat 75% van de waarden (*# of sets*) voor die quasi-identifier een natuurlijke persoon ondubbelzinnig identificeert.

Tabel 2b toont voor dezelfde quasi-identifiers het volgende:

1. Het aantal personen in groep van grootte 1 (*k =1,* dus ondubbelzinnig identificeerbaar)

Quasi-identifier:	$k = 1$	$k \leq 5$	$k \leq 10$	$k \leq 50$	$k \leq 100$
PC4	0	9	19	345	996
PC6	429	6,109	25,103	1,459,939	2,354,255
PC4+DoB	1,861,081	2,754,465	2,765,932	2,774,476	-
PC6+DoB	2,744,653	2,774,476	-	-	-
PC4+gender	4	27	103	889	2,555
PC6+gender	1,854	31,262	184,803	2,342,242	2,629,017
gender+YoB	5	14	53	250	516
gender+YoB+MoB	55	356	712	4,478	9,674
gender+YoB+MoB+PC4	137,035	279,100	2,196,950	2,774,476	-
gender+YoB+MoB+municipality	2,186	22,565	59,597	244,152	619,671
gender+DoB	2,014	14,506	40,322	1,392,622	2,725,472
gender+DoB+PC4	2,240,461	2,765,067	2,772,205	2,774,476	-
gender+DoB+PC6	2,758,578	2,774,476	-	-	-
town+gender	4	4	28	372	896
town+YoB	499	3,172	7,225	50,985	103,145
town+YoB+MoB	10,083	61,073	112,850	287,173	394,844
town+DoB	185,042	596,769	1,045,559	2,730,668	2,750,700
town+YoB+gender	1,153	7,195	16,333	102,018	150,135
town+YoB+MoB+gender	22,260	109,126	170,351	398,601	826,744
town+DoB+gender	288,409	1,029,601	1,813,559	2,750,669	2,764,050

Tabel 2b: per quasi-identifier: aantal personen in groepsgrootte k

2. Het aantal personen in groep van grootte 1 t/m 5 ($k \leq 5$)
3. Het aantal personen in groep van grootte 1 t/m 10 ($k \leq 10$)
4. Het aantal personen in groep van grootte 1 t/m 50 ($k \leq 50$)
5. Het aantal personen in groep van grootte 1 t/m 100 ($k \leq 100$)

Nota bene: de maat $k=1$, ondubbelzinnige identificeerbaarheid, is niet de enige maat die relevant is bij analyse van anonimiteit. Afhankelijk van aanwezigheid van andere informatie kan een anonimiteitsgroep verder worden gereduceerd. Een anonimiteitsgroep kan daarom ook het best zo groot mogelijk worden gemaakt. Een minimale waarde van k kan, afhankelijk van de aan- en afwezigheid van andere informatie, een bruikbare norm zijn. Om die reden zijn grotere groepsgroottes meegenomen in tabel 2b.

Amsterdam versus Terschelling

Het volgende illustreert hoe dezelfde quasi-identifier bij alle burgers in de onderzoekspopulatie ongeveer even identificerend is. Daarna zullen we een voorbeeld geven waarbij de mate van identificerendheid juist sterk verschilt.

Dit is een voorbeeld van een quasi-identifier in de Landelijke Medische Registratie:

QID_A = *geslacht + geboortejaar + geboortemaand + 4-cijferige postcode* (in tabel 2a/2b: gender + YoB + MoB + PC4)

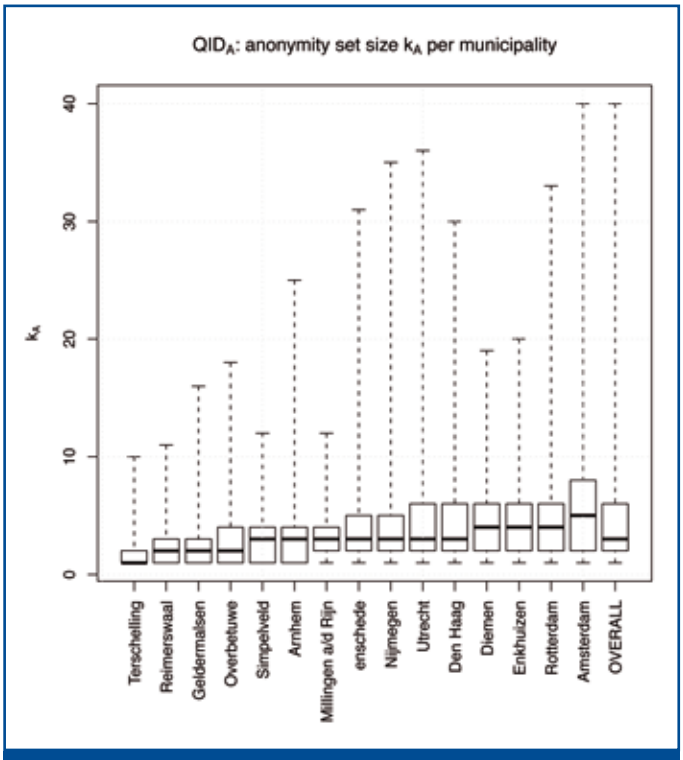
> In deze conceptie heeft een claim over anonimiteit alleen betekenis als inhoud is gegeven aan subject, belang en aanvaller

Het tellen van de grootte van anonimiteitsgroepen en het aantal groepen per grootte levert de uitkomsten op die zichtbaar zijn in Figuur 2a.

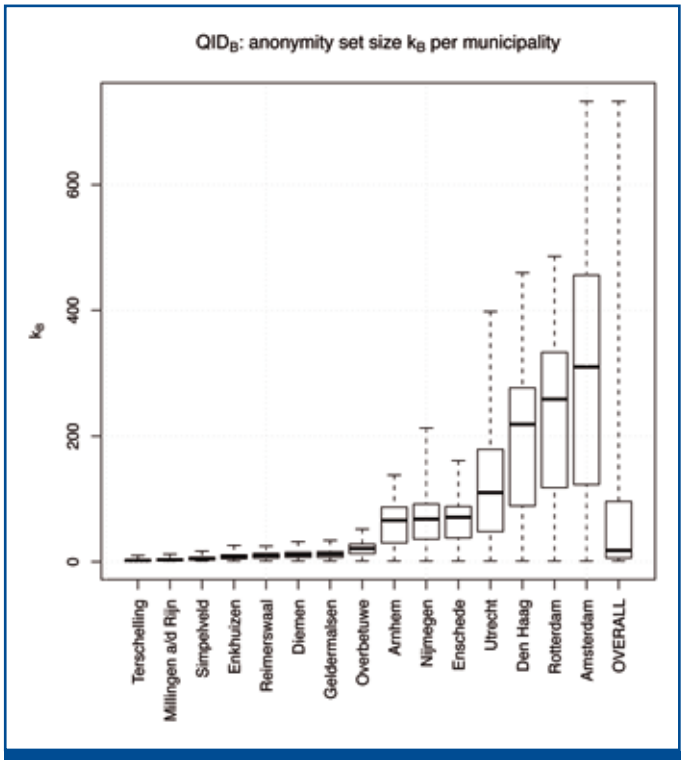
In Figuur 2a is per gemeente weergegeven wat de omvang is van de kleinste en grootste anonimiteitsgroep (de uitlopers van de stippellijn); en in de verticale rechthoeken het eerste, tweede (dikgedrukt horizontaal streepje) en derde kwartiel. We zien dat de anonimiteit van inwoners van Terschelling en inwoners van Amsterdam min of meer gelijk is: allen zitten in groepen van $k\_a < 10$, dat wil zeggen: indien een kwaadwillende beschikt over een bepaald gedeelte van de LMR en daarnaast beschikt over (toegang tot) de volledige GBA-administratie van deze gemeenten, dan kan deze de LMR-records herleiden tot 10 of minder personen.

> Inventariseer het aantal mogelijke combinaties en tel per combinatie het aantal personen dat dezelfde informatie deelt

Ter illustratie is bij de studie ook een andere database bekeken: de Bijstands Fraude Statistiek (BFS) [4]. Die database bevat informatie over onderzoek van gemeenten naar bijstandsfraude. Elk record komt overeen met één afgerond onderzoek. Er is een kolom die aangeeft of er wel of geen sprake bleek te zijn van fraude, en een andere kolom die in het eerste geval het bedrag bevat dat gemoeid is met de fraude. Uit de BFS-database is de volgende quasi-identifier gekozen:



Figuur 2a: grootte kA van anonimiteitsgroepen bij QIDA (LMR)



Figuur 2b: grootte kB van anonimiteitsgroepen bij QIDB (BFS)

QID_B = *geslacht + geboortejaar + geboortemaand + gemeentenaam*
(in tabel 2a/2b: gender + YoB + MoB + municipality)

De resultaten van die telling staan in Figuur 2b. In die figuur wordt duidelijk dat de groottes van anonimiteitsgroepen per gemeente wél (aanzienlijk) kunnen verschillen: inwoners van Terschelling zijn aanzienlijk makkelijker te herleiden dan inwoners van Amsterdam. Op basis van deze verschillen zou er bij het ontwerp van bijvoorbeeld een enquête voor kunnen worden gekozen om bij onderzoek onder inwoners van Terschelling omwille van privacybescherming bepaalde informatie *niet* te vragen die in het algemeen wél 'privacyveilig' zou kunnen worden gevraagd van inwoners van Amsterdam. Dit soort grafieken heeft ook gebruikswaarde voor het individu: die kan er beter geïnformeerde keuzes mee maken over het wel/niet prijsgeven van bepaalde informatie.

Je kunt bij een enquête kiezen om bij onderzoek bepaalde informatie *niet* te vragen op Terschelling en wél in Amsterdam

Beleid

De Stichting Perinatale Registratie Nederland hanteert de volgende richtlijn ten aanzien van niet-herleidbaarheid [5]:

2.1 Basisvereisten

Bestanden zijn 'niet-herleidbaar' wanneer tegelijkertijd tenminste aan alle van de volgende vereisten is voldaan:

a) De geboortedatum van de vrouw ontbreekt: alleen de leeftijd is opgenomen.
b) De geboortedatum van het kind ontbreekt: alleen het jaar van geboorte, alsmede de weekdag waarop de geboorte plaats vond is opgenomen.
c) Van de postcode zijn alleen de eerste drie cijfers opgenomen.

2.2 Aanvullende vereisten

Naast bovengenoemde basisvereisten dienen voor 'niet-herleidbaarheid' tevens de volgende bewerkingen uitgevoerd te worden:

a) Exacte waarden dienen zoveel mogelijk vervangen te worden door categorieën: zo dient bij tijdstippen het exacte moment vervangen te worden door een interval waarin dit moment valt, en bij geboortegewicht het exacte gewicht in grammen door een gewichtscategorie van bv. 100 gram.
b) Voor relatief zeldzaam voorkomende waarden zal specifieke 'niet-herleidbaarheid' toegepast moeten worden.

Het wordt niet alleen duidelijk welke gegevens in herleidbaarheid resulteren, maar ook welke gegevens *niet*

Bij het maken van dergelijk beleid zijn de kwantificaties zoals hierboven besproken van praktisch nut: het wordt niet alleen duidelijk welke combinatie van gegevens in herleidbaarheid resulteert, maar ook duidelijk welke combinatie van gegevens *niet* in herleidbaarheid resulteren. Zo kan besloten worden om bepaalde gegevens, mits deze van voldoende belang zijn voor de (beleids)onderzoeksdoelen, tóch te verwerken, waar deze anders vanwege twijfel niet zouden zijn verwerkt. (Dit is overigens niet bedoeld als pleidooi voor bovenmatige gegevensverwerking; verwerking van gegevens moet minimaal zijn en bovendien altijd noodzakelijk voor het doel van de gegevensverzameling; zeker bij mogelijk identificeerbare gegevens is dit een vereiste vanuit Wbp.)

Privacy by Design impliceert dat ontwerpbeslissingen zijn geïnformeerd met privacyargumenten

Conclusie

Privacy by Design impliceert ontwerpbeslissingen die (gedeeltelijk) zijn geïnformeerd met privacyargumenten. Met kwantificatie van anonimiteit kan de maker van een enquête de ontwerpbeslissing om bepaalde vragen wel/niet te stellen, of om de vraagstelling om privacyredenen af te stemmen op verschillende populaties, beter beargumenteren. Een aanvullend idee is om kwantificatie na verwerking te gebruiken om bepaalde gegevens alsnog te onderdrukken of generaliseren. Idealiter zouden burgers zelfs wellicht zélf kunnen berekenen hoe identificeerbaar ze zijn op basis van door hen verstrekte gegevens.

Dankwoord

Mijn dank gaat uit naar Guido van 't Noordende (UvA) voor het reviewen van een conceptversie van dit artikel.

Verwijzingen

[1] *Andreas Pfitzmann en Marit Hansen: "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management", documentversie 0.34, 2010 (.pdf) http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf*

[2] *Matthijs R. Koot, Guido van 't Noordende en Cees de Laat: "A Study on the Re-Identifiability of Dutch Citizens", 2010 (.pdf): http://dare.uva.nl/document/204557*

[3] *Landelijke Medische Registratie http://www.dutchhospitaldata.nl/Registraties/LMR.php*

[4] *Bijstandsfraudestatistiek http://www.cbs.nl/nl-NL/menu/themas/arbeid-sociale-zekerheid/methoden/dataverzameling/korte-onderzoeksbeschrijvingen/bijstandsfraudestatistiek.htm*

[5] *Stichting Perinatale Registratie Nederland: "Regels 'niet-herleidbaarheid'", 2011 (.docx) http://www.perinatreg.nl/uploads/76/143/Regels_niet-herleidbaarheid_versie_1_0.docx*

COLUMN

ZORGEN-DOSSIERS, HET RECHT OP NIET-WETEN EN KNUTSELEN MET PATIËNTGEGEVENS

Toen ergens in 2008 bij mij de EPD-brief op de mat viel, was een van de eerste zaken die ik deed het aantekenen van bezwaar tegen de opname van mijn medische gegevens in het EPD. Dat zal u misschien niet zo heel erg verbazen. Het bleek informatiebeveiligingstechnisch toch niet helemaal snor te zitten met dat EPD en ook maakte ik me zorgen over mijn medische privacy. Ik hoorde namelijk alleen maar jubelverhalen en weinig aandacht voor privacy en beveiliging. De bezwaren die ik voelde bleken bij de heren en dames Senatoren ook te leven en aldus zag het EPD haar parlementaire einde in 2011.

Recent mocht ik spreken op het congres over ICT & EPD van de NVMA; het was niet een gebruikelijk praatje, ik vertelde er over social media en het gebruik daarvan door medisch hulpverleners en patiënten. Uiteraard vertelde ik er ook over privacy, het gevaar van publieke medische informatie en datalekken. Maar, zoals zo vaak het geval is, bleken de meest interessante gesprekken pas later gevoerd te worden tijdens de koffie. En gek genoeg gingen die dus niet over het EPD an sich, maar wel over allerlei zaken die problematisch zijn (geworden) door de digitalisering binnen de medische sector. Terwijl ik me een weg probeerde te worstelen naar de koffiebar werd ik als eerste aangeklampt door twee dames. Zij vertelden mij over 'het recht op niet-weten', patiënten hebben namelijk het recht om – indien zij dit aangeven – juist geen informatie te krijgen over (mogelijke) ziektes. Het recht op niet-weten wordt bijvoorbeeld vaak gebruikt door personen waar binnen de familie de ziekte van Huntington, hetgeen erfelijk is, bij familieleden geconstateerd is. Huntington is een slopende ziekte met de dood als eindpunt. Uit wetenschappelijk onderzoek is gebleken dat personen die al weten dat zij het gen hebben waardoor zij uiteindelijk de ziekte zullen krijgen veel vaker ernstig depressief worden en zelfs ook vaker zelfmoord plegen. De dames vreesden dat het recht op niet-weten onder druk was komen te staan in het tijdperk waar e-Health een steeds grotere plek ingenomen heeft. Hoe moest dat recht op niet-weten immers gegarandeerd worden als een medisch dossier niet alleen online kwam maar ook altijd inzichtelijk voor de patiënt is? Daar zal vast een technische oplossing voor zijn opperde ik, maar vreemd genoeg had niemand hier echt over nagedacht.

De dames gedag zeggende werd ik alweer aan mijn arm gegrepen. Deze keer door een heerschap dat zich bezig hield met de (on)mogelijkheden van het wissen van informatie. Hij vertelde me dat het vreselijk lastig was om (informatie uit) een medisch dossier gewist te krijgen. De druk op de knop om te deleten was theoretisch gezien nog wel een mogelijkheid die aangegrepen kon worden. Maar, zo vertelde hij me, de systemen van ziekenhuizen zijn er doorgaans niet goed op ingericht om informatie echt te wissen. Als een patiënt wenst dat informatie gewist wordt, dan zou dat hele dossier gewist moeten worden en vervolgens zou een oudere versie daarvan met een back-up teruggezet moeten worden. Dat, vertelde de heer me, is iets wat ziekenhuizen echt niet gaan doen omdat het bijna onmogelijk is, duur is en veel tijd kost. Om nog maar te zwijgen over de vraag op welk moment in tijd dat dossier dan wel correct was geweest. Dat tijdstip bepalen zou beslist geen sinecure zijn.

Ik rook inmiddels de koffie, maar voor ik een kopje kon oppakken voelde ik een tikje op mijn schouder. Mag ik u even spreken over een probleem wat ik heb?, hoorde ik achter me. Ik keek om en zag een alleraardigste jongeman. Hij hield zich bezig met de technische kant van ziekenhuissystemen en was dus verantwoordelijk voor het draaiend krijgen en houden daarvan. Medisch studenten, die hun stage komen lopen in het ziekenhuis, moeten leren om te gaan met de dossiers en de ICT daaraan verbonden. Daarvoor was een mooie sandbox in het leven geroepen alwaar deze studenten zich helemaal konden uitleven. Maar eh, zo prevelde hij, nu gebruiken ze daarvoor echte data… Volgens mij mag dat niet, vervolgde hij, maar wat moet ik nu doen? Ik vertelde hem dat daar doorgaans – indien men toch echt compliant wil zijn met de wet – zogenaamde dummy data voor gebruikt wordt, zeker daar waar het gevoelige gegevens betreft. De jongeman had zelfs al een script geschreven waarmee hij de echte data kon omtoveren in dummy data. U begrijpt dat ik hem met klem adviseerde om dat aan de directie te vertellen en te bepleiten dat hij zijn scriptje mocht runnen. Enfin, het was een enerverende wandeling naar de koffiebar en u voelt hem al aankomen… Die koffie heb ik uiteindelijk nooit meer in mijn handen gekregen.

Mr. Rachel Marbus, @rachelmarbus op Twitter

WEBSHOPS BALANCEREN TUSSEN FRAUDEPREVENTIE EN OMZETOPTIMALISATIE

Maikel Lobbezoo is VP Business Development bij Adyen en verantwoordelijk voor onder meer risk management. Hij is te bereiken via maikel.lobbezoo@adyen.com

De omzet door online verkoop van producten en diensten vormt voor veel winkels en bedrijven een steeds belangrijker inkomstenbron. Volgens Thuiswinkel.org groeide deze e-commerce omzet in Nederland in 2011 met negen procent naar negen miljard euro. Een recent rapport van Cisco IBSG Economics & Research Practice schat de wereldwijde e-commerce omzet in 2015 op 1,4 biljoen dollar. Met de toename van deze online transacties groeit de kans op betaalfraude en stijgt het volume eveneens. Webwinkeliers lopen in veel gevallen de grootste risico's. Welke mogelijkheden hebben zij om hiermee om te gaan?

Wereldwijd bestaan honderden online betaalmethoden. Iedere methode beschikt over eigen kenmerken qua betaalgemak en risico. Tegelijkertijd is het voor webwinkeliers bijna geen doen om rechtstreeks relaties te onderhouden met alle leveranciers van betaalmethoden. Daarnaast zijn partijen die online betalingen willen verwerken, gebonden aan allerlei al dan niet lokale regels en wetten. De bekendste en misschien wel belangrijkste hiervan is *PCI-DDS Certified*. Deze bekende certificering is een beveiligingseis voor winkeliers en financiële dienstverleners voor het opslaan, verwerken en verzenden van privacygevoelige gegevens van kaarthouders.
Bij het gros van de e-tailers wordt het betaalverkeer daarom verzorgd door een Payment Service Provider (PSP). Deze PSP's beschikken over de vereiste certificaten en onderhouden relaties met de aanbieders van betaalmethoden. Zij nemen desgewenst de hierboven genoemde lasten rondom het betaalverkeer over en ontsluiten de betaalmethodes voor de webwinkeliers. Deze zijn vanzelfsprekend cruciaal voor e-tailers. Zij bieden hun klanten graag een breed scala aan betaalmethoden om te voorkomen dat klanten een transactie niet voltooien omdat hun betaalmethode niet beschikbaar is. PSP's faciliteren hierin en geven desgewenst advies over de voordelen en nadelen van de verschillende betaalmethodes.

Online betaalfraude

Een rapport over online betaalmethoden in 41 landen wijst uit dat credit card-betalingen internationaal erg populair zijn met een marktaandeel van zo'n 40% in de Verenigde Staten en 60% in Groot-Brittannië en in Frankrijk. In Nederland zijn iDEAL en acceptgiro's de meest gebruikte online betaalmethoden.
Bij het online betalen is het schaderisico per betaalmethode verschillend. Zo biedt iDEAL de webwinkelier wel een betalingsgarantie, maar het is voor de consument bijna onmogelijk om geld terug te vorderen als er iets mis gaat bij de levering. Daartegenover staat de creditcard- of wallet payments, zoals PayPal. Deze zijn zeer consumentvriendelijk. Klanten kunnen hun betaling binnen zes maanden na de transactie terugdraaien wanneer ze fraude vermoeden, of wanneer goederen niet geleverd worden of beschadigd zijn. De winkelier loopt hierdoor het risico dat betalingen terecht of onterecht

teruggeclaimd worden. Bij de ouderwetse factuur die ook wel 'open invoice' wordt genoemd, loopt de e-tailer het risico dat een product of dienst helemaal niet betaald wordt.
In 2011 nam het totale omzetverlies als gevolg van betaalfraude bij Europese online retailers toe tot 1,63 procent, meldt het European Online Fraud Report [1]. Het European Online Fraud Report verschijnt jaarlijks en is gebaseerd op een enquête onder Amerikaanse en Europese e-tailers, uitgevoerd door ondermeer Merchant Risk Council (MRC) Europe. Bekende voorbeelden zijn waar mensen pakketten credit card-gegevens kopen en vervolgens transacties gaan doen met deze data. Veelal verloopt zo'n proces in twee fasen. Allereerst wordt een kaart geverifieerd bij een digitale downloadsite, waarbij een kleine transactie wordt gedaan. Nadat de kaart op deze manier is geverifieerd, vindt een online aankoop plaats van fysieke goederen.
Bij open invoices kennen we het sprekende voorbeeld van de crimineel die voor iedereen in een flatgebouw een DVD bestelt en deze bij levering uit de postbussen in het trapportaal haalt om door te verkopen. De webwinkelier kan in dit geval de omzet afboeken. Hij zal het geld nooit ontvangen.

Fraudebeperking

Om goed te kunnen bepalen of er sprake is van betaalfraude moet er informatie beschikbaar zijn over de betaalhistorie van een individu of moet er andere contextuele informatie voorhanden zijn. Want door naar trends te kijken, kunnen uitschieters beter worden geïdentificeerd. Vervolgens kan er actie worden ondernomen. Er is een veelvoud aan anti-betaalfraude maatregelen beschikbaar. Aanbieders zijn de leveranciers van betaalmethoden, de banken én de PSP's. De maatregelen van de PSP's zijn vaak gebundeld in een pakket met technologische tools en parameters; de webwinkelier kan er zelf voor kiezen om ze te gebruiken of niet. Hieronder worden een aantal van de meest gebruikte technieken vanuit de PSP's besproken.
Bij betaalfraude wordt vaak een verschil geconstateerd tussen het IP-adres en het land waar de kaart vandaan komt. Dit komt omdat gestolen creditcard-gegevens via het internet gekocht worden en dus overal vandaan kunnen komen. Op basis van deze informatie kunnen transacties worden aangemerkt als verdacht en zelfs automatisch worden geweigerd. Het is aan de webwinkelier om te bepalen hoe stringent hij dit instelt. Vrijwel in alle gevallen combineert de winkelier een automatische controle met een handmatige check.

> Door naar trends te kijken, kan mogelijke fraude beter worden geïdentificeerd

Andere technieken bieden de mogelijkheid om kaarten die uitgegeven zijn in een bepaald land, of shoppers uit een bepaald land, te detecteren en vervolgens te blokkeren. Dit luistert zeer nauw omdat duidelijk moet zijn welke impact deze acties hebben op de omzet. Er moet worden voorkomen dat grote groepen welwillende klanten worden buitengesloten.
Een andere mogelijkheid om fraude te detecteren/op te sporen, is door te bekijken hoe vaak iemand een transactie doet en dit te relateren aan het 'normale' aankoopgedrag bij de e-tailer. Wanneer iemand succesvol fraude pleegt, zal deze persoon geneigd zijn het proces een aantal keren te herhalen voor maximaal resultaat. Dit kan eenvoudig worden gecontroleerd en geanalyseerd. Het werkt echter vooral in situaties waar de koopfrequentie normaal gesproken lager dan één aankoop per dag is. Bij downloadsites en gamesites is deze methode een stuk lastiger toe te passen.
Tenslotte is er nog *device fingerprinting* waarmee een profiel van een gebruiker wordt samengesteld op basis van instellingen van een mobiele telefoon, laptop of tablet. Daarbij kan worden gekeken naar de ingestelde tijdzone, lettertypes en plug-ins. Device fingerprinting kan helpen fraude te voorkomen door inlognamen te vergelijken met apparaatprofielen.

Risicobeperking

In de praktijk worden veel maatregelen nogal rigoureus toegepast. Kort gezegd staat een optie 'aan' of 'uit'. Daarnaast worden preventieve maatregelen vaak reactief toegepast, bijvoorbeeld wanneer er een incident heeft plaatsgevonden Hoe begrijpelijk het ook is, dit leidt vaak tot een situatie waarbij het middel erger is dan de kwaal. De online shop verliest de eigenlijke doelstelling van winstoptimalisatie uit het oog en richt zich vooral op het preventieve aspect. Bij veel webwinkeliers wordt gemiddeld drie procent van de transacties geweigerd op basis van de ingestelde fraudeparameters. Het 'charge back'-percentage bedraagt gemiddeld een half procent. Charge backs zijn de bedragen die webwinkeliers terug moeten storten op verzoek van klanten. Bij de drie procent geweigerde transacties bestaat een deel uit 'false positives'. Dit houdt in dat er onterecht betalingen worden geweigerd, waardoor er omzet wordt misgelopen.

Het aantal fraudegevallen zal toenemen wanneer de parameters losser worden ingesteld en er minder transacties worden tegengehouden. Het netto effect op de omzet van de webwinkelier is in de praktijk echter vaak positief. Wanneer twee procent van de betalingen geweigerd wordt en het aantal charge backs stijgt met 0,2 tot 0,3 procent, kan dit voor de e-tailer tonnen tot miljoenen extra omzet per jaar betekenen. Het vinden van de juiste balans tussen geweigerde transacties en gemiste inkomsten is geen sinecure. Het vereist maatwerk waarbij factoren als marktsegment, locatie van de webwinkelier en van de klant, betaalmethode en het gebruikte apparaat een rol kunnen spelen.

Voor deze manier van denken en handelen moet de e-tailer op een andere manier naar de data kijken. Hierin kan samenwerkt worden met de PSP, die de mogelijkheid biedt om alle parameters van het betaalsysteem gecontroleerd aan te passen. De e-tailer kan het aantal geweigerde transacties en het aantal charge backs of wanbetalers afzetten tegen gemiste omzet. Op basis van die gegevens kunnen de systemen worden aangepast en kunnen bepaalde fraudemaatregelen strikter of juist minder strikt toepast worden in plaats van een maatregel 'hard' aan of uit te zetten.

Via een A/B-test met twee verschillende fraude-instellingen kan de e-tailer na een periode van enkele weken evalueren welke optie het meest gunstige effect heeft op de omzet. Door op basis van een analyse een nulpunt te creëren, kunnen aanpassingen in de fraude-instellingen naar waarde beoordeeld worden. Deze aanpassingen kunnen worden ingegeven door toename van betaalfraude of door de wens naar omzetoptimalisatie. Na de analyse kan ingeschat worden hoe de veranderingen in de verschillende instellingen eruit moeten zien. Het effect hiervan wordt vervolgens gecontroleerd en geëvalueerd waardoor er een actief, 'lerend' model op maat ontstaat. Het biedt de e-tailer regie over de betaalrisico's en hoe hij hiermee omgaat.

> Het vinden van de juiste balans tussen geweigerde transacties en gemiste inkomsten is geen sinecure

In dit proces zou de webwinkelier een beroep kunnen doen op de Payment Service Provider, die vanuit zijn expertise op dit vlak een belangrijk adviserende rol voor de e-tailer kan spelen. De PSP ziet immers de ontwikkelingen bij de leveranciers van betaalmethoden, overkoepelend over alle klanten en vanuit nationale en internationale wet- en regelgeving.

Links

[1] *European Online Fraud Report: http://www.internetretailer.com/mobile/2012/05/31/online-fraud-fighting-takes-different-forms*

WAT IS EEN CERT OF CSIRT?

Roeland Reijers, Interim Manager, Adviseur Informatiebeveiliging en CERT expert.
Roeland heeft 15 jaar ervaring in interim management, informatie beveiliging, architectuur en incident management. De afgelopen 7 jaar heeft hij voornamelijk gewerkt voor en met CERTs en de ontwikkeling van CERTs wereldwijd. Don en Roeland hebben gezamenlijk de Nationale CERT voor Curaçao en de Caribische regio opgezet en ze zijn nog steeds betrokken bij de ontwikkeling van deze CERT. Roeland is op dit moment betrokken bij het opzetten van een Informatie Beveiligings Dienst (CERT) voor de gemeentelijke sector vanuit KING en VNG en ontwikkelt voor het NCSC een sectoraal CERT- en samenwerkingsmodel voor de vitale sectoren.

Don Stikvoort MSc(Hons) CTNLP, Adviseur en Coach, eigenaar van S-CURE (Security & CERT Advisering) en AVALON Coaching & NLP (Life & Executive Coaching, NLP & Communication Trainings/Workshops).
Don heeft 25 jaar ervaring in IT/internet en security, in vele functies van opbouw, via architectuur en management tot consultancy en auditing. Hij is een van de pioniers van het internet in Europa. Hij was de voorzitter van de tweede Europese CERT (thans SURFcert geheten) van 1992 tot 1998, toen hij zijn eerste eigen bedrijf begon. Sindsdien heeft hij aan de wieg van meer dan 10 CERT's in binnen- en buitenland gestaan, waaronder ook CERT-AMC en GOVCERT.NL (thans NCSC). High level security audits en CERT audits en certificeringen doet hij eveneens internationaal, zowel als het opzetten van security beleid. De afgelopen jaren, na training en certificering in o.a. Engeland en Australië, treedt Don ook op als life- en executive coach, en is hij in 2011 begonnen met het geven van workshops en certificeringstrainingen op het gebied van NLP en communicatie.

In de afgelopen jaren zijn CERT's of CSIRT's flink in opkomst. Hoewel een security-afdeling niet altijd CERT of CSIRT hoeft te heten, zijn de taken die een CSIRT normaal gesproken uitvoert wel opgenomen in de taken van de security-afdeling. Maar wat is nu eigenlijk een CERT? Wat doet zo'n clubje mensen en waarom is dat allemaal zo geheim? En waarom zitten deze mensen bij onze concurrenten te overleggen? In dit artikel proberen we in te gaan op deze vragen.

Wat is een CERT of CSIRT?
CERT staat voor "Computer Emergency Response Team" en wordt ook wel als CSIRT (Computer Security Incident Response Team) aangeduid. Het is de gangbare benaming voor de functie binnen organisaties die zich richt op het voorkomen en genezen van computer/netwerk gerelateerde veiligheidsincidenten. Een betere term voor CERT zou ISIMC zijn omdat dat preciezer laat zien waar het om gaat: *Information Security Incident Management Capability*. "Information Security" laat zien waar het werkelijk om gaat bij beveiliging – niet om computers, maar om informatie als onderdeel van de bedrijfsprocessen en met name het primaire proces. "Incident Management" laat blijken dat het gaat om veel meer dan alleen "emergency response": preventie en "lessons learnt" zijn net zo belangrijk. "Capability" betekent dat het om een functie gaat binnen een organisatie. Nu wordt die functie natuurlijk door mensen verricht, dus is het zeker ook een team – maar dat team kan zowel bij elkaar zitten als verspreid door een organisatie! ISIMC mag dan een betere term zijn, CERT is algemeen in zwang, en wordt ook hier verder gebruikt. De eerste CERT's ontstonden in 1989, de allereerste (die van Carnegie Mellon University) is de generieke naam geworden (5). Nu zijn er enkele honderden CERT's bekend wereldwijd, en dat aantal groeit gestaag. Door de open aard van het Internet zijn veiligheidsincidenten niet meer plaatsgebonden - de CERT's werken daarom al vanaf het begin samen. Thans bestaat die samenwerking op meer lagen: wereldwijd, regionaal (binnen Europa bijvoorbeeld), binnen sectoren, maar ook tussen nationale overheden.

Een CERT is toch alleen voor heel grote organisaties?
Deze vraag duidt vaak op een te beperkt begrip van wat een CERT is. Het is vooreerst een functie. Die functie kan door een team van fulltimers die in dezelfde kamer zitten worden verricht - maar het kan ook een gedistribueerde en part-time opzet kennen. De oplossing hangt af van de eigen eisen en mogelijkheden. Een CERT is daarom eerder te zien als een bedrijfsmatig model voor het doelgericht omgaan met veiligheidsincidenten dan als een aantal computerexperts die samen in een kamertje "crackers" te slim af proberen te zijn. Het CERT model wordt vooral gebruikt om een aantal zaken beter te organiseren, met name autoriteit (mogen optreden), escalatie (door de rangen heen kunnen gaan waar nodig), "awareness raising" en samenwerking met andere spelers in het

CERT veld. Een CERT is er dus voor alle organisaties.

Wat voor soort CERT's zijn er zoal?
Deze vraag is het beste te beantwoorden door de meest gebruikelijke soorten CERT's kort aan te geven.
Organisatie/bedrijf intern gerichte CERT: zulke CERT's dienen de beveiliging van de eigen interne organisatie – of dat nu om een bank gaat, een ministerie, een universiteit, een raffinaderij, een ziekenhuis of een hotelketen; het hoeft niet altijd "CERT" te heten of goed georganiseerd zijn om toch al de facto "CERT" te zijn: immers is deze functie te allen tijde van belang en wordt ook altijd wel op de een of andere manier ingevuld;
NREN CERT: NREN staat voor National Research and Educational Networks, die universiteiten en scholen met elkaar verbinden: een NREN CERT treedt coördinerend op voor de CERT activiteiten van de "klanten";
Overheid CERT: treedt coördinerend op voor de CERT activiteiten van ministeries en andere gouvernementele organisaties (zoals bijv. gemeenten);
Militaire CERT: treedt coördinerend op voor de CERT activiteiten van de militaire organisaties;
Nationale CERT: treedt coördinerend op voor een heel land: in de praktijk zal een sterke nadruk liggen op signalering, advisering en stimulering – plus de bescherming van organisaties binnen de vitale sectoren en de kritieke informatie infrastructuur, met als focus de bescherming van de nationale veiligheid;
CERT voor klanten: bijvoorbeeld de CERT functie die een Internet of mobiele provider voor zijn klanten heeft – of een commerciële CERT functie die verkocht wordt aan betalende klanten. Een derde voorbeeld betreft zogenaamde "vendor CERT's" die zorgen voor de veiligheid van software producten van IT-vendors.

Hoe werken al die CERT's samen?
De CERT's werken op vele niveaus samen.
Binnen logische eenheden: een Overheid CERT binnen de Overheid, een NREN CERT binnen een research/scholen netwerk, enzovoorts;
Binnen landen: een Nationale CERT met name, maar ook een Overheid CERT of soms zelfs een NREN CERT als voorloper, kan binnen een land coördinerend/adviserend optreden;
Tussen landen: Overheid en Nationale CERT's hebben onderling veelal bijzondere banden;
Binnen sectoren: bijvoorbeeld binnen de financiële sector in een land, zoals in Nederland de FI-ISAC (een ISAC is een "Information Sharing and Analysis Center" op security gebied) en ook op Europees niveau binnen een sector wordt samengewerkt; maar ook tussen IT-vendors (in Nederland de MSP-ISAC): opmerkelijk in al deze gevallen, maar zeer gebruikelijk is dat concurrenten elkaar helpen als het om security incidenten gaat;
Binnen regio's: In Europa wordt in/via TF-CSIRT en haar "trusted backbone" de Trusted Introducer samengewerkt; In de Asia-Pacific regio idem in/via APCERT; Wereldwijd wordt FIRST, het Forum of Incident Response and Security Teams, door CERT's als platform gebruikt om elkaar te ontmoeten.

Waarom doet de politie niet gewoon het CERT werk?
Een logische vraag – er gebeurt op je computer iets wat niet door de beugel kan. Je doet aangifte. De politie doet onderzoek en zorgt ervoor dat de dader gepakt en gestraft wordt. Waarom kan dat niet net zo op het internet? Waar zijn die CERT's voor nodig? Opsporing en vervolging is niet voldoende. Binnen het digitale domein is ook behoefte aan tijdige waarneming en directe opvolging bij incidenten. Zoals dat in de fysieke wereld wordt opgepakt door de brandweer, pakken CERTs dit op voor het digitale domein. Je kunt een CERT dus zien als een digitale brandweer.
Verder was het altijd al zo dat organisaties en bedrijven interne incidenten kenden, ernstig en minder ernstig. Die losten en lossen ze in de regel zelf op – er is vaak niet eens sprake van strafbare feiten. Dat is nu met het Internet nog steeds zo, alleen zijn zulke incidenten dan vaak niet meer strikt intern – ze hebben een wisselwerking met de buitenwereld, via het net. Het getroffen bedrijf wil dan graag in contact komen met die buitenwereld om dat probleem op te lossen – en vaak gebeurt dat met collega's in andere organisaties, of met de hulp van telecomproviders. Om dit te laten werken is er nu dat "CERT-systeem" – het zijn al die CERT's die met elkaar praten. Er is nog steeds lang niet altijd sprake van een strafbaar feit – of er is om wat voor reden dan ook geen aangiftebereidheid.

Ten tweede is het zo dat CERT's wereldwijd een bijzonder flexibele en snelle manier van samenwerken gevonden hebben. Veel partijen nemen ook hun verantwoordelijkheid om problemen te helpen oplossen – een vorm van internetzelfregulering. Waar nodig wordt lokaal de politie ingeschakeld. De samenwerking tussen CERT's en politie wordt ook geleidelijk steeds beter, vooral met de toenemende kennis en ervaring op dit gebied bij de politie. Natuurlijk werkt de politie ook internationaal samen, o.a. via Interpol en Europol. Deze samenwerking is echter minstens één orde complexer dan die der CERT's, omdat in elk land andere wetten en procedures gelden, waar de politie zeer direct mee te maken heeft. Daarom worden dergelijke gecompliceerde en dure opsporingen in de regel alleen voor zware gevallen gebruikt. Zeer nuttig en nodig – maar veel trager en beperkter toepasbaar dan de CERT samenwerking.
In feite zou er om in deze situatie structureel verbetering te brengen, een soort "maritiem recht" voor het Internet moeten komen, wat overal geldig is. Het probleem daarbij is natuurlijk dat het Internet overal is – en dat er niet zo'n helder concept als "buiten de territoriale wateren" voor te vinden is. Toch is dit een uitdaging die op termijn aangegaan zal moeten worden.

Wat brengt de toekomst?
De CERT wereld is thans 23 jaar oud. Qua volwassenheid is echter niet meer dan het 16e levensjaar bereikt, schatten we. Inderdaad een spannende fase, met allerlei veranderingen. Professionalisering is één van de trends – CERT's worden "mainstream" en willen hun processen goed onderbouwen en inrichten – goed geschoold personeel hebben – kwaliteit nastreven en deze ook kunnen aantonen – enzovoorts. Daarmee komen we bij een tweede trend – accreditatie en certificering. Hebben we al sinds 2000 met de komst van de Trusted Introducer (1) een CERT accreditatie (later door FIRST (2) geadopteerd voor hun lidmaatschapssysteem), in 2009 is er in Europa een pilot gedaan waarbij met behulp van een CERT maturity model gekeken wordt hoe certificering in zijn werk zou kunnen gaan. In 2010 is hieruit met succes een onafhankelijke certificering voortgekomen (3). Deze is inmiddels toegepast op 7 teams, waarvan er nu 6 gecertificeerd zijn. De allereerste was onze eigen GOVCERT.NL! - thans NCSC (4). Het is te verwachten dat deze certificering zich doorzet en meer en meer gebruikt zal worden als "vertrouwensbasis" – bijvoorbeeld dat organisaties die het internet naspeuren op incidenten, hun logs alleen zullen geven aan CERT's die, doordat ze gecertificeerd zijn, aannemelijk kunnen maken dat ze serieuze en betrouwbare partners zijn voor de uitwisseling van vertrouwelijke gegevens. Het is te verwachten dat ook nationale overheden dergelijke eisen gaan stellen aan belangrijke CERT's, als voorwaarde voor privaatpublieke samenwerking. Deze trend tekent zich binnen de EU al af.

Samenvatting
CERT's voorkomen en genezen incidenten op het gebied van de informatiebeveiliging. Elke organisatie, van groot tot klein, heeft een CERT functie nodig, hoe uitgebreid of beperkt die ook is: we kunnen veiligheidsincidenten nu eenmaal niet negeren. CERT's bestaan in een veelheid aan organisaties, en ook op overheids- en nationaal niveau. Ze werken nationaal, in Europa en wereldwijd zeer goed samen, en dat al meer dan 20 jaar. De CERT community is snel groeiend en ambitieus, maar doordat ze zo jong is, valt er nog veel te verbeteren aan de maturity. Zo is de eerste certificering pas in 2010 ontstaan. Om meer te weten, zie o.a.:

- Artikel Don Stikvoort: "CERT: Veiligheidsincidenten voorkomen en genezen" (6)
- ENISA website met vele nuttige documenten voor CERT's (7)

Literatuur en links

(1) https://www.trusted-introducer.org/

(2) http://www.first.org/

(3) https://www.trusted-introducer.org/ti_process/certify.html

(4) https://www.ncsc.nl/

(5) http://www.cert.org/

(6) http://www.pvib.nl/download/?id=17674950&download=1

(7) http://www.enisa.europa.eu/activities/cert

CONSUMERIZATION + CORPORATE IT = ANTIBIOTICA KUUR ≠ INFORMATIEBEVEILIGING…

Richard van Lent is Directeur Business Development bij mITE Systems. mITE is specialist op het gebied van enterprise mobility oplossingen voor bedrijven en biedt advies, consultancy, implementatie en operationeel management van smartphones, tablets, mobiele applicaties en "bring-your-own-device" (BYOD). Richard is bereikbaar via r.van.lent@mite.nl.

We mogen gerust stellen dat het fenomeen "consumerization" op de globale mobiele werkplek een feit is en dat de consequenties die daaruit voortvloeien voor bedrijven verstrekkende gevolgen zullen gaan hebben op het gedrag van de eindgebruikers/werknemers, het mobiele beleid en de toegepaste technologieën voor het operationele beheer. Een van de kenmerkende wapenfeiten, die consumerization in gang heeft gezet, is dat Apple er 24 jaar over gedaan heeft om +/- 67 miljoen Mac's te verkopen terwijl er in de afgelopen 2 jaar evenveel iPads zijn verkocht!

Een ander kenmerk van de kracht van consumerization is het transitionele vraagstuk van het gebruik van eigen middelen en mobiele apparatuur (het fenomeen "BYOD") op het bedrijfsnetwerk. BYOD krijgt een steeds grote vlucht en zou dus ook als onderwerp hoog op de agenda van de CIO moeten staat. Tot 2010 zijn we vooral opgegroeid in een bedrijfsomgeving waarbij IT de eindgebruikers heeft voorgeschreven wat wel en niet was toegestaan op de bedrijfslaptop. Hierbij werd de volledige gebruikersomgeving en de bijbehorende toepassingen door IT naar deze laptops gepusht. Op zich een prima en inzichtelijk model "ook wel de IT-Push genoemd" waarbij alle risico's en verantwoordelijkheden door het bedrijf zelf werden genomen (Ouder-Kind beleid).

Echter, dit model blijkt een houdsbaarheid datum te hebben en is dus ingehaald door zaken als "De Cloud", "Social Media", "Mobiel Werken" etc. De eindgebruiker wil steeds vaker zelf bepalen welke middelen worden gebruikt, hoe er wordt gecommuniceerd en hoe informatie wordt geconsumeerd. We spreken dan ook over een "Consumer-Pull". Bij het "IT-Push" model was het gevoelde bedrijfsrisico voor informatiebeveiliging relatief beperkt omdat IT hier bijna altijd in controle was en vooral ook een controlerende taak had. Bij het "Consumer-Pull" model zullen we gaan ervaren dat de rol van IT veel meer faciliterend gaat worden en zal de relatie tussen bedrijf en werknemer gaan evolueren op basis van een gelijkwaardige relatie (Ouder-Ouder beleid) met een gedeelde aansprakelijkheid en verantwoordelijkheid voor het gebruik van mobiele toestellen op het bedrijfsnetwerk.

> Door consumerization verandert "IT-push" in "Consumer-pull"

Met het Consumer-Pull-model, en het geweld waarmee nieuwe mobiele toestellen, besturingssystemen en toepassingen in de markt worden geïntroduceerd, wordt er een sterke wissel getrokken op de snelheid en flexibiliteit van bedrijven (technisch, organisatorisch en operationeel). Hierbij wordt het voor bedrijven steeds belangrijker om op de juiste manier om te gaan met al deze nieuwe trends zoals BYOD, mobiele technologieën en bewegingen in de markt zonder hierbij de grip op de informatiebeveiliging te verliezen.

Vooralsnog is de volgende vergelijking nog steeds waar: Consumerization ≠ Corporate IT. Dit lijkt momenteel dan ook het enigma in de markt. Maar is dat terecht? Kijk naar het begin van het internettijdperk waarbij grote bedrijven erg huiverig waren om hun bedrijfsnetwerk te ontsluiten op het publieke internet vanwege de beveiligingsrisico's (of het gevoelde bedrijfsrisico). Ook dit vraagstuk was destijds een transitioneel vraagstuk net als BYOD dat nu voor mobiel werken is.

Ook kan worden gesteld dat internet, als globaal netwerk en technologie, transformeel is geweest in onze samenleving en dat mobiliteit/mobiel-werken eveneens alle kenmerken vertegenwoordigt om de samenleving weer significant te beïnvloeden. Het steekhoudende middel om mobiel werken en BYOD gecontroleerd toe te staan op bedrijfsnetwerken heet informatiebeveiliging. Informatiebeveiliging helpt controle te houden op de aan BYOD gerelateerde bedrijfsrisico's in termen van reputatie schade, financiële schade, schade op intellectuele eigendomsrechten etc. Bovenstaande is het, met het steeds centraler staande mobiele device, aanlokkelijk om mobiele toestellen binnen het bedrijfsnetwerk voorbij het e-mail domein te laten treden.

Het is juist daarom interessant om te zien hoe er momenteel wordt aangekeken tegen het fenomeen "Data Leakage" op mobiele toestellen als het gaat om de beveiliging van bedrijfsgegevens en het voorkomen van het weglekken van bedrijfsgegevens op deze toestellen. Bedrijven en IT-afdelingen zijn momenteel druk bezig om de juiste technologieën te zoeken en te vinden om dit potentiële risico van het lekken van bedrijfsgegevens op mobiele toestellen te voorkomen of in ieder geval in te perken. In dit proces wordt er echter wat minder aandacht geschonken aan hoe dit zich vertaalt naar de organisatorische aspecten zoals bijvoorbeeld het beleid (afspraken tussen de werkgever en werknemer) en de operatie (ITIL processen binnen IT die vooral zijn ingericht voor de vaste werkplek en laptop omgevingen – dus niet mobiele toestellen).

> Daar waar bedrijven 15 jaar geleden huiverig voor het ontsluiten van internet waren, zijn ze dat nu voor consumerization

Dat je als bedrijf zorgdraagt om het weglekken van bedrijfsgegevens op mobiele toestellen te voorkomen of te beperken is op zich een pragmatische en juiste aanpak. De vraag die echter ook gesteld moet worden is wat nu precies bedoeld wordt met bedrijfsgegevens! Het blijkt namelijk dat verreweg de meeste bedrijven niet precies weten welke informatie binnen de eigen organisatie leeft en sterker nog wie nu precies toegang hebben tot welke informatie. Een van de belangrijke bevindingen is dat "Data Classificatie", met het ontsluiten van mobiele toestellen op bedrijfsnetwerken, als agendapunt moet worden meegenomen op de agenda van de CIO. Het feit dat data classificatie momenteel nauwelijks wordt toegepast maakt dat alle bedrijfsgegevens als "Vertrouwelijk" worden aangemerkt en als zodanig worden behandeld en beheerd.

Dit heeft veel weg van een dokter die een antibioticakuur aan een patiënt voorschrijft voor een pijntje in de arm. En zoals we allemaal weten heeft een antibioticakuur twee grote nadelen: het is duur en op lange termijn niet doeltreffend. In de mobiliteitsmarkt worden er momenteel oplossingen aangeboden die wellicht op lange termijn onjuiste informatiebeveiligingsvraagstukken proberen op te lossen.

Data classificatie is ook vanuit de wet- en regelgeving belangrijk zoals de WBP en het GBA of vanuit informatiebeveiligingsoogpunt zoals ISO/IEC-27000 en de NEN-7510 norm in de zorgsector. Het "Consumer-Pull" model kent uiteraard vele uitdagingen op het gebied van beveiliging als het gaat om het

mobiele toestel zelf en de beschikbare toepassingen daarop. Momenteel wordt er door bedrijven vooral gekeken naar het beheerd en gecontroleerd ontsluiten van mobiele toestellen op toestel en netwerk niveau waarbij de meeste organisaties wel een vorm van twee-factor authenticatie hebben ingericht.

De stap voorbij het e-maildomein presenteert echter beveiligingsvraagstukken die vele malen groter zijn en waarbij de inrichting van de autorisatie naar geclassificeerde bedrijfsgegevens en toepassingen binnen de organisatie goed geborgd moet zijn als het gaat om de technische, organisatorische en operationele aspecten.

Ook hier laat de markt al mogelijke deeloplossingen zien om op de informatie- en applicatielaag informatiebeveiliging mogelijk te maken.

Bedrijven doen er verstandig aan om vooral te bepalen waar ze zelf staan als het gaat om de eigen volwassenheid. Op technisch niveau gaat het dan vooral over de toestellen op de werkplek, het netwerk, de toepassingen en informatiebeveiliging.

De organisatorische aspecten hebben vooral betrekking op het gedrag, beleid en governance model.

Op operationeel niveau moet vooral gekeken worden naar hoe flexibel en schaalbaar de huidige ITIL processen, en dus ook de mensen en middelen, zijn ingericht om mobiel werken ook naar de toekomst toe goed te kunnen blijven ondersteunen.

Ten aanzien van deze verschillende typen aandachtsgebieden, onderkent mITE een aantal belangrijke uitdagingen waar elk bedrijf dat zijn mobiele oplossingen goed wil beveiligen mee te maken krijgt. Dit zijn:

1. Het vastleggen van een goed beleid tussen werknemer en werkgever en deze rand voorwaardelijk maken (gaat dus over gewenst gedrag, aansprakelijkheid en verantwoordelijkheid).
2. De inrichting van authenticatie, netwerktoegangscontrole (NAC) en "repository" scans op toestellen.
3. De inrichting van toestel- en applicatiebeheer en distributie om het beleid actief te kunnen toepassen.
4. Het inrichten van een centraal gecontroleerde omgeving voor documentbeheer en het delen van documenten.
5. De inrichting van de autorisatie en classificatie tot andere informatiebronnen en toepassingen dan e-mail.
6. Het herzien van de huidige ITIL processen die wellicht veel flexibeler zullen moeten worden ingericht voor de gehele levenscyclus van mobiele toestellen en de daarop gebruikte toepassingen en diensten om eindgebruikers beter en veiliger te kunnen bedienen.

In de komende edities van informatiebeveiliging zullen we de risico's en oplossingen achter deze uitdagingen nader bespreken.

Uw IT-Beveiliging verbeteren ?

Richtlijnen
Quickscans
Security By Design
Wij zorgen ervoor!
Audits
Implementaties
Processen
Security Controls
Testen
Risicoanalyses
Beleid

ViRaSo-IT
Enhancing your IT Security

info@viraso-it.nl

Informatiebeveiliging
Applicatiebeveiliging
Infrastructuurbeveiliging

INFORMATIEBEVEILIGING VERANDERMANAGEMENT?

Mustapha Sloot is Principal Consultant bij 3-Angle. Hij is te bereiken via mustaphasloot@3-angle.nl.

Compliancy vereist dat u uw informatietechnologie en -beveiliging aantoonbaar onder controle heeft. Gerard Klop van Motiv legt aan de hand van RSA Archer uit hoe u met een applicatie voor Governance, Risk & Compliancy niet alleen grip krijgt op uw IT, maar ook een helder beeld van de risico's voor uw bedrijfsvoering.

Informatiebeveiliging is een onderwerp dat over het algemeen niet als 'sexy' wordt ervaren. Het kost geld en moeite, wordt ervaren als beperking, en als het goed ingeregeld is merk je er meestal niets van. We zijn immers gewend om pas bij risico's stil te staan als de dreiging daarvan groter wordt. Dit heeft tot gevolg dat het onderwerp veelal gemeden wordt en slechts leeft bij de specifiek daarvoor aangestelde medewerker.
Op gezette tijden wordt de organisatie min of meer gedwongen om er wel aandacht aan te besteden. Veelal is dit door een incident of een audit met tegenvallende resultaten. Dan wordt vaak een projectachtige opdracht geformuleerd met als achterliggende gedachte het 'even' te gaan regelen. Dit resulteert vaak in deeloplossingen of dossiers die in kasten verdwijnen.
Informatiebeveiliging is geen geïsoleerde actie maar hoort eigenlijk een integraal onderdeel te zijn van alle processen waarin informatie gebruikt of verwerkt wordt. Het dient daarmee ook niet op de maatregelen gefocust te moeten zijn maar op het op een verantwoorde manier omgaan met de risico's. Deze risico's zijn vaak complex en niet voor iedereen transparant. Het hiermee om leren gaan vereist veelal een attitudewijziging in de organisatie. Dit is niet af te dwingen met het voorschrijven van maatregelen, maar vereist een borging van het 'risicodenken' en het daarnaar handelen door de gehele organisatie.

De navolgende beschrijving is gebaseerd op de ervaringen gedurende de afgelopen twee jaar bij een ziekenhuis in Noord-Holland.
De trigger voor de acties waren aanbevelingen naar aanleiding van een NEN 7510 audit. Hierbij werden wij ingeschakeld om de organisatie te helpen de aanbevelingen weg te werken. Tijdens deze actie bleek dat bij de zaken die wel 'geregeld' waren de onderlinge samenhang ver te zoeken was, de verantwoordelijkheden onduidelijk en de activiteiten waren niet gebaseerd op een adequate risicoanalyse.
We zijn toen begonnen met het scholen van de beveiligingsfunctionaris op het gebied van risicoanalyses. Hierbij hebben we gekozen voor de CCTA Risk Analysis and Management Method (CRAMM). Enerzijds omdat dit goed aansluit bij de maatregelen uit de 7510, anderzijds omdat deze schaalbaar is, en startend met een risicoanalyse op het primaire proces. Binnen CRAMM is deze later uit te breiden waarbij de voor het aanwezige proces gedefinieerde componenten ook aan de nieuwe analyse gekoppeld kunnen worden.
We zijn toen om deze analyse heen gaan bouwen aan de inrichting van het ISMS. Hierbij zijn we uitgegaan van de 7510, die processen beschreven die nodig waren om een volgende stap te kunnen zetten.
Zo werd als eerste een beveiligingsforum ingesteld onder voorzitterschap van de Raad van Bestuur. Het is immers nodig dat de besluitvorming kan escaleren tot het hoogste niveau binnen de organisatie. Hiermee was de basis gelegd voor de verdere inrichting van het ISMS framework.
Bij alle volgende stappen en processen hebben we als uitgangspunt gehanteerd om heel basaal te beginnen, met andere woorden: alleen de strikt noodzakelijke processtappen benoemen maar daarbinnen wel de PDCA borgend zodat, indien dat nuttig en zinvol is, vanuit de evaluatie een verdieping plaats kan vinden.
Het resultaat hiervan was dat na een jaar het volledige ISMS in opzet en vastgesteld door de Raad Van Bestuur aanwezig was. De ISMS-processen leidden tot:
Verantwoordelijkheden zijn belegd met het proces om dat te beheren,
GAP-analyses zijn uitgevoerd met als resultaat verbeterplannen, alle stappen om tot een vastgestelde maatregelenset te komen zijn geborgd in processen en de planning, evaluatie en rapportage van het beveiligingsforum zijn geborgd.
Informatiebeveiliging implementeren betekende voor het betreffende ziekenhuis dus met name een veranderingsproces met 'en passant' daarbij dat daardoor maatregelen werden geïmplementeerd.

CONFIDENTIAL

Once again we look at Business Attributes from the SABSA Business Attributes Taxonomy, looking at each from new perspectives. In this Issue we examine one of the oldest favourites, the attribute 'confidential'.

Confidentiality it is the very foundation upon which information security is built. For many people the two are synonymous. It can be traced back thousands of years to when information technology comprised only written documents and verbal communications. Julius Ceasar is legendary for his use of simple encipherment, which could protect a message in transmission even if the messenger were captured and tortured. Military and government IS policy has changed little over the past two millennia insomuch that 'secrecy' is still the basis of the approach.

The question addressed here is: how to measure confidentiality? In SABSA thinking it is essential to stick to the well-known management wisdom – if you wish to manage something then you must be able to measure its performance. The Ceasar cipher provided two classes of confidentiality – enciphered and non-enciphered (and yes the second one is relevant because not everyone could read written Latin). As a modern equivalent example the UK Government Protected Marking System (GPMS) provides five classes of confidentiality protection. The classes are defined by the level of impact that would be experienced, should an unauthorized disclosure take place. For more details see http://protectivemarking.co.uk/images/downloads/gpms.pdf .

This example provides one specific means of measuring confidentiality based on potential level of impact. It is not perfect because it does not distinguish between types of impact – only levels of impact. Thus if we look at 'top secret', there is no distinction between financial/economic damage, political damage and widespread loss of life, since all are bundled in the same basket. Does this matter? Well it might do when we come to implementing controls, at which point the specifics of the information characteristics will affect which types of control we can best use (technical, process or people). Added granularity would provide for a more focused and therefore more cost-efficient control strategy.

This 'impact-based' approach to measuring confidentiality is reflected in most commercial organisations today. Confidentiality is often rated on a 1 to 4 scale, C1 being the lowest and C4 being the highest. These four levels are mapped to impact levels, usually expressed as financial impacts, scaled according to the needs of the enterprise. It is then assumed that for a given impact level, there is a set of standard controls that are needed to secure the information assets from unauthorized disclosure. This approach is increasingly being recognized as far too crude, and often means that systems are over-controlled in some ways and under-controlled in others, and process/people controls are often ignored. There is a lack of granularity provided to those who must design, build and implement the secure systems. A C4 rating tells nothing of the specific context from which that rating was derived, nothing about the type of impact (only the level), nothing about who is authorized and who is not and nothing about the time span over which confidentiality must be maintained.

This latter point is probably the most gaping hole in this entire approach. Some information is confidential for a few moments whilst a transaction takes place, after which it can be widely known. Other types of information has a confidentiality lifetime of a few weeks or months, such as during the preparation of financial reports that would be sensitive regarding stock market prices, but will then be public. Other information needs to be guarded for years, even decades before it can be disclosed, and all these time factors have huge effect on the selection of the most effective and cost-efficient controls to be used. A C4 rating conveys nothing of this need.

Finally there is measuring the size and nature of the community (or domain) of people who are allowed to know the information. How are its boundaries defined? The UK GPMS attempts to address this through a security clearance scheme, but this is very crude and once again lacks the granularity that would really bring clarity of vision to the selection of the best controls for the specific purpose.

How can SABSA help with this? In SABSA each attribute is considered in its business context. Each is assigned one or more measurement approaches, each with a specific metric to be calculated and measured for its performance in live operations, and each associated with a performance target that articulates 'risk appetite' – how much risk can you live with? Through this approach the control strategy and the selection of specific controls for keeping information assets confidential are highly focused on the multi-dimensional nature of confidentiality in a way that other methods cannot achieve. The result should be better control for lower cost. That's the added value of SABSA Business Attributes Profiling.

The Attributer

ACHTER HET NIEUWS

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

En weer een lek in Internet Explorer, dat actief wordt misbruikt door hackers. De Duitse overheid adviseert burgers om maar een andere browser te gebruiken. De Nederlandse overheid adviseert de burgers (eigen verantwoordelijkheid) om Microsoft's Enhanced Mitigation Experience Toolkit te gebruiken. Wie kent dat tooltje? Denken wij dat burgers weten hoe dat werkt? We snappen dat de overheid niet een belangrijke partij durft te schofferen, maar voegt zo'n vreemd advies wel iets toe? Ligt hier misschien een taak voor het PvIB? Durven wij wel een dergelijk falen aan de kaak te stellen? Dilemma's waar onze redacteuren vast wel een mening over hebben...

Maarten Hartsuijker

Als ik het advies van de Duitse overheid lees moet ik steeds aan mijn familie en schoonfamilie denken. Ik wil ze niet tekort doen, echt niet, maar in gedachten zie ik nog steeds een familielid de muis optillen en tegen het scherm duwen als ik zeg: je moet met de muis (dat ding daar) op dat icoontje (daar op het scherm, ja) klikken. Toegegeven: zo erg is het al jaren niet meer. Maar zelfstandig een nieuwe browser installeren? Dat zie ik nog niet iedereen doen.

Bedrijfsmatig is dit nog veel complexer. Een nieuwe browser uitrollen is eenvoudig, maar uit ervaring weet ik dat de helpdesk de volgende dag wordt overspoeld met vragen over waar de favorieten zijn gebleven, waarom websites ineens om inloggegevens vragen en waarom sites (met Active-X) het niet meer doen. En veel van die problemen herhalen zich op het moment dat de tijdelijke browser weer ingetrokken moet worden, omdat dubbel onderhoud en support ook wat van de organisatie vraagt.

Persoonlijk ben ik de eerste die Internet Explorer in dit soort gevallen laat vallen. En geef ik zeker systeembeheerders het advies om (al dan niet tijdelijk) een andere browser te gaan gebruiken. Maar ik ben blij dat onze overheid, die met de capaciteiten van iedereen rekening moet houden, hier niet lichtzinnig mee omspringt. Al helpt het advies van de Duitse overheid vermoedelijk wel om de problematiek stevig op de kaart te zetten en de druk op Microsoft op te voeren. Die zien hun klanten natuurlijk niet graag weglopen. De fix-it is op het moment van schrijven net uit en het Technet blog meldt dat de definitieve patch morgen komt.

Als ethisch hacker weet ik hoe makkelijk antivirus-software misleid kan

worden. En dat een Windows-firewall geen bescherming biedt tegen drive-by exploits zoals deze. Dus misschien moeten we, met pijn in ons hart, gewoon maar vast stellen dat iedereen die voor het gebruiken van een tekstverwerker en e-mail op cursus gaat aan geen enkel technisch advies iets heeft. En dat velen die wel een nieuwe browser downloaden hier vervolgens vrolijk hun oude Java-software in blijven gebruiken.

Lex Borger

Microsoft schofferen? Dat is niet aan de orde, ze doen het juist goed. Zeker in vergelijking met Adobe, Oracle en Apple. Ze hebben een strak, tijdig proces en transparante, complete meldingen.

En wat moeten burgers hier van begrijpen of hier aan doen? Die hebben al moeite met de basisbeginselen: niet klikken op links in onverwachte email, geen websites bezoeken van twijfelachtige reputatie, niet standaard als administrator inloggen. Daarnaast moet alleen software installeren die je gebruikt en die software ook bijhouden - maar wacht, daar heb je nou weer wel administrator privileges voor nodig. En hoe bepaal je ook al weer of een email 'onverwacht' is of een website 'twijfelachtig'? Oh ja, je hoort een antivirusscanner te gebruiken, ook al vertelt iedere test je dat je daar maar een fractie van de malware mee detecteert. Ik ben tot de conclusie gekomen dat het verhaal voor 'de burger' wel heel complex is geworden. En als simpel goed is, is complex...

Dus wat te doen als professional? Het falen aan de kaak stellen? Dat is zó vingerwijzerig, dus eigenlijk heel Nederlands. Een alternatief is het om de ontwikkelaars beter gedrag aan te leren: niet alleen leren wat de fouten zijn die we collectief maken (zoals de OWASP top-10), maar ook hoe het begrijpbaar kan worden voor de gebruiker. Houd het simpel en duidelijk. Limiteer de keuzes die de gebruiker kan maken en sta slechte keuzes gewoon niet toe. En dit is iets wat Apple wél goed begrijpt.

Gerrit Post
Internet quo vadis?

Probleem in de Internet Explorer. Wist u dat dat überhaupt kon? Ooit over nagedacht, bij stilgestaan? Echt niet! Sommige dingen zijn een 'fact of life' een 'commodity'. Sorry voor het afschuwelijke jargon maar het drukt het wel heel goed uit. OK en dan is er een probleem, wat gaan we er dan aan doen? Typische overheidsreflex is dan: als we het niet snappen en zelf in de hand hebben, dan verbieden we het. De Duitse overheid heeft kennelijk wel begrepen dat een verbod op de IE een beetje lachwekkend zou zijn en dus raden ze het gebruik af. Voor sommige mensen staat dat misschien wel gelijk met het af raden om adem te halen. Zinvol lijkt de reactie in ieder geval niet. "Doe maar even geen internet". Een poosje geleden heb ik op hele kleine schaal, namelijk thuis, een poging gedaan om over te gaan op Firefox. Is gesneuveld. Alhoewel onze digitale wereld nog niet zo oud is, is daar dus ook zeker sprake van gewoontes die zich niet makkelijk laten veranderen. Is dat erg? Nee hoor. Wel erg is dat het kennelijk niemands probleem is dat er weinig kennis over het gebruik van onze digitale wereld is. Er wordt nogal geroepen dat onze jongens en meisjes zo digitaal bewust zijn maar dat waag ik te betwijfelen. Degenen die ik ken zijn veel handiger

in het omgaan met apps dan ik maar als er iets is met Windows hangen ze wel aan de telefoon. Een virusscanner krijgen velen niet of moeizaam geïnstalleerd. "Is dat dan nodig?" Ouderen hebben nog minder digitale kennis in huis. In algemene zin is men zich volstrekt niet bewust van de risico's. En daar zit nou juist het knelpunt. Wat ik bedoel te zeggen is tweeledig: ten eerste is leven wat wij hier en nu doen aan alle kanten omgeven met risico's. Die zijn er letterlijk overal, in huis en daarbuiten. Ook op de digitale snelweg kun je aangereden worden en gewond raken. De eisen die wij stellen aan deelname aan het digitale verkeer zijn 'nihil'. Misschien moeten we daar eens over nadenken. Misschien dat een overheid daar iets kan betekenen, of een beroepsorganisatie als PvIB. Een awareness campagne voor 200.000 gebruikers. Kijk, dan gaan we praten! Ten tweede - aan de andere kant - is de digitale snelweg tot nu toe van iedereen en voor iedereen. Denken, verwachten dat overheden daar regels voor gaan geven kan die overheden de mogelijkheid geven om in te grijpen in het digitale verkeer. Ik kan zo een aantal overheden (nationale en supranationale) bedenken die niets liever zouden willen en heel weinig excuus nodig hebben. Als we dat niet willen moeten we onze eigen verantwoordelijkheid nemen. We moeten er dus voor zorgen dat we een vrij toegankelijk internet hebben en houden maar onszelf bewust zijn van de risico's en ons er zo goed als mogelijk tegen wapenen of - en dat zal vaak voorkomen - we accepteren het risico. Misschien is er in de toekomst ruimte voor een verzekering tegen digitale schade? Misschien moet PvIB zich ook nog eens beraden op de maatschappelijke rol die zij in de derde vijf jaar van haar bestaan wil spelen.

CERTIFICATIE OP NEN 7510, WAT ZEGT DAT?

Mr.drs. Shirin Golyardi is consultant bij NEN Gezondheidszorg. Zij is te bereiken via Shirin.golyardi@nen.nl

De afgelopen jaren is een trend ontstaan dat zorginstellingen certificatie tegen NEN 7510 tot doel stellen. De vraag is of certificatie op de norm, en daarmee een mooi certificaat aan de muur, daadwerkelijk leidt tot betere informatiebeveiliging.

De afgelopen vijftien tot twintig jaar is automatisering in de zorg sterk gegroeid. De politiek mag dan afscheid hebben genomen van het landelijk EPD, dit betekent niet dat de opmars van de digitalisering niet gewoon doorzet. Deze digitalisering heeft ook aangetoond dat de kans op incidenten en verlies van vertrouwelijke informatie is toegenomen. En niet alleen de kans is toegenomen, maar ook de impact van deze incidenten is groter. Lag in vroegere tijden één papieren dossier op de achterbank van een taxi, tegenwoordig kan een USB-stick zoekraken met daarop informatie over duizenden patiënten. Mede door deze ontwikkeling is informatiebeveiliging op de agenda's gekomen van directies en raden van bestuur van zorginstellingen. Sinds 2004 heeft de Nederlandse zorgsector een eigen norm hiervoor ontwikkeld: NEN 7510. Deze norm biedt zorginstellingen handvatten voor het organiseren en borgen van informatiebeveiliging. In 2011 is de norm geheel herzien. Bij deze herziening hebben het managementsysteem voor informatiebeveiliging en de risicoanalyse een centrale plek gekregen. De risicoanalyse biedt inzicht in de risico's en de te nemen maatregelen. Het managementsysteem borgt dat de maatregelen goed worden ingebed en dat er periodiek wordt beoordeeld of het geheel nog voldoet of verbeterd moet worden. De centrale plaats van het managementsysteem in NEN 7510: 2011 vergemakkelijkt het zorginstellingen om informatiebeveiliging in te bedden in een bestaand kwaliteitsmanagementsysteem en daarmee te voorkomen dat voor beide onderwerpen aparte managementsystemen worden opgezet.

Veel zorginstellingen kiezen voor een projectmatige aanpak voor de implementatie. Dit leidt er toe, dat veel energie wordt besteed aan het inbedden van de structuur voor informatiebeveiliging en procedures voor omgang met vertrouwelijke informatie. Daarbij is er wel een risico dat deze energie niet wordt vastgehouden voor wat betreft bewustzijn en houding en gedrag van mensen. Nadat het project is afgerond, vervaagt de aandacht en daarmee het bewustzijn binnen de organisatie. En juist het bewustzijn binnen de organisatie – lees medewerkers, management en directie – is de essentie van informatiebeveiliging. De keuze voor en het implementeren van technologische oplossingen is vaak geen probleem; ICT-afdelingen worden bemand door competente medewerkers. Het probleem van de inbedding van de norm zit in het kennisniveau van en het gedrag van het personeel. Houding en gedrag zijn onderdeel van een bedrijfscultuur en moeilijk te beïnvloeden, veranderingen vergen jaren. Het is belangrijk dat zorginstellingen op alle niveaus – van de werkvloer tot aan de directie en/of de raad van bestuur – een continue aandacht hebben voor informatiebeveiliging. Dit betekent dat er periodiek gekeken moet worden naar de resultaten van de risicoanalyse en deze opnieuw moet worden beoordeeld. Hieruit ontstaat een continue proces van plan-do-act-check dat de informatiebeveiliging naar een hoger plan trekt.
Om informatiebeveiliging een langetermijn-karakter te geven, is het belangrijk dat in de risicoanalyse en in de te nemen maatregelen veel aandacht is voor de 'zachte kant' van de organisatie. Welke campagnes worden ondernomen om bestaand personeel te verleiden tot een gedragsverandering en in hoeverre heeft dit ook een continu karakter naar nieuwe medewerkers? Aandacht moet er ook zijn voor consequent handelen binnen de zorginstelling, zowel positief als negatief. Maar één van de belangrijkste aspecten hierbij blijft wel de betrokkenheid van de directie en het voorbeeldgedrag dat zij toont. In hoeverre is de directie zelf bewust van haar handelen en de risico's die dit met zich meebrengt?

Wil informatiebeveiliging ook op lange termijn succesvol zijn, dan zal een organisatie een combinatie moeten maken van een heldere organisatiestructuur met duidelijke taken, verantwoordelijkheden en werkwijzen, ondersteund door adequate technische maatregelen. Maar vooral gedragen door medewerkers die zich bewust zijn van de consequenties van hun handelen en zich daar ook naar gedragen.

HOE GOOGLE WEET WAT WIJ NIET VERTELLEN

Maarten Hartsuijker is beveiligingsconsultant en ethisch hacker bij Classity en bereikbaar via @classityinfosec.

Dat Google een grote honger heeft naar informatie over haar gebruikers zal voor weinig mensen nog een verrassing zijn. Begin dit jaar is er in aanloop naar (en na implementatie van) de wijzigingen in Googles privacy policy veel over geschreven.

De belangrijkste verandering in Googles privacy policy is dat de zoek / marketinggigant voor zichzelf de consolidatie van gebruikersgegevens mogelijk maakt. Google geeft aan dat het hiermee in lijn acteert met hoe de rest van de grote online bedrijven met persoonsgegevens omgaan. Voor bedrijven als Microsoft heeft juist Google de trend gezet. Microsoft wijzigde (met het oog op de Cloud visie achter Windows 8) eind oktober haar privacy policy op een vergelijkbare wijze als Google dat eerder dit jaar deed.

Zelf in control…

Een door bedrijven veel aangevoerd argument in de bescherming van online privacy is dat gebruikers zelf de controle hebben over wat bedrijven van ze weten (of niet). Je hoeft immers geen GMail account aan te maken. Of Google Docs te gebruiken. En je kunt op elk moment besluiten om een eerder aangemaakt profiel weer te verwijderen. En als je je Google account netjes uitgelogd hebt en daarna van de zoekdienst gebruik maakt, dan weet Google niet dat JIJ op dat moment naar specifieke interesses aan het zoeken bent, toch?

…of geen invloed meer?

Vergeet het maar! Het Google netwerk en de techniek is inmiddels zo omvangrijk en ver gevorderd dat ze inmiddels het merendeel van jouw online activiteit kunnen volgen. En met de wijzigingen in hun privacy policy is ook de aggregatie van al die informatie over identiteiten een stap dichterbij gekomen.

In de discussie over Google en online privacy wordt het accent vaak gelegd op de diensten die wij als gebruiker zien. Docs, Mail, Search, Play, Youtube... Dit zijn de diensten die consumenten veel gebruiken en waar velen een persoonlijk profiel voor hebben aangemaakt. Dit zijn ook de diensten waarbij je als gebruiker zelf kunt kiezen om ze wel of niet te gebruiken. Om er wel of niet op in te loggen of om er veel of weinig gegevens op te plaatsen. Je kiest daar zelf wat je met Google deelt. En hetzelfde geldt natuurlijk voor je relatie met een partij als Facebook. Maar hoe zit het eigenlijk met de indirecte verrijkingsmogelijkheden?

Handige Google diensten

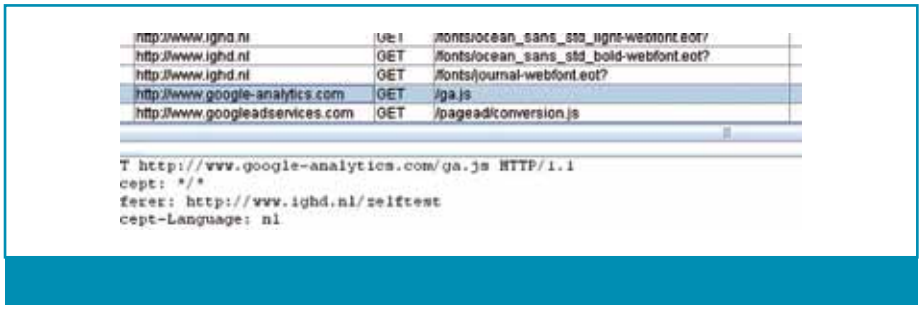
Net zoals Facebook de Like-knop heeft, heeft Google een aantal diensten (en dan laten we software als Chrome en Android voor het gemak even buiten beschouwing) die hier een hele grote rol in spelen: Google Ads, Google Code, Youtube, Google maps, Analytics en Google+. Via deze verschillende diensten biedt Google bedrijven gratis handige hulpmiddelen voor in hun website. Google Ads (advertenties), Youtube, Google maps en Google+ buttons kennen we allemaal. Veel bedrijven integreren ze in hun website om een film te tonen, de bedrijfslocatie bij een bezoek makkelijk te vinden of om de site te promoten binnen je Google+ Circles. Google Code en Analytics zijn voor velen minder bekend, maar bij webontwikkelaars en –beheerders des te meer.

jQuery

Google code biedt één van de meest gebruikte Javascript bibliotheken aan: jQuery. Veel websites gebruiken jQuery om websites slimmer te laten werken. Omdat het een relatief groot bestand is, verwijst de website vaak naar de servers van Google om dat bestand op te halen.

Analytics

Google Analytics biedt bedrijven gratis website statistieken. Hiervoor plaatsen ze in elke pagina een stukje Google programmatuur waarmee google voor het bedrijf bijhoudt hoeveel de verschillende pagina's worden gebruikt.
Hoewel al deze gratis hulpmiddelen handig en onschuldig lijken, zijn het de grootste privacyverslinders die er zijn. Elke keer als een website een filmpje, kaart of +1 knop opneemt, kan Google met de bezoekers van de site meekijken. En hetzelfde geldt voor elk geïntegreerd Analytics of JQuery script.



Maar als ik uitgelogd ben weet Google toch niets?

Zo werkt de techniek helaas niet. In haar privacy policy legt Google uit dat het naast cookies ook met "unique device identifiers" werkt. Dit betekent dat ze zichzelf het recht hebben gegeven om naast jouw identiteit ook het websitegebruik op basis van de identiteit van jouw computer(s) te volgen. Dit kan middels zogenaamde super cookies. Een supercookie is een samenstelling van alle gegevens die jouw computer uniek maken. Je schermresolutie, je browser, welke plugins je gebruikt, enzovoort. Deze supercookies zorgen ervoor dat jouw computer ondanks welke privacyinstelling dan ook toch gewoon herkenbaar is. Als jij regelmatig met een Google account op een computer inlogt, kan Google met een redelijke zekerheid vaststellen dat jij de primaire gebruiker van de computer bent. Het internetgebruik op die computer is daarmee (ook als je je Google account een dag niet gebruikt) goed tot op een gebruiker of een gezin te herleiden. Dit alles nog los van het feit dat een gezin vaak langere tijd hetzelfde IP adres, of een IP adres uit dezelfde regio heeft, waarmee de betrouwbaarheid van het supercookie verder vergroot kan worden. Deze voorbeelden gelden uiteraard enkel voor privacybewuste gebruikers. Veel gebruikers nemen überhaupt niet de moeite om uit te loggen en zijn daardoor per definitie eenvoudig onder de eigen identiteit te volgen.

Als we de mogelijkheden van device en user tracking koppelen aan het feit dat het merendeel van de websites één of meerdere Google diensten geïntegreerd heeft, kunnen we vaststellen dat Google veel meer over ons (of onze computer, ook dat is gewoon een identiteit met verkoopbare kenmerken) weet dan we het bedrijf zelf vertellen. Zo weet Google na het schrijven van dit artikel dat ik contact heb gezocht met IGHD verslavingszorg en jellinekminnesota.nl. Dat ik vermoedelijk relatieproblemen heb en er graag aan wil werken met eroverpraten.nl. En dat ik op het gezondheidsplein en bij Consumed meer over antidepressiva te weten wilde komen om daarna bij sky dive Ameland 1m27s over de "eensprongs cursus" te lezen.

Zou een profiel als het mijne voor bijvoorbeeld een verzekeraar interessant zijn? Zou er interesse zijn voor de afname van op dit profiel gebaseerde advertenties? Niet zozeer om extra diensten te verkopen aan deze doelgroep, maar om vast te stellen dat als Google bij een bezoek een advertentiehit heeft op basis van de profilering, een premieopslag of extra medische keuring noodzakelijk is? Risicoreductie is en blijft natuurlijk de manier om een solvabel portfolio te ontwikkelen...

Recht om vergeten te worden

De mogelijkheden die bedrijven als Google en Facebook hebben om internetters te profileren zijn eindeloos en reiken veel verder dan wij in eerste instantie zien. Als privacybewuste consument zou ik graag niet alleen inzage hebben in de gegevens die Google in directe zin over mij verzamelt, maar ook in alles wat daar indirect aan te relateren is. De huidige oplossingen bieden mij alleen schijncontrole. Paradoxaal genoeg is de uitvoering van deze wens vanwege privacyconsequenties onmogelijk. Wat niet onmogelijk is, is dat Google gebruikers van een computer de mogelijkheid geeft om gegevens over het internetbezoek vanaf die computer niet te loggen. En om alles dat in het verleden is gelogd en/of geaggregeerd te verwijderen.

Als privacybeschermers gebruikers écht de controle over Googles verzameldrift willen geven, moet de aandacht verder gaan dan enkel de zaken die direct aan een gebruikersprofiel gerelateerd zijn. Het is voor Google immers kinderspel om gegevens die onder een ogenschijnlijk onherleidbaar computerprofiel zijn opgeslagen toch eenvoudig -en met een zeer hoge mate van waarschijnlijkheid- naar een individu te herleiden. De huidige uitdagingen waar het afspraken rondom privacybescherming betreft lijken groot, maar wil je internetters meer dan schijnprivacy bieden, dan is de werkelijke uitdaging nog veel groter.

COLOFON

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

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

Redactieraad
Tom Bakker (Allianz)
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
Maarten Hartsuijker (ANWB)
Aart Jochem (NCSC)
André Koot (i3advies)
Rachel Marbus (KPMG, IT Advisory)
Gerrit Post (G & I Beheer BV)
Bart van Staveren (UWV)

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

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

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

Abonnementen 2012
De abonnementsprijs bedraagt 115 euro per jaar (exclusief btw), prijswijzigingen voorbehouden.

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

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

creative commons

ISSN 1569-1063

VERANDERD STRAATBEELD

Zoals wellicht bekend is Berry inmiddels een grijzende man geworden. Een man die inmiddels met grote regelmaat in het verleden duikt om zijn verhalen uit oude vervlogen tijden te vertellen. De goede oude tijd? Nee hoor, er is heel veel veranderd en een aantal zaken niet in de goede zin van het woord, maar het is beslist niet zo dat alles vroeger beter was. In de tijd dat ik begon te werken moest ik mij iedere ochtend om 8 uur melden op mijn werk en om een uur of 16:30 stapte ik weer op de fiets om het avondeten te nuttigen. In de avond konden we kijken naar de televisie en de keus was toentertijd een stuk simpeler. Nederland 1 en Nederland 2 en omdat ik nogal in de buurt van de Duitse grens woon had ik ook Duitsland 1, 2 en 3. Vijf zenders en daar moesten we het mee doen. Geen internet, geen videorecorder en een kleurentelevisie waar je met een beetje geluk kon zien wie de programma's presenteerde.

Tegenwoordig is dat gelukkig allemaal sterk verbeterd, ik hoef mij niet meer acht uren op mijn werk te bevinden in een kamer waar je met je collega's de tijd probeerde door te komen. Ik ben werkzaam bij een bedrijf dat het nieuwe werken heeft omarmd, gelukkig wel, want ik werk nu met regelmaat thuis. Mijn thuis is ook anders geworden, met de 52" plasma schermen, waar een haarscherp beeld één van de honderd zenders kan laten zien. Twee zenders tegelijkertijd kijken is wel mogelijk maar niet handig en dus heb ik een harddiskrecorder die voor mij twee programma's tegelijk kan opnemen en mocht dat nog niet voldoen, dan ga ik naar Uitzending Gemist die mij de beelden levert over mijn internetverbinding van 50 Mb.
Mijn 27" Mac kan ieder moment van de dag verbinding maken met het netwerk van mijn baas en eigenlijk is mijn bureau verplaatst van een kantoorgebouw naar mijn eigen huis. Op kantoor heb ik namelijk geen bureau meer. Tja, er is veel veranderd, ook mijn vrouw moest nogal aan dit fenomeen wennen want ineens is haar man thuis op het moment dat hij eigenlijk weg zou zijn, buren vragen haar of ik een sabbatical heb omdat mijn auto met regelmaat voor de deur staat en met een nog veel grotere regelmaat op de gekste momenten van de dag weg is. Naast mijn Mac staat een iPad, een machine die niet alleen voor thuis is maar die ik op mijn werk ook gebruik. Mail, agenda en contacten worden allemaal gesynchroniseerd op mijn iPad (en mijn iPhone overigens) en het praktische gebruik is geweldig. De Nokia die mijn baas mij verstrekte is al heel lang geleden een lade in geloodst en wordt niet meer gebruikt. Mijn werkgever staat dat toe want die heeft de praktische kanten van een iPad ten opzichte van de door-de-baas-verstrekte laptop ook al lang gezien. Rondkijkend op mijn werk zie ik diverse soorten apparatuur en zo nu en dan ook de laptops die mijn baas verstrekt heeft. Niemand lijkt zich er zorgen over te maken dat zijn mail en contacten met slechts vier cijfers beschermd is. Nog sterker; men vindt het eigenlijk grote flauwekul dat als men de backoffice wil bereiken men dan gebruik moet maken van een token.
Ik schijn de enige binnen onze organisatie te zijn die zich druk maakt over de beveiliging van eventueel lekkende gegevens. Verslagen van strategische besprekingen die de Raad van Bestuur voeren zouden op straat kunnen liggen door onoordeelkundig gebruik. Klantgegevens worden even naar de privé e-mailbox gezonden om ze daar op de privélaptop te zetten, alleen omdat dat zo makkelijk is. Jammer dat de laptop per ongeluk in de trein blijft liggen. Ik zie de chocoladeletters al op de hoofdpagina van de landelijke dagbladen met een foto van ons gebouw en de mededeling dat daar de gegevens weg komen. Malware op telefoons, die alle bijlagen bij de email doorzendt naar een ander adres. Je moet er niet aan denken maar het gaat een keer gebeuren! Een op de drie Europese bedrijven staat BYOD niet toe (bron: Computable) en dat kan ik heel goed begrijpen.
Jullie zullen nu ongetwijfeld willen weten waarom ik dan ook een eigen device gebruik. Het antwoord is simpel: het is niet de vraag of het een keer fout gaat maar wannéér het fout gaat. BYOD is net als Griekenland; we weten dat er een moment komt dat we de gyros weer met de Drachmen gaan afrekenen en niemand lijkt zich daar over te bekommeren.

Berry

SHARE INFORMATION

MINIMIZE RISK

Secured eCollaboration

A unique add-in for Microsoft SharePoint® providing document encryption and enhanced access control.

ASK FOR A FREE TRIAL!

SC MAGAZINE

Verdict: "A very nice encryption solution. Priced in the middle of the group, but it delivers protection very well."

cryptzone

www.cryptzone.com

CRYPSYS secure computing

sales@crypsys.nl | www.crypsys.nl | 0183 - 62 44 44