juni 2010 nummer 4

special Privacy

INFORMATIEBEVEILIGING

Ik twitter dus ik ben

Wat kun je nou op internet vinden?

Het effect van Web 3.0 op Privacy

Verslag: Black Hat 2010 Barcelona

Paspoortwet brengt burgers in gevaar

PvIB
Platform voor InformatieBeveiliging

ib

Voorwoord/colofon

Beste lezer,

Privacy blijft een actueel onderwerp. Steeds weer een privacyprobleem van Facebook (vergt misschien al een special op zichzelf) en weer eens een lek van persoonsgegevens (nu weer accounts van OV-chipkaartgebruikers op straat). Dus is het weer tijd voor een special van Informatiebeveiliging.
Deze special is vanuit de redactie met name door Lex Dunn en Aart Jochem gemaakt (compliment heren!). Wij hebben een groot aantal mensen weten te activeren om na te denken over het onderwerp en we zijn er ook in geslaagd om verschillende bijzondere bijdragen te verkrijgen. Lex en Aart hebben de rode draad in hun leeswijzer toegelicht, dus ik verwijs daar naar. Ik wil wel aandacht vragen voor een artikel dat op een andere wijze ontstond dan dat wij voor ogen hadden. Enige tijd geleden heeft Aaron Boudewijn bezwaar gemaakt tegen het opnemen van zijn vingerafdruk in het paspoort. We hadden afgesproken dat hij zijn beweegredenen en het proces in een artikel voor deze special zou verwoorden. Helaas bereikte ons een paar weken geleden het bericht dat hij plotseling, op zeer jeugdige leeftijd, is overleden. Als redactie hebben we in het online-condoleanceregister ons medeleven betuigt met zijn verwanten. Mede in zijn nagedachtenis heeft Miek Wijnberg van de stichting Vrijbit, waar Aaron nauw bij betrokken was, het op zich genomen om het artikel te schrijven. Hartelijk dank daarvoor!

In het vorige nummer heb ik flink wat wijzigingen binnen de redactiecommissie aangekondigd. Dat heeft met dit nummer zijn beslag gekregen. We hebben de gemiddelde zittingsduur van de redactieleden flink weten te verkorten ☺ doordat Renato Kuiper afscheid heeft genomen van de redactie. Dat is een flink verlies, want hij is niet alleen een aantal jaren redactielid geweest, hij was ook vijf jaar de hoofdredacteur van dit blad. Gelukkig blijft hij actief voor het PvIB, onder meer doordat hij lid is van de professionaliseringscommissie. We verwachten natuurlijk ook wel regelmatig bijdragen vanuit die commissie... Hoe dan ook, we willen Renato hartelijk bedanken voor zijn inzet bij het uitbouwen en professionaliseren van dit blad.

We hebben wel goede vervanging gevonden. Twee mensen om precies te zijn. Maarten Hartsuijker is toegetreden tot de redactie. Maarten heeft al een groot aantal bijdragen aan dit blad geleverd, vooral technische artikelen, en hij heeft altijd wel ideeën voor nieuwe artikelen. En ook Rachel Marbus is toegetreden tot de redactiecommissie. Dat doet ons deugd om meer dan alleen de reden dat de inhoudelijke redactie eindelijk wordt uitgebreid met een vrouw. Rachel mogen we wel als autoriteit op het gebied van privacybescherming beschouwen en ze zal dan ook als vaste columnist haar licht over dat onderwerp laten schijnen. En dat doet ze voor het eerst in dit nummer; de privacy special van 2010. Het kon niet toepasselijker, toch?

We verwachten dat deze special een mooie bijdrage levert en we wensen u veel leesplezier.

André Koot
Hoofdredacteur

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

Redactie
André Koot (hoofdredactie, werkzaam bij Univé-VGZ-IZA-Trias),
e-mail: A.Koot@Unive.nl
Cynthia Kremer (eindredactie, Motivation Office Support bv, Nijkerk)
e-mail: ibmagazine@pvib.nl

Redactieraad
Said El Aoufi (Metapoint)
Tom Bakker (Delta Lloyd)
Lex Borger (Domus Technica)
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
Rob Greuter
Maarten Hartsuijker (ANWB)
Aart Jochem (GOVCERT.NL)
Rachel Marbus (BetterID4all)
Gerrit Post (G & I Beheer BV)

Advertentieacquisitie
e-mail: adverteren@pvib.nl

Vormgeving en druk
De Drie Poorten, Nijkerk

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

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

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

ISSN 1569-1063

Inhoud

Inleiding Privacy Special

Auteurs: Lex Dunn en Aart Jochem > Lex Dunn CISSP ISSMP is Security Officer bij een grote, internationale ICT-dienstverlener. Hij is een van de redacteuren van het blad Informatiebeveiliging en editor van een schriftelijke CISSP-cursus. Hij is bereikbaar via lex.dunn@capgemini.com.

Ir Aart Jochem CISSP is teamleider bij GOVCERT.NL, het incident response team van de Nederlandse overheid. Hij is ook een van de redacteuren van het blad Informatiebeveiliging en is bereikbaar via aart.jochem@govcert.nl.

Lex Dunn Aart Jochem

"Ben jij ook zo bang, dat alles automatisch wordt
Dat je geen eten meer krijgt, maar pillen op je bord
En dat men als het nodig is, alles van je weet
En dat je niet meer hoeft te werken voor je zweet"
(Toontje lager - 1982)

Privacy is een term met een redelijk emotionele lading. Het raakt iedereen, en iedereen heeft er dan ook wel een mening over, alhoewel die meningen soms lijnrecht op elkaar staan (net als de belangen). Ook komt het vrijwel dagelijks aan de orde in de pers en onze vakliteratuur.

Een paar willekeurige voorbeelden:
22 april 2010 Van der Hoeven werkt aan cookieverbod (www.binnenlandsbestuur.nl/nieuws/2010/04/van-der-hoeven-werkt-aan-cookieverbod.157049.lynkx)
8 April 2010 Microsoft zegt: Privacy is niet dood (www.security.nl/artikel/32996/1/Microsoft%3A_Privacy_is_niet_dood.html)
23 Maart 2010 Justitie moet afblijven van OV-chipkaart foto's (www.security.nl/artikel/32836/1/Justitie_moet_afblijven_van_OV-chipkaart_foto%27s.html)
22 Maart 2010 EU-waakhond wil privacywetgeving voor browsers (www.security.nl/artikel/32821/1/EU-waakhond_wil_privacywetgeving_voor_browsers.html)
16 Februari 2010 Student naar rechter om privacy paspoort (www.nu.nl/binnenland/2185458/student-rechter-privacy-paspoort.html)
10 December 2009 Facebook zet privacy overboord (webwereld.nl/nieuws/64564/facebook-zet-privacy-overboord.html)

Maar wat is privacy nou precies? Van Dale zegt er het volgende van:
pri·va·cy [prajvesie] de; v(m) de mogelijkheid om in eigen omgeving helemaal zichzelf te zijn.

Het gaat om het recht om met rust gelaten te worden.[1] Niet een onbelangrijk recht, het is verankerd in de Nederlandse grondwet en het Europese Verdrag voor de Rechten van de Mens.[2]

Deze definitie laat nogal wat ruimte voor interpretatie en krijgt pas invulling in concrete gevallen. Ook dan is er discussie over het bereik van het begrip privacy. Het is een zogenaamd waardebegrip. In de praktijk blijkt dat ondermeer uit grote verschillen in de omgang met persoonlijke gegevens: veel websites laten zich niet veel gelegen liggen aan de privacy van hun gebruikers. Facebook en Google zijn natuurlijk bekend vanwege hun omgang met privacy, maar uit het jaarverslag 2009 van het College Bescherming Persoonsgegevens (CBP) blijkt dat ook bij kleinere (lees: minder bekende) bedrijven en organisaties regelmatig de plank mis wordt geslagen wat betreft privacy. De politie ging in de fout met de Automatische Kentekenherkenning (ANPR) door alle gescande kentekens, die geen match opleverden, langer vast te houden dan noodzakelijk. Maar ook enkele Arbo-diensten en ziekenhuizen bleken niet conform de Wet Bescherming Persoonsgegevens (WBP) te handelen. En het verzamelen van gegevens via het internetbedrijf Advance gebeurde zonder de deelnemers te informeren over de verwerkingen van de door hun ingetikte gegevens.

Niet alleen de ruimte voor interpretatie maakt het moeilijk om het goed te doen. Vaak botst het recht op privacy met andere belangrijke zekerheden, zoals veiligheid of vrij ondernemerschap. Of juist met efficiency. In het digitale tijdperk is het gemakkelijk alles te bewaren en moeilijk iets te vergeten. Privacy moet daarom soms bevochten worden, niet alleen in totalitaire staten, maar ook in een gezonde democratie. In Nederland kennen we een toezichthouder (College Bescherming Persoonsgegevens CBP) en burgerrechtenorganisaties

1 'Het recht om met rust gelaten te worden' werd als eerste geponeerd in een artikel door Warren en Brandeis in Harvard Law Review in 1890.
2 In de Nederlandse Grondwet is het artikel 10. Dat kent een meer algemene bepaling over privacy en een gespecialiseerde over informationele privacy (algemeen is lid 1, informationeel is lid 2 en 3). Deze laatste zijn de basis voor de Wet Bescherming Persoonsgegevens (WBP). In het Europese Verdrag voor de Rechten van de Mens is het artikel 8.

(Bits of Freedom, Privacy First, Vrijbit). Er zijn politici die zich sterk maken voor het recht om met rust gelaten te worden, zoals Sophie In 't Veld, en juristen die de wetten begrijpen en kunnen toepassen, zoals Rachel Marbus en Arnout Engelfriet. En er zijn beveiligingsprofessionals die een gezonde balans moeten vinden tussen privacy en beveiligingsmaatregelen of compliancy en efficiency.

Grote vraagstukken liggen momenteel bij parlementariërs en senatoren. Hoe gaan we om met centrale opslag van vingerafdrukken, DNA-profielen, kind- en patiëntgegevens of slimme energiemeters in de huizen? Op 1 juni heeft de Eerste Kamer zich uitgesproken over het Elektronisch Patiënten Dossier (EPD). Bij het schrijven van dit artikel lijkt het erop dat de Eerste Kamer dit wetsontwerp gaat afserveren.
In deze tweede Privacy Special van Informatiebeveiliging proberen we u een breed overzicht te geven van de ontwikkelingen rondom het thema privacy. Niet alleen in de techniek, maar ook vanuit juridisch oogpunt en van uit het standpunt van 'Nederland'. En uiteraard heeft Berry zo zijn mening over privacy. Ook het menselijke aspect, iets waar we als paranoïde beroepsgroep tegen aanlopen, krijgt aandacht. Rachel Marbus, auteur van het artikel in deze uitgave over identiteitsmanagement nieuwe stijl en tevens twitterdiva, konden we overhalen iets te vertellen hoe het is om je open te stellen in sociale media.

Privacy is binnen de PvIB een actueel onderwerp. Binnen korte tijd werden er twee themasessies aan dit onderwerp gewijd. Op 15 april 2010 werd voor de Young Professionals een Masterclass 'Kijk op Privacy' georganiseerd. Een verslag van deze middag vindt u in dit nummer. Op 20 mei 2010 kwam het thema aan de orde tijdens de sessie 'Ik heb niets te verbergen, dus ik heb niets te vrezen' in Amersfoort. Een verslag van deze bijeenkomst komt in het volgende nummer van IB.

(Foto door Tristan Nitot)

Wat is er voor u van belang? Wat is een goede aanpak? Met gezond verstand nadenken over het omgaan met persoonsgegevens brengt u al een eind op weg. Denk erover na met als uitgangspunt dat iedereen eigenaar is van gegevens over zijn persoon en ervan uit mag gaan dat verwerking van deze gegevens zorgvuldig gebeurt. De volgende vijf punten kunnen als leidraad dienen bij de bescherming van uw klantenbestand (met dank aan Menno Borst, IT Risk Management bij Maxeda):

Richtlijn #1 - Klantbescherming
- Consument dient actief gebruik van zijn informatie te bevestigen.
- Consument moet zelfstandig in staat is om zijn klantinformatie in te zien, te veranderen of te verwijderen.
- Gebruik van klantinformatie dient aangemeld te zijn bij het CBP (er zijn gronden voor vrijstelling van de meldplicht, het CBP heeft hiervoor een handreiking geschreven).[3]

Richtlijn #2 - Opslag van klantinformatie
- Fysieke opslag van klantinformatie moet tot een minimum worden beperkt.
- Digitale klantadministratie moet gecentraliseerd zijn (geen excel-sheet).
- Toegang tot klantinformatie dient tot een minimum beperkt te zijn.
- Back-ups zijn met extra maatregelen beschermd (encryptie van opslag).

Richtlijn #3 - Logische toegangsbeveiliging
- Applicatietoegang ingericht op basis van minimale rechten 'least priviliged rights'.
- Applicatietoegang alleen voor individuele gebruikers, geen groep accounts;
- Database toegang alleen via noodaccount.
- Medewerkers tekenen een geheimhoudingsverklaring.
- Wachtwoordbeleid dient op hoogste niveau te worden nageleefd.

Richtlijn #4 - Encryptie van transactieverkeer
- Communicatie dient vanaf de bron tot aan de ontvanger volledig encrypted plaats te vinden.

Richtlijn #5 - Externe partijen
- Externe partijen dragen zorg voor compliancy ten opzichte van WBP.
- De richtlijn privacy dient onderdeel te zijn van het contract met externe partijen.

Menno Borst heeft deze vijf punten (uitgevaardigd als het privacybeleid van Maxeda Holding en al haar werkmaatschappijen zoals de Bijenkorf, V&D, Hunkemüller, Praxis, M&S Mode) gepresenteerd tijdens de PvIB themasessie Security Trends 2010 op 18 maart 2010.

We hopen dat we u met deze Privacy Special een breed beeld van het thema hebben gegeven. Mocht u opmerkingen of suggesties hebben, dan vernemen we die graag via ibmagazine@pvib.nl.

Links
Het jaarverslag 2009 van het CBP: www.cbpweb.nl/Pages/jv_2009.aspx

1 'Zie hiervoor de website van het CBP: www.cbpweb.nl/hvb_website_1.0/i2.htm

Informatietechniek, entrepreneurs en wetgevers in de clinch met het grondrecht op privacy

Auteur: Mr. V.A. de Pous > Mr V. (Victor) A. de Pous is een nationaal en internationaal bekende jurist en auteur van ontelbare publicaties, zoals boeken, artikelen en white papers, die zich vooral richten op de sociale en juridische aspecten van de informatiemaatschappij. Daarnaast is Victor de drijvende kracht achter velerlei initiatieven zoals de International Telework Foundation. Victor is de uitgever van de lezenswaardige periodiek NEWSWARE.

Of de persoonlijke levenssfeer nu een 'sitting duck' of 'moving target' is, overheid en bedrijfsleven schieten voortdurend in de roos. Dat gebeurt zowel door toepassing van technologische vindingen en nieuwe zakelijke modellen, als door wetgevers die misdaad en terrorisme met informatiewapens willen bestrijden. De van huis uit analoge burger ontbeert in de zo geprezen informatiemaatschappij meer dan ooit het recht om met rust gelaten te worden. Weg met de anonimiteit; leve registratiewoede. En steeds vaker geeft de burger vrijwillig zijn privacy op. Je doet alleen mee als je op Facebook zit en je je vrienden dagelijks vertelt wat je uitspookt.

Het was crimefighter en Tweede Kamerlid Teeven (VVD) die in 2008 weer eens de belegen drogreden uit de kast haalde. 'Wie niets te verbergen heeft, heeft niets te vrezen'. De oud-officier van justitie is een fervent voorstander van de Europese richtlijn dataretentie, op grond waarvan ook in Nederland verkeersgegevens van internet en mobiele telefonie bewaard moeten blijven en op eerste verzoek aan Justitie ter beschikking worden gesteld. De communautaire wet is exemplarisch voor het post-11/9 tijdperk, waarin terroristenbestrijding prioriteit heeft. Na veel debat bij ons werd de wettelijke bewaarplicht voor ISP's en hostingbedrijven van verkeersgegevens van internet op zes maanden bepaald. Voor telefonieaanbieders geldt een termijn van twaalf maanden ten aanzien van de nawgegevens. Ondertussen moet iedere aanbieder van een openbare dienst of openbaar netwerk de gegevens ook nog eens zorgvuldig beveiligen, mede op basis van een beveiligingsplan. Regels voor een minimumniveau zijn opgenomen in het Besluit beveiliging gegevens telecommunicatie.

Voor de marktpartijen spelen geen fundamentele privacykwesties, maar harde pecunia in een sterk op prijs concurrerende markt. Zij kanten zich fel tegen deze bewaarplichten vanwege het administratief lastenverzwarend karakter. Niet onbelangrijk, maar wel van beduidend geringer gewicht dan het recht op privacy. Dat is en blijft een groot goed. Het gaat om een uiterst belangrijke, zo niet essentiële basisvoorwaarde voor het welzijn van de mens, dat terecht legislatief beslag heeft gekregen in onze grondwet. Privacy, het recht op bescherming van de persoonlijke levenssfeer, stamt van origine uit de Verenigde Staten. Daar bedachten twee rechtsgeleerden, Brandels en Warren, tegen het einde van de 19e eeuw het recht om met rust gelaten te worden én verschoond te blijven van ongerechtvaardigde publiciteit. Een omschrijving die in de informatiemaatschappij 2.0 met haar virtuele sociale netwerken niets aan waarde heeft ingeboet.

Naast het passieve privacyrecht ontstond grosso modo 50 jaar geleden de gedachte haar aan te vullen met een actieve component: het recht van het individu om te bepalen wat er met zijn informatie gebeurt. Noem het informationele privacy. Ook in dit kader dringt een verwijzing naar internet met Google, Hyves en Facebook zich nadrukkelijk op. Enerzijds geven mensen blijkbaar gemakkelijk hun persoonlijke levenssfeer in een online-omgeving op. Anderzijds constateren we omstreden privacybeleid van sociale netwerken en zien tevens ernstige fouten in de programmatuur van de websites, zodat ook langs deze weg, onbedoeld en ongewenst, inzage wordt verstrekt in bijvoorbeeld vertrouwelijke communicatie.

Informatietechniek

Waar staan we anno 2010? In de wereld van sociale netwerken, cloud computing, augmented reality, EDP's, RFID-applicaties, chipkaarten voor het openbaar vervoer, bewakingscamera's, intelligente energiemeters, rekeningrijden en vele andere ICT-toepassingen, zullen de automatisch geregistreerde gegevens in veel gevallen te herleiden zijn tot een identificeerbaar natuurlijk persoon. Neem als voorbeeld een zoekvraag aan Google. Twee jaar geleden publiceerde de zogenoemde Artikel 29-werkgroep van de samenwerkende privacytoezichthouders van de Europese Unie een scherpe opinie. De communautaire privacyregelgeving is in beginsel altijd van toepassing op het verwerken van persoonsgegevens door zoekmachines. Bovendien geldt deze hoofdregel in

veel gevallen als het hoofdkantoor van de aanbieder van de zoekmachine buiten de Europese Unie is gevestigd. Zes maanden bewaren van de persoonsgegevens is het maximum.

Voor de goede orde: in de 27 lidstaten van de Europese Unie is de privacywetgeving geharmoniseerd. In Nederland is de richtlijn omgezet in de Wet bescherming persoonsgegevens, die in september 2002 inwerking trad. De WBP gaat uit van de verwerking van persoonsgegevens; een ruimer begrip dan aanleg en gebruik van persoonsregistraties. Onder de vergrootte reikwijdte vallen vrijwel alle vormen van omgang met persoonsgegevens zoals het verzamelen, de opslag, het bewaren, het vergelijken, het koppelen, het raadplegen en het verstrekken van persoonsgegevens aan een derde.

Gegevens zijn pas persoonsgegevens in de zin van de wet, als die gegevens informatie bevatten over een natuurlijk persoon en die persoon identificeerbaar is. De verwerking van persoonsgegevens moet altijd rechtmatig gebeuren. Dat wil zeggen op een behoorlijke en zorgvuldige wijze én in overeenstemming met de wet. Dat is goed beschouwd de crux van de Wet bescherming persoonsgegevens.

Zoals gezegd, ook sociale netwerken kunnen met de persoonlijke levenssfeer van haar leden in de knel komen. Zo gaf Facebook eind vorig jaar met zoveel woorden te kennen de privacy van haar 400 miljoen gebruikers op te heffen. De profielpagina op de site wordt namelijk standaard ´open´ gezet. Het zijn echter vooral private organisaties die tegen zijn en aan de bel trekken, waaronder de Amerikaanse stichting Electronic Frontier Foundation. En niet de leden. Ook in Nederland roept de Consumentenbond sociale netwerksites op om de profielpagina's per definitie juist 'dicht' te zetten.

Cloud computing

Zowel zoekmachines als het interactieve Web 2.0 zijn verschijningsvormen van cloud computing. Daarbij gaat het om nieuw automatiseringsmodel, waar ICT verandert van een product in een dienst. De gegevensverwerking vindt via breedbandnetwerken plaats in gekoppelde, geografisch verspreide datacenters. Soms zelfs in verschillende landen en op verschillende continenten, in wisselende samenstelling wat één virtuele computerfabriek vormt. Goed beschouwd wordt het netwerk de computer. Dat maakt technologie- en informatiemanagement ronduit complex. Het meest ingewikkelde kader doet zich voor bij third-party cloud computing, dus in de omstandigheid wanneer een gebruikersorganisatie diensten afneemt van een externe leverancier. De eindgebruiker of gebruikersorganisatie heeft dan geen controle over en kennis van exacte locatie van de geleverde ICT-onderdelen en het virtuele informatiesysteem.

Ook de Europese privacytoezichthouders maken zich zorgen over cloud computing. Zo constateren zij allerlei organisatorische verschillen in de publieke en private sector en ook ICT-ontwikkelingen en grensoverschrijdende gegevensverwerking. Dat zorgt voor complexiteit. In toenemende mate kunnen we scenario's schetsen waarbij verantwoordelijken en bewerkers beiden een rol spelen en waarbij het lastig is vast te stellen wie welke verantwoordelijkheid heeft. Tegen deze achtergrond heeft de Artikel 29-werkgroep van de privacytoezichthouders in Europa, die op naleving van de wetgeving ter zake toeziet, recent een belangrijke opinie aangenomen, die uitleg geeft over de begrippen 'verantwoordelijke' en 'bewerker'. Dat zijn sleutelbegrippen van onze privacywetgeving.
Burgers moeten immers weten aan wie ze vragen kunnen stellen over de over hen opgeslagen persoonsgegevens en waar ze zo nodig hierover een klacht kunnen indienen. Zonder helderheid over de vraag wie de verantwoordelijke is, moeten burgers spoorzoeken en lopen zij het risico van het kastje naar de muur te worden gestuurd.

Spam

Aardig dat de wetgever uit privacyoogpunt burgers door middel van het nieuwe telecommunicatierecht wil beschermen tegen commerciële bellers, faxers, e-mailers, tweets en sms'ers. Geen bericht, zonder voorafgaande toestemming, luidt de hoofdregel van het elektronische junkmailrecht in de business-to-consumer markt in de Europese Unie. Voor Nederland ging dit spamverbod echter niet ver genoeg en onze wetgever bracht vervolgens ook de zakelijke markt onder de werkingssfeer van de opt-in regeling, die vorig jaar oktober van kracht werd. Een bedrijf mag ineens niet langer een ander bedrijf ongevraagd een aanbod langs elektronische weg doen. Maar wat heeft dat met privacy te maken? En de sancties liegen er niet om. Wie toch spamt, hangt een bestuurlijke boete van 450.000 euro boven het hoofd, die de OPTA-overtreders van de telecommunicatiewetgeving kan opleggen.

Voor toezicht op onze privacy kennen we een andere organisatie, het College Bescherming Persoonsgegevens. Ook die is bevoegd om in voorkomende gevallen administratiefrechtelijke sancties op te leggen. Hier bedraagt de maximale geldboete slechts een procent van het maximum dat OPTA kan opleggen namelijk, 4500 euro. Betekent dit proportionele verschil dat de politiek van mening is dat het klassieke grondrecht op bescherming van de persoonlijke levenssfeer bijna volledig gemarginaliseerd moet worden tegenover het recht op bescherming tegen spam, dat uit Nederland wordt verstuurd?

Relatief recht

Vergeet niet dat het recht op privacy geen absoluut maar een relatief recht betreft. Dat betekent dat de belangen van het individu in het concrete geval afgewogen worden tegenover de andere belangen. Denk aan fraude-, misdaad- en terrorismebestrijding. Zoals het wettelijk kader zich nu toont, fungeert de noodzaak tot de aanpak van criminaliteit nogal eens als vrijbrief voor allerlei ingrijpende, privacybeperkende maatregelen, terwijl bijvoorbeeld het gerechtvaardigde commercieel ondernemersbelang om in redelijkheid gebruik te maken van de informatietechniek - zoals goedkope e-mailings aan prospects - het aflegt tegen het recht om met rust gelaten te worden.

Consensus over privacy zal waarschijnlijk minder dan ooit te voren ontstaan. Voor overheid en bedrijfsleven geldt vaak het uitgangspunt dat beide graag over zo veel mogelijk informatie van personen willen beschikken. En overheidsorganisaties leggen in toenemende mate bewaarverplichtingen op. Straks mogen we niets meer weggooien. En de burger? Tja, wat wil de burger in de informatiemaatschappij eigenlijk? Gratis (ICT-)diensten tegen verstrekking van zijn persoonsgegevens?

Identiteitsmanagement nieuwe stijl: hoe scheid ik al mijn rollen?

Auteur: mr Rachel Marbus > Rachel Marbus is juridisch adviseur op het gebied van ICT & Recht en eigenaar van BetterID4ALL. Daarnaast is zij verbonden aan het Tilburg Institute for Law, Technology, and Society (Tilt) waar ze in 2010 zal promoveren op een proefschrift over identiteit en identiteitsmanagement in de online-wereld.

In een wereld waarin het steeds gemakkelijker wordt om meer van mensen te weten te komen en al die informatie aan elkaar te koppelen, wordt het steeds lastiger om jezelf af te schermen. De snelheid, permanentheid, koppelbaarheid en kopieerbaarheid van informatie zet in toenemende mate de privacy van personen onder druk. Identiteitsmanagement probeert de persoonlijke informatiestromen in goede banen te leiden. Maar, de realiteit laat zien dat de huidige benadering van identiteitsmanagement tekort schiet. Zij neemt de technologie als uitgangspunt en stelt dat identiteit gelijk is aan een verzameling attributen (gegevens, kenmerken) van een persoon. Identiteit gezien als sociaal fenomeen biedt daarentegen inzichten die behulpzaam kunnen zijn bij het tegemoetkomen van de gerezen problemen rondom privacy en identiteit. In het onderstaande artikel pleit Rachel Marbus er daarom voor identiteitsmanagement breder te zien dan slechts het klassieke identificatie-, authenticatie- en authorisatieproces. Ook het beheer van de sociale dimensie van identiteit dient eronder te worden geschaard, juist omdat deze nieuwe zienswijze de knelpunten op het gebied van identiteit en privacy duidelijker blootlegt en mogelijke oplossingsrichtingen biedt.

Maria koopt een boek over communicatiestijlen bij Bol.com zodat ze zich kan voorbereiden op de zware gesprekken die haar op het werk te wachten staan. Ze vraagt opnieuw haar Digid-code aan omdat ze voor de zoveelste keer haar wachtwoord is vergeten en de jaaraangifte verstuurd moet worden. Ze zet de foto's van het vrijgezellenfeest van haar vriendin op Hyves en plaatst ook meteen een krabbel op de pagina van een andere vriend die pas geleden zijn baan verloren is. Op al deze verschillende momenten is Maria dezelfde persoon die ze altijd al was en toch is ze overal net even anders. Maria neemt verschillende rollen in en bij al die rollen hoort een ander publiek. Dan weer is ze klant of werknemer, dan een burger en op een ander moment een vriendin.

In een klassieke benadering van identiteitsmanagement wordt gekeken vanuit de techniek; een entiteit dient aangemeld te worden bij het systeem en vervolgens kan deze entiteit bepaalde handelingen juist wel of juist niet verrichten. Dit gaat uit van een vrij platte benadering van het begrip identiteit als een samenraapsel van een aantal attributen (zoals naam, e-mailadres en kleur haar) die tezamen een identiteit zouden zijn. Dat hierbij eigenlijk geen sprake is van identiteit wordt duidelijk als de sociologische betekenis van het begrip in ogenschouw wordt genomen. Identiteit is een breder en rijker begrip en het bevat veel meer dan slechts een verzameling attributen. In het onderstaande artikel wordt daarom een pleidooi gevoerd voor een andere benadering van identiteitsmanagement die breder is dan de klassieke benadering, juist omdat die laatste in huidige tijden steeds vaker tekort lijkt te schieten en tot vele vragen leidt op het gebied van privacy en identiteit.

Wat is identiteit?

Identiteit is een begrip dat lastig te vatten is in een omschrijving, laat staan in een definitie. Juist daarom wordt binnen de sociale wetenschappen regelmatig niet het vertrekpunt 'wat is identiteit?' maar 'hoe komt identiteit tot stand?' ingenomen als gesproken wordt over identiteit. Diverse auteurs gebruiken overigens steeds vaker sociologische inzichten voor een betere begrip van identiteitsmanagement.[1] De laatste jaren wordt daarbij vaak het werk van gerenommeerd socioloog Goffman[2] gebruikt om meer inzicht te krijgen in identiteit(en) en het beheer daarvan binnen de technologisch gemedieerde wereld. Volgens Goffman komt identiteit tot stand in sociale interactie.[3] Dat gaat ongeveer als volgt: ik presenteer mezelf zoals ik graag gezien wil worden. Anderen zien mijn zelfpresentatie en reageren daarop. Aan de hand van de reacties die ik krijg op mijn zelfpresentatie, stel ik deze vervolgens bij. Dit is een doorlopend proces waarin sprake is van een continue wisselwerking tussen personen. Belangrijk voor een goed begrip van identiteitsmanagement is het werk van Goffman op het gebied van 'audience segregation' (publieksscheiding).[4] Een persoon neemt in zijn leven meerdere rollen in. Hij is vader, werknemer, broer, vriend, klant, burger, enz. Bij al deze rollen hoort een bepaald publiek. Wil een persoon al die verschillende rollen in het leven goed kunnen uitvoeren, dan moet hij de rollen en de diverse publieken strikt van elkaar

1 Zie bijvoorbeeld het werk van danah boyd, R.E. Leenes, B. van den Berg en ook het Europese Privacy and Identity Management for Europe (PRIME) project: www.prime-project.eu.
2 Erving Goffman, 1922-1982.
3 E. Goffman, The presentation of self in everyday life, 1959 Anchor books.
4 E.Goffman, Stigma. Notes on the management of spoiled identity, Simon and Schuster 1963 (first Touchstone edition 1986), p. 63.
5 Goffman 1959, p. 137.

gescheiden houden.[5] Als publieken (en dus de verschillende rollen) samenvallen kan dit ertoe leiden dat een persoon niet langer geloofwaardig is binnen een bepaalde rol of dat een zorgvuldig opgebouwde reputatie teniet wordt gedaan.[6] Als een baas zijn werknemers tegenkomt in de sauna kan dit zijn autoriteit ten opzichte van hen teniet doen. De verhoudingen op de werkvloer kunnen daardoor problematisch worden. Ook de context van bepaalde informatie over iemands identiteit is daarbij erg belangrijk. Informatie over een persoon die uit een specifieke context wordt gehaald en binnen een andere wordt gebruikt, kan iets geheel anders gaan betekenen en kan zelfs een verkeerd beeld van die persoon weergeven. De opmerking: 'Ik loop heel graag naakt' is vrij normaal op een chatsite over naturisme, maar in een werkomgeving zul je dit niet snel zeggen. De context van de informatie over een persoon en het gescheiden houden van de verschillende publieken bij de diverse deelrollen zijn dus van groot belang voor het goed kunnen functioneren in de maatschappij.

Wat is de klassieke benadering van identiteitsmanagement?

Binnen de klassieke visie op identiteitsmanagement wordt op een andere manier naar het begrip identiteit gekeken. Dit werkt door in de omgang met identiteiten en het beheer daarvan. Een individu moet - technisch gezien - geïdentificeerd (herkend) kunnen worden voordat hij daadwerkelijk gebruik kan gaan maken van zijn identiteit in een specifieke omgeving (identificatie, authenticatie, autorisatie). Dit gebeurt door bepaalde aspecten (ook wel aangeduid met attributen of kenmerken) over iemand vast te leggen en samen te begrijpen als zijn identiteit. Dit kan heel eenvoudig een e-mailadres zijn in combinatie met een aantal andere persoonlijke gegevens, maar kan ook meer gegevens van een persoon omvatten. Deze identiteit kan dan worden herkend bij opvolgende bezoeken aan de specifieke omgeving. Hierbij dient opgemerkt te worden dat datgene wat een individu vervolgens na identificatie door het systeem doet binnen een omgeving, doorgaans niet geschaard wordt onder deze meer technische visie op identiteit. Het sociale begrip van identiteit daarentegen stelt dat het juist van essentieel belang is om datgene wat personen doen na de identificatie - te weten sociale interactie - mee te nemen in het proces van identiteitsmanagement. Sterker nog, het maakt er juist onlosmakelijk deel van uit. Identiteit en het beheer daarvan stopt namelijk niet na het identificeren, de vorming van identiteit begint dan namelijk pas echt gestalte te krijgen. Identiteit is dus niet slechts een verzameling attributen, maar het geheel van alle verschillende rollen en de daarbijbehorende publieken van een individu. Deze rollen veranderen naar verloop van tijd en ook zullen sommige daarvan verdwijnen terwijl nieuwe rollen zich aandienen. Onze identiteit is dus niet alleen flexibel en dynamisch, maar vooral ook erg rijk en veelomvattend.[7]

Waarom is de klassieke benadering niet langer afdoende?

De klassieke benadering waarin iemands identiteit beperkt wordt tot een verzameling van een aantal attributen aan de hand waarvan hij herkend kan worden door een systeem is - wellicht technisch gezien noodzakelijk - slechts een beperkte visie omdat het de dynamische en flexibele kant van de identiteit van personen niet omvat. Identiteitsmanagementsystemen gaan doorgaans uit van deze klassieke benadering. Voor het beheer van de identiteiten die bij één persoon horen is deze persoon daarom vaak op zichzelf aangewezen en op de mogelijkheden die verschillende omgevingen hem bieden. Soms is daarbij relatief veel vrijheid, denk aan een identiteit op een sociale netwerksite waar personen zelf in de hand hebben (tot op bepaalde hoogte) wat zij over zichzelf vertellen en wat zij laten zien. Een andere keer is de vrijheid beperkt doordat een aanbieder van een dienst of een bepaalde omgeving dwingend vastlegt welke gegevens een persoon over zichzelf moet prijsgeven voordat hij gerechtigd is van de dienst of de omgeving gebruik te maken. Denk daarbij aan het kopen van een boek via een site als Bol.com. Bol heeft een correct adres nodig waar zij de bestelling heen kan sturen en daarnaast moet zij weten of de persoon die de bestelling plaatst in staat is te betalen.

In de offline wereld is het nog redelijk gemakkelijk om al die verschillende rollen en publieken van elkaar gescheiden te houden. De muren van het kantoor en die van mijn huis voorkomen dat mijn werk en privé met elkaar in aanraking komen. In de technologisch gemedieerde wereld blijkt de publieksscheiding lastiger. Steeds vaker worden verschillende rollen van één persoon samengebracht vanuit de gedachte dat de digitale 'sleutelbos' verkleind moet worden (denk aan initiatieven als OpenID of Open Social),

6 Goffman 1963, p. 63.

7 Deze rijkheid van de identiteit is met de komst van technologie steeds groter geworden juist doordat er meer mogelijkheden bestaan om meer informatie over een persoon te verstrekken en aan elkaar te koppelen.

8 In de wetenschap wordt hiernaar wel in toenemende mate onderzoek gedaan. Het gaat daarbij om zogenaamde privacy enhancing identitymanagement systems Zie bijvoorbeeld het werk binnen PRIME (Privacy and Identity Management for Europe).

maar ook is het gemakkelijker voor derden om de rollen van één persoon samen te brengen (denk aan het gebruiken van zoekmachines als wieowie.nl en spezify.com). Publieksscheiding en het behouden van een privésfeer rondom een bepaalde deelrol is daardoor vaak lastig en soms zelfs onmogelijk. Tot op heden bestaat er nog geen werkend identiteitsmanagementsysteem dat rekening houdt met de behoefte van personen om verschillende rollen van elkaar gescheiden te houden.[8] Wel wordt er al mondjesmaat gewerkt met de principes van de publieksscheiding binnen specifieke sectoren. Vooral de wetenschap neemt hierin het voortouw. De nieuwe sociale netwerksite Clique is daar een goed voorbeeld van.[9] Op deze (non-profit) sociale netwerksite kan een persoon verschillende, strikt van elkaar gescheiden, deelidentiteiten aanmaken onder één account. Ook kan hij de informatie die hij over zichzelf prijsgeeft zeer gericht aan bepaalde aan te wijzen personen kenbaar maken.

Wat zou identiteitsmanagement dan moeten zijn?

Kijkend naar de sociale visie op persoonlijke identiteit, kan gezegd worden dat identiteitsmanagement dus ook te maken heeft met het beeld dat iemand presenteert van zichzelf en het beeld dat anderen van deze persoon hebben door die presentatie. Daarnaast is sprake van een complex dynamisch proces rondom persoonlijke identiteit en de interactie die met identiteiten plaatsvindt. Identiteitsmanagement bestaat daardoor naast het meer technische aspect van het identificeren ook uit het beheren van de presentatie van het zelf en het beheren van het beeld dat anderen van ons hebben of het beeld dat anderen ons opleggen wat mede deel gaat uitmaken van onze identiteit. Deze kant van het identiteitsmanagement blijft vaak onderbelicht in de literatuur.[10] Als geschreven wordt over identiteitsmanagement wordt meestal eerst en vooral aandacht besteed aan het technische proces en de vereisten die dit met zich meebrengt. Juist doordat er zoveel meer gaande is rondom de identiteit(en) van personen en de steeds grotere rijkheid daarvan pleit ik ervoor het begrip identiteitsmanagement niet te laten stoppen na het technische aspect. Juist de fase na identificatie waar personen interactief met elkaar, de overheid of het bedrijfsleven worden, laat zien dat er veel meer is dat beheerd dient te worden. Het beheer van identiteit stopt dus niet na het identificatie-, authenticatie- en autorisatieproces.

Identiteitsmanagement is daarom:

1) het technische proces rondom het kunnen herkennen van eenzelfde identiteit voor de toegang tot een bepaalde dienst of omgeving (identificatie, authenticatie, authorisatie) en;
2) het sociale proces rondom het beheren van de verschillende identiteiten en de informatie daaraan verbonden van een individu. Daarbij behoort tevens het beheer betreffende de publieksscheiding.

Hoe nu daadwerkelijk dit tweede gedeelte van identiteitsmanagement te realiseren, is een vraag die ten dele nog open ligt. Een initiatief als Clique geeft in ieder geval weer dat er wel degelijk technische mogelijkheden zijn om binnen het ontwerp van online-omgevingen te werken met privacyverhogende principes en het gedachtegoed van publieksscheiding. Echter, de vragen op het gebied van privacy en identiteit kunnen niet alleen worden opgelost door de technologie. De mens zelf zal daarbij ook een bepalende rol gaan spelen die wellicht voor een gedeelte te maken zal hebben met zelfcensuur[11] en een sterker bewustzijn van de hoeveelheid aan verschillende soorten rollen die hij in het leven inneemt en de betekenis daarvan. Het laatste woord is daarmee niet gesproken en een definitieve allesomvattende oplossing lijkt een utopische gedachte, maar door op deze manier naar identiteitsmanagement te kijken, is mijns inziens een start gemaakt om niet alleen te denken in termen van problemen maar vooral ook in die van mogelijke oplossingsrichtingen.

Conclusie

Persoonlijke identiteit is een complex sociaal gegeven waarbinnen een aantal factoren samenkomen die in wisselwerking met elkaar vormgeven aan het begrip. Persoonlijke identiteit is dimensioneel gekleurd en contextafhankelijk en krijgt haar invulling binnen de interactie tussen personen. Identiteit als sociaal begrip kent dus een grote mate van dynamiek en complexiteit. In de technologisch gemedieerde wereld zijn mensen in toenemende mate sociaal met elkaar in verschillende hoedanigheden. Zij spelen spellen met elkaar in gamewerelden, creëren gemeenschappen in virtuele werelden en onderhouden contacten via sociale netwerksites. Ook contacten met de overheid en bedrijven vinden in toenemende mate plaats binnen de online wereld. De huidige stand van de techniek op het gebied van identiteitsmanagement neemt deze sociale dimensie van identiteit niet mee binnen haar systemen en de ontwikkeling daarvan. Omdat datgene wat personen doen na de eerste fase van het identiteitsmanagement doorgaans niet mede geregeld wordt, ontstaan vraagstukken op het gebied van het beheer van identiteit en de privacy van personen. Deelrollen blijken in de online-praktijk van alledag moeilijk gescheiden te houden, contexten lopen in elkaar over en de privacy van personen staat steeds vaker onder druk. Door zich bewust te zijn van het feit dat er bij het beheer van identiteitsmanagement dus meer op het spel staat dan het enkele technische beheer - identificatie, authenticatie en authorisatie - en dat er na deze fase nog veel meer gebeurt met de identiteit van personen, kan een begin gemaakt worden om te kijken naar mogelijke oplossingen voor de gerezen problemen.

9 www.clique.primelife.eu. Clique komt voort uit wetenschappelijk onderzoek van de vakgroep TILT (Tilburg Institute for Law, Technology, and, Society).

10 De hier gepresenteerde visie op identiteitsmanagement is aanmerkelijk breder van aard dan doorgaans wordt verstaan onder identiteitsmanagement. Vergelijk daarvoor de definitie van Valkenburg & Jurg 2007, p. 36. '[identiteitsmanagement] bestaat uit processen en alle onderliggende techniek voor het aanmaken, beheer en gebruik van elektronische identiteitsgegevens'.

11 Zie hierover de column van mijn hand elders in deze special getiteld: 'Ik twitter dus ik ben'.

Arnoud Engelfriet: 'veiligheidsbeleid te veel gebaseerd op angst'

Grijp niet meteen naar het uiterste middel

Auteur: Sandra Kagie > Sandra Kagie is freelance tekstschrijver (website: www.sanscriptproducties.nl). Als ervaren tekstschrijver en eindredacteur verricht zij uiteenlopende werkzaamheden op het gebied van tekst en taal. In het recente verleden is ze als eindredacteur nauw betrokken geweest bij Informatiebeveiliging. Dit artikel is geschreven naar aanleiding van een interview met Arnoud Engelfriet, ICT-jurist, gespecialiseerd in internetrecht.

Onze vereniging publiceert elk jaar voor de leden een handig boekje met zaken als de statuten, het huishoudelijk reglement, besluiten uit het afgelopen jaar en handige tips voor de leden. Ook zetten we hier altijd een lijst met contactgegevens van alle leden in. Dit doen we al jaren, maar het aantal leden groeit gestaag dus nu is voorgesteld om dit boekje voortaan via de website te verspreiden. Maar hebben we dan geen privacyprobleem?

Een van de vele vragen die Arnoud Engelfriet, ICT-jurist , gespecialiseerd in internetrecht, recentelijk beantwoordde op zijn blog (blog.iusmentis.com). De bovenstaande vereniging heeft volgens Engelfriet inderdaad een privacyprobleem. Het publiceren via internet van namen, adressen en dergelijke contactgegevens van leden kan echt alleen met een expliciete toestemming van die leden. En die moet vooraf worden gevraagd.
Aan nieuwe leden zou de vereniging die toestemming via het inschrijfformulier kunnen vragen, maar bestaande leden zullen moeten worden geraadpleegd.
Engelfriet vraagt zich bovendien af of het echt wel nodig is de persoonsgegevens van de leden op deze manier online te zetten. De kans op misbruik is immers aanwezig en waarom moet de hele wereld weten wat het telefoonnummer van verenigingslid X is? Je zou de gegevens volgens hem veel beter op een met een wachtwoord beveiligd deel van de site kunnen zetten, waarvan alleen leden het wachtwoord weten.
Of je dan kunt volstaan met één wachtwoord of dat elk lid zijn eigen wachtwoord moet hebben, is volgens hem een volgende vraag. In geval van een kleine vereniging is één wachtwoord nog wel beheersbaar, maar wanneer het een club betreft met enkele honderden leden lijkt een wachtwoord per lid wel echt verplicht.

Privacygerelateerde vragen zoals deze beantwoordt Engelfriet op zijn blog, maar ook in zijn dagelijkse praktijk als jurist heeft hij er veel mee te maken. Zo kreeg hij bijvoorbeeld een vraag naar aanleiding van het publiceren op internet van de tijden van alle deelnemers aan een bekende marathon. Een van de deelnemers, in het dagelijks leven werkzaam in een managementfunctie bij een groot bedrijf, was niet zo blij met deze publicatie. De man was in de onderste regionen gefinisht en deze magere prestatie was nu op de website van de organisatie voor iedereen heel gemakkelijk na te gaan.
"Was hij eerste geworden dan was hij waarschijnlijk niet naar me toegekomen, maar nu zat hij er toch mee in zijn maag", geeft Engelfriet aan. Ook in dit geval geldt dat de gegevens niet zomaar op internet geplaatst mogen worden. Hiervoor moet eerst aan elke deelnemer toestemming worden gevraagd door de organisatie.

Kern: noodzaak én alternatief
Twee voorbeelden van vragen met betrekking tot privacy waar mensen mee

Arnoud Engelfriet (Foto: www.arnoud.engelfriet.net)

zitten en die de kern van het probleem weergeven. Schending van privacy komt namelijk in de basis altijd op hetzelfde neer. Engelfriet: "Er zijn steeds twee vragen die beantwoord moeten worden. A. is er een noodzaak om iemands privacy te schenden? En B. is er een alternatief mogelijk waardoor iemands privacy in mindere mate wordt aangetast? Deze overwegingen gelden ten aanzien van de gegevens die de sportvereniging op internet wil plaatsen, maar ook ten aanzien van het ophangen van beveiligingscamera's in een winkel of het plaatsen van een bodyscanner op luchthaven Schiphol. In alle gevallen moet je volgens de wet kiezen voor het minst inbreukmakende alternatief. Middelen moeten dus in verhouding staan tot het doel. Een gezond uitgangspunt."

'Security theater'
Onder het mom van het bieden van veiligheid wordt onze persoonlijke vrijheid meer en meer ingeperkt. Engelfriet: "Een ontwikkeling die Bruce Schneier, (red. autoriteit op het gebied van informatiebeveiliging), heel treffend aanduidt met

de term ‘security theater’. Hiermee doelt de Amerikaanse beveiligingsgoeroe op de maatregelen die worden genomen om mensen een veilig gevoel te geven, zonder dat bewezen is dat de genomen maatregelen daadwerkelijk een bijdrage leveren aan de veiligheid. Voorkom je met het plaatsen van bodyscanners op Schiphol daadwerkelijk een terroristische aanslag? Of is het louter een reactie op een onfortuinlijk incident?”, vraagt Engelfriet zich in de lijn van Schneier af. “Veiligheidsbeleid wordt veel te veel gebaseerd op angst en niet op rationele analyse. Een heilloze weg. We zouden ons veel vaker de relevante fundamentele vragen moeten stellen, zoals: Wat willen we nu eigenlijk bereiken? En is dit het beste middel om dit beoogde doel te bereiken?”

Bruce Schneier beschrijft in zijn boek ‘Beyond Fear’ een stappenschema met betrekking tot het invoeren van beveiligingsmaatregelen. Allereerst moet worden vastgesteld wat men probeert te beschermen. Vervolgens moet worden beoordeeld wat de risico’s zijn. Daarna moet worden onderzocht in hoeverre de maatregelen deze risico’s kunnen beperken en welke nieuwe risico’s ontstaan door de maatregelen. En tot slot moet worden onderzocht welke kosten of andere nadelen de maatregelen met zich meebrengen.

Een dergelijke aanpak vergt volgens Engelfriet een compleet nieuwe denkwijze. “Nu wordt in geval van beveiliging altijd geredeneerd vanuit de oplossing – vaak een product”, geeft hij aan. “En in het meest gunstige geval wordt helemaal aan het eind van een traject nog even stilgestaan bij het privacyaspect. Privacy wordt gezien als een kostenpost en zeker niet als een sellingfeature.” Ter illustratie vragen we Engelfriet naar de discussie rond het Elektronisch Patiënten Dossier, het EPD. “De beveiliging hiervan is slecht doordacht en ook met aspecten van privacy is veel te weinig rekening gehouden”, geeft hij aan. “De beslissing wie uiteindelijk inzage mag hebben in welke gegevens moet veel meer bij de patiënt zelf worden gelegd. Een gemiste kans als je het mij vraagt.”

Nieuwe wetgeving?

De Wet Bescherming Persoonsgegevens is de bekendste en belangrijkste wet op het gebied van de bescherming van de privacy in Nederland. Er bestaat geen algemene Wet op de Privacy. Wanneer in Nederland vaker de genoemde fundamentele vragen zouden worden gesteld, is er volgens Engelfriet geen behoefte aan nieuwe wetgeving op dit gebied. “Die vraag is irrelevant. Uiteindelijk kunnen we ons allemaal beroepen op het grondrecht ‘recht op privacy’. Het is vervolgens aan de overheid om aan te geven waarom jouw privacy moet worden geschonden. ‘Je hebt toch niks te verbergen’, het argument dat voorstanders van maatregelen die de privacy inperken vaak gebruiken, is hiertoe onvoldoende. Dat argument impliceert namelijk een omkering van de bewijslast. De uitspraak is bovendien gebaseerd op een naïef vertrouwen in de overheid. Het is namelijk nooit honderd procent zeker dat jouw gegevens met respect behandeld zullen

Het Nieuwe Rijk

Een persiflage is geslaagd als je bij de eerste aanblik erin gelooft en pas na grondiger bestudering beseft dat je in de maling genomen wordt. Mijn petje dan ook af voor de bedenkers van de folder ‘Nieuw reisdocument aangevraagd?’, waarmee veel burgers gisteren aan het ontbijt werden verrast. Menigeen zal zich in zijn beschuitje hagelslag hebben verslikt.

Voor wie de folder niet heeft gekregen; daarin werd de burger op de mogelijkheid gewezen kosteloos zijn burgerservicenummer op zijn linkerarm te laten tatoeëren.

We beginnen kennelijk zó gewend te raken aan kliklijnen, telefoontaps, winkelcentrumcamera’s, verplichte identiteitskaarten, elektronische patiëntendossiers en andere bedreigingen van onze privacy dat we met álles rekening houden: what’s next?

Wie persifleert overdrijft. Maar het is helemaal niet zo’n gekke gedachte in dit verband te herinneren aan de Tweede Wereldoorlog, toen de bezetter bij zijn jacht op verdachte burgers geholpen werd door een bijna onontkoombare persoonsregistratie, ontworpen door een al te ijverige overheid.

Bron: Het nieuwe rijk; column door Frits Abrahams, NRC Handelsblad - 25 november 2009

Grijp niet meteen naar het uiterste middel

worden. Zo is vaak onduidelijk hoelang gegevens in een database bewaard zullen worden en wie er in de toekomst allemaal toegang krijgt tot de gegevens. Feit is echter wel dat je wanneer je bepaalde gegevens eenmaal hebt afgegeven, je er geen controle meer over hebt."

Engelfriet noemt in deze het voorbeeld van het nieuwe biometrische paspoort met vingerafdruk dat sinds september vorig jaar is ingevoerd. "Het is in Europees verband verplicht gesteld, maar Nederland gaat verder: van alle volwassenen moeten de vingerafdrukken in een grote databank worden opgeslagen. Daarmee bestempelt de overheid in feite iedere burger tot potentiële verdachte. Om nog maar niet te spreken van het gevaar van identiteitsfraude", waarschuwt hij. "De overheid heeft misschien geen kwade bedoelingen, maar voor criminelen is zo'n databank zeker een gewild doelwit."

Nederland vs. Amerika

Dat Nederland net als Amerika is te bestempelen als een controlemaatschappij beaamt Engelfriet. Het feit dat er geen land is waar zoveel wordt afgeluisterd als in Nederland zegt in zijn ogen genoeg. "Verschillen zijn er echter ook", geeft hij aan. "Traditioneel gaat men in Europa zorgvuldiger om met privacy. Dit is nu eenmaal historisch bepaald. In Amerika is privacy buiten de muren van je eigen huis simpelweg geen issue. In Nederland gelukkig wel. Zo wordt de Nederlandse regering door verschillende belangenorganisaties scherp gehouden als het om privacy gaat. De controlemaatschappij zal er niet door worden teruggedraaid, maar een goede zaak is het zeker wel."

De technologie de schuld geven van het ontstaan van deze controlemaatschappij is volgens Engelfriet onzin. "Technologie is slechts een middel. Het maakt het verzamelen van gegevens mogelijk. Maar het gaat er natuurlijk om hoe je deze technologie inzet. Vroeger gaven we massaal met briefjes voor de melkboer aan dat we niet thuis waren. Als er vervolgens werd ingebroken, werd er echter niet naar de melkboer gewezen... terecht lijkt me. Maar waarom dan nu wel wijzen naar technologie en bijvoorbeeld sociale netwerken als Twitter en Hyves? Feit is wel dat mensen deelnemen aan sociale netwerken in de naïeve veronderstelling dat ze informatie delen met vrienden en bekenden. Wanneer iemand vervolgens informatie over zichzelf terugvindt op een plek waar hij of zij dit niet had verwacht, geeft dat een ongemakkelijk gevoel. Bovendien realiseren we ons vaak niet dat internet niks vergeet", waarschuwt Engelfriet. "Wat te denken van de premier van Nederland in het jaar 2040? Ik ben ervan overtuigd dat hij of zij nu een Hyvespagina heeft. En zeer waarschijnlijk staan daar foto's of opmerkingen op waaraan hij of zij in 2040 niet meer herinnerd wil worden. We moeten dus nadenken over de manier waarop we als maatschappij omgaan met gegevens op internet zoals bijvoorbeeld dertig jaar oude Hyves-profielen."

Tot slot van het gesprek vragen we Engelfriet naar de manier waarop bedrijven met grote hoeveelheden persoonsgegevens om zouden moeten gaan. "Bedrijven moeten er steeds weer bij stilstaan of het echt nodig is de betreffende gegevens te bewaren", adviseert hij. "Vervolgens moet gekeken worden of de toegang tot de database met gegevens voldoende is afgeschermd. Zijn hiervoor technisch gezien de optimale middelen gebruikt en wordt deze beveiliging nageleefd? Vragen die veel te weinig worden gesteld. Bovendien is het belangrijk de situatie praktisch gezien werkbaar te houden. Ik zie in de praktijk gevallen waarin bedrijven het zo moeilijk maken voor medewerkers om bepaalde zoekvragen uit te voeren dat zij zich genoodzaakt voelen te gaan werken met schaduwdossiers. In alle opzichten een onwenselijke situatie. Ten aanzien van de sfeer en de werkbaarheid in zijn algemeenheid moeten werkgevers tot slot rekening houden met de menselijke behoefte aan privacy. Werknemers die zich continu gecontroleerd voelen, zijn namelijk ongelukkiger en daardoor minder productief. Opnieuw geldt dat middelen in verhouding moeten staan tot het beoogde doel. Begin met andere woorden nooit bij het uiterste middel. Microfoons in de kantine om roddelen tegen te gaan? Misschien is een assertiviteitstraining of juist een training in omgangsvormen meer op zijn plaats."

"Welk probleem zijn we aan het oplossen en welk middel is hiertoe het meest effectief? Wanneer we deze afweging steeds weer zouden maken, kunnen veiligheid en privacy wel degelijk hand in hand gaan", besluit Engelfriet.

Over Arnoud Engelfriet

Arnoud Engelfriet is ICT-jurist, gespecialiseerd in internetrecht waar hij zich al sinds 1993 mee bezighoudt. Hij werkt als partner bij juridisch adviesbureau ICT-Recht. Zijn site Ius mentis is een van de meest uitgebreide sites van Nederland over internetrecht, techniek en intellectueel eigendom. Sinds 2007 blogt Engelfriet dagelijks over internetrecht.

Ook is hij medewerker van het Tijdschrift voor Internetrecht en secretaris van de Stichting Copyright en Nieuwe Media. Daarnaast is hij actief op tientallen websites en forums, waaronder Zibb, Security.nl, Marketingfacts, Tweakers, Netters en Rechtenforum.

Geraadpleegde bronnen
www.arnoud.engelfriet.net
Security.nl - Bits of Freedom tegen invoeren bodyscan; 30-12-2009
Privacyschending in Nederland: het gaat verder dan je denkt; door Bart de Koning, HP De Tijd - 26 november 2009
www.hetnieuwerijk.nl
Het nieuwe rijk; column door Frits Abrahams, NRC Handelsblad - 25 november 2009

Wat kun je nou op internet vinden?

Lex Dunn Aart Jochem

Auteurs: Lex Dunn en Aart Jochem > Lex Dunn CISSP ISSMP is Security Officer bij een grote, internationale ICT-dienstverlener. Hij is één van de redacteuren van het blad Informatiebeveiliging en editor van een schriftelijke CISSP cursus. Hij is bereikbaar via lex.dunn@capgemini.com.

Ir Aart Jochem CISSP is teamleider bij GOVCERT.NL, het incident response team van de Nederlandse overheid. Ook is hij lid van het redactieteam van Informatiebeveiliging. Hij is bereikbaar via aart.jochem@govcert.nl.

Er is ongelooflijk veel informatie te vinden op internet. Sinds de start in de 70'er jaren van de vorige eeuw is de hoeveelheid pagina's exponentieel toegenomen, met name na de introductie van online sociale netwerken en krachtige zoekmachines. Veel mensen zoeken bewust de publiciteit op internet, voor anderen hoeft dat niet zo nodig. Desondanks is er over hen ook het nodige op internet terechtgekomen. Maar wat kun je nou allemaal vinden?

Aan de hand van een 'bekende Nederlander' onderzoeken we wat je zo al tegenkomt. Onze hoofdredacteur André Koot, al langjarig werkzaam in de informatiebeveiliging en fervent gebruiker van de mogelijkheden van internet, heeft zich belangeloos ter beschikking gesteld voor deze praktijkoefening.

Uiteraard begin je zo'n exercitie op Google: 'Andre Koot' heeft circa 45.500 hits (status 29 april 2010). De eerste paar links verwijzen inderdaad naar 'onze' André (LinkedIn, Twitter), maar ook anderen komen aan bod. Een André Koot met een bedrijf voor machineverhuur, tuinaanleg en -renovatie, aannemingsbedrijf en rioolinspectie, een André Koot met een foto van zijn zwenklader TL70S (misschien dezelfde). Ene 'André Koot' is penningmeester

Iedereen is een bekende Nederlander

van Atletiekvereniging Zuidwal in Huizen, en we vinden hun verenigingsblad (PDF-document) met daarin de telefoonnummers van alle leden en het bestuur. Niet onze 'André Koot', maar toch wel erg veel informatie waarvan de leden misschien niet op de hoogte zijn dat deze publiekelijk op internet staat.
Om wat meer gericht te zoeken beperken we het tot 'André Koot UVIT', maar dat levert ook nog zo'n 2.220 hits op (status 29 april 2010). De eerste link daarvan blijkt echter erg belangrijk te zijn voor ons verdere onderzoek, want deze verwijst ons naar Twitter, en daar blijkt André het pseudoniem 'meneer' te gebruiken. Hij is een actief Twitteraar, heeft al meer dan 2600 tweets op zijn naam staan en meer dan 300 volgers. Zijn locatie is Meppel, ook een handig gegeven in onze zoektocht. Uit zijn tweets blijkt dat hij regelmatig het openbaar vervoer gebruikt en dat 'privacy' en 'cloud' en 'identity', maar ook 'burgerrechten' zijn favoriete onderwerpen zijn.

Het pseudoniem 'meneer' is ook een actieve gebruiker op Wikipedia. Behalve de voorkeur voor onderwerpen als identity management en informatiebeveiliging, wordt ook André's grote ijver duidelijk: een groot deel van de beschrijving van landelijke top level domeinen is van zijn hand. Opvallend is dat 'meneer' ook mee heeft geschreven aan het Wikipedia-artikel over privacy. Wat een toeval.

Ook op andere websites met sociale netwerken blijkt André actief te zijn. Op Facebook vinden we al gauw zijn profiel terug (zonder daarvoor maar te hoeven inloggen), zelfs met een foto, die u al kent als u dit blad regelmatig leest ;-) André heeft een aantal vrienden, waarvan we hier vanwege privacy overwegingen de namen niet zullen publiceren, maar hij houdt van muziek van Annie Lennox en Supertramp, en blijkt fan te zijn van onder andere Linux, Firefox en Maserati (iedereen heeft zo zijn droom). Ook de Electronic Frontier Foundation (www.eff.org) blijkt zijn belangstelling te hebben.

Hij heeft natuurlijk een profiel op LinkedIn, met dezelfde foto als op Facebook. Hij is Security Manager bij UVIT, maar blijkt ook les gegeven te hebben aan de Hogeschool Arnhem en Nijmegen. Kennelijk gaat het reizen met het openbaar vervoer niet altijd even goed, want hij heeft een indrukwekkende lijst van groepen, die hij op LinkedIn volgt (en daar moet je natuurlijk wel de tijd voor hebben). Hier kunnen we ook zijn e-mailadres vinden, altijd handig voor een poging tot 'social engineering', of een gerichte aanval via een bewerkt PDF-bestand, waarbij we in de begeleidende e-mail zouden kunnen verwijzen naar een van zijn favoriete thema's. Als afzender zouden we dan een van zijn meer dan 500 contacten kunnen gebruiken. Overigens leuk om te zien dat André kennelijk op een lijn wordt gezet met Barack Obama, want lezers van zijn profiel hebben ook dat van de Amerikaanse president geraadpleegd!

Dichter op de man

Eens kijken of we wat meer over zijn persoonlijke omstandigheden kunnen vinden. Zoeken in de Telefoongids van KPN of in de Gouden Gids levert niks op. Terug naar Google: zoeken op André Koot met Meppel levert meer informatie. Op de website van de Protestantse Gemeente in Meppel staat niet alleen zijn telefoonnummer, maar ook nog een ander e-mailadres. Het telefoonnummer is niet terug te zoeken via diverse sites, waarop je telefoonnummers kunt relateren aan een adres,

maar ook hier biedt Google weer uitkomst. Via datzelfde telefoonnummer blijkt André lid te zijn van de wedstrijdorganisatiecommissie – baan van de AV de Sprinter in Meppel. En dat hij in 2008 via internet een petitie tegen een nieuwe asfaltcentrale in Meppel heeft ondertekend weten we ondertussen ook.

De telefoongids van ixquick.com werkt trouwens beter. Adres en telefoonnummer rollen er snel uit. Ixquick is een metazoekmachine, die zich profileert als privacy-vriendelijk. Volgens eigen zeggen bewaren ze geen IP-adressen en zoekresultaten kunnen via een proxy bezocht worden. Een waardevol aanbod voor mensen die privacy tijdens het surfen op prijs stellen, of zonder sporen na te laten onderzoek willen doen.

Oké, André houdt dus kennelijk van atletiek, wat levert dat gegeven ons op? Onder andere de uitslag van de 20e Nijeveense Triatlon van 14 juni 2008, waar drie Koot'en hebben meegedaan aan het onderdeel Triatlon Sprint Afstand – Estafette, en zowaar de eerste plaats hebben weggesleept met een tijd van 1:01:54. André met zijn twee zoons?

Via een zoekopdracht met de adresgegevens zien we dat André door Alexa en aboutus wordt gekoppeld aan e107.nl. Hij blijkt de oprichter van de Nederlandse site over dit op PHP gebaseerde CMS.

Nee, we gaan niet verder hier, we gunnen André ook zijn privacy. Maar denkt u eens even in wat er verder nog mogelijk zou zijn. De gegevens vormen een goede start voor verdere social engineering-pogingen. Een adres en een uitbundige stijl op social networking-sites geeft vele mogelijkheden. Als we André's tweets zouden volgen op internet komt daar op enig moment wel een bericht voorbij dat hij op vakantie is. Een ideaal moment dus om zijn huis leeg te gaan halen (via Ixquick.com hadden we zijn adres ook al gevonden), eventueel na een verkenning van de buurt via Google Maps. Een vrijstaand hoekhuis in een wijk met veel begroeiing. Als André bijvoorbeeld bankdirecteur zou zijn, zouden we via de atletiekvereniging kunnen achterhalen waar en wanneer zijn zoons trainen. Een koud kunstje om na zo'n training zoonlief op te pakken, en André voor te stellen hem te ruilen tegen een aanzienlijk bedrag uit de kluis van zijn bank. Een vergezocht scenario? Dit is in de praktijk al minstens één keer gebeurd, een paar jaar geleden in Duitsland.

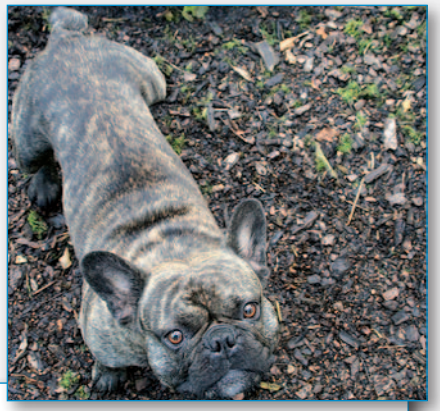
Wat kunnen we nog meer vinden?

De resultaten zijn gevonden met een korte tijd rondneuzen op internet. Door gebruik te maken van tools zoals Maltego van Paterva kunnen ingewikkelde verbanden relatief snel gevonden en gevisualiseerd worden. Met dergelijke tools wordt het ook mogelijk om verbanden tussen groepen personen en organisaties te vinden en grafisch weer te geven. Dat hebben we hier niet gedaan.

Conclusie

Het blijkt redelijk eenvoudig te zijn om van iemand een profiel samen te stellen aan de hand van informatie op internet, die met algemeen beschikbare middelen gevonden kan worden. Het is dus niet alleen aan inlichtingendiensten en overheden voorbehouden, maar iedereen kan het doen en dat gebeurt dan ook frequent. HRM-afdelingen zoeken op internet naar informatie over sollicitanten, bedrijven gebruiken informatie van sites als LinkedIn om een ZZP'er te beoordelen, potentiële klanten onderzoeken de reputatie van een bedrijf of webwinkel waar ze zaken mee willen doen, en helaas vinden criminelen en terroristen ook de nodige informatie over hun doelen.

Het plaatsen van persoonlijke informatie op internet is een onomkeerbaar proces: wat er eenmaal opstaat, krijg je nooit meer weg. Bovendien is die informatie wereldwijd voor iedereen beschikbaar, niet alleen voor je vriendengroep op Hyves of Facebook. Mensen moeten zich hiervan bewust zijn vóórdat ze persoonlijke informatie op het internet plaatsen. Websites zouden hiervoor nadrukkelijker moeten waarschuwen, en zorgen dat de controle over die persoonlijke gegevens bij de eigenaar blijft. Onderzoek door de Nederlandse Patiënten Consumenten Federatie (NPCF)[1] toont aan dat het EPD een stuk acceptabeler zou zijn als het zo was ingericht dat elk verzoek voor het raadplegen van medische gegevens onder normale omstandigheden eerst door de eigenaar van die gegevens geautoriseerd zou worden, en dat er bij raadpleging in uitzonderlijke omstandigheden (je wordt na een auto-ongeluk bewusteloos een willekeurig ziekenhuis ingedragen) naderhand door de eigenaar inzicht kan worden verkregen in die raadpleging(en).



Reactie André Koot:

Niet alle hondjes heten Fikkie

Het was even spannend toen Lex en Aart aankondigden dat ze mij eens wilden bespioneren. Wat zouden ze vinden en vooral wat zouden ze niet vinden? Al lezende merkte ik dat ze veel boven water hebben gekregen, maar gelukkig niet alles wat er te vinden is. Je moet wel weten waar je naar kunt zoeken. Voorkennis is belangrijk. Vooral informatie uit het verleden, uit het pre-internet tijdperk, is niet gemakkelijk boven water te krijgen, maar ook die oude info is nog wel te vinden.

En niet alle informatie die ze vonden gaat over mij. Er zijn meer hondjes die Fikkie heten. Voorkennis is ook belangrijk om de gegevens van kennis te scheiden.

Ik heb gemerkt dat het niet moeilijk is om veel informatie te achterhalen. De afgelopen jaren probeerde ik wel bewust om mijn privéleven en mijn professionele leven te scheiden. Dat blijkt niet voldoende. De verschillende personalia zijn niet keihard te scheiden. Er bestaat altijd wel ergens een relatie tussen de verschillende ikken. De ene stap kan zomaar leiden tot een volgende. Alleen door bewust niet actief te zijn op het internet kun je de scheiding deels in stand houden. Als je dat niet lukt, moet je maar hopen dat er heel veel Fikkies zijn.

1 Het onderzoek is in 2003 uitgevoerd in opdracht het NICTIZ, het rapport is te downloaden van http://www.mointor.npcf.nl/index.php?option=com_content&view=article&id=1160:autorisatie-epd&catid=122:ict-in-de-zorg&Itemid=129

Het effect van Web 3.0 op Privacy

Auteur: Lex Borger > Lex Borger is een principal consultant bij Domus Technica. Hij is te bereiken via e-mail: lex.borger@domustechnica.com.

Tim Berners-Lee droomt al meer dan tien jaar van een semantisch web. Huidige ontwikkelingen, die we Web 3.0 noemen, lijken het voor het eerst mogelijk te maken: interpretatie van gegevens in context, in plaats van letterlijk zoeken, aggregatie van informatie die vanuit verschillende websites komt... Meer en meer informatie wordt opgeslagen. Moore's Law gaat ook op voor de informatiegroei. Elke seconde wordt al een uur video op YouTube gezet. Overheden en bedrijven digitaliseren archieven. We maken centrale registraties - verwijzingen naar informatie, zoals het landelijk EPD, of centrale basisregistraties, zoals het GBA. De VS verzamelen zoveel gegevens over terrorisme dat ze door de bomen het bos niet meer zien.

Uiteindelijk is niet alleen het hele netwerk verbonden, maar de informatie inhoudelijk ook. En het is nog eens voor iedereen en overal toegankelijk. We zijn langzaam naar deze situatie toe gegroeid, maar de laatste tijd lijkt het weer sneller te gaan. Het Martini-gevoel (any time, any place, anywhere) heeft met de verkoop van miljoenen smartphones en tablets een aardige boost gehad, die trouwens nog lang niet over is. Al deze ontwikkelingen maken misbruik van die informatie eenvoudiger. En ook het karakter van het misbruik verandert. Waar het de afgelopen jaren ging om het verkrijgen van informatie die iets persoonlijks identificeerde, PII (personally indentifiable information), gaat het nu ook om PEI (personally embarrassing information). Dit komt vooral voort uit web 2.0 - de sociale netwerken. Er wordt door onszelf of onze vrienden zoveel informatie op het internet gezet dat we niet meer comfortabel zijn om daar in een andere context mee geconfronteerd te worden. Dat uit de hand gelopen Koninginnedagfeest kan bij een sollicitatie lastig zijn. Maar ook de PII wordt steeds complexer. Je kunt bijvoorbeeld bij misbruik van je creditcard nog een nieuwe krijgen, maar als je medisch dossier op straat komt, ligt het op straat en is er niets meer aan te doen. Nu zal dat voor het gros van de wereldburgers niet uitmaken, maar voor wie het wel uitmaakt: het zal je maar gebeuren! De ACLU heeft al jaren geleden een prachtig filmpje gemaakt wat goed illustreert wat de gevolgen zijn voor onze privacy als het semantische web echt werkelijkheid wordt (www.aclu.org/pizza/). In de VS zijn ze er inmiddels achter dat het niet handig is om een universeel toegangssleutel voor persoonlijke informatie te hebben, zoals het SSN (social security number). Maar je komt, eenmaal het pad ingeslagen, daar niet meer vanaf.

Dit artikel is een weergave van de presentatie van Lex op 22 april op het evenement 'Offline met AxiCom' over de betekenis van Web 3.0 op onze privacy. Het is een persoonlijke bespiegeling van Lex op het onderwerp privacy binnen 'web 3.0'.

Privacyprincipes

Toch weten we principieel best hoe we onze privacy moeten beschermen, of het nu web 1.0, 2.0 of 3.0 betreft. Het eerste principe is om informatie gedistribueerd te houden. Geen grote centrale databases maken. Als je ze maakt, beperk dan de waarde van de informatie en scherm ze goed af. Het tweede principe is om de informatie die op verschillende locaties staat niet met elkaar te verbinden. Maak geen brede indexen, of als je die maakt, weet wat je indiceert en scherm het goed af. Het derde principe is om de waarde van de informatie zelf te beperken door de informatie te versleutelen of 'tokenization' toe te passen.

Het frappante is dat die aspecten die web 3.0 nou net die semantische waarde geven: interpretatie in context, aggregatie van informatie, brede verbondenheid van informatie en universele toegankelijkheid juist regelrecht ingaan tegen deze privacyprincipes. Gebrek aan semantiek is dus kennelijk wat we nodig hebben om onze privacy nog enigszins te behouden.

Het effect van Web 3.0 op privacy.

Google

Laten we dan even kijken wat er nu gaande is in de wereld. Google komt steeds centraler te staan in ons dagelijks leven. Staan we er wel genoeg bij stil dat het bedrijf Google niet aan de zoekmachine verdient, maar wel aan het verzamelen van ons collectief en individueel zoekgedrag? En hetzelfde geldt voor de andere diensten van Google. 'Do no evil' is een nobele belofte, maar wat als door een hackpoging van een land de authenticatiemodule van Google gebroken zou worden?

Facebook hinkt op twee gedachten. Ze weten dat ze op een berg aan waardevolle en privacygevoelige data zitten. Ze zeggen dan ook de privacy van hun leden hoog in het vaandel te hebben. Maar dat belet ze niet om regelmatig met de privacyinstellingen van de profielen van alle gebruikers te gaan rommelen, en wel op zo'n manier dat de privacy steeds het onderspit delft.

Twitter weet niet waarmee het geld moet verdienen en zet voorzichtig stappen richting het integreren van advertenties. Aan de andere kant hebben we het hier over privacy, Twitter en privacy gaan gewoon niet samen, punt uit.

Ook de Nederlandse overheid heeft een aantal initiatieven lopen waar je privacyvraagtekens bij mag zetten. De kilometerregistratie - elke gereisde kilometer wordt dan ergens centraal opgeslagen. Het is net de OV-chipkaart, maar dan erger. En juist over die OV-chipkaart heeft het CBP een aardig inhoudelijk dossier gemaakt. (www.cbpweb.nl/Pages/th_ovc_start.aspx).

Pizza bestellen op de Web 3.0-manier.

Nederland staat nog steeds in de top drie van landen met de meeste telefoontaps per burger en wil vingerafdrukken centraal opslaan. En waar maken mensen zich druk over? Over het landelijk gedeeld EPD. In dit geval zijn de privacyprincipes die ik eerder noemde tenminste nog toegepast. Er wordt geen medische informatie centraal opgeslagen, en de verwijsindex wordt beschermd met sterke authenticatie en encryptie.

Toekomst

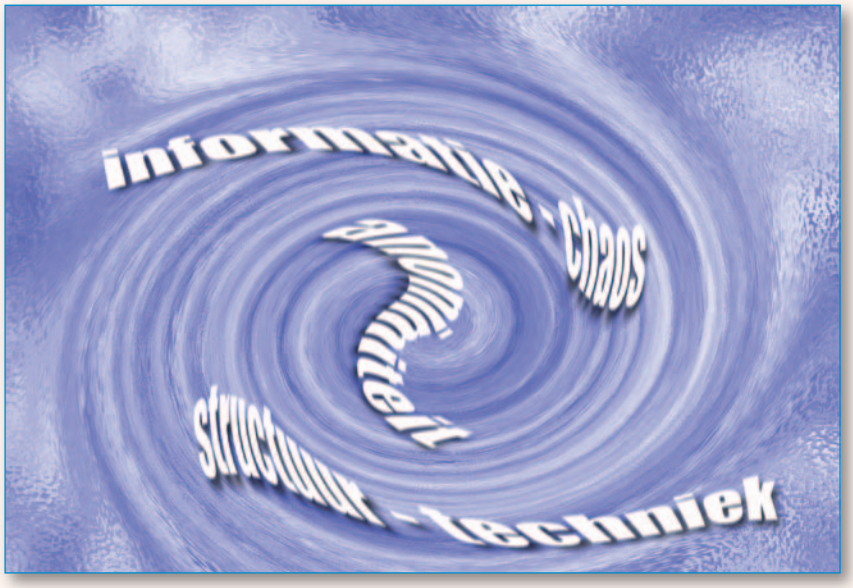
Waar gaat dit allemaal naartoe? Het lijkt nu net alsof ik iedereen bang wil maken voor Web 3.0, maar dat is niet het geval. Ik hoop wel dat we met zijn allen goed nadenken welke weg we inslaan, want zoals ik eerder zei: informatie die op straat komt te liggen is niet terug te halen.

Uiteindelijk komt het terug op twee principes die op elkaar inspelen, lang voordat het internet bestond of zelfs Tim Berners-Lee geboren was.

1 Informatie wil vrij zijn. Veel vrije informatie creëert een chaos. In die chaos heeft privacy best een aardig bestaansrecht, in de hooiberg van informatie is de speld niet te vinden. Privacy is anonimiteit en hoe meer informatie, hoe beter.

2 Technologie wil structureren. En als techniek daar beter in wordt, vreet het weg aan de chaos en wordt het vervangen door structuur.

Toch is er een verschuiving gaande, doordat zowel de hoeveelheid informatie en de structurering daarvan zo'n vlucht genomen hebben. Anonimiteit is niet langer gewaarborgd en privacy gaat iets anders betekenen. We zien dat al met 'generatie Y', die geen moeite heeft om privacygevoelige data te delen, maar wel scherpe verwachtingen heeft over hoe die informatie gebruikt wordt - en juist niet gebruikt wordt. De cyclus spiraliseert voort. En wij moeten ons zowel als privépersoon en als professional beseffen dat we dit niet tegen kunnen houden, dus dienen we er verantwoordelijk mee om te gaan.



Anonimiteit gevangen in de informatietechnologiespiraal.

Black Hat 2010 Barcelona

Auteur: Lex Dunn > Lex Dunn CISSP ISSMP is Security Officer bij een grote, internationale ICT-dienstverlener. Hij is een van de redacteuren van het blad Informatiebeveiliging en editor van een schriftelijke CISSP-cursus.
Hij is bereikbaar via lex.dunn@capgemini.com.

Op 14 en 15 april vond in Barcelona de Europese versie van de Black Hat-conferentie plaats. In voorgaande jaren werd deze conferentie in Amsterdam gehouden, maar Jeff Moss (de oprichter en directeur van Black Hat) is uitgeweken naar Barcelona om meer ruimte te hebben voor een extra 'track'. Het resultaat: drie parallelle stromen en zo'n honderd deelnemers meer volgens Jeff. Het totale aantal wil de Black Hat-organisatie niet prijsgeven, maar mijn persoonlijke schatting is zo'n driehonderd deelnemers.
Het centrale thema voor de sessies was 'attribution'. Letterlijk: 'dat wat toegekend, toegeschreven wordt'. Het kennen van de vijand om aan de hand daarvan een 'passende reactie' uit te voeren kwam in alle presentaties wel in een of andere vorm naar voren. De drie stromen op de eerste dag waren 'Big Picture', 'Application Security' en 'Hardware'. Op de tweede dag waren de presentaties onderverdeeld in 'Exploit', opnieuw 'Application Security' en 'Forensics / Privacy'. Vooral deze laatste stroom mocht zich verheugen op veel belangstelling van de deelnemers.

De keynote-spreker was Max Kelly, CSO bij Facebook, afkomstig van de FBI. Facebook is genoegzaam bekend, en wordt dan ook regelmatig gebruikt voor activiteiten van minder allooi (bijvoorbeeld om vrienden van een bepaald persoon te vinden, en deze dan uit zijn/haar naam te benaderen, of het schoonwassen van spam e-mail lijsten). Max gaf zelf aan, dat "features can be used in a way you didn't think of, so try and find out what it is". De ontwikkelaars van Facebook proberen zelf te bedenken hoe Facebook ge/misbruikt zou kunnen worden, maar worden desondanks nog regelmatig verrast met nieuwe creatieve vormen van ge/misbruik. Facebook heeft ervoor gekozen om enerzijds een duidelijk beeld van het misbruik op te bouwen (Intelligence is King), en anderzijds misbruik met een stevige juridische aanpak te mitigeren. Onder de Amerikaanse wet- en regelgeving kunnen ze een boete eisen van honderd dollar per verstuurd spambericht. Dat dit al gauw richting een miljard kan gaan, bleek enige tijd geleden toen de door Facebook aangespannen rechtszaak tegen spammer Sanford Wallace resulteerde in een megaboete van 711 miljoen dollar.

Cybercrime of Cyberwarfare?
Iftach Ian Amit presenteerde zijn onderzoek naar mogelijke overeenkomsten en verschillen tussen cybercrime en cyberwarfare, om na te gaan of wellicht dezelfde groepen bij beide soorten activiteiten betrokken zijn. Bij het analyseren van aanvallen is het verschil tussen deze niet altijd duidelijk. In de praktijk blijkt dan ook dat er verbindingen te leggen zijn tussen cybercrime-organisaties, en idealistische groeperingen, die een bepaald land of ideologie aanhangen. Vaak zullen het ook dezelfde mensen zijn, die hun kennis gebruiken voor criminele activiteiten én voor ondersteuning van cyberwar. De doelen zijn dan ook niet alleen puur militair. Steeds vaker worden civiele doelen aangevallen als onderdeel van een militaire campagne. Een mooi voorbeeld is de oorlog in Georgië. In eerste instantie werden er DDoS-aanvallen uitgevoerd op de websites van de Georgische overheid, vermoedelijk om de publieke aandacht af te leiden van de tegelijkertijd optrekkende Russische troepen. Later werden de DDoS-aanvallen heviger, en uit analyse bleek dat hierbij Command & Control-servers van botnets waren betrokken, die ook bij criminele activiteiten werden ingezet. Ian voorziet dat deze vermenging tussen cybercrime en cyberwar zal intensiveren, de nu reeds beschikbare middelen (zoals botnets en cloud,

deze laatste als mechanisme waarin je redelijk gemakkelijk en anoniem grote hoeveelheden resources kunt gebruiken, en na gebruik weer kunt 'dumpen') zullen vanwege gebrek aan kennis en samenwerking in vooral de uitvoering van de opsporingsinstanties steeds vaker voor dit soort doeleinden worden gebruikt.

Een voorbeeld van een tool om je aanvallers te leren kennen is Maltego. Het tool is al langer op de markt in zowel een commerciële versie als een gratis te gebruiken (beperktere) versie. Binnenkort komt versie 3 uit en Roelof Temmingh gaf een overzicht van de nieuwe mogelijkheden. Niet alleen kun je hiermee bijvoorbeeld netwerkinformatie achterhalen, door gebruik van de analysemogelijkheden van OpenCalais en Alchemy kun je allerlei analyses daarop loslaten (beide zijn voorbeelden van analysetools om verbanden in vrije tekst te onderzoeken en naar boven te halen). Met name de mogelijkheid om verbindingen tussen entiteiten te onderzoeken levert bruikbare resultaten om maatregelen op te baseren. Roelof gaf zelf twee voorbeelden: het aan de hand van 'whois' informatie uitzoeken welke domeinen er allemaal met een bepaalde merknaam te maken hebben (zodat je eventuele misleidende websites kunt opsporen), en het laten zien van de sociale netwerken van bepaalde personen door middel van een analyse van Facebook. (Waardoor je soms verrassende inzichten krijgt. Zo blijkt de harde kern van Black Hat uit slechts negen personen te bestaan, maar zit Jeff Moss daar niet bij!).

Uit analyse bleek dat Command & Control-servers van botnets waren betrokken

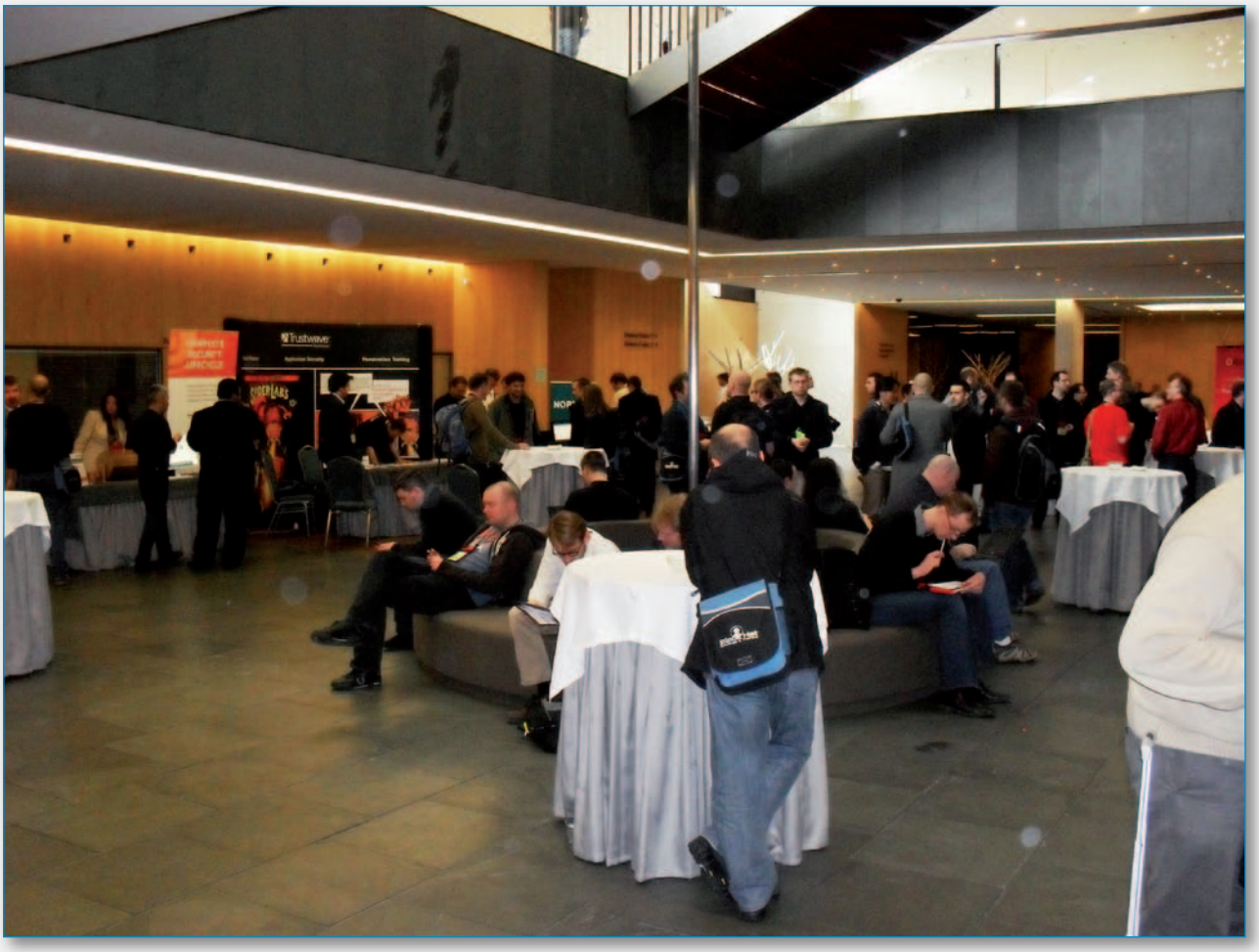
Hackers gehackt!

Een presentatie, die niet alleen mij, maar alle aanwezigen bijzonder aansprak (gezien het spontane en langdurige applaus) was het verhaal van Andrzej Dereszowski over 'Targeted attacks: from being a victim to counter attacking'. Andrzej heeft onderzoek gedaan naar de nieuwste gerichte aanvallen (bekend van de recente 'Chinese' aanval op Google, en vaak aangeduid met de afkorting APT voor Advances Persistent Threats). Deze aanvallen hebben als gemeenschappelijk karakter dat ze gericht zijn op één organisatie of bedrijf (soms zelfs op één persoon), en dat ze gebruikmaken van allerhande informatie om die aanval zo succesvol mogelijk in te steken. In de meeste gevallen kregen medewerkers van het betreffende bedrijf een e-mail met een bijgesloten PDF-document over een actueel onderwerp. Door het openen van dit PDF-document door middel van Adobe PDF reader met de inmiddels genoegzaam bekende kwetsbaarheden wordt een backdoor op de machine van het slachtoffer geïnstalleerd. Andrzej heeft een recent voorbeeld van zo'n aanval aan de hand van het meegestuurde PDF-document uitvoerig geanalyseerd. Niet alleen wat betreft de manier waarop de backdoor via de PDF kwetsbaarheid wordt geïnstalleerd, maar ook het netwerkverkeer dat hiermee gepaard gaat. Uit zijn analyse kwam naar voren dat er een zogenaamde RAT (Remote Access Tool) werd gebruikt. In dit specifieke geval Poison Ivy. Vervolgens heeft hij de rollen eens omgedraaid, en met 'hacker'-technieken onderzocht of er niet een te exploiteren kwetsbaarheid in Poison Ivy zat. En jawel, ook hackers schrijven geen foutloze code ;-). Met behulp van deze kwetsbaarheid heeft Andrzej een tool gemaakt om een Poison Ivy-controller over te nemen, zonder dat de betreffende hacker dat in de gaten had. Alleen al voor deze prestatie (de hacker gehackt) kreeg Andrzej ruimschoots waardering, maar het verhaal gaat nog verder. Hij heeft deze tool ter beschikking gesteld aan een kennis, die voor een niet nader te noemen overheidsorganisatie op het gebied van Incident Respons werkte. Deze heeft vervolgens met de tool een uitvoerige analyse gedaan van wat er door middel van de PDF-kwetsbaarheid allemaal aan gevoelige bedrijfsinformatie gestolen werd. Dat bleek heel veel te zijn, maar wellicht nog verontrustender was dat bleek dat hier een georganiseerd proces (welhaast 'industrieel' opgezet) aan ten grondslag ligt. Bedrijfsinformatie wordt op grote schaal gekopieerd naar de werkstations van de 'verzamelaars', en vervolgens via USB-sticks overgebracht naar een andere plaats, waar de documenten door 'analisten' op bruikbaarheid worden onderzocht. Dit was een voorbeeld van een presentatie waarvan ik toch misschien slapeloze nachten zou krijgen, van dit soort aanvallen en hun impact zijn we ons wellicht nog te weinig bewust.

Ook hackers schrijven geen foutloze code

Total Information Awareness

De laatste presentatie was van Moxie Marlinspike, geen onbekende voor Black Hat en daarbuiten, onder andere vanwege zijn aanval op het SSL-certificaat. Dit keer gaf Moxie zijn beeld bij de ontwikkelingen rondom privacy, en zijn zorgpunten daarbij. In het verleden zijn er vanuit de diverse overheden talloze pogingen ondernomen om volledige controle te krijgen over wat er zich op Internet afspeelt. Denk bijvoorbeeld aan het classificeren van cryptografie als wapens door de Amerikaanse overheid, en het daarbij behorende exportverbod op bijvoorbeeld Netscape. Phil Zimmerman slaagde erin dit exportverbod te omzeilen door zijn PGP in boekvorm uit te geven (1995). Begin jaren 2000 kwam John Poindexter met zijn 'Total Information Awareness'-programma, om alle digitale gegevens centraal op te slaan. Dit werd als wetsvoorstel afgewezen. "Gelukkig", dachten de voorvechters van privacy. Maar wat is de situatie vandaag? De Amerikaanse overheid heeft geen 'Total Information Awareness', maar Google wel. En door de manier waarop Google zijn mogelijkheden aan de gebruikers presenteert, en steeds verder uitbreidt, bestaat er dus nu een grote database met digitale informatie over alles en iedereen. Omdat Google bijvoor-



beeld alle gegevens over zoekacties opslaat, heeft Moxie een tool ontwikkeld (Google Sharing), die het mogelijk maakt om anoniem op Google te zoeken. Dit soort tools worden door de privacy-voorvechters ontwikkeld om de gebruiker een keuze te geven anoniem te blijven (zelfs voor Eric Schmidt van Google, wiens statement over privacy het nodige stof deed opwaaien).
Een voorbeeld om anoniem te kunnen surfen is TOR, dat al jaren wordt gebruikt om surfsessies op het internet te anonimiseren. Dank zij de inspanningen van Marco Bonetti is TOR nu ook beschikbaar voor gebruikers van mobiele devices, zoals bijvoorbeeld de iPhone. In zijn presentatie gaf Marco aan wat de bedreigingen van HTML5 zijn voor privacy, en hoe je deze met TOR kunt omzeilen.

Conclusie

Black Hat geeft in een aantal presentaties een degelijk technisch inzicht in de mogelijkheden om ICT te gebruiken voor andere doelen dan waarvoor het bedoeld was. En dan niet alleen als een handleiding hoe dat misbruik te plegen, maar vaak ook met een overzicht van mogelijke mitigerende maatregelen. Alle presentatoren dekken zich wel van te voren in: 'Don't try this at home, this is only intended for educational purposes' of iets soortgelijks. Alhoewel het technische niveau soms behoorlijk diep gaat, is deze conferentie ook een aanrader voor de CISO/CSO om voeling te houden met de ontwikkelingen, en lekker informeel kennis en ervaring te verbreden. Van andere deelnemers, die al vaker naar Black Hat waren geweest, kreeg ik de indruk dat er soms een herhaling van onderwerpen voorkomt. Of je dus elke Black Hat-conferentie moet / wilt bezoeken, laat ik graag aan de lezer over. Maar ook als je hier niet naar toe gaat, zijn er diverse blogs en Tweets, die ingaan op de ontwikkelingen en wat deze kunnen betekenen. Ook op de website van Black Hat zelf is het nodige materiaal te vinden (uiteraard pas ná de conferentie). Een ander mooi voorbeeld is Cupfighter.net. Een van de auteurs tikte naast mij vrolijk weg aan zijn blog over Maltego tijdens de presentatie van Roelof Temmingh.

Links

Blackhat website: www.blackhat.com
Maltego: maltego.blogspot.com/
Cupfighter: www.cupfighter.net/
Eric Schmidt over privacy: www.networkworld.com/community/node/48975
TOR voor mobile devices: sid77.slackware.it/
Boete voor Sanford Wallace: www.nu.nl/internet/2113310/spammer-moet-facebook-711-miljoen-dollar-betalen.html

Ik twitter dus ik ben[1]

Ik twitter. Ik Hyve. Ik heb een avatar op Second Life. Ik laat mezelf zien in al mijn facetten. Ik vertel, ik deel, ik becommentarieer en discussieer. Al enige jaren geleden merkte Nussbaum op dat openheid de nieuwe norm lijkt te zijn en dan vooral onder 'de jeugd van tegenwoordig'.[2] Nu ben ik wellicht niet meer helemaal te scharen onder de jeugd van tegenwoordig, maar toch, ook ik vertel veel over mijzelf in de online-wereld. Is dat erg? Wat voor gevolgen heeft dat? Sta ik daar wel bij stil? Wat vinden anderen nu eigenlijk van mij? Krijgen zij wel een juist beeld van de persoon die ik ben?

De kracht van openbaar zijn en openbaar leven ligt voor mij in de zelfcensuur. Want wie denkt dat hij mij helemaal kent door mijn online sporen te volgen, komt bedrogen uit. Ik vertel namelijk niet alles wat mij beweegt. En ik zeg ook niet altijd waar ik ben en met wie ik daar dan ben. Ook plaats ik niet zomaar rücksichtslos alle door mij gemaakte foto's. Ik kijk wel uit! Mijn Hyvesprofiel is alleen zichtbaar voor vrienden (en wie mijn vrienden zijn bepaal ik zelf). Niemand weet hoe mijn avatar in Second Life heet. En als ik boos of anderszins ontstemd ben, zal ik niet snel iets twitteren. En als ik wel iets twitter, dan denk ik eerst na voordat ik op de 'send'-knop druk (mocht me dan toch nog een onhandige tweet ontsnappen, kan ik hem direct na het plaatsen gelukkig ook weer wissen).

Een journalist vroeg ooit aan Angelina Jolie waarom zij toch zoveel over haar persoonlijke leven deelt met iedereen. Waarop mevrouw Jolie moest lachen en heel eenvoudig zei: "Maar je denkt toch niet dat ik werkelijk álles over mezelf deel wat er te vertellen valt?". Ook Angelina doet dus aan zelfcensuur. Dat mensen aan zelfcensuur doen is eigenlijk helemaal niets nieuws. Dat doen we namelijk al tijden (dus ook in offline tijden). Socioloog Erving Goffman maakte dat al duidelijk in zijn werk over identiteit waar hij stelt dat wij onszelf aan anderen presenteren zoals we graag gezien willen worden.[3] Wij laten de wereld zien wat wij willen dat zij ziet. Dus nee, dan twitter je niet dat je 'net lekker zit te poepen'. Dat is namelijk niet het beeld dat jij over jezelf aan de wereld wilt kenbaar maken.

De persoonlijke openheid in de online-wereld is dus een stuk relatiever dan wel eens gedacht wordt. Dat er soms toch zaken aan de aandacht ontsnappen en 'doorsijpelen' is echter ook een gegeven. De mens is nog steeds maar een mens en dus ook feilbaar in zijn zelfcensuur. Online voelen we ons verbonden met een groep 'vrienden', terwijl we misschien niet beseffen dat het woord 'vriend', online een heel andere betekenis heeft dan offline. In het offline-leven heb je een handjevol echte vrienden. Op Hyves is niet alleen iedereen die we toelaten op ons profiel 'een vriend', het zijn er ook nog eens vele malen meer dan dat handjevol. Veel sociale online-werelden zijn erop ingericht dat we ons veilig en prettig voelen als we daar verblijven. De inrichting 'dwingt' ons zoveel mogelijk te delen met een groot en uitgebreid vriendennetwerk. En vooral, dat wij dat in de openbaarheid doen. Niet voor niets zijn de standaardinstellingen van bijna alle sociale netwerksites 'openbaar'.[4] Wie zijn profiel wil afschermen moet daarvoor actief (veel) handelingen verrichten. Ook het wissen van een profiel gaat niet zonder slag of stoot, het vereist ten eerste een lange zoektocht naar het 'hoe' en vervolgens dringt zich de vraag op of je dan ook echt wel helemaal 'gewist' bent.

Dit alles beseffende: waarom dan toch nog steeds online zijn en in de openbaarheid jezelf delen met de hele wereld? Het is eigenlijk relatief eenvoudig. De mens is een sociaal wezen; legt graag contact met anderen. En doet dat tegenwoordig óók online. Online ontstaan daarnaast zo af en toe mooie initiatieven waarin mensen elkaar belangeloos helpen met het beantwoorden van kleine of grote vragen.[5] Wie veel online is en daar rondkijkt, beseft zich dat de inmiddels al legendarische woorden van de Vorstin - "Onze samenleving wordt steeds individualistischer. Persoonlijke vrijheid is los komen te staan van verbondenheid met de gemeenschap. [...] Met virtuele ontmoetingen is die leegte niet te vullen; integendeel, afstanden worden juist vergroot," - ook relatief geschat kunnen worden. Gelukkig is er nog steeds veel saamhorigheid, lol en verbondenheid te vinden (al is het maar voor even). Wat vaak vergeten wordt in alle verhalen over inbreuken op privacy, doemscenario's waarin geschetst wordt dat werkelijk alles en iedereen met een muisklik je hele leven kan blootleggen en de beschuldigende vinger die in de richting van de bazen van sociale netwerksites wijst, is dat het ook gewoon leuk is. Het is leuk om online te zijn, het is leuk om te delen met vrienden (en de rest van de wereld) en het is leuk je verbonden te voelen met een groep gelijkgestemden. Is de wereld dan echt individualistischer geworden door al die virtuele ontmoetingen? Nee. Want hoewel iedereen nog steeds een individu is (individualiteit is immers het wezenskenmerk van onze postmoderne samenleving) en de mogelijkheden tot individuele ontplooiing en zelfpresentatie enorm zijn toegenomen met de opkomst van de technologie, zie je dat men dat zelden alleen doet. Identiteit, individualiteit en zelfontwikkeling doe je namelijk niet alleen. Daar heb je een gemeenschap voor nodig en die bevindt zich nu niet alleen in onze wijk of op de straat, maar ook achter onze muisknop. Wij twitteren samen, dus wij zijn.

mr. Rachel Marbus
(@rachelmarbus op twitter)

1 Vrij naar: S. Jensen & R. Wijnberg, Dus ik ben, 2010.
2 E.Nussbaum, 'Say everything', New York Magazine, 12 februari 2007
3 E. Goffman, The presentation of self in everyday life, 1959.
4 Inmiddels is er wel een beweging gaande die stimuleert om de standaardinstellingen voor minderjarigen op privé te zetten. Zo is dat onder meer een van de afspraken binnen het door een zeventiental sociale netwerksites ondersteunde Europese Cyberbullying Pact.
5 Een mooi voorbeeld daarvan is het gebruik van de hashtag #durftevragen op twitter. Een open vraag kan daarmee gesteld worden aan de gehele twittergemeenschap. En meestal krijgt iemand daardoor vrij snel een antwoord op een – voor hem – prangende vraag.

ACTA: middel erger dan de kwaal?

Ronald van Erven > Ronald van Erven MSc. RE CISSP is information risk officer bij de Grafische Bedrijfsfondsen (http://www.gbf.nl). Hij is sinds 2002 actief betrokken bij de PvIB. U kunt hem benaderen via ronald.vanerven@pvib.nl

Een Amerikaanse wetenschapper begeeft zich naar het Amazonegebied om een oplossing voor een medisch kwaaltje te vinden. Hij komt tijdens deze reis in contact met een indiaanse medicijnman en deze geeft hem een bepaald wortelextract dat de oplossing blijkt voor het betreffende kwaaltje. De Amerikaanse wetenschapper vraagt direct patenten en auteursrechten aan om zijn ontdekking te beschermen. Helaas voor de lokale medicijnman, deze mag zijn wortelextract niet meer zomaar gebruiken en is onder het ACTA-handelsverdrag in overtreding. Sterker nog, de auteursrechtenorganisaties kunnen boetes opleggen en mensen laten oppakken.

Het doel van het verdrag is om de economische schade, als gevolg van de grootschalige handel in nagemaakte merkartikelen (denk aan tassen van Louis Vutton, de vele laaggeprijsde Rolex-horloges en dergelijke) en het downloaden van auteursrechtelijk beschermd materiaal onder andere via het internet, tegen te gaan. De auteurs rechtenorganisaties en lobbyisten zien in het verdrag een belangrijk instrument in de strijd tegen namaak en piraterij. Maar naar mijn idee zijn er wat problemen met de huidige gang van zaken. En in dit artikel ligt de focus op informatie- en (digitale) mediadragers.

Niet transparant

De afspraken met betrekking tot het handelsverdrag zijn tussen de auteurs-rechtenorganisaties en de Europese politici achter gesloten deuren en in het diepste geheim, tot stand gekomen. Door deze onderhandelingen (achterkamertjespolitiek) worden nationale overheden geconfronteerd met wetgeving waarop zij geen invloed hebben gehad.

Macht van de auteursrechtenorganisaties

Het doel van dit handelsverdrag is om auteursrechtenorganisaties meer (dwang)middelen te geven om onderling informatie te kunnen uitwisselen en opsporingsdiensten van deelnemende landen aan te zetten tot aanhoudingen. Kortom, een sterkere handhaving en meer onderlinge afstemming tussen auteursrechtenorganisaties en opsporingseenheden zonder tussenkomst van de rechterlijke macht.
Een onderdeel van dit handelsverdrag is het harmoniseren van een strafrechtelijke aanpak van namaak en piraterij binnen de EU. Hetgeen inhoudt dat wat nu in Nederland toegestaan is, straks verboden kan zijn.

Ook worden taken, verantwoordelijkheden en bevoegdheden van opsporingsorganisaties, ISP's en auteursorganisaties gedefinieerd. Zo wil BREIN dat internetproviders al het verkeer van hun gebruikers gaan controleren omdat die wellicht wel eens iets uit illegale bron downloaden. Op dit punt komen dan ook privacygerelateerde zaken om de hoek kijken. Dit kan zover gaan als de onderlinge ruil van e-books die verboden wordt. Dit terwijl je nu een boek, grammofoonplaat of DVD aan een vriend kan uitlenen of doorverkopen.

In het geval van e-books is er ook nog de zaak van de kopieerbeveiliging. Zodra je overstapt op een andere e-reader is er een kans dat de al aangekochte e-bibliotheek onleesbaar blijkt te zijn. Met dank aan de auteursrechtenlobby. Deze kopieerbeveiliging verhindert ook dat je een eenmaal gekocht e-boek kunt weggeven of tweedehands kunt verkopen. Tevens werkt de auteursrechtenlobby aan maatregelen om op afstand media te kunnen blokkeren op je mp3-speler of e-reader (recent in de pers: www.security.nl/artikel/33265/1/Hollywood_mag_output_jacks_op_afstand_uitschakelen.html).

U als consument/gebruiker, loopt risico's

Dit handelsverdrag regelt dat u bij de grenscontrole uw elektronische mediadragers moet afstaan voor een inspectie. Met andere woorden; de douane mag een kopie trekken van onder andere uw MP3-spelers, draagbare harde schijven/usb-sticks, laptops, digitale camera's en e-readers. Hoe is uw privacy gegarandeerd?

Anti-Counterfeiting Trade Agreement (ACTA) is een handelsverdrag voor internationale standaarden op het gebied van de handhaving van het intellectueel eigendomsrecht. Een handelsverdrag met ingrijpende gevolgen voor u als gebruiker van multimediamaterialen via internet en een carte-blanche voor auteursrechtenorganisaties.

Maar ook de ISP's kunnen de rol van censor krijgen en informatie die voor u relevant kan zijn, gewoonweg filteren (lees: blokkeren), of klanten afsluiten en op een (internationale) zwarte lijst zetten. De technische maatregelen liggen in het verlengde van het kinderpornofilter en zijn dus gemakkelijk qua techniek te implementeren.
Het kan bijvoorbeeld gebeuren dat u op uw computer met uw garagebandapplicatie een liedje aan het componeren bent en toevallig zijn er een aantal noten uit uw liedje dat overeenkomt met een al beschermd liedje. U bent in overtreding! U krijgt een boete en uw PC kan in beslag genomen worden. Onder dit handelsverdrag wordt elke vorm van creativiteit aan banden gelegd.

Tenslotte worden ISP's gechanteerd door dit handelsverdrag. De tekst luidt 'to remove or disable access to infringing material or infringing activity upon having reasonable grounds to know that the infringement is occuring', art. 2.18 option 2)' Met andere woorden; als de ISP het verboden verkeer niet filtert krijgt deze een boete.

Conclusie
Internet was ooit bedoeld, na vrijgave door de DoD, om vrij informatie uit te wisselen. Nu na een jarenlange geheime lobby van de auteursrechtenorganisaties treedt er censuur op en lopen we de kans dat het publieke internet langzaam zal doodbloeden. Mensen zullen overgaan naar netwerken waar privacy tooling en anonnymizors aanwezig zijn om een vorm van privécommunicatie tot stand te brengen dit versus het open informatie delen waar internet voor bedoeld is. Als u niet oppast en uw (creatieve) werk niet vastlegt kan het zijn dat, indien anderen hetzelfde werk wel vast leggen, u in overtreding bent.

Ik geloof dat mensen best willen betalen voor informatie/media maar de mediaorganisaties spelen onvoldoende in op de moderne trends en wensen van de gebruikers, de markt. De prijs en distributiemethoden maar ook de belastingen over media spelen een rol en hierdoor kiezen gebruikers voor alternatieven om toch aan hun informatie en mediabehoeften te voldoen.

Echter de mediabranche kiest voor de juridische weg en hierdoor wordt de auteursrechtenlobby een te invloedrijke branche, waar zeer veel geld te verdienen is en dictatoriale trekjes de kop opsteken.

Tenslotte de casus, dat ieder mens uniek is. Onder dit handelsverdrag zou ik mijn DNA-profiel maar alvast juridisch beschermen. Het kan namelijk gebeuren dat als u uzelf niet juridisch beschermt en iemand in het buitenland maakt een kloon van u en hij zorgt wel voor de juiste bescherming, dat u in overtreding bent...kortom u bent een merk!

Bronnen voor onderbouwing:
http://www.wikipedia.nl
http://www.bof.nl
http://www.brein.nl
http://films.nfb.ca/rip-a-remix-manifesto/
http://www.opensourcecinema.org/

Achter het nieuws

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

Anti-Counterfeiting Trade Agreement (ACTA)

Deze tweede Achter het nieuws gaat over de ontwikkelingen rondom de Anti-Counterfeiting Trade Agreement (ACTA). De ontwikkelingen rondom dit nieuwe verdrag, en met name de manier waarop het tot stand dreigt te komen, kregen de afgelopen tijd ruimschoots aandacht in de pers (zoals bijvoorbeeld in deze column van Peter Rietveld: www.security.nl/artikel/33259/1/Het_schijndebat.html). Wat vinden onze redacteuren daarvan?

Voor meer informatie over de inhoud en achtergronden van ACTA verwijzen we u naar het artikel van Ronald van Erven, elders in dit blad.

Gerrit Post: "Goedbeschouwd is ACTA de stuiptrekking van een 'oude' economie die halsstarrig pogingen blijft doen zich niet aan te passen aan de 'nieuwe' manier waarop de wereld(handel) ingericht gaat worden. Het is ook vooral de aloude reflex die autoriteiten/overheden hebben om alles wat ze niet begrijpen, of wat ze niet goed uitkomt, te willen verbieden. De historie wijst uit dat dit uiteindelijk niet gaat lukken. Een aantal landen, ongetwijfeld zal ons land daarbij zijn, zal veel in het werk stellen om de beoogde doelen te bereiken. Een aantal anderen, we weten allemaal welke, zal dit met de mond belijden maar er weinig tot niets mee doen. Dus, lekker laten voor wat het is. Uiteindelijk waait het over of het verzandt in 'multilaterale' discussies.

Als beveiligers kunnen we een parallel trekken met het Jericho-initiatief. We kunnen informatie op diverse manieren met veel inzet van middelen beveiligen. Uiteindelijk, als de inzet hoog genoeg is, wordt toch het doel bereikt en blijkt dat je als beveiliger altijd achter de feiten aanloopt. Anders denken is dan dus geboden!"

Renato Kuiper: "Het ACTA-verdrag is ontstaan als antwoord op het feit dat de internetgebruiker veel mogelijkheden heeft om software, muziek en films te downloaden. Dit gaat ten koste van de inkomsten van de oorspronkelijke leveranciers van die media. Het ACTA-verdrag is erg strak gereguleerd. Als ISP moet je meewerken aan het verkrijgen van bewijsmateriaal en tegelijkertijd een filterende werking hebben op de content die een internetgebruiker gaat downloaden. Deze strakke regulering zorgt ervoor dat het 'big brother'-effect erg zal toeslaan en dat de ISP 'een partij wordt' in de opsporing en mogelijke inlichtingenketen. Elke internetgebruiker die iets downloadt wordt mogelijk op een zwarte lijst gezet. En misschien downloadt hij legitiem informatie en wordt dit door een foutje als belastende content gezien….

Het ACTA-verdrag is veel te zwaar. Kijk naar de reden waarom mensen zo massaal downloaden. Maak de content goedkoper en als dat niet het probleem oplost gebruik dan betere beveiligingstechnieken. Helaas bewezen deze beveiligingstechnieken in het verleden dat ze niet goed werken en dat je legaal gekochte content ook niet meer kon zien of horen. Het is een probleem dat je niet met deze verregaande strakke regelgeving moet willen oplossen."

Saïd El Aoufi: Met betrekking tot ACTA-verdrag wil de overheid internetproviders dwingen om opsporingssoftware in te zetten die de inhoud van het internetverkeer van gebruikers bekijkt. Internetproviders worden hiermee een verlengstuk van de opsporingsdiensten. Monitoren van het alle internetverkeer tast de privacy aan.

De entertainmentindustrie beweert dat gemiste verkoop gerelateerd is aan het downloaden. Uitgaande van het feit dat downloaden financieel negatieve gevolgen heeft voor deze industrie, is dan elke download een gemiste verkoop? Daarbij is downloaden alles wat de gebruiker op internet doet.

De industrie moet meer investeren in onderzoek naar hoe op een legale manier via internet producten zijn te verspreiden, in plaats van zich in te kopen door middel van de wet- en regelgeving. Het beleid moet zich richten op commerciële partijen en aanbieders en niet zo zeer op individuele downloaders. Daarnaast zullen de maatregelen van ACTA niet helpen. Bijvoorbeeld door de inzet van encryptie of werken met servers die in landen staan die geen handtekening onder het verdrag hebben gezet. Internetproviders zullen de encryptie moeten breken, willen ze hun verplichtingen nakomen. Encryptie zal gegarandeerd een enorme vlucht nemen en dan is niets meer te controleren. Het verbod kan dus een averechts effect hebben. En de internetproviders krijgen op deze manier de problematiek van de entertainmentindustrie in de schoenen geschoven."

Aart Jochem: "Een eigenaar van rechten moet verhaal kunnen halen als die rechten worden geschonden. In een kapitalistische economie en een democratisch land zijn daar allerlei wegen voor. Het is frappant dat een industrie zoveel landen zover krijgt om in het geheim afspraken te maken en de handhaving zo op elkaar af te stemmen dat een efficiënte machine ontstaat om misbruikers aan te pakken. Dat is dan weer niet zo democratisch. Inmiddels is een concept van de overeenkomst gepubliceerd, een veel te late correctie.

Maar nu is de weg vrij en kunnen we gebruikmaken van het momentum; pak ook de handhaving van privacywetgeving aan, stem het af en maak het effectief en efficiënt. De drempel van verschillen in wetgeving bleken te slechten voor auteursrechten, dit moet ook lukken voor het recht op privacy. Of de industrie hier ook zo om staat te springen en of zo'n beweging van de grond komt is een tweede."

Identity Management en Privacy

Auteur: Leon P. Kuunders > Leon P. Kuunders is werkzaam bij Trusted-ID als senior identity en access management consultant en bereikbaar via leon.kuunders@trusted-id.eu

Identity Management is een hot topic. Het beheer van virtuele identiteiten wordt algemeen gezien als dé bouwsteen voor ICT-toepassingen, of dit nu in 'the cloud' gebeurt of lokaal, als dienst voor een breed publiek of voor een select gezelschap. Hoe zit het met de bescherming van die virtuele identiteiten met hun niet zo virtuele persoonsgegevens? De auteur gaat in op een aantal ontwikkelingen binnen de rijksoverheid, zoals ook het verplichte gebruik van het burgerservicenummer.

Naar digitale identiteiten wordt erg veel onderzoek gedaan. Die onderzoeken vallen uiteen in grofweg twee verschillende categorieën: digitale identiteiten als maatschappelijk verschijnsel; en digitale identiteiten als onderdeel van organisatorische ICT. De scope van deze onderzoeken is navenant verschillend. De eerste categorie heeft als scope alles en iedereen in de maatschappij, de tweede categorie heeft als scope alles en iedereen binnen de organisatie. In de recent door het Ministerie van Binnenlandse Zaken (BZK) uitgebrachte studie 'Gedeelde en samengestelde identiteiten in de publieke dienstverlening'[I] wordt dit verschil mooi geduid:

"Het is belangrijk om op dit punt te wijzen op verschillende noties van identiteitsmanagement die hier bij elkaar komen: een ICT-beheer perspectief en een meer sociologisch getint perspectief […] In het ICT-beheer perspectief [creëert] de gebruiker een elektronische identiteit (account) bij de dienstverlener (service provider) en de toegang (authenticatie, identificatie, verificatie, autorisatie, of in het algemeen 'access control') en het beheer van die identiteit wordt dan ook identiteitsmanagement genoemd.
In deze technische benadering van identiteitsmanagement gaat het om het beheren van de rechten van gebruikers tot bepaalde voorzieningen en gaat het niet om aspecten van identiteitsmanagement zoals impressiemanagement […] Dat laatste past binnen het meer sociologische perspectief op identiteitsmanagement. […] naarmate een digitale identiteit rijker wordt in termen van informatie die het bevat over een concrete persoon, [schuift] deze meer en meer het sociologische perspectief binnen."

Duidelijk is dat in deze studie identiteit wordt gezien als een verzameling kenmerken. Een identiteit is dan, beheerstechnisch gesproken, simpelweg een *pointer* met *attributen*. Dat klinkt niet alleen erg technisch, het is het ook. U bent een *primary key*, een nummer. In de studie van BZK wordt dit nog eens benadrukt als de volgende definitie van digitale identiteit wordt aangehaald.

"[T]he term identity is often used to refer to the unique set of attributes that makes up a particular person, to which an identifier refers by using a subset of attributes that is sufficiently discriminating to individuate a subject. In that case the identity of the person is understood as the complete set of attributes which uniquely describes her and this is what the identifier (often also called identity) refers to."

Deze definitie, opgesteld door Hildebrandt en Koops[II], gaat er expliciet vanuit dat de identiteit wordt gevormd door het geheel aan attributen waarnaar de identifier verwijst. Het is een mooie definitie, die in het kader van privacy en Identity Management vanuit het ICT-beheer perspectief wel een, laten we zeggen, curieus gevolg heeft. De studie volgt verder de definitie van Digital Persona van Clarke *'A model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual.'* Clarke ziet de digitale identiteit als een verzameling kenmerken, met behulp van transacties onderhouden, die samengevoegd de publieke persoonlijkheid van de houder weergeven. Het mag duidelijk zijn dat de studie zich daarmee (alleen) op het sociologisch getint perspectief van Identity Management richt. Wie bezig is met Identity Management in een ICT-beheer perspectief komt er

dus achter dat veel studies die notie buiten scope plaatsen. Maar er zijn natuurlijk wél de nodige overeenkomsten tussen beide!

Achtergrond Privacy wetgeving

Wat is een persoonsgegeven? Wie de WBP er op na slaat ziet de definitie van een persoonsgegeven als *'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.'* De eerder genoemde definitie van 'identity' zoals Hildebrandt en Koops die hanteren sluit daar dan niet op aan. Want hun definitie plaatst de persoon expliciet buiten de identiteit. De persoon komt pas in beeld in de combinatie van de gegevens mét hun identifier, en alleen dan is er sprake van persoonsgegevens. De gegevens die binnen de definitie vallen zijn op zichzelf dan géén persoonsgegevens. And to make matters worse: in de Memorie van toelichting bij de WBP wordt de definitie van persoonsgegeven verder toegelicht met *'Uitgangspunt is dat een persoon identificeerbaar is indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden.'* Maar wat is dat, onevenredige inspanning? Deze verschilt per verantwoordelijke en is dus niet eenvoudig vast te stellen.
Het definitieprobleem van persoonsgegeven is onder meer beschreven in de eerste evaluatie[IV] van de WBP, waar de conclusie al was *'de onbepaaldheid van het begrip persoonsgegeven [brengt] onduidelijkheid met zich mee over de reikwijdte van de wet [wat] leidt tot uiteenlopende interpretaties.'*

Verplicht gebruik van BSN voor medewerkers rijksoverheid

De staatsecretaris van Binnenlandse Zaken heeft in verband met het gebruik van het burgerservicenummer in de bedrijfsvoering van de overheid in maart 2010 een brief[XII] uitgestuurd naar alle ministeries. In die brief schrijft de staatssecretaris dat het gebruik van het burgerservicenummer in de bedrijfsvoering mag, en zelfs verplicht is, indien aan de voorwaarden daarvoor is voldaan. Het CBP heeft de staatssecretaris inmiddels verzocht dit voornemen niet uit te voeren.[XIII] De voorwaarden die de staatsecretaris in de brief noemt zijn hier genummerd opgenomen met daarbij hun implicaties:

1. *In de eerste plaats heeft de bepaling slechts betrekking op overheidsorganen. Dit impliceert dat de hoedanigheid van het orgaan in bepaalde gevallen dient te worden vastgesteld (is het orgaan in dit kader overheidsorgaan of niet?).*

De definitie van 'overheidsorgaan' geeft de staatssecretaris niet in de brief. Deze is echter opgenomen in de Wabb[XIV] *'een orgaan van een rechtspersoon die krachtens publiekrecht is ingesteld, of een ander persoon of college, met enig openbaar gezag bekleed.'* De definitie is ook herleidbaar via een verwijzing naar de 'Overheid.nl Web Metadata Standaard', vanuit NORA/MARIJ aangegeven. Daar is een overheidsorgaan onderdeel van het element 'overheid: authority'.[XV] In dat element wordt expliciet doorverwezen naar de definitie die door de Erfgoedinspectie is opgesteld.XVI De Erfgoedinspectie onderscheidt twee categorieën overheidsorganen, namelijk: (1) organen van een rechtspersoon, die ingesteld zijn volgens het publiekrecht en; (2) een ander persoon of college met enig openbaar gezag bekleed; het gaat hier om privaatrechtelijke rechtspersonen en natuurlijke personen die bekleed zijn met enig openbaar gezag. Het begrip *enig openbaar gezag* houdt in, dat men krachtens wettelijk voorschrift eenzijdig kan ingrijpen in de rechtspositie van natuurlijke personen of rechtspersonen. Bijvoorbeeld *een garage* is in die definitie een overheidsorgaan bij het melden van een uitgevoerde APK keuring aan de RDW.

2. *Voorts betreft het de verwerking van persoonsgegevens. De gegevensverwerking is gereguleerd, in het algemeen op grond van de Wbp. Uiteraard dient te worden vastgesteld of de gegevensverwerking als zodanig rechtmatig plaatsvindt, alvorens kan worden vastgesteld of daarbij het burgerservicenummer van degenen waarop de gegevens betrekking hebben, kan worden gebruikt.*

Dit is het doelbindingsprincipe: voor elke verwerking dient te worden vastgesteld waaraan deze verwerking haar rechtmatigheid ontleend. Om rechtmatig het BSN te kunnen verwerken, dienen dus wel de bepalingen uit de Wabb te worden gevolgd. Artikel 12 Wabb luidt: *'Indien bij het verwerken van persoonsgegevens een burgerservicenummer wordt gebruikt, vergewist de gebruiker zich ervan dat het burgerservicenummer betrekking heeft op de persoon wiens persoonsgegevens hij verwerkt.'* De definitie van gebruiker is volgens artikel 1, lid d, sub 1 'een overheidsorgaan', zie daarvoor dan verder weer de reactie op 1. hierboven. Dit betekent dus controleren of het burgerservicenummer bij de naamgegevens hoort (zoals ook al in het artikel wordt aangegeven). Alleen hoe doe je dat?
Het lijkt erop dat de enige zinnige oplossing hiervoor is, het aansluiten van de IdM-registraties van de verschillende ministeries op de Beheervoorziening BSN. Dit volgt uit artikel 15 van Wabb waarin staat *'Aan een overheidsorgaan worden in verband met de uitvoering van artikel 12 op zijn verzoek uit de registraties, bedoeld in artikel 3, eerste lid, onder d, de gegevens verstrekt, die hij nodig heeft teneinde na te gaan: a. of aan een bepaalde persoon reeds een burgerservicenummer is toegekend en zo ja, welk burgerservicenummer; b. aan welke persoon een bepaald burgerservicenummer is toegekend; c. of het Nederlandse document, met behulp waarvan een persoon zich identificeert, een document is als bedoeld in artikel 1, eerste lid, onder 1°, 2° of 4°, van de Wet op de identificatieplicht.'* Alleen de IdM-registraties hebben de volledige scope van rijksdienstmedewerkers onder beheer en kunnen deze controle met zekerheid uitvoeren.

3. *Ook geldt ten aanzien van het gebruik van het burgerservicenummer, de algemene regel dat het verwerken ervan toereikend, ter zake dienend en niet bovenmatig is (artikel 11 Wbp).*

De Wbp schrijft over persoonsnummers in artikel 24 van de Wbp *'Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald.'* Aangenomen dat het burgerservicenummer moet worden gebruikt (er is eigenlijk geen middenweg na de brief van de staatssecretaris), dan nog blijft staan dat alléén indien het afnemende systeem vanuit andere systemen dan Identity Management persoons- en identiteitsgegevens betrekt, het gebruik van het burgerservicenummer verplicht is. Immers, indien Identity Management leidend is ten opzichte van het afnemende systeem, dan is het uitwisselen van het burgerservicenummer bovenmatig (en niet ter zake dienend).

4. *Ten slotte dient te worden vastgesteld of de desbetreffende gegevensverwerking geschiedt in het kader van het uitvoeren van de taak van het desbetreffende overheidsorgaan*

Deze opmerking verschuift de kern van het probleem omtrent de verwerking van het burgerservicenummer in de bedrijfsvoering weer naar de ministeries. Want het geschil met het CBP is er juist op gericht dat niet duidelijk is of een bepaalde gegevensverwerking tot de taak behoort of niet. Anders gezegd: is de bedrijfsvoering onderdeel van de taak van de rijksoverheid? Als daarop het antwoord ja is, en dat lijkt het standpunt te zijn van de staatssecretaris, dan wordt de bedrijfsvoering daarmee gelijkgesteld aan bijvoorbeeld het opstellen van beleid. De vraag dringt zich dan bijvoorbeeld op of, indien (onderdelen van) de bedrijfsvoering kunnen worden uitbesteed, dit ook met het maken van beleid kan gebeuren.

Voor Identity Management zou het strikt volgen van de WBP betekenen dat per gegeven en per verwerking moet worden geëvalueerd of dit gegeven bij de verwerking door een bepaalde partij aangemerkt moet worden als persoonsgegeven, of niet. Voor een geautomatiseerd systeem leidt dat tot een onwerkbare situatie, waarbij mogelijk pas na expliciete toestemming en onder het 4-ogen principe gegevensuitwisselingen kunnen worden uitgevoerd. Hoezo automatisch?

Privacy reglement Binnenlandse Zaken

Bij de invoering van Identity Management op het ministerie van Binnenlandse Zaken werd dit definitieprobleem onderkent.[V] Het privacyreglement dat daar voor Identity Management is opgesteld verruimt dan ook de definitie van de te beschermen gegevens. Waar de WBP zich slechts uitlaat over *persoonsgegevens* wordt in het privacyreglement consequent de term *persoons- en identiteitsgegevens* gehanteerd.[VII] Daarmee krijgt het reglement een bredere reikwijdte: het heeft niet alleen meer betrekking op de combinatie van attributen + identifier (zoals in de definitie van Hildebrandt en Koops), nee, de attributen *an sich* vallen daarmee onder de reikwijdte van het reglement. Daarmee krijgt het reglement zin waar het het beheer van *identiteiten* betreft, ten opzichte van het beheer van *personen*. Zo is het reglement bijvoorbeeld ook van toepassing op de verwerking van gegevens waarvan juist de bedoeling is dat ze niet tot een natuurlijke persoon te herleiden zijn.

Een verdere verbijzondering in het reglement ten opzichte van de WBP heeft te maken met de termen referentiële- en attributieve identiteitsgegevens.[VIII] Daarmee wordt een verschil gemaakt in de type gegevens die binnen IDM worden verwerkt. Referentiële gegevens zijn bijvoorbeeld het paspoortnummer, of het burgerservicenummer van de medewerker: met één gegeven is zekerheid over de identiteit te krijgen. In de definitie van Hildebrandt en Koops zijn dit de identifiers. Attributieve gegevens zijn de rest, de niet identifiers, die in combinatie ook tot zekerheid over de identiteit kunnen leiden. Het verschil tussen deze twee type gegevens is maar gedeeltelijk terug te vinden in de memorie van toelichting bij de WBP waar gesproken wordt over *direct* identificerende gegevens en *indirect* identificerende gegevens. Daar zijn echter direct identificerende gegevens met nadruk ook combinaties van verschillende attributieve gegevens, zoals naam + geboortedatum + geboorteplaats. De auteur van dit artikel kan als een helft van een tweeling uit eerste hand verhalen over hoe die definitie van *direct* niet altijd tot een *zekere* 'match' leidt. Met alle vervelende gevolgen van dien.

Burgerservicenummer

In het privacyreglement voor Identity Management wordt ook het gebruik van het burgerservicenummer geregeld. Achterliggende gedachte daar is tweeledig. Enerzijds kan met behulp van een persoonsnummer[IX] het aantal te verwerken gegevens worden geminimaliseerd. Anderzijds kunnen met behulp van een persoonsnummer fouten en dubbelingen worden tegengegaan. Die dubbelingen kunnen ontstaan doordat de verschillende onderdelen van de rijksoverheid, te beginnen bij de ministeries, steeds meer (soms ook gedwongen) samenwerken. Argument daarbij is dat met de synergievoordelen die dat oplevert wel 1 miljard euro kan worden bespaard.[X] Een medewerker van Financiën krijgt bijvoorbeeld ook een contract bij Economische Zaken, werkt flexibel in het kantoor, of het pand, van de rijksoverheid dat voor hem of haar het dichtste bij of het best bereikbaar is en kan *ad hoc* op verschillende projecten worden ingezet. Facilitaire systemen dienen deze verschillende use scenario's te ondersteunen. En omdat de verschillende ICT-systemen van de ministeries nog niet zijn samengevoegd is het idee dat minimaal een unieke *(referentiële) identifier* noodzakelijk is, om dubbelingen en fouten te voorkomen en deze ondersteuning te bieden. Het verwerken van een persoonsnummer stelt echter wel extra eisen aan de verwerking binnen Identity Management. Zo is het rücksichtsloss overnemen van gegevens in combinatie met het burgerservicenummer onverstandig. Daarmee wordt identiteitsfraude gefaciliteerd, terwijl zekerheid over identiteit juist als een van de doelstellingen van Identity Management is vastgelegd! Precies om deze reden heeft de wetgever in de Wet Algemene bepalingen burgerservicenummer ook de eis opgenomen dat *elke verwerker van het nummer* zich ervan verzekerd dat de gegevens die worden verwerkt *in combinatie met* het nummer juist zijn.[XI]

Attributieve gegevens kunnen in combinatie ook tot zekerheid over de identiteit van een persoon leiden

Dit stelt organisaties binnen de rijksoverheid voor een specifiek probleem: in de ketenprocessen waarmee facilitaire dienstverlening aan de organisatie wordt geboden, wordt het aantal verwerkers van gegevens steeds groter. Wat is de toegevoegde waarde als elke verwerker an sich dezelfde controle weer uitvoert? Is het dan niet veel gemakkelijker om die verantwoordelijkheid te beleggen bij één van de deelnemers in zo'n ketenproces? Maar wat als blijkt dat die initiële controle niet goed was? Of als de partij die deze initiële controle uitvoert wordt geoutsourced? En hoe zit het met het gevolg van deze steeds grootschaligere voorzieningen? Werken ze nog wel goed op hún niveau? Zie verder het kader over verplicht gebruik van het BSN voor medewerkers van de rijksoverheid.

Afsluiting

De Identity Management implementaties die bij de rijksoverheid worden uitgevoerd kennen allemaal hun eigen dynamiek en normen. Op het gebied van privacybescherming is geprobeerd deze implementaties zoveel mogelijk te stroomlijnen. Maar om diverse redenen (vaak cultuurverschillen) is dat niet altijd even goed gelukt. Het privacyreglement voor Identity Management dat door BZK is opgesteld doet dienst als een template voor een aantal andere ministeries. Gezien de veranderende organisatievormen bij die rijksoverheid, met steeds meer samenwerking in (keten-)processen over de grenzen van de organisatie heen en met partijen van buiten de rijksoverheid, is bescherming van persoons- en identiteitsgegevens steeds moeilijker. Tel daarbij op de verdergaande verrijking (denk dan aan attributen voor bijvoorbeeld claims based access control!) van identiteiten en het wordt duidelijk dat de tweedeling van Identity Management in een *ICT-beheer perspectief en een meer sociologisch getint perspectief* slecht houdbaar blijft. Deze twee noties convergeren en leiden tot Identity Management dat verdwijnt in, en onderdeel is van, de (ICT-)infrastructuur.
Een radicaal andere inrichting van Identity Management bij de rijksoverheid, waarbij de medewerker centraal komt te staan, ligt dan ook voor de hand. Door het inzetten van technieken uit het veld van *user-centric-identity-management* is de bescherming van (ook) de persoonlijke levenssfeer van de medewerker in rijksoverheiddienst wel te verzekeren. Wie ook de verwerker van diens gegevens is, of in de toekomst wordt.

Het privacyreglement hanteert consequent de term persoons- en identiteitsgegevens en krijgt daarmee een bredere reikwijdte

I Van der Hof en Leenes, Tilburg, April 2010
II Hildebrandt, Mireille, Bert-Jaap Koops and Katja de Vries (2008) FIDIS D7.14a: Where Idem-Identity meets Ipse-Identity. Conceptual Explorations, Place.
III www.cbpweb.nl/downloads_wetten/wbp_mvt.pdf
IV Zie www.wodc.nl/images/1382A_samenvatting_tcm44-61968.pdf
V Aan de lezer de opdracht de use cases hiervoor te verzinnen.
VI Zie files.trusted-id.nl/BesluitPrivacyreglementIdentityManagement12-10-2009.pdf
VII persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon; identiteitsgegeven: elk gegeven dat als kenmerk van een (virtuele) identiteit is aangemerkt.
VIII Gebaseerd op werk dat Van der Hoven heeft gedaan aan de TU Delft. Die verwees in zijn thesis 'Information Technology and Moral Philosophy' (1995) naar werk van Keith Donnellan uit 1966 ('Reference and Definite Descriptions'). Het onderscheidt kan worden gebruikt om architectuurprincipes vanaf te leiden (met name invloed op de verwerking van referentiële gegevens).
IX Maar al te vaak worden de termen 'persoonsnummers' en 'personeelsnummers' door elkaar gebruikt. Tekenend is bijvoorbeeld het verschil tussen het nummer van de medewerker in de personeeelsadministratie, en diens burgerservicenummer. Het gebruik van het eerste nummer is niet aan specifieke wettelijke eisen gebonden, van het tweede wel. Het eerste nummer representeert een contract, het tweede nummer een natuurlijk persoon. Ook de staatssecretaris haalt in diens brief (zie kader) deze twee type nummers door elkaar. Dit leidt uiteindelijk tot verkeerde aannames bij de inrichting van Identity Management systemen en dito succesvolle implementaties.
X Zie www.binnenlandsbestuur.nl/vakgebieden/digitaal-bestuur/na-de-verkiezingen-gaat-het-mes-in-ict.163904.lynkx 'Guusje ter Horst. 'Werkgroep 19 is wat ons betreft het doorzetten van reeds ingezet beleid. Bij de behandeling van de Vernieuwing Rijksdienst hebben wij gezegd dat departementen moeten samenwerken bij bedrijfsvoering én beleid. Dus: weg met de koninkrijkjes. Er is één rijksoverheid en daarbinnen moet je flexibel kunnen werken.' Met dit meest verregaande scenario denkt de werkgroep per jaar 1 miljard euro te besparen.'
XI Artikel 10 WBP schrijft voor dat de verwerker zekerheid dient te hebben dat de te verwerken gegevens bij de betreffende persoon behoren. Daarin kan niet blindelings worden vertrouwd op de aanlevering vanuit één bron, maar moet de mogelijkheid worden gecreëerd voor het bevragen van een tweede bron (effectief gezien is het gebruik van zogenaamde sectorale nummers beter). Dat is waar het gebruik van het BSN bijdraagt aan het voldoen aan de WBP.
XII files.trusted-id.nl/GebruikBSNbedrijfsvoering20100309.pdf
XIII www.cbpweb.nl/downloads_med/med_20100427_gebruik_bsn_in_bedrijfsvoering_overheid.pdf – het bericht is origineel gepubliceerd op 26 januari 2009, op 27 april 2010 heeft het CBP een nieuwe mededeling gedaan waarbij ze nogmaals op hun, in deze brief vastgelegde, standpunt hebben gewezen.
XIV Wet algemene bepalingen burgerservicenummer
XV standaarden.overheid.nl/owms/3.5/doc/eigenschappen/overheid.authority.html
XVI www.erfgoedinspectie.nl/archieven/wet-en-regelgeving/archiefwetgeving/reikwijdte

PvIB Masterclass 'Kijk op Privacy'

Auteur: Hong Gie Ong > ir. Hong Gie Ong CISSP CISA werkt als security consultant bij Capgemini en is bereikbaar via hong-gie.ong@capgemini.com.

Als onderdeel van een serie events voor de PvIB Young Professionals, vond afgelopen 15 april, de Masterclass 'Kijk op Privacy' plaats bij de Rijksauditdienst op de locatie van het Ministerie van Financiën in Den Haag.
Sprekers van die dag waren Rina Steenkamp, Technoloog bij het College Bescherming Persoonsgegevens (CBP) en auteur van de nieuwe Richtsnoeren Beveiliging Persoonsgegevens, alsook Judith Unk, functionaris Beveiliging en Privacy bij het Uitvoeringsinstituut WerknemersVerzekeringen, oftewel, het UWV. Frans van Oostrum, hoofd van het bureau integriteit bij UWV, was ook aanwezig voor toelichting van een aantal treffende voorbeelden aangaande privacy van persoonsgegevens waar het UWV regelmatig mee te maken heeft.

Onze persoonsgegevens, onze identiteit. We bevinden ons in een informatiemaatschappij, waarbij we er niet om heen kunnen dat overheid, bedrijven en organisaties inzage moeten krijgen in onze persoonsgegevens, om handelingen die met onze persoon te maken hebben, uit te voeren. Denk maar eens aan verzekeringen, belastingen, abonnementen, lidmaatschappen, post, de loonstrook, banktransacties en ga zo maar door. Internet en digitalisering van gegevens en persoonsgegevens in het bijzonder, maken dat regelgeving noodzakelijk is om de burger te beschermen, zodat diens persoonsgegevens niet zomaar onverlet bij anderen kunnen belanden voor wie het niet bedoeld is. Tijd voor een sessie die een Kijk op Privacy tracht te geven in het licht van Europese en Nederlandse privacywetgeving in het bijzonder.

Toelichting op de Wbp

In Nederland is belangrijke regelgeving rondom bescherming van persoonsgegevens vastgelegd in De Wet bescherming persoonsgegevens (Wbp). Het College Bescherming Persoonsgegevens (CBP) houdt toezicht op naleving van de Wbp. Het CBP is het zelfstandig bestuursorgaan (ZBO) dat bij wet in Nederland als toezichthouder is aangesteld voor het toezicht op het verwerken van persoonsgegevens.

Afhankelijkheden Wbp

Aan de hand van de weergegeven pyramide wordt door Rina toegelicht, hoe de Wbp samenhangt met Europese regelgeving inzake omgang met persoonsgegevens van burgers. Als basis dient de zogenaamde Richtlijn 95/46/EG welke de hoofdlijnen bevat, die verder uitgewerkt zijn in de wet- en regelgeving van de Europese lidstaten. De Wbp is de Nederlandse 'implementatie' van die Richtlijn 95/46/EG. In de richtlijn staat ondermeer dat elk land een toezichthouder moet hebben. Elk van de EU-lidstaten heeft dus een eigen variant op het CBP. Echter de bescherming van persoonsgegevens en privacy komt ook in meer richtlijnen aan de orde, zoals de Richtlijn 2002/58/EG (e-privacy) en in Nederland in wetten zoals de Wet GBA (Gemeentelijke Basis Administratie) en de Wet SUWI (Structuur Uitvoeringsorganisatie Werk en Inkomen).

Doel van de Richtlijn 95/46/EG

Doel van de richtlijn is enerzijds dat organisaties binnen de EU vrij en onbelemmerd hun activiteiten moeten kunnen ontplooien, en daarbij persoonsgegevens moeten kunnen verwerken. Anderzijds moet dat wel

1 www.cbpweb.nl/Pages/med_20080218_werkprogr_wp29_2008.aspx

op zo'n manier gebeuren, dat ook de rechten van de betrokkenen daarbij gewaarborgd zijn.
Alle artikelen van de richtlijn zijn te zien in het overzicht van slide 'Richtlijn 95/46/EG' uit de voordracht van Rina.

Toezicht en handhaving
Er is een samenwerkingsverband van Europese toezichthouders dat opinies afgeeft over bepaalde privacyzaken die in heel veel lidstaten spelen. Bijvoorbeeld het gebruik van sociale netwerken, het gebruik van cookies en spyware, gebruik van zoekmachines, en passagiersgegevens. Onderwerpen waarbij het eigenlijk niet zo veel nut heeft om dat als nationale toezichthouder alleen te willen onderzoeken, terwijl het eigenlijk in heel Europa speelt. Deze groep, WP29 (Working Party 29) is opgericht op grond van artikel 29 van Richtlijn 95/46/EG en is een onafhankelijk Europees adviesorgaan inzake gegevensbescherming en de persoonlijke levenssfeer, waarvan de taken zijn omschreven in artikel 30 van Richtlijn 95/46/EG en in artikel 15 van Richtlijn 2002/58/EG (e-privacy). Belangrijke doelstelling, is het aandragen van privacybevorderende oplossingen voor problemen die zich als gevolg van nieuwe technologische toepassingen voordoen[1].

Intermezzo van auteur:
Een van de interessante ontwikkelingen om in de gaten te houden, is de implementatie in de lidstaten van de Europese regelgeving inzake cookies[2] sinds eind 2009. Het nieuwe artikel 5 lid 3 e-Privacyrichtlijn eist voor het plaatsen van een cookie de toestemming van de gebruiker, pas nadat de internetgebruiker is voorzien van duidelijke informatie over onder andere het doel van de verwerking. Er zijn namelijk nog een aantal issues die getackeld moeten worden voordat dit echt geïmplementeerd kan worden. Kan goedkeuring bijvoorbeeld worden gezien als de standaardinstellingen van een browser all cookies accepteert? Wordt er van de gebruiker verwacht dat deze weet hoe die de default instellingen van zijn browser moet aanpassen? Zie bijvoorbeeld ook gerelateerde berichtgeving:

ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp159_nl.pdf
www.emerce.nl/nieuws.jsp?id=3028862

Toelaatbaarheid en randvoorwaarden
Een aantal artikelen uit de richtlijn, gaat verder in op de toelaatbaarheid en randvoorwaarden. Hier moet gedacht worden aan, persoonsgegevens verwerken mag, mits..., en het verwerken van bepaalde persoonsgegevens (zoals het BurgerService-Nummer BSN) mag niet, *tenzij*...

Transparantie en zeggenschap
De artikelen 10 tot en met 15 gaan in op transparantie en op zeggenschap voor de betrokkenen. Hoe krijgen betrokkenen bijvoorbeeld inzage in hun persoonsgegevens, hoe kunnen zij die corrigeren en bij wie kunnen zij terecht als hun persoonsgegevens niet kloppen? Hiervoor moeten voldoende mogelijkheden aanwezig zijn. Verder kunnen betrokkenen zich onder bepaalde voorwaarden verzetten tegen verwerking van hun persoonsgegevens, al is dit recht niet onbeperkt. In het organisatieontwerp, procesontwerp en in de functionaliteit van de geautomatiseerde gegevensverwerking moet rekening worden gehouden met transparantie en zeggenschap. Bij de praktische uitwerking moet ondermeer worden gedacht aan 'mijn<organisatie>'-internetfunctionaliteit. Ook het geheime telefoonnummer is een voorbeeld van het geven van zeggenschap

aan betrokkenen. Als transparantie en zeggenschap goed worden toegepast is dit zowel in het belang van de betrokkene (voldoende zeggenschap over wat er met zijn of haar persoonsgegevens gebeurt) als van de organisatie (betere gegevenskwaliteit).

Kwaliteit, vertrouwelijkheid en beveiliging
De artikelen 6, 16 en 17 gaan in op de kwaliteit van de gegevens en op de vertrouwelijkheid en de beveiliging van de verwerking. Dit wordt nader toegelicht in de volgende paragrafen.

Kwaliteit: doelbinding
Doelbinding ligt in het verlengde van toelaatbaarheid en randvoorwaarden. Hier wordt aangegeven dat het doel van de verwerking dient te worden vastgesteld en men moet blijven toetsen of (verdere) verwerking daarmee in overeenstemming is.

Kwaliteit: dataminimalisatie
Een ander basisbeginsel van de bescherming van persoonsgegevens is dataminimalisatie. Verwerk wat nodig is, maar niet méér. Bijvoorbeeld: geen volledige creditcardgegevens afdrukken op nota's; geen onnodige kopieën van identiteitsbewijzen etc. Dataminimalisatie betekent ook: geef niet onnodig veel mensen toegang tot onnodig veel gegevens.
Dataminimalisatie raakt alle aspecten van informatisering, onder meer het datamodel, procesontwerp, organisatieontwerp alsook het ontwerp van de gebruikersinterface en de autorisaties. Wat hier ook toegepast kan worden zijn zogenaamde Privacy Enhancing Technologies, zoals anonimisering of pseudonimisering van gegevens.

Informatiebeveiliging: algemene eisen
De richtlijn stelt op hoofdlijnen eisen aan de beveiliging van persoonsgegevens. De verantwoordelijke voor de verwerking dient passende beveiligingsmaatregelen te treffen, waarbij (in artikel 6 lid 1d) specifiek aandacht wordt gevraagd voor de integriteit van de verwerkte persoonsgegevens.

Informatiebeveiliging: eisen aan personeel
Personeel mag alleen persoonsgegevens verwerken in opdracht van de verantwoordelijke, waarbij verwerken niet alleen 'iets doen met', maar ook 'kennisnemen van' inhoudt. De verantwoordelijke kan naleving onder meer bevorderen door het toepassen van logische toegangsbeveiliging, opleiding en geheimhoudingsovereenkomsten.

Informatiebeveiliging: eisen aan uitbesteding
Bij uitbesteding dient gekozen te worden voor een verwerker die voldoende beveiligingswaarborgen biedt (de richtlijn spreekt over een 'verwerker', de Wbp over een 'bewerker'. Met beide termen wordt hetzelfde bedoeld). De afspraken over de beveiliging moeten worden vastgelegd in het contract, en de verantwoordelijke moet toezien op naleving van de afspraken (waarbij bijvoorbeeld gebruik kan worden gemaakt van TPM, Third Party Mededelingen). De verwerker mag alleen verwerken in opdracht van de verantwoordelijke.

Interessant is om op te merken dat uit de richtlijn volgt, dat de partij waaraan wordt uitbesteed, juridisch gezien niet altijd een verwerker is, maar ook een verantwoordelijke kan zijn. Voor meer informatie wordt door Rina verwezen naar Opinion 1/2010 on the concepts of 'controller' en 'processor'[3] van WP29. Voor ICT-dienstverleners is het van belang dat ze weten of ze verantwoordelijken zijn of bewerkers, omdat de Wbp meer verplichtingen aan verantwoordelijken oplegt dan aan bewerkers.

Hierbij kwamen vragen uit de zaal naar voren over het toestaan van cloud computing bij verwerkers. Aspecten die hierbij een rol spelen; men weet niet waar de data precies worden opgeslagen (verdeeld over meerdere internationale datacenters?), welk land, en welke wetgeving van toepassing is. Genoemd wordt dat er wel regelingen zijn met bijvoorbeeld organisaties in de VS die zich kunnen voegen bij het Safe Harbor[4] framework en principes, wanneer ze met Europese instanties gegevens willen uitwisselen/verwerken. Dit framework zou ontwikkeld zijn door de US Department of Commerce in consultatie met de EU, met als doel dat ondanks dat de VS een andere benaderingswijze heeft op privacy van persoonsgegevens dan Europa, Amerikaanse bedrijven toch de verschillende zienswijzen kunnen overbruggen en kunnen inspelen op de Europese Richtlijn 95/46/EG. Hoe dat met andere landen zit komt in deze sessie verder niet aan de orde, maar onmogelijk zou het niet zijn volgens een voorbeeld in de zaal waarbij deze weg was ingeslagen. In ieder geval spelen contracten die een

3 ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf
4 www.export.gov/safeharbor/
5 Principles van de OESO

uitbesteder met zijn verwerker afsluit, hier een belangrijke rol en is het altijd raadzaam om uiteraard een juridische specialist hierbij te betrekken.

Achtergrond en Verkenningen 23 (A&V23)

Verder omhoog de pyramide in; de uitwerking die nu nog vigerend is, is Achtergrond en Verkenningen 23 (A&V23), geschreven in 2001, gepubliceerd door toen nog de Registratiekamer, de voorloper van de College Bescherming Persoonsgegevens en is te downloaden via www.cbpweb.nl.

Het doel was, en is, inzichtelijk te maken hoe de toezichthouder de wet interpreteert. De A&V23 bevat een risicoclassificatie, waarbij op basis van een aantal kenmerken van de verwerking en de te verwerken gegevens men tot een aantal risicoklassen komt. Dit vertaalt zich naar Risicoklasse 0, I, II en III, en op basis daarvan worden er in de A&V23 beveiligingsmaatregelen aanbevolen.

Ervaringen met de A&V23

Het CBP heeft een onderzoek laten uitvoeren naar de ervaringen van partijen die de A&V23 gebruiken (wat zou er beter kunnen) wat een scala aan bevindingen heeft opgeleverd.

- Een van de criteria voor een hogere risicoklasse is dat er sprake is van complexe informatieverwerking. Maar wat is dan groot, wat is complexe informatieverwerking? Met moderne middelen kan veel meer, is dat dan complex?
- Voorziet de algemene risicoclassificatie ook wel in specifieke risico's, bijvoorbeeld als je bij de verwerking cloud computing toepast, kun je dan wel over risicoclassificaties spreken?
- Beleving van de betrokkenen.
- Moeten de risicoclassificaties 0, I, II en III niet fijnmaziger?
- Zijn het er niet te veel?
- Zijn het wel altijd de juiste maatregelen?
- Zijn de risico's niet te divers om te kunnen worden afgedekt met eenzelfde set van beveiligingsmaatregelen?
- Biedt een hogere risicoklasse wel meer waarborgen?
- Doet de risicoanalyse recht aan de risico's voor betrokkene?

Richtsnoeren beveiliging van persoonsgegevens

Het CBP is bezig om de A&V23 te vervangen door Richtsnoeren. Deze zijn echter nog niet gepubliceerd. De basis voor de beveiliging van persoonsgegevens wordt gevormd door adequate informatiebeveiliging. Beveiligingsmaatregelen treffen op basis van risicoanalyse, daarbij gebruikmakend van de methoden en standaards die binnen de specifieke situatie het meest passend zijn. In de zorg kan bijvoorbeeld gebruik worden gemaakt van de norm NEN 7510, een nadere uitwerking van de Code voor Informatiebeveiliging voor de zorg.

Een internetbedrijf zou gebruik kunnen maken van het Raamwerk beveiliging webapplicaties van GOVCERT, in combinatie met de Code voor Informatiebeveiliging voor de meer organisatorische beveiligingsaspecten. Het is belangrijk de kennis en kunde die in het vakgebied informatiebeveiliging aanwezig zijn daadwerkelijk toe te passen.

De belangen van de organisatie en van de betrokkenen lopen vaak parallel. Dit is echter niet noodzakelijkerwijs het geval. Daarom wordt aanbevolen om de privacyrisico's te analyseren met behulp van een Privacy Impact Assessment (PIA). Een PIA helpt om de risico's die een verwerking voor betrokkenen met zich mee brengen in kaart te brengen en om waar nodig maatregelen te nemen.

Momenteel is het CBP bezig om gezamenlijk met een aantal belanghebbende partijen een PIA te ontwikkelen voor de Nederlandse markt, zoals die nu al bestaat in het Verenigd Koninkrijk. Daarmee wordt uitvoering gegeven aan het Kabinetsstandpunt advies Commissie Brouwer-Korff en evaluatie van de Wet bescherming persoonsgegevens, waarin de wenselijkheid van de ontwikkeling van een Nederlandse PIA wordt benadrukt.
Het plan is om de structuur van de PIA op te hangen aan de Privacy Principles van de OESO,[5] waardoor het ook vertaald kan worden naar andere landen.

Handhaving

Binnen de waarborgen voor de beveiliging van persoonsgegevens vormen extern toezicht en handhaving het sluitstuk. De basis wordt gevormd door de waarborgen binnen de verwerking zelf. Toezicht door de Functionaris voor de Gegevensbescherming, interne audits, externe audits en penetratietests vormen essentiële aanvullingen.

Vervolgens volgen twee voorbeelden aangaande handhaving door het CBP in de praktijk:

- Informatiebeveiliging ziekenhuizen

www.cbpweb.nl/Pages/pb_20090608_lod_ziekenhuizen.aspx
'CBP legt last onder dwangsom op aan vier ziekenhuizen - Informatiebeveiliging

ziekenhuizen niet op orde'
Toegepaste norm: NEN7510, die samen met de IGZ (gezondheidszorg) is uitgevoerd.

- Regionale EPD's
www.cbpweb.nl/Pages/pb_20090527_reg_epd.aspx
'CBP: Twee regionale elektronische patiëntendossiers in strijd met de wet - Patiënten niet geïnformeerd over opname van hun gegevens'

Raakvlakken informatiebeveiliging: Toegangsbeveiliging was onvoldoende en er moest meer logging plaatsvinden.

Deze en overige CBP-nieuws en -publicaties zijn te vinden op:
www.cbpweb.nl/Pages/ind_zw.aspx

Uit de zaal komt verder naar voren dat er veel aandacht is voor de bescherming van digitale gegevens, maar dat er eigenlijk ook een groot issue is met papieren dossiers die toegankelijk zijn doordat deze of op de printer blijven liggen, op bureaus en balies liggen of gaan 'wandelen'. Ondanks dat dit in risicoanalyses zou moeten zijn afgedekt, is de praktijk vaak dat degenen die met de persoonsgegevens werken op de werkvloer en die met de dossiers rondlopen, vaak niet betrokken worden bij dat proces van risicoanalyse. De verantwoordelijken, de informatie-eigenaren zouden hier een nadrukkelijkere rol moeten spelen. Deze discussie is voor vervolg vatbaar.

Hands-On informatie: PIA en Compliance-instrumenten

- PIA (Britse toezichthouder)
www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

- Compliance instrumenten CBP (onder meer quick scan en raamwerk privacy audit)
www.cbpweb.nl/Pages/ind_wetten_zelfr_compliance.aspx

Algemene informatie

• Gegevensbescherming in Europa
ec.europa.eu/justice_home/fsj/privacy

• Nederlandse wet- en regelgeving
wetten.overheid.nl

• CBP
www.cbpweb.nl
www.mijnprivacy.nl

• Ministerie van justitie
www.justitie.nl/onderwerpen/opsporing_en_handhaving/Wbp/

Weblogs

• Recht en techniek (Nederlands)
blog.iusmentis.com/
www.ict-recht.com/
www.solv.nl/weblog/

• Recht en techniek (Internationaal)
blog.tech-and-law.com/

• Gegevensbescherming (Europees)
www.edri.org/

Het CBP heeft een koerswijziging doorgemaakt en richt zich op handhaving. Het CBP is van mening dat de privacy-advisering door marktpartijen zou moeten worden ingevuld, en ziet dit ook steeds meer gebeuren.

Rina Steenkamp heeft haar bijdrage aan deze masterclass op persoonlijke titel geleverd.

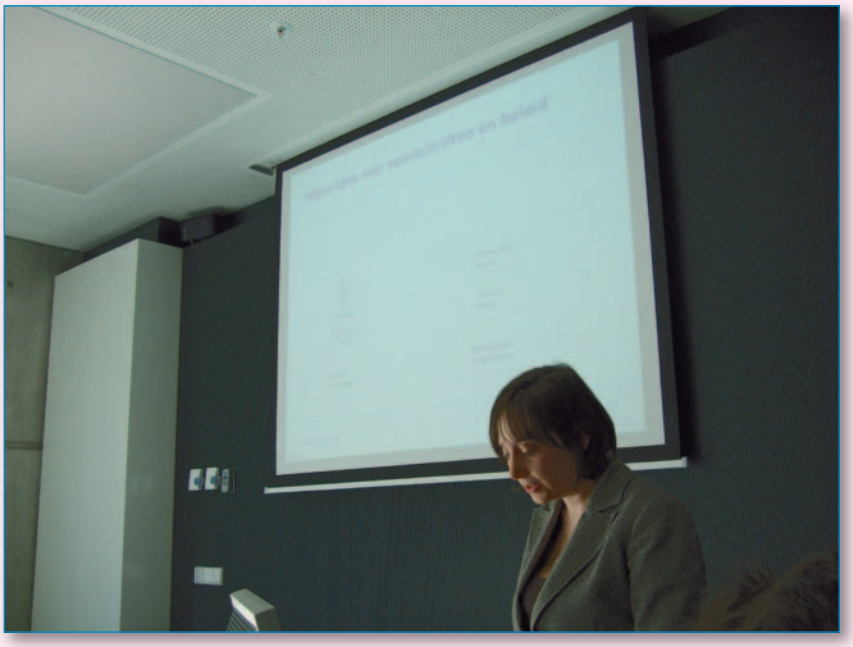
Prakijkcase: UWV
Functionaris Beveiliging en Privacy
Judith Unk

Frans van Oostrum
Hoofd Bureau Integriteit

Onderdeel van Bestuurszaken bij UWV voor advies naar Raad toe.

Als praktijkcase vertelt Judith Unk, Functionaris Beveiliging en Privacy bij de UWV (Uitvoeringsinstituut WerknemersVerzekeringen), over bescherming van persoonsgegevens bij de UWV als een van de grootste verwerkers van persoonsgegevens in Nederland. Eerst volgt een introductie waar deze organisatie voor staat, waar zij vandaan komt en een toelichting van de omgeving waarin zij zich nu bevindt. Het UWV is een semi-overheidinstelling dat tot doel heeft mensen te begeleiden naar werk en als dat niet lukt tijdelijk aan inkomen te helpen via:

- WW
- WIA (nieuwe WAO)
- WAjong



Vandaar ook hun nieuwe slogan: 'Mensen Perspectief Geven'. Het UWV wil in 2013 de beste publieke dienstverlener van Nederland worden. Verder wordt de huidige situatie waar het UWV mee te maken heeft in Nederland geschetst.

Huidige situatie in Nederland:
441.000 werklozen
900.000 Arbeidsongeschikten

Het UWV beschikt over 180 kantoren en 20.000 medewerkers. Het is officieel ontstaan in 2002 en komt uit een fusie van zes organisaties die elk hun eigen polisadministraties geautomatiseerd hadden. Voor iedere uitkering bestond een eigen systeem. IT-technisch een enorm complexe consequentie qua migratie. Inmiddels is het UWV van meer dan 800 systemen naar 200 of minder systemen gegaan. En tijdens deze 'verbouwing', was het 'gebouw' gewoon open. Er wordt steeds meer in ketenverband gewerkt, bijvoorbeeld in de samenwerking met de Belastingdienst, waar veel berichtenverkeer mee wordt uitgewisseld en waar een deel van het werk naartoe is overgegaan (vroeger inde UWV zelf de premies, nu doet de Belastingdienst dat, zodat werkgevers nog maar aan een instantie hoeven af te dragen).

Het UWV is gefuseerd met het CWI (Centrum voor Werk en Inkomen). Ging zij in het verleden uit van een wetgerichte structuur (tak voor WW, tak voor WAO etc.), werkt zij tegenwoordig in een klantgerichte/procesgerichte structuur. De dagkoersen van de politiek spelen een belangrijke rol, aangezien aanpassingen in de relevante wetgevingen van invloed zijn op het werk van het UWV. Elk jaar wordt er circa 19 miljard aan uitkeringen verstrekt.

Wie staan er bij het UWV geregistreerd?
Het aantal geregistreerde verzekerden is iedereen die in loondienst is of was.

Een toelichting volgt op het belang van Privacy bij het UWV, aan de hand van:
- Raamwerk privacy audits
- A&V23
- Informatiebeveiliging

Privacy Incidenten in de pers
Het belang van privacy wordt benadrukt door een aantal voorbeelden in de pers.

- Patiëntendossiers niet veilig (Trouw, mei 2009, regionale EPD's).
- Hackers stelen miljoenen elektronische patiëntendossiers in VS (Webwereld, nov 2008).
- Medische gegevens op straat (Telegraaf, juni 2009).
- Digid gekraakt: 'Ik weet alles van haar' (Metro, april 2010)
- UWV en Achmea verzuimen servers te vergrendelen (maart, 2009)

Het laatste voorbeeld betreft het UWV. Vorig jaar was er iemand die de serverruimten van de UWV inliep. Echter, het betreft de serverruimte van een externe hostingpartij aangezien het UWV dit heeft uitbesteed aan leveranciers. Interessant om op te merken is ook, dat ondanks dat dit bij een van de leveranciers is gebeurd, wel het UWV in het nieuws komt. Uit de zaal wordt aangegeven dat het inderdaad vaak zo is dat wie het meest interessant is voor de media (de grotere brand name) in het nieuws komt, en niet altijd de partij wiens fout het was.

Vraag uit de zaal: wat heeft UWV gedaan naar aanleiding van dit persbericht?
Het UWV heeft eerst onderzocht wat er daadwerkelijk gebeurd was, woordvoerders

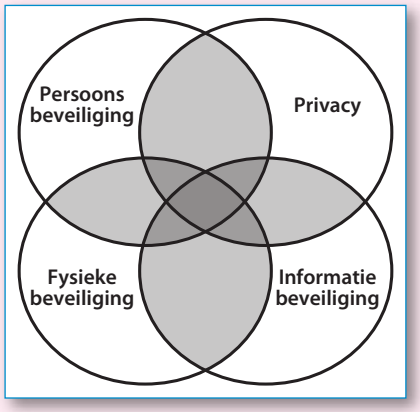
laten kortsluiten met de IT-mensen, aangegeven dat ze het betreuren en het reële beeld weergegeven alsook het daadwerkelijke risico toegelicht. Echter dit had dan natuurlijk weer minder aandacht in de media omdat dat wellicht niet de 'leuke' headlines zijn.

Ervaringen met CBP-product: raamwerk privacy audits

Vervolgens wordt gekeken in hoeverre het Raamwerk privacy audits iets zegt over de eisen bij een verwerker door een bewerker: Er moet sprake zijn van een:

- formeel contract;
- beveiligingsovereenkomsten met de verwerkers;
- continu proces van toezicht op de externe dienstverlener.

Daarbij had er net een maand geleden een audit plaatsgevonden en was er een TPM afgegeven. UWV had aan al die voorwaarden voldaan, maar toch vond zo'n incident plaats. Hierop volgt discussie uit de zaal of dit nu iets zegt over of men nu wel of niet moet uitbesteden. Er wordt gesuggereerd dat zo'n incident eigenlijk niet te voorkomen is, ongeacht wel of geen uitbesteding. En is een hostingpartij eigenlijk niet te



klein om echt aansprakelijkheid te kunnen dragen voor zoiets groots? Daarbij wordt aangegeven dat er dusdanige hoge eisen aan de UWV-systemen worden gesteld, zoals een permanent back-upsysteem, het gelijktijdig kunnen meedraaien van een tweede systeem enz. En bijvoorbeeld het kunnen overleven van een atoombom. Dus wanneer men naar al die zaken kijkt en het UWV zou dit zelf moeten regelen, dan is het maar de vraag hoeveel dit de maatschappij zou gaan kosten mocht dit allemaal binnen de sociale zekerheid geregeld moeten worden! De discussie wordt vanwege de tijd on-hold gezet.

Persoonsgegevens bij het UWV

Welke persoonsgegevens heeft het UWV eigenlijk allemaal? Qua vertrouwelijkheid van de gegevens zit het UWV vergeleken met andere overheid en semi-overheidsinstanties, heel hoog. Het UWV heeft persoonsgegevens omtrent:

- naw-gegevens van iedereen in dienstverband;
- inkomensgegevens daarvan;
- alle uitkeringsgegevens;
- medische gegevens van mensen die ooit een uitkering hebben aangevraagd; het percentage dat is afgekeurd, medische beperkingen, onder andere psychiatrische rapporten en uitslagen van aidstests bijvoorbeeld. Het gaat heel ver met de persoonsinformatie waarover de UWV beschikt.

Bedreigingen in de praktijk

Judith benadrukt dat de informatie bij het UWV geld waard is. Klanten kunnen niet kiezen of ze wel of geen persoonsgegevens bij UWV willen neerleggen. UWV draagt een maatschappelijke verantwoordelijkheid om zorgvuldig met deze gegevens om te gaan. Derden hebben soms belang bij deze persoonsgegevens en het UWV loopt risico dat deze gegevens onterecht bij derden belanden.

Om dit verder te illustreren wordt een aantal voorbeelden genoemd door middel van telefoontapes, van opnames bij het klantencontactcentrum van het UWV. Deze praktijkvoorbeelden worden ook voor interne bewustwording gebruikt en zijn ter beschikking gesteld door het bureau integriteit bij het UWV.

Derden proberen gegevens te ontlokken bij UWV-medewerkers

Het betreft voorbeelden waarbij door zogenaamde social engineering, het klantencentrum wordt benaderd met vragen als:

- Is mijn ziekmelding wel doorgekomen?;
- Informatie omtrent Curriculum Vitae;
- Kunt u nagaan wat mijn laatste werkgevers waren?;
- Zijn mijn verhuisgegevens wel goed doorgekomen en wat hebben jullie daarover staan?

In de voorbeelden echter, waren het niet klanten zelf die gegevens opvroegen maar een derde partij (bijvoorbeeld een incassobureau), dat zich voordeed als de klant, om bepaalde gegevens te achterhalen. De medewerkers van het UWV worden geacht alleen bepaalde zaken te mogen controleren aan de telefoon, niet willekeurige informatie vanuit hun UWV-systemen te communiceren aan de telefoon. De voorbeelden spreken enorm tot de verbeelding aangezien dit een ieder van ons kan treffen als lijdend voorwerp. Het bleek in een bepaald geval zelfs te gaan om een

regelmatige beller die zich voordeed als een 'interne' en perioden lang informatie trachtte te ontfutselen op deze manier. Het bureau Integriteit kreeg dit in de gaten en uiteindelijk werd de persoon in kwestie opgepakt. Het bleek te gaan om een incassobureau. Deze informatie is dus letterlijk geld waard.
Nog even op een rijtje; wie zijn er uit op onze informatie bij het UWV:
- handelsinformatiebureaus;
- schuldeisers;
- boze ex-en;
- verzekeraars;
- buren;
- ?

Intern: mogen UWV-medewerkers alles zien?
Omdat UWV-medewerkers toegang hebben tot de systemen kunnen ze ook veel persoonsgegevens inzien. Hierbij wordt mogelijk ook de privacy van klanten geschaad. Wanneer het voorvallen met BN'ers betreft, dan zijn mensen en dus wellicht ook medewerkers, zeer geïnteresseerd in bepaalde informatie. Maar die informatie is ook nodig om hun werk te kunnen doen. Zo heeft een politie het nodig om aangiftes in te zien, maar moeten aangiftes tegen BN'ers niet voor alle politiemensen zichtbaar zijn. Alleen als ze het nodig hebben voor hun zaak.

Een ander voorbeeld zijn de videobeelden van Wesley en Yolanthe, die via een beveiligingscamera in een parkeergarage zijn opgenomen. Het materiaal komt in handen van RTL-boulevard. Of het voorbeeld van de informatie van het zichtbare kenteken van de dader van de aanslag op Koninginnedag vorig jaar. Waarom moesten bepaalde medewerkers dit kenteken opzoeken?

Dilemma's; klantgerichtheid versus privacy
In een aantal dilemma's wordt het verschil tussen klantgerichtheid en privacy duidelijk gemaakt.

Bij UWV wil men natuurlijk de klant snel en gemakkelijk helpen. Het UWV wil geen logge organisatie zijn, maar waar leg je de grens? Wanneer geef je te veel informatie bloot?
Het ziekenhuis krijgt inzage in bepaalde medische gegevens van een patiënt versus privacygevaar als die informatie in verkeerde handen valt. Het is toch handig dat het ziekenhuis weet welke medicijnen niet mogen worden toegepast vanwege allergie voor die medicijnen van de patient? De camera's in de parkeergarages zijn er toch voor de veiligheid van mensen en auto's, maar als die gegevens in verkeerde handen vallen, zijn de betrokkenen daar ook niet van gediend.

Doelbinding
Het begrip uit de Wbp 'doelbinding' maakt duidelijk waar het om gaat. De camera's in de parkeergarage zijn opgehangen met het doel de veiligheid te garanderen. Ook Yolanthe is hierbij gebaat. Maar als dezelfde camera's worden gebruikt voor het doel om als nieuwsitem op RTL-boulevard een leuk item op te leveren, wordt de privacy van Yolanthe en Wesley aangetast.

Om aan doelbinding te voldoen dient er ofwel toestemming van de betrokkene te zijn, zoals Rina in haar verhaal over het Wbp al eerder aangaf, of een wettelijke verplichting aanwezig te zijn. Bij het UWV betreft het voornamelijk wettelijke verplichtingen. Maar ook toestemming van de betrokkene komt voor. Veel mensen hebben namelijk allerlei verzekeringen. Wanneer iemand een huis koopt zijn er vaak arbeidsongeschiktheidsverzekeringen gekoppeld aan de WIA, waarbij het UWV dan de schriftelijke verklaring nodig heeft van de betrokkene dat deze akkoord gaat en het UWV deze informatie mag doorgeven.

Ervaringen met CBP-product: Risicoclassificaties (A&V23)
Als het een complexe verwerking betreft, dan komt het in risicoklasse III. Maar wat is nu een complexe verwerking? Het is te onduidelijk. Wat doet het UWV met deze risicoclassificatie? Er wordt wel gebruikgemaakt van de tips, de gedachten en de richtlijnen, maar er moet toch meer uitgegaan worden van de risico's die gelopen worden in relatie tot de schade. Dat is nuttiger dan de eindeloze discussie in welke risicoklasse iets zou horen. Bij het UWV komt iets al heel gauw in risicoklasse II of III.

Privacy in de context; kan niet zonder informatiebeveiliging
In het tactisch beleid van het UWV zijn 4 zuilen onderkend:

- privacy;
- informatiebeveiliging;
- fysieke beveiliging;
- persoonsbeveiliging.

Deze zuilen hebben van alles met elkaar te maken, deels niet, maar voor een groot deel overlappen ze elkaar. Sommige gebieden, gaan alle onderdelen aan. In het tactische beveiligingsbeleid komen deze aspecten verder aan de orde.

De Wbp stelt de wettelijke kaders, maar maatregelen vallen vaak in het domein van

informatiebeveiliging. Zaken zoals social engineering en papier, zijn ook onderdeel van de Code van Informatiebeveiliging. Omdat IT-ontwikkelingen heel snel gaan is om privacy te beschermen, informatiebeveiliging heel belangrijk.

Beleid bij het UWV
UWV heeft een strategisch en tactisch Beveiligings- en Privacybeleid. Het tactisch beleid is vooral gebaseerd op de Code van Informatiebeveiliging en de Wbp, zoals veel organisaties dit kennen. Het strategisch beleid zegt iets over wet, theorie en standaarden; hoe je in hoofdlijnen moet omgaan met persoonsgegevens, een goed ingeregelde AO/IC dient te hebben, goed huisvaderschap en standaarden, wat weer input is voor het tactisch beleid.

Maatregelen ter bescherming van de privacy
Deze vallen uiteen in Organisatorisch, Logisch en Fysiek niveau.
Voor wat betreft Organisatorisch, gaat het om Preventie en Repressie.

Preventie, toepassing van:
- functiescheiding;
- instructie Gegevenslevering Aan Derden (IGAD); wie krijgt welke gegevens onder welke voorwaarden;
-medisch beroepsgeheim;
- tactisch B&P beleid;
- bewustwordingscampagnes: de mens is de zwakste schakel.

Repressie, toepassing van:
- bij misstanden: onderzoek door bureau Integriteit;
- bij misstand vastgesteld: arbeidsrechtelijke sancties.

De **logische** maatregelen vallen uiteen in:
- afdichten van systemen: Netwerkbeveiliging, Logische toegangsbeveiliging, Autorisatiebeheer;
- nadenken over nieuwe ontwikkelingen: beveiliging digitale dossiers, e-dienstverlening naar klanten (wel gemakkelijk om via internet te doen, maar hoe veilig is het).

Voorbeelden van fysieke maatregelen: fysieke toegang, oude UWV voor fusie met CWI: closed shop (niemand kwam het pand binnen, tenzij je een afspraak had), nu fusie met CWI: WERKpleinen met gemeentes: open shop. Hier liggen nog verdere uitdagingen en moeten bepaalde zaken nog beter afgestemd worden op beleidsniveau. Een verandering van een werkproces kan inhouden dat een beveiligingsbeleid moet worden aangepast. Verder is er speciale aandacht voor het afschermen van medische dossiers; waar leg je die? Hoe bewaak je het archief en het scheiden van medische en claimgegevens?

Conclusie:
UWV beschikt over veel privacygevoelige gegevens en heeft de verantwoordelijkheid om deze te beschermen. Privacybescherming heeft in hoge mate te maken met informatiebeveiliging. De Code van Informatiebeveiliging, de Richtlijnen en de A&V23 zijn belangrijke input voor normen en richtlijnen, maar Judith benadrukt dat het 't belangrijkst is, om te denken in risico's. Wat gebeurt er als bepaalde gegevens op straat komen te liggen? Het voorbeeld van het Telegraafgebouw waarvan men vanaf de UWV-torens op uitkijkt, wordt indien nodig veelvuldig aangehaald voor verdere bewustwording, omdat UWV bij fouten al gauw de voorpagina haalt. Op deze manier kan je het belang van een goede bescherming van persoonsgegevens duidelijk maken aan het management.

Judith Unk en Frans van Oostrum hebben hun bijdrage aan deze masterclass op persoonlijke titel geleverd.

Afsluiting en Borrel
Uit de betrokkenheid van de zaal, blijkt dat privacy in de huidige maatschappij en de stroom van technologische ontwikkelingen en dienstverlening iets is wat een ieder aangaat en bij een ieder meer dan ooit leeft. Eén van de zaken die maar weer eens naar voren komt, is dat ondanks de vele technische uitdagingen waar eigenlijk iedere organisatie mee te maken heeft, privacy en dus ook (informatie-)beveiliging van (persoons-)gegevens toch ook nog van een behoorlijke menselijke aard is.
De middag eindigde met een borrel op het binnenplein van het Ministerie van Financiën, waar het zonlicht dat door het imposante raamwerk naar binnenviel en het zeer geïnteresseerde publiek, een leerzame Kijk op Privacy heeft opgeleverd.

Paspoortwet brengt burgers in gevaar

Auteur: J.M.T. Wijnberg > J.M.T. Wijnberg is voorzitter van de vereniging Vrijbit; zij is bereikbaar via bestuur@vrijbit.nl

De huidige Paspoortwet werd op 9 juni 2009 goedgekeurd door de Eerste Kamer. Invoering werd op 28 juni 2009 van kracht voor diplomatieke en dienstpaspoorten en vanaf 21 september dat jaar voor iedere burger die een nieuw paspoort of ID-kaart aanvraagt.

Aaron Boudewijn, de student die landelijke bekendheid verwierf als eerste weigeraar van vingerafdrukken die beroep aantekende bij de bestuursrechter om de paspoortwet buiten werking te laten stellen, was gevraagd in deze special over Privacy te schrijven. Vrijbit werkte nauw met hem samen en probeert bij deze zijn toezegging postuum gestand te doen.

DE LEEGTE ZONDER JOU IS MET
GEEN PEN TE BESCHRIJVEN
DE LEEGTE ZONDER JOU ZAL ALTIJD
BIJ ONS BLIJVEN
MAAR VEEL FIJNE HERINNERINGEN
VERZACHTEN ONZE SMART
VOORGOED UIT ONS MIDDEN
MAAR VOOR ALTIJD IN ONS HART

Totaal onverwacht is onze liefste Aaron van ons weggenomen.
Lieve Aaron, we zijn je dankbaar voor alle Liefde die je ons hebt gegeven.

AARON SJORS BOUDEWIJN
Tiel, 6 juli 1985 – Utrecht, 24 april 2010

Je blijft in onze herinnering als een grote lieverd, steun en toeverlaat, vrije denker en strijder voor rechtvaardigheid.

Je ouders Anton Boudewijn en Margreet Post,
al je broers en zussen, schoonzus en zwagers,
je neefjes en nichtjes,
opa en oma
en de anderen die veel van je houden.

Aaron ligt opgebaard in zijn ouderlijk huis:
Hellouwlaan 9, 4006 XH Tiel.

Op woensdagavond 28 april is er van 18u30 tot 20u30 de mogelijkheid om hier van Aaron afscheid te nemen.

We zullen Aaron herdenken op donderdag 29 april om 10u30 in de aula op de Algemene Begraafplaats aan de Papesteeg in Tiel, waarna Aaron begraven wordt.

Na de begrafenis is er gelegenheid om nog even samen te komen in het Rouwcentrum van De Haan, Molenstraatje 36, 4001 CB Tiel.

Correspondentieadres:
Hellouwlaan 9, 4006 XH Tiel.

In memoriam Aaron Boudewijn

Bij de voorbereidingen voor deze Privacy Special kwamen Aart Jochem en Lex Dunn via André Koot in contact met Aaron Boudewijn. Vlak daarvoor had Aaron de landelijke pers gehaald met zijn bezwaren tegen de opslag van biometrische kenmerken, die worden afgenomen tijdens het aanvraagproces voor een paspoort of identiteitskaart. Aaron toonde zich desgevraagd bereid om een artikel over dit onderwerp te schrijven voor deze Privacy Special. Helaas bereikte ons eind april het tragische bericht dat Aaron onverwacht was overleden. Wij wensen zijn familie veel sterkte met het verwerken van dit verlies.

Het principiële bezwaar tegen de Paspoortwet is dat deze een onrechtmatige inbreuk maakt op de bescherming van de persoonlijke vrijheid. De Europese verordening (EG nr. 2252/2004) die aan de Paspoortwet ten grondslag ligt, verplicht tot de opname van biometrische gegevens in de documenten zelf. Het beoogt uitsluitend, om als het wettelijk verplicht is een paspoort/ID-kaart te tonen, a) de authenticiteit van het document en b) de identiteit van de houder door middel van direct beschikbare vergelijkbare kenmerken met die uit het document, te kunnen controleren. De Nederlandse regering gaat veel verder met het registreren van deze biometrische kenmerken, door ze ook op te slaan in een decentraal overheidregister en in de toekomst in één nationaal centraal 24/7 on-line reisdocumenten/opsporingsregister. Dit maakt zo'n onnodig grote inbreuk op de bescherming van de persoonlijke levenssfeer dat dit strijdig is met de Grondwet, de Wet Bescherming Persoonsgegevens, het EVRM, het Internationaal verdrag inzake burgerrechten en politieke rechten Bupo[1] en uitspraken van het Europese Hof voor de Rechten van de Mens.

Hoe zit het met de veiligheid?
Officieel zou de Paspoortwet ertoe moeten leiden dat de veiligheid van de samenleving wordt vergroot door look-a-like fraude met paspoorten/ID-kaarten tegen te gaan. Of de veiligheid nu echt bevorderd wordt met het tegengaan van een vorm van fraude die hooguit enkele tientallen keren per jaar voorkwam valt te betwijfelen. Maar er is alle reden om aan te nemen dat de wet potentieel iedere burger individueel, en de samenleving als geheel actief in gevaar brengt.

Omdat lichaamskenmerken als vingerafdrukken en gezichtscan een onlosmakelijk deel van iemands identiteit uitmaken is het verdedigbaar dat een persoon het onacceptabel acht dat enige overheid de mens zou kunnen dwingen om deze lichaamskenmerken af te geven. Het digitaal registreren van persoonsgebonden biometrische kenmerken houdt bovendien automatisch in dat er van mensen naast hun fysieke identiteit ook een virtuele identiteit ontstaat, met alle risico's die daaraan verbonden zijn. Vincent Icke verheldert dit door te stellen dat digitale bestanden ipso facto exact reproduceerbaar zijn en zich onttrekken aan alle maatschappelijke *checks and balances* die wij tot nu toe hebben uitgevonden.[2]
Wie echter in het huidige digitale tijdperk geen principieel bezwaar heeft zou minstens het zelfbeschikkingsrecht over zijn of haar gegevens dienen te hebben.[3] De kern van dat zelfbeschikkingsrecht ziet er als volgt uit: persoonsgegevens moeten alleen worden afgegeven en mogen alleen worden verwerkt voor een bepaald en gerechtvaardigd doel (doelbindingsbeginsel), het datasubject moet inzicht hebben in (en heeft daarom een inzagerecht) welke gegevens er over hem zijn opgeslagen en verwerkt (transparantiebeginsel), er mogen niet meer gegevens worden bewerkt en bewaard dan voor het gerechtvaardigde doel nodig is (proportionaliteitsbeginsel), en de kwaliteit en juistheid van de gegevens moeten zijn gewaarborgd en kunnen door het datasubject worden afgedwongen (kwaliteitsbeginsel). Het zelfbeschikkingsrecht werd in 1983 in artikel 10 van onze Grondwet opgenomen. Ook begon het Europese Hof voor de Rechten van de Mens (EVRM) in de jaren tachtig artikel 8 EVRM uit te leggen als een recht op zelfbeschikking over je persoonsgegevens.

Lichamelijke integriteit en recht van informationele zelfbeschikking

Biometrische identificatie
Allereerst is er het probleem dat biometrische identificatiemethodes minder betrouwbaar zijn dan de overheid graag wil doen voorkomen. Staatssecretaris Bijleveld, verantwoordelijk voor de invoering van de nieuwe Paspoortwet, mag nog zo stellig keer op keer beweren dat de biometrische paspoorten echt veel veiliger zijn dan de oude, feit blijft dat het om een methode gaat die gebaseerd is op kansberekeningen en dus automatisch leidt tot een aantal onterechte herkenningen en onterechte afwijzingen. Naast deze inherente kans op foute koppelingen tussen personen en documenten of gegevens kan biometrie geen uitspraak doen over juistheid van deze documenten en gegevens, noch over de juistheid van de koppeling zelf. Daarom kan biometrie – in tegenstelling tot wat veel mensen denken – geen uitsluitsel geven over wie iemand is, alleen over de waarschijnlijkheid dat iemand de persoon is die hoort bij het eerder vastgelegde biometrische gegeven.[4]
De wetenschap gaat uit van zo'n 3 à 5 procent foutmarge voor vingerafdrukidentificatie. Daar begint de ellende voor mensen waarvan bij identificatie geen 1 op 1 match kan worden geconstateerd en zij zich tegenover een onfeilbaar gewaard systeem moeten verdedigen dat zij wel degelijk de persoon zijn die zij voorgeven te zijn. Door de verschuiving die plaatsvindt in ons rechtssysteem van 'onschuldig totdat het tegendeel is bewezen' naar de omgekeerde bewijslast, komen mensen dan, wanneer ze ten onrechte als verdachte worden aangemerkt, in grote problemen.
Problemen die ze zelf maar moeten zien op te lossen, want van hulp van de overheid is er op dit vlak weinig te verwachten.[5]

Gechipte biometrische paspoorten/ ID-kaarten
Alle persoonsgegevens van de paspoorten/ ID-kaarten worden vastgelegd in een contactloze RFID-chip. Hoewel de gegevens versleuteld zijn is dit een kwetsbaar systeem qua veiligheid omdat het onbevoegden de mogelijkheid geeft om via uitleesapparaten de gegevens te kunnen kopiëren, klonen en na ontsleuteling van de encryptie deze gegevens rechtstreeks te kunnen gebruiken om mensen te benadelen. Jeroen van Beek bewees in augustus 2008 al hoe de nieuwe 'onvervalsbare' paspoorten met microchip binnen een paar minuten gekopieerd en aangepast konden worden.[6]

BSN en biometrische kenmerken

Het vergt weinig fantasie te bedenken hoe men gedupeerd kan raken als anderen zich voor jou persoon gaan uitgeven. In februari 2010 bleek dat de Mossad voor het plegen van een aanslag gebruik had gemaakt van valse Britse paspoorten. De gevaren dat dit ook met Nederlandse documenten kan gebeuren is evident, maar ook wie 'slechts' slachtoffer wordt omdat er op zijn naam bezittingen worden ge- of verkocht kan gigantisch in de problemen

raken. Door financieel geruïneerd te worden, in de schulden te raken of een onterechte vermelding te krijgen bij het Bureau Krediet Registratie te Tiel waardoor men bijvoorbeeld geen lening voor een grote aankoop of hypotheek meer kan afsluiten.

Overheidsregister

Alle persoonsgegevens van de paspoorten/ID-kaarten worden momenteel bij elkaar opgeslagen in een decentrale digitale reisdocumentenadministratie. Het gaat om naam, paspoortnummer, nationaliteit, geboortedatum, geslacht, einde datum geldigheid paspoort/ID-kaart, Burger Service Nummer, gezichtsscan en vingerafdrukken.

Computerdeskundigen en experts in de bescherming van persoonsgegevens zijn het er al jaren unaniem over eens, dat het opslaan van al deze gegevens bij elkaar het slechtste is wat je kunt doen. Als onbevoegden, van binnen uit of buitenaf zich toegang verschaffen tot deze gegevens hebben ze in feite het complete datapakket wat synoniem is voor de burger te pakken. Gegevens die het mogelijk maken om via gezichtherkennende camerasystemen te detecteren waar mensen zich bevinden en door koppeling aan alle mogelijke bestanden te gebruiken zijn voor het classificeren van mensen aan de hand van profielen tot en met het real-time volgen of overnemen van iemands identiteit. Als men, zoals de Paspoortwet uitdrukkelijk beoogt al deze gegevens ook nog eens centraal zou gaan opslaan kan dit tot een nationale ramp leiden.

Hierbij dient altijd in het oog te worden gehouden dat schade van slachtoffers door fouten of fraude met biometrische gegevens als onherstelbaar moet worden gekenmerkt.

Bevoegd gezag

De afgifte en opslag van de paspoort/ID-kaart gegevens valt momenteel onder de verantwoordelijkheid van de burgemeesters. Dat leden van Vrijbit gebleken is dat lang niet iedere burgemeester zich hiervan in kennis had gesteld, veel gemeenteraadsleden hierover onwetend waren, en er totaal geen extra maatregelen genomen werden om de gemeentelijke administratie extra te beveiligen stemt somber. Dat minister Hirsch Ballin op 24 maart 2010 aan de Tweede Kamer schreef dat de gegevens in de database 'volkomen veilig' zijn[7] is eerder zorgwekkend dan geruststellend. Waar de staatssecretaris, desgevraagd nog volmondig toegaf aan de Eerste Kamerleden en de pers dat de database nooit honderd procent te beveiligen is, blijkt de minister die nu verantwoordelijk is dit niet te onderkennen.

Justitiële toepassing

Gegevens uit de huidige reisdocumentenadministratie mogen gebruikt worden door inlichtingen- en veiligheidsdiensten en kunnen worden opgevraagd door politie en justitie.Het gebruik van bevoegde instanties kan ook grote gevaren opleveren voor de burger. Als men bijvoorbeeld nagaat hoe eenvoudig vingerafdrukken nagemaakt kunnen worden is het doemscenario duidelijk dat iedereen het risico loopt om als verdachte te worden aangemerkt wanneer ergens zijn vingerafdrukken worden aangetroffen op een plaats waar een misdrijf heeft plaatsgevonden. Als dit misdrijf in verband wordt gebracht met mogelijk terrorisme is men zijn leven helemaal niet meer zeker en kan het maar zo gebeuren dat een onschuldige burger wordt uitgeleverd aan de VS, alwaar men daar vanuit een cel maar moet zien te bewijzen onschuldig te zijn. Waar inlichtingen- en veiligheidsdiensten gegevens voor gebruiken en met wie zij de gegevens delen onttrekt zich aan iedere controle. Dat foute registratie of verkeerde interpretatie door deze instanties iemand in grote pro-

Wat is Vrijbit?

De vereniging Vrijbit stelt zich ten doel zich grensoverschrijdend in te zetten voor het recht op privacy, vrije communicatie en toegang tot informatie.

Vrijbit is een onafhankelijke organisatie en bestaat louter uit vrijwilligers. Vrijbit steunt mensen die zich tegen de afbraak van privacy verweren en actie ondernemen om de controledrift een halt toe te roepen. Elke eerste zondag van de maand vanaf 14:00 uur organiseren we daarom in Utrecht werkvergaderingen voor leden en aangemelde belangstellenden. Verder organiseert Vrijbit film- en debatavonden, verzamelt nieuws en informatie en houdt lezingen. Vrijbit voert actie en staat initiatieven van derden bij met raad en daad.

Hoe is Vrijbit ontstaan?

Vrijbit is ontstaan uit de oproep tot een volksopstand als protest tegen de toenmalige plannen van de regering om de vingerafdrukken van iedere burger vanaf zes jaar te registreren en op te slaan in één centrale database.

Op 24 juni 2008 werd de vereniging Vrijbit opgericht met de gedachte het niet bij een eenmalig protest te laten. Sindsdien groeit het ledental gestaag en neemt de bewustwording van de burger inzake privacyverloedering in ras tempo toe.

blemen kan brengen is duidelijk.
Al met al wordt door de Paspoortwet een infrastructuur ingericht die zeer geschikt is voor het organiseren van een politiestaat.

Foute registratie
De foutmarge van opslag en verwerking van vingerafdrukken in de documenten wordt door Bart Jacobs van de Radbout universiteit te Nijmegen op statistisch minstens een procent geschat.[8] Omgerekend gaat dat om 150 gevallen per dag. De staatssecretaris heeft opdracht gegeven om bij uitgifte van de reisdocumenten niet de juistheid van de gegevens te verifiëren.

Honderdduizenden mensen bleken geen goed leesbare vingerafdruk te kunnen geven. Deze afdrukken worden dan door het aanvraag station RAAS als ongeschikt bestempeld. Deze ongeschikte vingerafdrukken worden zowel opgenomen in de reisdocumentenadministratie als verwerkt in de reisdocumenten.
Wie met verkeerde vingerafdrukken in een paspoort of ID-kaart wordt aangetroffen bij de grens, loopt echter volgens de staatssecretaris geen enkel gevaar, omdat in artikel 4, derde lid, van de Europese Verordening is bepaald dat een negatief resultaat van de vergelijking van vingerafdrukken op zichzelf geen afbreuk doet aan de geldigheid van het paspoort of reisdocument voor overschrijding van de buitengrenzen.[9]

Situatie bezwaarden
Heel veel burgers zijn zich nog steeds niet bewust van de bezwaren en gevaren van de Paspoortwet, denken dat dit niet ook de ID-kaarten betreft of betrekken de consequenties pas op zichzelf als men een nieuw identiteitsdocument moet gaan aanvragen.

Mensen die tijdig op de hoogte waren hebben vlak voor de invoering van de biometrisch-gechipte paspoorten/ID-bewijzen nog een ongechipt exemplaar aangevraagd. Deze personen komen pas medio volgend jaar voor de keus te staan om al dan niet de afgifte van biometrische gegevens te weigeren. Veel mensen kwamen pas later tot de ontdekking wat biometrische opslag door de overheid betekent en hebben daarom vlak voor 21 september 2009 nog gauw een paspoort/ID-kaart aangevraagd om in elk geval geen vingerafdrukken te moeten afgeven.

Het merendeel van de burgers voelde zich echter gedwongen om hun biometrische gegevens af te geven omdat men anders niet meer normaal kan functioneren in de samenleving. De verstrekking van de zogenaamde 'reisdocumenten' betreft immers feitelijk de verstrekking van nationale

identiteitsdocumenten, waar iedere burger vanaf 14 jaar over dient te kunnen beschikken. Zonder geldig paspoort/ID-kaart kan men immers niet functioneren in veel sectoren van de maatschappij, worden mensen essentiële levensbehoeften ontnomen.

Zij die niet over een geldig ID-bewijs beschikken en principieel weigeren om hun vingerafdrukken af te staan aan de overheid leven onder mensonterende toestanden. Men kan onder andere geen arbeidscontract meer afsluiten, geen uitkering of studiefinanciering aanvragen, zich niet inschrijven bij de Kamer van Koophandel, geen notariële acte laten opmaken, geen rijbewijs halen, geen kind aangeven, zich niet beschikbaar stellen bij verkiezingen, is uitgesloten van reguliere ziekenzorg en loopt dagelijks het risico om door opsporingsambtenaren als verdachte beboet, gearresteerd of geregistreerd te worden.[10]

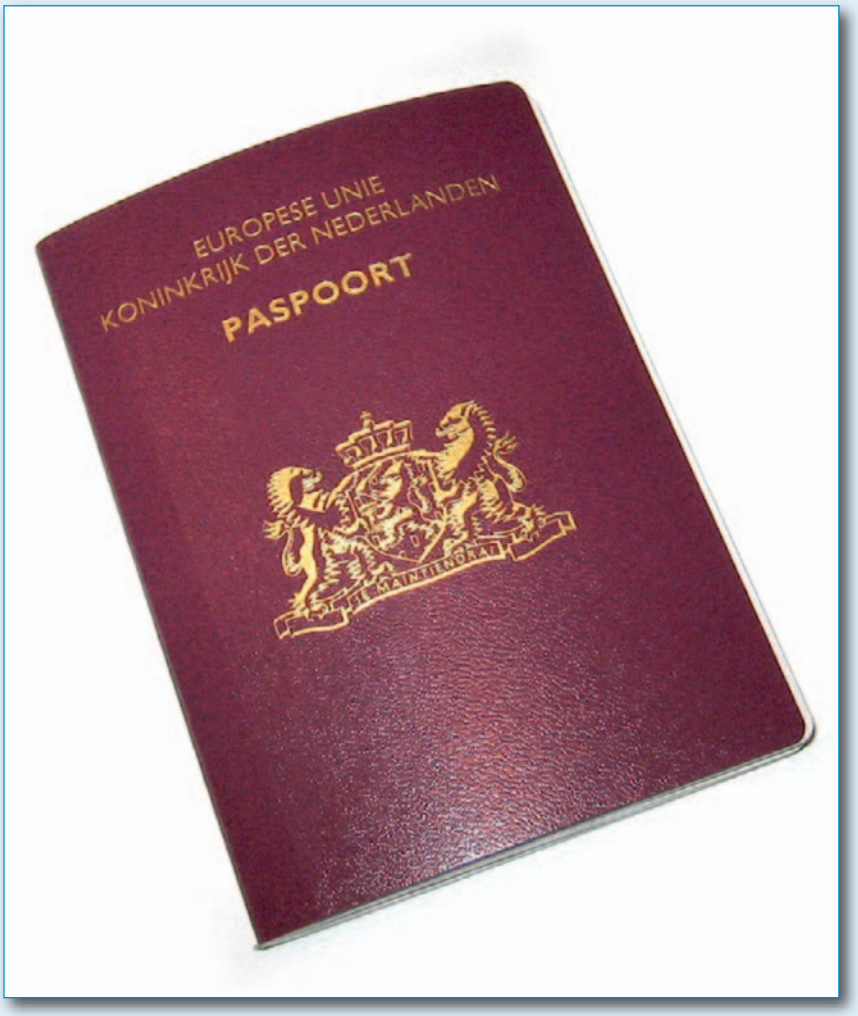
Verzet tegen de paspoortwet
De Nederlandse regering heeft het nagenoeg onmogelijk gemaakt voor mensen om bezwaar te maken tegen de vingerafdrukopname en er is niet voorzien in een alternatief voor bezwaarden.

Dat was samen met het feit dat een nationale rechtsgang alleen al qua tijd, geen uitzicht geeft op een effectieve oplossing, terwijl wel onherstelbare schade kan worden aangericht bij mensen die hun gegevens afstaan, de reden voor Vrijbit om op 2 augustus 2009 bij het Europese Hof voor de Rechten van de Mens (EHRM) een rechtzaak hierover aan te spannen tegen de Staat der Nederlanden. We vroegen het EHRM de nationale Paspoortwet buiten werking te laten stellen omdat deze indruist tegen het EVRM.[11] Deze zaak loopt nog, en intussen zijn er, ondanks het feit dat nationale processen jaren zullen gaan duren en naar verwachting alsnog ook zullen belanden bij het EHRM, door bezwaarden zowel bestuursrechtelijk als civielrechterlijke processen opgestart.
Ook zijn er mensen die na het afgeven van hun vingerafdrukken een zaak aanspannen om de opslag hiervan uit de overheidsdatabase te doen verwijderen.
Er zijn voorts mensen die zorgen fysiek

niet in staat te zijn om hun vingerafdrukken te kunnen laten afnemen. Er zijn mensen die gaan emigreren en mensen die als vogelvrij proberen zo goed mogelijk te overleven zonder identiteitsdocumenten. Velen behelpen zich met een rijbewijs, maar kunnen daardoor niet meer naar het buitenland reizen.

Op 10 maart schreef Vrijbit een brief aan alle burgemeesters van ons land met het verzoek zelf processen aan te spannen tegen de verplichting van de Staat om de Paspoortwet te moeten toepassen 'zoals die luidt' terwijl men als bevoegd gezag op grond van de Algemene wet bestuursrecht deze wetgeving dient te toetsen op strijdigheid met de hogere wetgeving van het EVRM, als inwoners zich bij hun bezwaar hierop beroepen.[12]

Heel voorzichtig begint ook in politiek Den Haag een kentering zichtbaar te worden. Zo versoepelde de staatsecretaris van Binnenlandse Zaken bijvoorbeeld recentelijk de nieuwe identificatie-eisen uit de Kieswet, door 5 jaar verlopen identiteitsbewijzen ook als geldig aan te merken. Het onderzoek van de Wetenschappelijke Raad voor het Regeringsbeleid(WRR), naar sleutelmomenten en sleutelfiguren in de ontwikkeling van de Paspoortwetgeving, duidt er wellicht op dat de overheid er inmiddels ernstig rekening mee houdt zich in rechte of via de volgende Paspoort-enquête te moeten verantwoorden voor de onrechtmatige overheidsdaad die men



pleegde met het invoeren van de Paspoortwet.

Hopelijk komt er onder een nieuw kabinet een politieke oplossing voor de kwestie zodat het intrekken van de Paspoortwet niet via uitputtende rechtzaken bevochten moeten worden of geforceerd tot stand komt als bijvoorbeeld blijkt dat de biometrische data van de bevolking via de gemeentelijke reisdocumentenadministraties in handen zijn gekomen van criminele organisaties.

1 Internationaal verdrag inzake burgerrechten en politieke rechten Bupo
2 Vincent Icke- Gullivers Web HTML-versie
3 Prof. mr. E. J. Dommering, hoogleraar informatierecht aan de Universiteit van Amsterdam (IViR) en advocaat te Amsterdam (Brinkhof) 'Privacy als het zelfbeschikkingsrecht van de 21e eeuw ' Mediaforum 2009
4 Position paper V16 NL van het Nederlands Biometrie Forum www.biometrieforum.nl/tiki-index.php?page=position_paper
5 De portal van het Centraal Meldpunt Misbruik ID-fraude is per 1 maart 2010 ondergebracht bij Postbus 51
6 Elektronisch paspoort onveilig door slechte lezers - Brenno de Winter webwereld.nl/article/view/id/52186
7 www.bzk.nl/actueel/kamerstukken/@126023/antwoorden-op_16
8 www.radio1.nl/contents/14071-sp-controleer-vingerafdruk-in-paspoort?autostart=17240
9 7-4-2010 Beantwoording Kamervragen kenmerk 2010Z05459
10 Sinds 1-1-2005 kan het iedere onschuldige burger overkomen om, bijvoorbeeld als getuige van een ongeluk, op grond van de Wet op de Uitgebreide ID-plicht (WU-ID) een geldig identiteitsbewijs te moeten tonen. Wie niet onmiddellijk aan de vordering dit te tonen voldoet is, ondanks dat de wet geen draagplicht kent, strafbaar en kan derhalve afhankelijk van het inzicht van de betrokken opsporingsambtenaar beboet of gearresteerd worden.
Bij inwerking treden van de wet 'identiteitsvaststelling verdachten, veroordeelden en getuigen, kan het zelfs iedereen in voorvermeld geval overkomen dat er ter plekke vingerafdrukken en gezichtsscan worden afgenomen en rechtstreeks voorzien van een Strafketendossiernummer in justitieregisters worden opgenomen.
11 EHRM Vrijbit vs Staat Nl no 45692/09
12 10-5-010 brief Vrijbit aan alle burgemeesters zie www.vrijbit.nl

Laagste privacybewustzijn van Europa

‘Nederland is niet immuun voor autoritaire tendensen’

Auteur: Ella Broos > Ella Broos is communicatiemanager en gespecialiseerd in crisishantering, woordvoering en ICT-onderwerpen.

Ze ontving in februari van dit jaar de tegenhanger van de Big Brother Award: de Winston Award, een positieve privacyprijs. Ze zegt daarover: “Het is vooral mooi dat je door zo’n prijs weer een platform hebt om je boodschap uit te dragen. En dat was ook wel weer tijd. De privacybeweging is een tijd stil geweest. Dat is niet goed. In heel Europa is het besef over de risico’s van privacyschendingen in Nederland het laagst.” Aan het woord is Sophie in ‘t Veld, fractievoorzitter voor D66 in het Europees Parlement.

Sophie In 't Veld

Op 5 februari werden de grootste privacyschenders van de afgelopen jaren bekendgemaakt, althans, volgens de organisator van de Big Brother Awards, Bits of Freedom. Minister Ter Horst viel in de prijzen met als argumentatie ‘Mede door haar toedoen stevent Nederland in sneltreinvaart af op een controlemaatschappij, waar veiligheid altijd boven persoonlijke vrijheid gaat’. Maar het goede nieuws was dat er een positieve aanmoedigingsprijs voor Sophie in ‘t Veld werd uitgereikt, vanwege haar aanhoudende waarschuwingen aan het adres van burgers, bedrijven en overheden dat we zienderogen aan privacy inboeten. In ‘t Veld: “In Nederland leeft het beeld ‘wat maakt het uit dat anderen dingen over ons weten’. Maar dat is niet de kern waar het privacydebat om draait. Het gaat feitelijk om de vraag: Wie heeft toegang tot de informatie die we -vrijwillig of niet- overal achterlaten en wat gebeurt er vervolgens mee?”

Boeven vangen

In ‘t Veld somt op wat er allemaal van de gemiddelde Nederlander wordt vastgelegd: “Telefoongesprekken, sms-verkeer, kentekens, reisroutes, e-mailverkeer, sitebezoek, financiële transacties. En dan weten we sinds kort ook nog de dat Nederlandse overheid wereldkampioen afluisteren is. Een bijkomend probleem is dat niet al deze gegevens van de overheid zelf komen. Ze gebruikt ook gegevens van derden: van telecombedrijven, banken, creditcardmaatschappijen en zoekmachines. Enorm rijke databestanden, waarmee je complete profielen kunt aanmaken die je rechtstreeks aan personen kunt linken.” Wanneer al die informatie effectief wordt ingezet om boeven te vangen, is dat prima, vindt ze. “Maar daar gaat het mis. Het opslaan van al die gegevens van miljoenen mensen schept veel schijnveiligheid. Het is een fictie dat je met een simpele druk op de Enter-knop boeven en terroristen kunt vinden in een databestand. Het is een vergaarbak van informatie, waar op de verkeerde manier mee wordt omgegaan. Datamining en -profiling wordt het genoemd en het wordt in Amerika veelvuldig toegepast. Opsporingsdiensten stellen een profiel op op basis van deze gegevens en mocht je daar als argeloze burger enigszins inpassen, dan ben je verdachte. En dan is het aan jou om aan te tonen dat daar geen grond voor is. Omgekeerde bewijslast dus en dat is verre van wenselijk.”

Obsessie

Die verzameldrift van gegevens en het verkeerd gebruik wordt allemaal weerlegd door overheidsdiensten met het argument dat dit nodig is om terroristische aanslagen te voorkomen. Maar, zegt In ‘t Veld: “Aanslagen zijn niet te voorkomen door deze maatregelen. We leven in een tijd van angst en wantrouwen en veiligheid is een obsessie geworden. Maar 100% veiligheid bestaat niet en het opslaan van de gegevens van iedere burger is al helemaal geen oplossing. Kijk maar naar de aanslag op de Koninklijke bus tijdens Koninginnedag 2009. Dit soort mensen haal je niet uit zo’n enorme gegevensbak. Maar wat je er wel mee doet is fouten maken. Verkeerde mensen beschuldigen, het mensen lastig maken, ze het reizen moeilijk maken. Want je moet niet denken dat die gegevens allemaal correct en keurig geordend zijn. In Amerika is er onder de regering Bush een onderzoek gedaan naar de profiellijsten die daar circuleren. Wat bleek? Het is een rommelig, amateuristisch geheel. En op basis daarvan worden onterechte arrestaties verricht en reisverboden opgelegd.”

Dictatuur

Veiligheid als argument om in persoonlijke levens rond te snuffelen, het stuit In ‘t Veld tegen de borst. “Vraag aan een willekeurige collega in het Europees Parlement die in een dictatuur heeft geleefd of een land veiliger wordt wanneer de regering toegang heeft tot alle persoonlijke

gegevens. Spanje, Portugal, het voormalige Oostblok; allen hebben ze een dictatoriaal verleden. Nee, natuurlijk wordt het daar niet veiliger van. Het wordt beangstigender wanneer de overheid alles van je weet, ook als je 'niets te verbergen' hebt. En dat is wat er hier, vooral in Nederland aan de hand is. We denken dat het allemaal wel meevalt. We denken dat we niet vatbaar zijn voor autoritaire tendensen. Daarom laten we toe dat de overheid steeds verder gaat. Maar we zijn er helemaal niet immuun voor. We moeten beseffen dat een dictatuur geen extern opgelegd ding is: een dictatuur wordt gemaakt door mensen. En daar moeten we voor waken."

Vrijheidsdrang

Naïef, noemt ze de Nederlanders. Omdat we veel laten gebeuren, daar waar een land als Duitsland enorm bezig is met het thema privacy. "In een onderzoek onlangs onder de Europese landen, de Eurobarometer, bleek dat het bewustzijn van privacythema's in Nederland dramatisch laag is. Voor politici is het geen aansprekend item en als burger wil je er niet aan denken. Duitsland is een voorloper op dit gebied. Mede door de nieuwe liberale minister van Justitie, die specifiek opkomt voor burgerrechten. De Britse bevolking en ook de Amerikanen zijn wars van overheidsbemoeienis en ook van dit soort massale gegevensopslag, en spreken hun regeringen erop aan. Het is daar echt een thema in de verkiezingen. Hetzelfde zie je in voormalige dictaturen. Daar is een groot besef van vrijheid en vrijheidsdrang. Men wil geen regering die iedere burger in beeld brengt."

En ook in haar 'thuishaven', het Europees Parlement is veel aandacht voor privacy, schetst ze. "Net als in de Eerste Kamer in Nederland. Het lijkt of daar, net als in het EP, met meer distantie naar dingen wordt gekeken, er is meer ruimte en tijd voor reflectie. Dan wordt een thema als dit goed uitgediept en wordt duidelijk hoe belangrijk het is." Overigens heeft ze nog een verwijt aan de nationale politiek: het fenomeen Policy Laundering. Dit is letterlijk het witwassen van wetgeving. "Als je iets op nationaal niveau niet voor elkaar krijgt, zoals in Nederland bijvoorbeeld het internationaal uitwisselen van passagiersgegevens of de vrijheid van douaniers om zonder aanleiding laptops van passagiers te doorzoeken, dan ga je een stapje hoger op. Je zoekt het op Europees of mondiaal niveau. Als het daar dan wel lukt zo'n regel er doorheen te krijgen, kun je in het Nederlands parlement zeggen: 'Kijk, het is een internationaal verdrag, dus dat moeten we hier in Nederland ook toepassen'. Zo heeft ook de Nederlandse regering het diverse malen gedaan."

Gegevens als betaalmiddel

In de Europese Commissie zijn er vier personen aanspreekbaar op digitale thema's: Eurocommissaris Kroes heeft de Digitale Agenda (het bevorderen van digitale ontwikkelingen), mevrouw Reding heeft als thema de bescherming van privacy en persoonsgegevens, Commissaris Malmström is verantwoordelijk voor veiligheid en politiesamenwerking, en de heer Almunia nam de portefeuille van Kroes over en gaat over Mededinging. Dit laatste is een thema waar Sophie in 't Veld zich momenteel sterk mee bezighoudt. "We willen een onderzoek naar de mededinging in de sector zoekmachines en online adverteerders. Als je ziet over hoeveel persoonsgegevens Google beschikt, dan zie je dat deze alleen al daardoor anderen uit de markt kan drukken. Als gebruiker heb je dan geen alternatief meer, en dat is heel slecht voor de markt. Je moet kunnen kiezen." Ze stoort zich aan het feit dat je bepaalde zaken alleen kunt aanschaffen door een wederdienst te leveren zoals het achterlaten van allerlei persoonlijke gegevens. "Internetdiensten zijn helemaal niet gratis", stelt ze. "Je betaalt er geen geld voor, maar wel informatie. Als ik via internet iets wil aanschaffen, een abonnement op een krantensite bijvoorbeeld, moet ik een enorme hoeveelheid gegevens achterlaten. Waarom? Ik wil gewoon de krant lezen. Onder druk van de gebruikers worden er kleine verbeteringen aangebracht. Zo is het mogelijk om bij bijvoorbeeld Yahoo en Google nu met opt-in aan te geven wat ze wel van je mogen volgen en wat niet. Dat is een vooruitgang. Je moet gewoon de keuze hebben. Wil je ergens met geld voor betalen of betaal je door je persoonlijke gegevens achter te laten. Dat schimmige moet eraf."

Een andere missie: mondiale wetgeving. "De technologische ontwikkelingen gaan door. Het heeft geen enkele zin om wetgeving voor een bepaald grondgebied te maken. We moeten mondiale afspraken maken over zaken als uitwisseling van passagiers- en bankgegevens. Maar de nationale regeringen hebben er afzonderlijk te grote belangen bij dat burgers weinig rechtsbescherming hebben tegenover hun overheid. Dat obstakel moeten we absoluut overwinnen."

Herstel van de zwakste schakel

Sociale Bewijskracht

Auteur: Jan de Boer MSIT > Jan de Boer MSIT is als managing consultant werkzaam bij Capgemini. Zijn Master Thesis betrof de psychologie in de informatiebeveiliging. Zijn vakgebied is de integrale (informatie)beveiliging. Social Engineering is zijn hobby. Hij is bereikbaar op jan.de.boer@capgemini.com.

Dit is het vierde artikel in een serie van acht waarin wordt ingegaan op de psychologische trucs die door Social Engineers worden gebruikt om slachtoffers te manipuleren. Waarom en hoe werken ze? Hoe zijn ze te herkennen en wat is de beste verdediging? In dit artikel komt het aspect Sociale Bewijskracht (eigen gedrag afleiden van dat van anderen) aan de orde.

Social Engineering; een korte terugblik

In de informatiebeveiliging wordt de mens steeds omschreven als de zwakste schakel. Mede door extreme resultaten van security audits in de vorm van Social Engineering (SE), zoals het in ontvangst mogen nemen van vijf handvuurwapens, ben ik er steeds meer van overtuigd geraakt dat de beveiliging niet zit in firewalls, hoge hekken, SafeWord tokens en andere technische beveiligingsmaatregelen, maar in de mens zelf.

Uit een onderzoek onder 250 CIO's en CISO's van bedrijven en overheden naar (informatie)beveiliging is gebleken dat zestig procent GEEN aandacht schenkt aan het beveiligingsbewustzijn van de medewerkers. Een opmerkelijk hoog percentage aangezien zestien procent aangeeft dat er informatie is gestolen met behulp van SE en zelfs drieëntwintig procent aangeeft de dreiging van diefstal door SE als serieus te ervaren.

Bewaart u de contantgeldvoorraad wel achter een goed slot?

Deze artikelserie over het hoe en waarom van menselijk gedrag en hoe daar misbruik van kan worden gemaakt door profiteurs, is bedoeld als bijdrage aan een reeds bestaand bewustwordingsprogramma van een organisatie. Maar het is ook als zelfstandig bewustwordingsprogramma prima inzetbaar voor een risicogroep zoals secretaresses of bewakingspersoneel. De artikelen behandelen de psychologische mechanismen die door SE's worden gebruikt om tegenstanders te manipuleren. Er wordt ingegaan op de achtergrond van de werking en er vindt een verduidelijking plaats aan de hand van voorbeelden uit de praktijk. Verder worden maatregelen aangedragen om een aanval te herkennen en af te slaan.

Sociale Bewijskracht

Dit principe betekent dat ons oordeel over correct of incorrect gedrag samenhangt met het gedrag van anderen. Wanneer veel mensen een handeling op gelijke wijze uitvoeren,

Sociale Bewijskracht: Eigen ervaring

Bij een grote dienstverlener op het gebied van ICT werden speed-gates gebruikt om te voorkomen dat er meegelift kon worden met vaste medewerkers. De speed-gates gaven vanaf de centrale hal (met bewakers en gastvrouwen) toegang tot de verschillende torens en afdelingen. Om naar binnen of naar buiten te kunnen moest de pas voor de lezer worden gehouden. Maar ik wilde juist naar binnen en wel zonder pas! Het was me gelukt om via de fietsenstalling het pand binnen te komen (meegelift) maar verder dan de (grote) centrale hal kwam ik in eerste instantie niet. Toen een wat oudere en uiterst correct geklede medewerker uit een van de torens kwam en de centrale hal binnenging via de speed-gates, sprak ik hem aan en vroeg of hij mij binnen wilde laten. Ik had mijn pas verloren en die lag vermoedelijk in de toren. Hij was verbaasd: hoe was ik dan uit de toren gekomen in de centrale hal? Ik vertelde hem dat een collega van 'ons' mij naar buiten had gelaten om afscheid te nemen van een bezoeker. Maar nu had ik zijn hulp nodig om weer verder te gaan met het zoeken naar mijn toegangspas. En die lag in de toren. Hij vroeg me nog of ik wel een collega van hem was en vol overtuiging zei ik "tuurlijk". Daarop liet hij me binnen op zijn pas.
Twee weken later had ik een afspraak met deze man, die de CEO bleek te zijn van deze grote dienstverlener, om uit te leggen wat mijn opdracht en de resultaten waren.

Door aan te geven dat iemand anders mij al geholpen had, werd de CEO ervan overtuigd dat zijn gedrag correct was. Omdat hij slechts een korte tijd had om een beslissing te nemen, stond zijn besluit vast voor hij het in de gaten had.

bestempelen we deze als correct. Wanneer mensen uit onze directe omgeving een handeling op een bepaalde wijze uitvoeren of een bepaald gedrag goed- of juist afkeuren,

Het begin van toegang tot alle locaties?

dan zijn wij geneigd om ons dit gedrag eigen te maken. Dit 'voorbeeldgedrag' zie je in het dagelijks leven vooral terugkeren; kinderen kopiëren het gedrag van hun ouder, medewerkers nemen de waarden en normen aan van het management (Als hij het niet hoeft, hoef ik het ook niet te doen!). Zowel goed als slecht voorbeeldgedrag wordt gekopieerd door de omgeving. Hierin ligt tegelijkertijd ook de zwakte van het principe: het maakt ons kwetsbaar voor profiteurs. Het principe van sociaal bewijs is namelijk erg sterk.

Wanneer we onzeker zijn over bepaalde handelingen, zijn we het snelst geneigd om naar anderen te kijken om zelf ons gedrag te bepalen. Wanneer echter niemand weet wat de juiste handelingen zijn, moet je je in dat geval tot slechts één iemand richten en deze persoon duidelijk maken dat je hulp nodig hebt om tot een beslissing te komen.

Hoe kunnen profiteurs hier nu misbruik van maken? Indien een profiteur iemand benadert met een nogal ongebruikelijk verzoek, kan hij aangegeven dat hij zojuist dat verzoek ook aan een andere collega of zijn chef heeft gedaan. De collega of de chef heeft zojuist óók met het verzoek ingestemd. Dan is er toch niets meer op tegen om zelf óók aan dat verzoek te voldoen? Toch?

We staan dagelijks bloot aan een groot aantal van dit soort manipulaties. Niet door SE's (alhoewel?) maar door reclamemakers die ons willen laten geloven dat ongestelde vrouwen vrolijk en blij zijn en dat stoere mannen hun borsthaar trimmen en vochtinbrengende crèmes gebruiken. Laat ú zich verleiden tot ander gedrag?

Het principe van sociale bewijskracht werkt onder twee omstandigheden optimaal:

1. onzekerheid: wanneer iemand zelf niet weet hoe hij zich moet gedragen, ontleent hij zijn gedrag aan dat van anderen (zoals hierboven omschreven);
2. gelijksoortigheid: het gedrag van mensen die op ons lijken maakt ons het beste duidelijk hoe we ons zouden moeten gedragen. Hier is sprake van eigen waarneming. Voorbeeldgedrag wordt door anderen overgenomen.

Soms is voorbeeldgedrag zo verankerd in een gemeenschap dat het zinloos is om een vraag te stellen die daar tegenin gaat. Hoewel het voorbeeld niet over SE gaat, spreekt het wel tot de verbeelding. Probeer niemand van Shell te bewegen om een trap af te lopen zonder de leuning vast te houden. Dat gaat je niet lukken!

Verdediging

We kunnen ons tegen het principe van sociale bewijskracht verdedigen door in te zien dat het gedrag van andere mensen niet ten grondslag mag liggen aan ons eigen gedrag.

Ongeautoriseerde toegang tot de serverruimte.

Bovendien moeten we goed oppassen voor vervalsing van de handelingen van andere mensen die op ons lijken. We moeten dus door de reclames heen prikken, waarin een 'gewone' man of vrouw heel tevreden is met een bepaald product en inzien dat we hier genept worden.

Samenvatting

We zijn geneigd om ons eigen gedrag af te leiden van dat van anderen. Laat je niet wijs maken dat het gedrag van anderen automatisch inhoudt dat jouw gedrag daarvan afgeleid moet worden en dus per definitie goed is. Pas op voor vervalsing van de handelingen van andere mensen die op ons lijken.

Sociale Bewijskracht: Eigen ervaring

Op maandagmorgen om 7.00 uur belde ik de enige aanwezige medewerker van een secretariaat van een medische organisatie. We hadden bij netwerkbeheer in het weekend een ernstige uitbraak van een virus gehad en alle mailboxen van haar afdeling waren besmet; het virus was geïsoleerd maar het zou zeker een dag duren voordat de afdeling weer kon werken. Als ze haar login-ID en wachtwoord zou verstrekken dan zou ik even snel kunnen scannen en zou ze door kunnen gaan met werken. Ze was kennelijk nog niet helemaal wakker en werd door het tijdstip van mijn verzoek overdonderd. Ze verstrekte me haar gegevens. Vijf minuten daarna belde ik terug, bedankte haar voor de medewerking en gaf aan dat ze gewoon zou kunnen werken. Haar mailbox was virusvrij. Als ze me ook aan de wachtwoorden van haar overige medewerkers zou kunnen helpen dan zou iedereen die dag gewoon kunnen werken, anders zou ik doorgaan naar de volgende afdeling en pas aan het einde van de dag weer in staat zijn om haar directe collega's te helpen. Toen ik zei dat op de helpdesk, net als bij alle andere afdelingen, er voor noodgevallen een enveloppe aanwezig is met alle wachtwoorden, gaf zij toe dat dit ook op haar secretariaat het geval was. Ze verstrekte alle veertien login-ID's en wachtwoorden, waaronder die van de directeur en het hoofd van het behandelteam.

Door aan te geven dat het bijhouden van wachtwoorden bij alle afdelingen gebeurde, was het slachtoffer er van overtuigd dat zij correct handelde.

Privacybescherming: het kan én moet beter!

Ronald Koorn > Drs. ing. Ronald F. Koorn RE is partner bij KPMG IT Advisory. Hij houdt zich bezig met vraagstukken op het gebied van informatiebeveiliging, ICT-infrastructuren, e-business (e-procurement/e-factureren) en privacy. Hij heeft voor het ministerie van BZK het Witboek Privacy Enhancing Technologies geschreven. Hij heeft een bijdrage geleverd aan de privacy-instrumenten van het CBP, aan het Privacy Framework van de AICPA/CICA en aan het TRUSTe-programma in de VS. Ronald Koorn is te bereiken via koorn.ronald@kpmg.nl

Privacy is voor veel organisaties een te moeilijk begrip. Dit blijkt uit onderzoek dat NPS-Nipo in samenwerking met KPMG heeft uitgevoerd. Het goed doorgronden van en voldoen aan de privacyvereisten uit de Wet bescherming persoonsgegevens (Wbp) is na tien jaar nog niet op orde. De meeste organisaties blijven steken bij policy, procedures en autorisaties. Hoe moet het dan wel? Dit artikel gaat in op de belangrijkste onderzoeksuitkomsten, dilemma's en doet aanbevelingen voor een betere aanpak van de privacybescherming. Waarom is privacybescherming een uitdaging?

Organisaties verwerken steeds meer en gevoeligere persoonsgegevens van klanten, relaties en medewerkers. Deze gegevens worden in toenemende mate gedeeld binnen de eigen organisatie en met andere organisaties en ICT-dienstverleners. Privacy is door deze technische, juridische en maatschappelijke ontwikkelingen zowel een compliancerisico als een onderscheidende reputatiefactor.

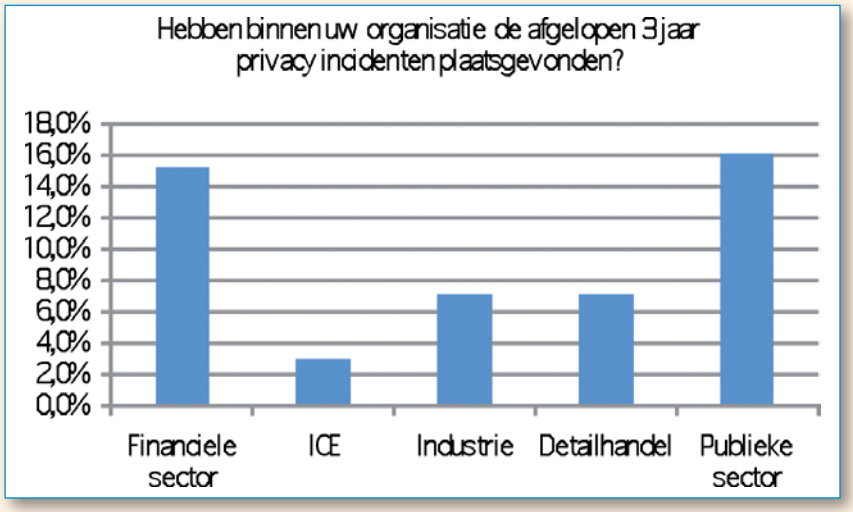


Fig. 1. Aantal respondenten dat aangeeft dat privacyincidenten hebben plaatsgevonden.

Bij privacy kan worden gedacht aan de bescherming van de persoonlijke levenssfeer, de bescherming van persoonsgegevens en de bescherming van vertrouwelijke communicatie. Privacy is onderwerp van maatschappelijke discussies en van (inter) nationale wet- en regelgeving. De discussies over het spanningsveld tussen privacy en andere belangen, zoals efficiënt gebruik van persoonsgegevens, uitbesteding/offshoring en fraude- en terrorismebestrijding, worden steeds heviger.
Daar komt bij dat het waarborgen van privacy door technologische ontwikkelingen met internet- en mobiele diensten, informatieketens, online sociale netwerken, biometrie, RFID, en dergelijke een complexer onderwerp is geworden. Anderzijds is een groeiend aantal maatregelen beschikbaar om privacy beter te kunnen beheersen, zoals e-authenticatie, gedifferentieerd identiteitsmanagement, privacyfunctionaliteit in database managementsystemen, enz.
Er lijkt een discrepantie te zijn tussen de aandacht die privacy krijgt in wet- en regelgeving en in de media enerzijds en de aandacht die privacy krijgt binnen organisaties. KPMG heeft daarom in samenwerking met TNS-NIPO een onderzoek gedaan onder meer dan 300 Nederlandse organisaties in private en publieke sectoren naar de begripsvorming rondom privacy. In hoeverre is privacy een belangrijk onderwerp voor deze organisaties en hoe gaan zij om met privacybescherming?

Belangrijkste uitkomsten

Uit het onderzoek komt naar voren dat er geen eenduidig beeld is van het begrip 'privacy' binnen organisaties en wat dit voor organisaties precies betekent. Begripsvorming ligt aan de basis van aandacht voor en strategie van privacy en de activiteiten die daaruit volgen. Zolang de organisatie zich niet bewust is van het volledige spectrum zal de waarborging van privacy ook niet sluitend zijn. Hierdoor lopen organisaties nog (te) aanzienlijke risico's.
Organisaties geven over het algemeen een volwassen indruk wanneer het om het treffen van maatregelen ter waarborging van de privacy gaat. De in het onderzoek genoemde maatregelen zijn bekend en worden toegepast. Kanttekening hierbij is dat maatregelen met name op operationeel niveau zijn aangebracht en bovendien sterk zijn gericht op wet- en regelgeving. Organisaties zijn dus met name compliancegericht. Zij richten zich minder op de 'bedrijfseconomische waarde' die privacy kan hebben (denk bijvoorbeeld aan de voordelen van het genereren van klantprofielen voor organisaties). Dit betekent dat

rganisaties de kansen, die het adequaat omgaan met persoonsgegevens kan hebben, nu waarschijnlijk nog grotendeels mislopen. Daarnaast is zowel de eindverantwoordelijkheid als de uitvoering van privacywaarborgende activiteiten nog sterk gefragmenteerd over verschillende afdelingen. Organisaties evalueren in beperkte mate in hoeverre zij privacywaarborgen hebben geïmplementeerd. Zelfevaluaties, interne of externe audits worden slechts zeer beperkt uitgevoerd. Zolang dit zo is, is het moeilijk te beoordelen of organisaties inderdaad voldoende maatregelen hebben getroffen en daarmee compliant zijn, zoals zij zelf aangeven.

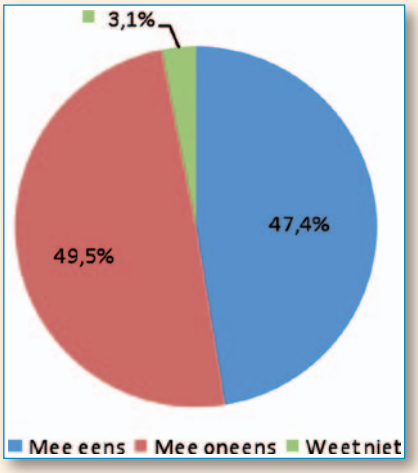


Fig. 2. Aantal respondenten dat aangeeft dat 'als we op een adequaat niveau maatregelen hebben getroffen voor informatiebeveiliging dan hebben we direct de privacybescherming geregeld'.

Hierna is een aantal uitkomsten van de privacysurvey opgenomen. De andere surveyresultaten staan vermeld in (fig.1).

Aantal privacyincidenten is hoog

Gemiddeld tien procent van de Nederlandse organisaties heeft in de afgelopen drie jaar privacyincidenten vastgesteld. In de financiële en publieke sectoren komen de meeste incidenten met verlies of openbaarmaking van persoonsgegevens voor. Aangezien security- en incidentmanagement veelal een verplicht proces is bij financiële en overheidsinstellingen, kunnen de hogere resultaten in deze sectoren ook zijn veroorzaakt doordat de meetinstrumenten binnen deze sector verder zijn ontwikkeld.

Privacybescherming = informatiebeveiliging?

Ongeveer de helft van de Nederlandse organisaties ziet privacybescherming als synoniem voor informatiebeveiliging. Hierdoor zijn de privacyrisico's binnen deze organisaties mogelijk onvoldoende in kaart gebracht en zijn dus mogelijk onvoldoende maatregelen getroffen om privacy te kunnen waarborgen.

Privacy gaat veeleer om een verantwoord gebruik van persoonsgegevens en niet louter om de afscherming ervan. Onderwerpen als privacybeleid, statements, verkrijgen van toestemming ('opt-in/out'), doelbinding, kwaliteit van persoonsgegevens, internationale gegevensuitwisseling en dergelijke, zijn specifiek voor privacybescherming en niet voor informatiebeveiliging. In een eerder artikel in het studieblad Informatiebeveiliging is dieper ingegaan op de overeenkomsten en verschillen tussen informatiebeveiliging en privacy (fig.2).

Wat belemmert privacybescherming?

Ook het toekennen van onvoldoende prioriteit aan privacy is een belangrijke belemmerende factor. Gebrek aan capaciteit en financiële middelen is hieraan gerelateerd. Over het algemeen geldt immers: hoe hoger de prioriteit binnen de organisatie, hoe meer mensen en middelen beschikbaar worden gesteld.

Onderbouwing privacycompliance

De meeste Nederlandse organisaties geven aan privacycompliant te zijn, maar evalueren de waarborging van privacy en bijbehorende getroffen maatregelen niet of nauwelijks.

Organisaties kunnen de kwaliteit van de door hun toegepaste privacywaarborgende maatregelen evalueren op basis van door het CBP ontwikkelde methodieken. Zo kunnen organisaties vaststellen in hoeverre zij compliant zijn aan wet- en regelgeving. Slechts een beperkt aantal organisaties voert een dergelijke evaluatie uit. 44% van de Nederlandse organisaties geeft aan geen van de genoemde evaluaties toe te passen, waarbij een kleine 17% aangeeft een privacyaudit te hebben uitgevoerd (intern dan wel extern). Ongeveer 85% van de Nederlandse organisaties geeft aan nu al privacycompliant te zijn of dit binnen een paar jaar te zijn. Deze conclusie lijkt te voorbarig aangezien evaluaties slechts beperkt worden uitgevoerd. De vraag is natuurlijk 'hoe meten of verifiëren deze organisaties in hoeverre zij compliant zijn?' Uit mijn praktijkervaring komt naar voren dat slechts een beperkt aantal van de organisaties in Nederland geheel compliant is met de Wet bescherming persoonsgegevens (minder dan 5%).

Belangrijke knelpunten betreffen:

- geen duidelijke privacyverantwoordelijkheden toegewezen;
- weinig tot geen inzicht of invloed van medewerkers of klanten in de over hen bewaarde persoonsgegevens;
- ICT-uitbesteding zonder stringente, contractuele privacyvereisten;
- monitoring van e-mail- en internetverkeer zonder goede informatie aan medewerkers of duidelijke procedure bij geconstateerde afwijkingen;
- geen veilige communicatie (bijvoorbeeld e-mails met attachments met persoonsgegevens);

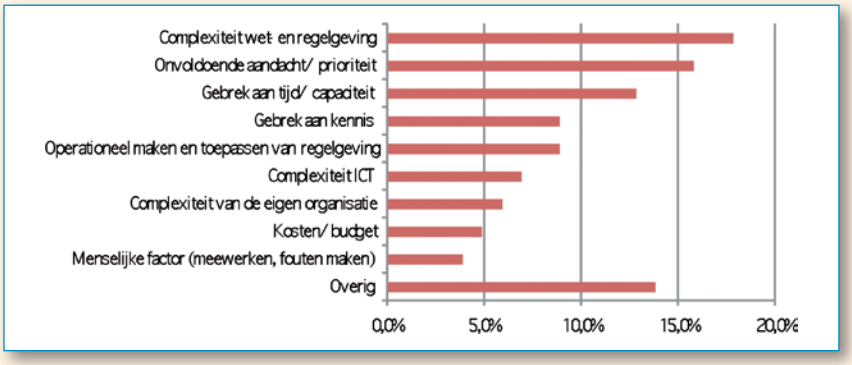


Fig. 3. Belemmeringen voor het toepassen van privacybeschermende maatregelen.

1 ICE: Information, Communication & Entertainment: omvat telecommunicatie-, media- en reissectoren.

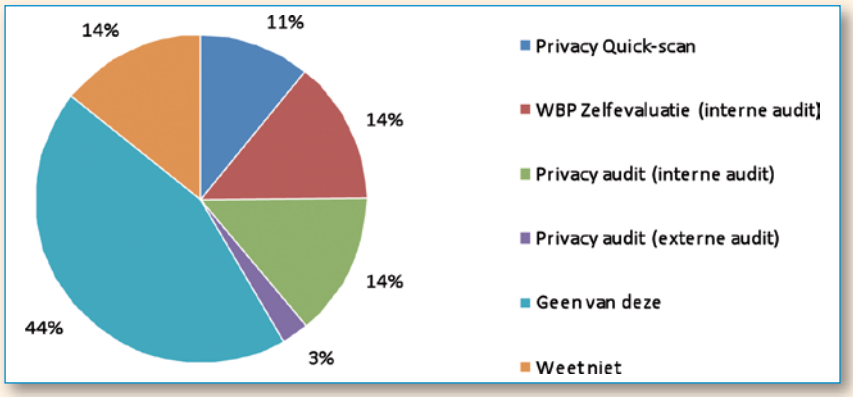


Fig. 4. Meetinstrumenten ten aanzien van privacycompliancy.

- testen met niet-geanonimiseerde persoonsgegevens;
- doorgifte van persoonsgegevens naar andere organisatieonderdelen of derde partijen buiten de EU;
- opslag van persoonsgegevens zonder afgedwongen bewaartermijn.

Verder zijn er slechts drie organisaties die (een gepubliceerd) privacycertificaat hebben.

Hoe moet het dan wel?

Voorgaande uitkomsten tonen aan dat er nog veel werk aan de winkel is. In deze paragraaf wordt ingegaan op een aantal maatregelen en een verbeterplan.
Er blijkt allereerst behoefte aan een helder begrip van wat privacy inhoudt en wat het betekent voor de eigen organisatie, dit is in feite een Privacy Impact Assessment.

- Wat verstaan we precies onder privacy en privacybescherming? Dit omvat ook de wijze waarop wordt omgegaan met de privégegevens van medewerkers in de werkomgeving, zoals door sociale netwerken, privémail, telefoon/PDA-gebruik, en dergelijke.
- Wat betekent dat voor de organisatie (risicoanalyse). Waar liggen de bedreigingen dan wel kansen (wat kan het de organisatie kosten en wat het kan het opleveren)?
- Hoe kan dat worden vertaald naar een concrete aanpak op strategisch, tactisch en operationeel niveau?

Belangrijk hierbij is dat alle activiteiten worden afgestemd op de specifieke organisatie. Het in beperkte mate toepassen van privacywaarborgende maatregelen hoeft niet per se slecht te zijn. De getroffen maatregelen dienen wél gebaseerd te zijn op een weloverwogen afweging van kosten en baten (economisch en sociaal-maatschappelijk). Hierbij dient uiteraard altijd de wet- en regelgeving betrokken te worden. Onvoldoende maatregelen treffen om de wet- en regelgeving na te leven is immers strafbaar. Daarnaast is het belangrijk te beseffen dat het managen van privacyrisico's, zoals alle risicomanagementprocessen, een continu en cyclisch proces is.

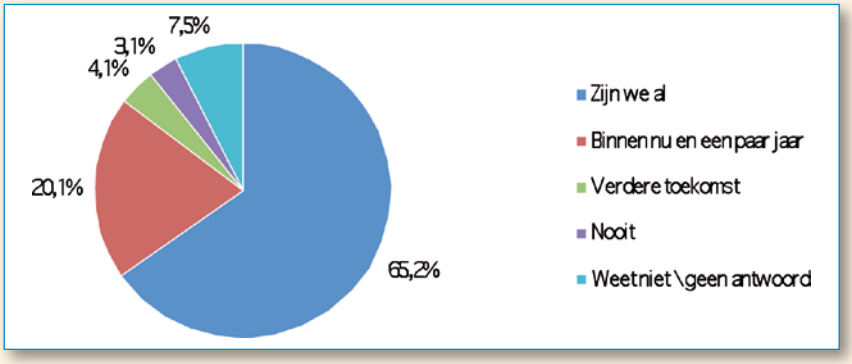


Fig. 5. Wanneer denken organisaties volledig te voldoen aan wet- en regelgeving?

Een effectief risicomanagementprogramma voor privacy voorziet in een mechanisme waarmee een organisatie privacyrisico's kan managen op een manier die consistent is met haar bedrijfsdoelen en -behoeftes, wettelijke verplichtingen en verwachtingen vanuit de markt. Een effectieve aanpak start met het erkennen dat privacy niet uitsluitend een technisch issue is, maar een strategisch issue dat tevens betrekking heeft op gegevens die niet elektronisch zijn vastgelegd.

Een programma van privacy risicomanagement vereist een collectief aan expertise van een variëteit aan afdelingen en specialisten (zoals van Juridische Zaken, ICT, lijnmanagement, Security, Marketing/Sales en Audit), inclusief professionals met ervaring met informatierisicomanagement en bedrijfsprocessen, alsook met privacywetgeving.
Het lijkt erop dat externe druk in de vorm van stringentere handhaving, hogere boetes en/of een publicitair privacy-incident, zoals grootschalige identiteitsdiefstal, nodig is om privacy op de directie-agenda te doen belanden. Dit is in landen als het Verenigd Koninkrijk, Duitsland en Verenigde Staten om deze redenen reeds gebeurd. Wanneer volgt Nederland? Alleen dan lijkt er voldoende steun voor het uitvoeren van een krachtig privacyprogramma.

Conclusie

Dit brede privacyonderzoek toont aan dat Nederlandse organisaties in private en publieke sectoren – ook na 20 jaar privacywetgeving en 10 jaar Wbp – aanzienlijk moeite hebben met de implementatie van privacymaatregelen en naleving van wetgeving. Toch zijn deze organisaties positief over de kwaliteit van hun privacybescherming. Dit baseren zij voornamelijk op het getroffen hebben van een aantal procedurele en technische maatregelen, vooral op operationeel niveau. Kaderscheppende maatregelen op strategisch en tactisch niveau ontbreken echter vaak.
Privacybescherming wordt nog erg benaderd vanuit complianceperspectief; de positieve bedrijfseconomische effecten worden nauwelijks erkend. Er vindt zelden evaluatie plaats of de getroffen maatregelen daadwerkelijk toereikend zijn. Desondanks denken veel organisaties nu al privacycompliant te zijn. Het valt te hopen dat in de toekomst organisaties deze optimistische claim kunnen onderbouwen met een privacy-audit en/of -certificaat.

Voorbeeld stappenplan

De volgende 12 stappen kunnen helpen bij het waarborgen van privacy binnen een organisatie. Zoals eerder opgemerkt, is het managen van de privacyrisico's een iteratief proces!

Stap 1: Verzeker sponsoring vanuit het topmanagement. Ook al is het een standaard aanbeveling, zonder deze steun blijft privacy veroordeeld tot een louter juridisch of ICT-project. Met toereikende ondersteuning kunnen voldoende middelen en continuïteit worden verzekerd. In veel gevallen betekent dit dat een interne senior jurist het management moet stimuleren. In andere gevallen is de aanwezigheid en het gebruik van een grote wijziging (zoals een systeemconsolidatie waarbij meerdere rechtsgebieden zijn betrokken) een stimulans voor privacy-investeringen.

Stap 2: Stel een projectmanager (geen jurist!) aan die het project coördineert. Voorzie dit project van voldoende middelen, inclusief personeel en tijd. Identificeer sleutelpersonen in de verschillende gebieden van de organisatie (HR, Marketing/Sales, Juridische Zaken, IT, Security, Audit) die participeren in het project.

Stap 3: Begrijp waarom de organisatie persoonlijke informatie verzamelt, gebruikt en /of verspreidt. Identificeer de informatiebehoeften en -eisen om de bedrijfsdoelstellingen te kunnen realiseren. Deze activiteiten moeten onderdeel zijn van de organisatiebrede informatiemanagementprocessen. Dit is een belangrijke, maar mogelijk ook de moeilijkste, stap richting beter Privacy Risk Management.

Stap 4: Inventariseer en analyseer de informatie die op dit moment in het bezit is. Komt de aanwezige informatie overeen met de actuele behoeften? Is er meer persoonlijke informatie aanwezig dan eigenlijk nodig is? Hebben klanten toestemming gegeven voor het verzamelen van deze specifieke gegevens?

Stap 5: Inventariseer en analyseer de methoden die worden gebruikt om persoonlijke informatie te verzamelen. Dit omvat een analyse van de website(s), applicaties, registraties, marketingacties, aanschaf van persoonsgegevens, enz.

Stap 6: Inventariseer in de wijze waarop de geregistreerde burger, klant of medewerker wordt geïnformeerd. Is de organisatie duidelijk en oprecht over waarom er bepaalde informatie wordt gevraagd? Is het doel waarmee de gegevens worden verzameld duidelijk uitgedrukt?

Stap 7: Na het analyseren van de aanwezige gegevens, de informatiestromen en de informatiemanagementprocessen, identificeer vervolgens de bijbehorende privacyrisico's.

Stap 8: Stel een privacy officer aan, of een organisatiebrede privacysponsor die genoeg autoriteit heeft om privacy-issues organisatiebreed aan te pakken.

Stap 9: Ontwikkel een organisatiebreed privacybeleid en vertaal dit in organisatorische, procedurele en technische maatregelen ('privacy control framework'). Zorg ervoor dat personeel en klanten zich bewust zijn van dit beleid en procedures en de implicaties hiervan begrijpen.

Stap 10: Train de medewerkers. Train zowel huidige als nieuwe medewerkers, vergeet daarbij de inhuur niet. Geef specifieke aandacht aan personeel dat in (direct) contact staat met klanten.

Stap 11: Waarborg dat persoonlijke informatie veilig is. Persoonlijke informatie, opgeslagen in elektronisch én papieren formaat, moet op verfijnd niveau worden beveiligd en beschermd tegen onbevoegde en ongewenste toegang.

Stap 12: Voldoen betrokken derde partijen en leveranciers aan de privacywetgeving? Bepaal dat zij minstens eenzelfde niveau van bescherming leveren en laat hen dat aantonen.

Nuttige links

http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm
http://www.privacyassociation.org/
http://privacy.org
http://privacy.cs.cmu.edu/research.html
https://www.bof.nl/

1 KPMG, Privacy: onbegrepen en onbeschermd, resultaten privacysurvey, juni 2010.
2 Koorn, R.F., Privacy Enhancing Technologies: ICT als oorzaak én oplossing van privacyuitdaging? - Studieblad Informatiebeveiliging 2006/XX.

Ik heb toch niets te verbergen?

Het eerste lentezonnetje schijnt in mijn gezicht en ik sta een beetje te peinzen terwijl ik mijn auto volgooi met diesel. Ik loop naar binnen en haal mijn tankpasje door de betaalautomaat en bedenk mij dat de leasemaatschappij weer weet dat ik om 16.02 uur in Amersfoort heb gestaan, nog 150 kilometer en ik ben thuis maar ik zal tijdens die rit nog zeker een keer geregistreerd worden bij Zwolle waar iedere auto op de foto wordt gezet om 'criminele bewegingen' in de gaten te houden. Onderweg nog even langs Albert Heijn om een paar boodschappen te doen die ik uiteraard afreken met mijn pinpas, en om de extra kortingen te incasseren bied ik ook mijn bonuskaart aan. Thuis op telebankieren zie ik dat ik inderdaad om 18.42 uur een bedrag van 43,24 euro heb gepind...

Een lang intro om uit te leggen dat ik mij weer eens zorgen maak. Zorgen over de vele bestanden waarin mijn gegevens liggen opgeslagen. Het aantal bestanden waarin mijn naam of andere persoonlijke gegevens is opgeslagen, is immens. Neem bijvoorbeeld de bestanden waar mijn werkgever inzage in heeft.
Om even een paar dingen te noemen; mijn werkgever weet met wie ik telefoneer, hoelang ik dat doe, waar ik op vakantie ga (tenminste als ik daar gebeld wordt), hoeveel ik verdien, hoeveel kinderen ik heb, hoe laat ik een parkeergarage van mijn werk inrijd, hoe laat ik in het bijbehorende gebouw ben, hoe ik mij in dat gebouw beweeg, naar welke websites ik ben geweest, hoe hard ik heb gewerkt (ARBO-tooling om toetsaanslagen te meten), mijn e-mailverkeer, mijn netwerkverkeer, mijn eetgewoonten en zo kan ik heel lang doorgaan.
Gelukkig mag mijn werkgever niet aan alle bestanden komen omdat deze goed geautoriseerd zijn, maar als je de juiste mensen bij elkaar weet te vinden kan een heel compleet beeld van mij worden gemaakt. En dat allemaal met data die op zich noodzakelijk is om een goede bedrijfsvoering te kunnen garanderen maar die enorm misbruikt kan worden. Iedere keer als ik weer een gezellige verjaardagsavond bederf met mijn inmiddels berucht geworden doemdenkscenario's hoor ik weer de meest dodelijke opmerking die hierbij te bedenken valt namelijk, dat de persoon niets te verbergen heeft. Dat hij of zij geen geheimen heeft en waarmee misbruik van data als normaal en niet storend wordt beschouwd. Ik heb ooit mijn vrouw een sms'je gestuurd met de mededeling dat ze wat minder geld moest uitgeven bij de voor haar favoriete modezaak. De afschrijving van 20 minuten eerder kwam ik toevallig tegen toen ik aan het elektronisch bankieren. Het heeft vier dagen geduurd voordat ze weer tegen mij sprak en het heeft nog veel langer geduurd voordat ik er achter was waarom ze zo boos was. Achteraf gezien volkomen terecht, maar gelukkig heeft haar boosheid mij wel tot denken gezet. De werkgever wordt vaak als 'big brother' gezien en datzelfde is van de gemeentelijke, provinciale en landelijke overheid te zeggen. Mijn zoon liep ooit stage bij de gemeente waarin ik zelf werkzaam was en hij vertelde mij wat hij allemaal kon vinden over mij en mijn huis, mijn te betalen gemeentelijke belastingen, mijn correspondentie met de gemeente enzovoort. Beangstigend dat een nieuwsgierige stagiair bij die informatie kan. Nee, ze mogen alles wel inzien want ik heb niets te verbergen. Nee ik heb inderdaad niets te verbergen maar het gaat niemand iets aan dat ik een boze brief naar de gemeente heb geschreven omdat ze het publieke groen achter mijn huis in mijn ogen verwaarlozen. En zo zijn er wel meer zaken te benoemen die niemand iets aan gaan maar die ik ook niet hoef te verbergen. Toch vertel ik alleen diegene aan wie ik het wil vertellen, wat mijn relaties met de gemeente zijn. Waarom maak ik me dan zo druk? Ik maak mij druk over de gegevensbeheerders die niet altijd even correct met de gegevens omgaan. Hebt u ook wel eens een uitnodiging van een wildvreemde garage gehad om uw auto een APK-beurt te laten geven? Ik moet mijn gegevens zelfs in het bel-me-niet register laten vastleggen om ongestoord mijn aardappelen naar binnen te kunnen schuiven. Dom dat ik het register heb gevuld met mijn naam want nu komen de ongevraagde colporteurs aan de deur. Waarom mogen zij ongestraft misbruik maken van dit register? Onschuldige voorbeelden maar ik wacht op de dag dat er iemand zich bij mij meldt met de vraag waarom ik niet eens zijn medicijnen ga gebruiken in plaats van de huidige medicijnen. Informatie die hij uit mijn elektronische patiëntendossier heeft geplukt.

Groetjes,
Berry

Verlies uw USB stick, maar nooit uw data!

De voordelen van SafeStick

- Automatische back-up & recovery
- Snelste en veiligste encrypted USB stick
- Remote delete en password reset
- Timer lockdown en brute force protection
- Geen extra software nodig

Zelf SafeStick proberen? Neem contact op via (0183) 62 44 44 voor een evaluatie stick.
De prijzen van SafeStick kunt u vinden op www.crypsys.nl/shop

SafeStick®

CRYPSYS Data Security B.V. - Benelux Distributeur van SafeStick
Edisonweg 4 - 4207 HG Gorinchem - Postbus 542 4200 AM Gorinchem

CRYPSYS data security