06/2011

INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 6- 2011

SPECIAL: PRIVACY

PRIVACYBESCHERMING MET U-PROVE

REKENEN MET VERCIJFERDE DATA

SOCIAL ENGINEERING EN PRIVACY

DE SOCIALE KRINGEN VAN GOOGLE+

FOX-IT

for a more secure society

Protecting secrets

Fighting cybercrime

Finding digital evidence

Innovating internet interception

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

VOORWOORD

PRIVACY ONDER CONTROLE

Voor u ligt de privacyspecial van Informatiebeveiliging en als gasthoofdredacteur heb ik de eer deze editie te mogen openen. Veel auteurs hebben hard gewerkt om er een prachtig nummer van te maken. Enkele van hen benoem ik hieronder, maar zonder een van hen daarmee tekort te willen doen: ik dank allen voor de mooie bijdragen! Ik zou u, lezer, natuurlijk nu kunnen vertellen dat het slecht gesteld is met onze privacy en dat onze gegevens continue blootgesteld zijn aan allerhande gevaren. Ik zou u ook kunnen vertellen dat onze privacyrechten uit de Wet bescherming persoonsgegevens lang niet altijd effectief zijn (of slechts zelden gebruikt worden door degenen die daar recht op hebben). Daarnaast zou ik kunnen zeggen dat wijzelf onze privacy steeds vaker te grabbel gooien door klakkeloos alles online te zetten. Maar, dat zal ik niet doen. Dat is gewoonweg te makkelijk. Laten we vooral samen kijken naar oplossingen voor de ontstane problemen. Pieter Rogaar neemt u mee in de wereld van de elektronische identiteitskaart en stelt voor om gebruik te maken van U-prove, een cryptografische oplossing waarmee meer en betere privacy voor burgers kan worden behaald. Jaap-Henk Hoepman zwengelt het debat aan rond het recht op inzage wat betreft onze gegevens en roept een ieder op eens gebruik te maken van PIM, de Privacy Inzage Machine van burgerrechtenorganisatie Bits of Freedom. Bart de Koning schetst een overzicht van de jaren van privacy-erosie binnen het politieke speelveld.

De auteur is optimistisch en constateert dat het steeds beter gaat met de maatschappelijke discussie. Er is serieus aandacht voor privacy, zelfs bij kopstukken als Teeven die in het verleden toch niet altijd even privacy-vriendelijk werd geacht. Thijs Veugen bespreekt een nieuwe techniek om bestaande en nieuwe toepassingen 'privacy vriendelijk' te maken. De auteur laat zien dat je door gebruik te maken van homomorfe encryptie de data zowel kunt versleutelen als ook nog kunt gebruiken zonder de privacy in gevaar te brengen. Uiteindelijk draait het allemaal om controle. Controle behouden over onze eigen gegevens, controle herpakken op het moment dat er iets misgaat met gegevens en het controleren van de controleurs. Westin had het nog niet zo verkeerd gezien in de jaren 60 toen hij schreef dat privacy is:
"the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

Ik wens u veel leesplezier,
Rachel Marbus

P.S. In mijn column geef ik u deze keer iets te overdenken. Geef uw privacy niet voor niets op. Uw gegevens zijn kostbaar. En als u dan wel uw privacy wilt opgeven… doe het dan goed!

INHOUDSOPGAVE

PRIVACYBESCHERMING MET U-PROVE BIJ DE ELEKTRONISCHE NEDERLANDSE IDENTITEITSKAART

Pieter Rogaar is in augustus 2011 afgestudeerd aan de Radboud Universiteit Nijmegen op het gebied van U-Prove en de toepasbaarheid ervan in bepaalde bestaande en nieuwe systemen, waaronder eNIK. Per 1 oktober 2011 werkt hij als junior adviseur bij KPMG IT Advisory, waar hij penetratietests voor klanten uitvoert en hen voorziet van strategisch security-advies.

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties sluit medio 2011 het vooronderzoek af voor de elektronische Nederlandse identiteitskaart (eNIK). Deze smartcard is de mogelijke opvolger van de huidige analoge identiteitskaart. Echter, er is nog veel onduidelijk over deze kaart. Niet alleen moet het parlement nog beslissen of de kaart er wel komt, ook is van alles nog niet ingevuld over de functionaliteit die de kaart moet kennen en de cryptografische methoden die op de kaart geïmplementeerd moeten worden. In dit artikel gaan we in op de eisen die aan de eNIK worden gesteld en de haalbaarheid van die eisen. Verder bekijken we U-Prove, een cryptografisch systeem dat door Microsoft gelanceerd is. Dit systeem stelt gebruikers in staat om geauthenticeerde identiteitsaspecten selectief te tonen aan derde partijen. Daarmee is het een interessante en privacyvriendelijke kandidaat voor de cryptografie waarop de eNIK wordt gebaseerd.

De belangen van verschillende partijen spelen een rol in de introductie van de eNIK. We bespreken hier de eisen van de overheid, burgers en derde partijen.

De eerste eis die aan de eNIK wordt gesteld, is dat hij minimaal hetzelfde kan als de huidige identiteitskaart, maar dan ook online. Natuurlijk heeft de gebruiker dan een smartcard- of RFID-lezer nodig. Deze eis houdt in dat een burger in staat moet zijn om bepaalde aspecten van zijn identiteit, zoals zijn naam of geboortedatum, te tonen aan een derde partij. Zulke identiteitsaspecten zullen we verder 'attributen' noemen. Een webwinkel kan bijvoorbeeld artikelen verkopen die niet geschikt zijn voor minderjarigen. Een klant gebruikt dan zijn eNIK om op afstand te bewijzen dat hij inderdaad ten minste achttien jaar oud is. De webwinkel vertrouwt deze mededeling, omdat zij met behulp van de door de overheid uitgegeven eNIK is gedaan.

Online leeftijdstoets makkelijker met eNIK

Ten tweede wordt de eNIK geacht de privacy van de burger ten opzichte van derde partijen te beschermen. De burger moet in staat zijn zelf te kiezen welke attributen hij wil delen met een derde partij. Verder moeten meerdere derde partijen niet kunnen samenwerken om geautomatiseerd rijkere profielen van hun gebruikers op te stellen. Als ik aan de ene webwinkel laat zien dat ik ouder ben dan achttien jaar, en aan de andere dat ik geboren ben in Rotterdam, dan moeten deze webwinkels hun gegevens niet kunnen koppelen aan de hand van de gegevens die in de interactie met de eNIK zijn verkregen. Als de eNIK bij elke transactie een kaartnummer meestuurt, is het bijvoorbeeld eenvoudig om de profielen bij

verschillende webwinkels te koppelen langs dit kaartnummer. Men noemt deze eis ook wel het vermijden van de constructie van 'hotspots'.

Naast deze twee voor de hand liggende eisen, hanteert het ministerie nog een derde eis: de kaart moet bij uitgifte afgesloten zijn en niet meer kunnen worden voorzien van nieuwe informatie. Waarschijnlijk komt deze eis voort uit angst voor problemen zoals die rond de OV-chipkaart zijn voorgekomen. Het is daarom begrijpelijk dat beleidsmakers de kaart graag afgesloten zien. Tegelijk is het belangrijk te beseffen dat smartcards met de huidige stand van de techniek afdoende zijn te beveiligen, mits ze vakkundig zijn geprogrammeerd en er een model is gekozen dat geschikt is voor het benodigde beveiligingsniveau. We zullen deze eis daarom wat losser opvatten.

De drie eisen die hiervoor worden genoemd, zijn in feite voldoende voor het ministerie en de derde partijen. Bekijken we het systeem echter vanuit het standpunt van de burger, dan is er nog een belangrijke vertrouwensrelatie die de burger graag minimaliseert namelijk, die tussen hemzelf en de overheid. Dat betekent dat de burger graag een systeem ziet dat hem in staat stelt om zijn attributen te tonen aan derde partijen, zonder dat de overheid iets over deze interactie te weten komt. Als ik bijvoorbeeld de eerdergenoemde webwinkel voor volwassenen bezoek, moet de overheid niet kunnen achterhalen dat iemand deze site heeft bezocht, dat iemand iets bewezen heeft (namelijk ouder dan achttien jaar te zijn) en al helemaal niet dat ik dat was. Merk op dat het rechtstreeks toepassen van DigiD als eNIK-achtig systeem onder meer hierop spaak loopt.

Een mogelijke toekomstige toepassing van de eNIK is het toestaan van attributen van derde partijen op de kaart. Een polisnummer, OV-jaarkaart of medische informatie kunnen dan ook worden opgenomen op de kaart. Vanzelfsprekend zullen ook voor de toegang tot deze attributen de eerdergenoemde eisen worden gesteld. Zo kan niemand zomaar de attributen uitlezen, zeker niet als deze door een andere derde partij op de kaart zijn gezet.

Fig. 1. Een U-Prove token laat de gebruiker kiezen welke attributen hij vrijgeeft en welke verborgen blijven.

U-Prove helpt privacy te borgen

U-Prove

Over de specifieke cryptografie die op de kaart wordt opgenomen, staat in de eisen niets vermeld. De in maart 2010 door Microsoft gelanceerde technologie U-Prove[1)] is hiervoor een interessante kandidaat. U-Prove is in 2000 bedacht door Stefan Brands en beschreven in zijn proefschrift [Brands, 2000]. Microsoft heeft de technologie gekocht en heeft deze nu vrijgegeven onder hun Open Specification Promise. Dit betekent dat Microsoft belooft geen rechten op U-Prove te doen gelden met betrekking tot hun patenten. Wat hen betreft is iedereen vrij deze technologie te gebruiken en aan te passen. Microsoft doet echter geen uitspraken over patenten die eventuele derde partijen kunnen doen gelden op het systeem.

U-Prove draait om de notie van tokens. Een U-Prove-token is een dataelement dat bepaalde attributen bevat, en dat is ondertekend door een uitgevende partij. In dit geval is de uitgevende partij de overheid. De bezitter van zo'n token, in dit geval de burger, kan met behulp van het token een willekeurig deel van de attributen in het token tonen aan een derde partij. Zo'n token zou bijvoorbeeld de verzameling attributen die op mijn analoge identiteitskaart staat, kunnen bevatten. Ik kan dit token dan gebruiken om alleen mijn voor- en achternaam te tonen aan een derde partij, en de rest van de attributen in het token verborgen te houden. Bij een analoge identiteitskaart zou dat neerkomen op fig. 1. De overheid wordt bij deze mededeling helemaal niet betrokken: het bewijs wordt offline (d.w.z. zonder contact met de uitgevende instantie) geleverd. De derde partij weet wel zeker dat de inhoud van de mededeling klopt: deze partij kan de digitale handtekening van de overheid controleren die op het publieke deel van het token is aangebracht.

In functioneel opzicht corresponderen tokens met pseudo-identiteiten. Als ik twee tokens gebruik om mijn attributen te tonen aan twee partijen, is er geen manier om de attributen die ik aan de ene partij toon, te koppelen aan de attributen die ik aan de andere partij toon. Echter, als ik een token bij twee partijen gebruik, zullen deze partijen aan de hand van de unieke digitale handtekening van de overheid kunnen

vaststellen dat de twee mededelingen met hetzelfde token zijn geleverd, ook als ze heel verschillende attributen uit dat token te zien hebben gekregen. Op die manier kunnen ze daarna een hotspot creëren door de vrijgegeven attributen bij elkaar te voegen, samen met hun eigen informatie over mij. Op dat moment voldoet deze controlemogelijkheid niet aan de tweede eis van eNIK.

U-Prove voor eNIK

Om de eisen aan eNIK te vervullen, kunnen we U-Prove aanwenden. We vullen dan de eNIK met een fiks aantal door de overheid uitgegeven U-Prove-tokens die allemaal de attributen bevatten die op onze analoge identiteitskaart stonden. Willen we nu een paar attributen tonen aan een derde partij, dan kiezen we een van de tokens die op onze eNIK staan, bijvoorbeeld door middel van een menu op de computer. In feite kiezen we welke pseudo-identiteit we willen gebruiken voor deze communicatie met deze partij. We gebruiken dit token om de attributen die we willen tonen, te tonen aan deze partij. De overheid wordt niet van deze interactie op de hoogte gesteld en de derde partij kan niet meer attributen achterhalen dan we in deze interactie vrij hebben gegeven.

Merk op dat het aantal pseudo-identiteiten dat we in dit voorstel ondersteunen, wordt beperkt door het aantal tokens dat op de eNIK staat opgeslagen. Natuurlijk kunnen later, indien nodig, meer tokens worden toegevoegd, maar dit gaat wel in tegen het concept van een gesloten kaart dat het ministerie wenst. IBM heeft een soortgelijk systeem, Idemix[2)], ontworpen dat met een gesloten kaart wél oneindig veel pseudo-identiteiten ondersteunt. Het nadeel van Idemix is dat het veel complexer (en dus langzamer) is dan U-Prove. In experimenten met een kaart met vijf attributen in een U-Prove-token duurde het tonen van één attribuut 0.8 seconden[3)]. Het leveren van een gelijkwaardig bericht met Idemix kostte 30 seconden [Mostowski et al, 2011].

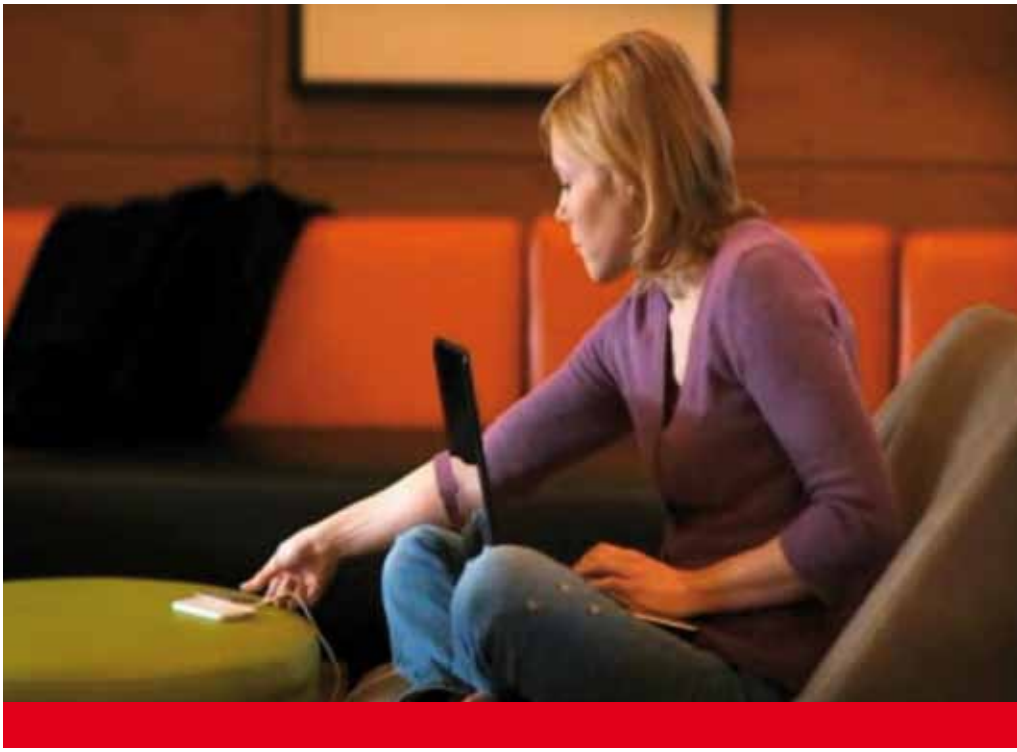
Indien U-Prove inderdaad gaat worden gebruikt voor de eNIK, is het relevant na te denken over de manier waarop de pseudo-identiteiten beheerd gaan worden. Uit privacyperspectief is het ideaal voor iedere transactie een nieuw token te gebruiken. Dit kost wel veel opslagruimte, en is waarschijnlijk voor de meesten wat overdreven. Aanbieders van diensten hebben belang bij het herkennen van hun klanten, dus net als bij een klantenkaart kunnen ze voordelen bieden voor terugkerende klanten, die kunnen worden herkend aan hun opnieuw gebruikte token. Verder kunnen soortgelijke aanbieders worden voorzien van hetzelfde token. Dat zou een verdere ruimtebesparing op kunnen leveren. Ieder politiek forum weet dan bijvoorbeeld zeker dat ik dezelfde ben als op het andere forum, maar mijn werkgever kan daar nooit achter komen. Hoe de gebruiker effectief kan worden gevraagd welk token moet worden gebruikt, is nog een open vraag. Het computerprogramma dat met het token communiceert zou bijvoorbeeld op basis van een privacyprofiel suggesties kunnen doen voor het te gebruiken token.

Eis gesloten kaart onnodig beperkend

Hoewel de functionaliteit die we hierboven beschrijven, geheel beschikbaar is in de huidige versie van U-Prove, is het systeem nog volop in ontwikkeling. Zo beschrijft Brands in zijn proefschrift de mogelijkheid van het doen van ingewikkelder mededelingen dan het selectief tonen van bepaalde attributen. Een voorbeeld hiervan, dat ik in mijn afstudeerscriptie heb beschreven en geïmplementeerd, is de mededeling dat een bepaald attribuut in een gegeven interval ligt [Rogaar, 2011]. In plaats van het tonen van zijn geboortedatum, kan een burger dan bewijzen dat zijn geboortedatum minstens achttien en hoogstens 65 jaar geleden is. Een ander voorbeeld van een complexe mededeling is 'deze burger is in Rotterdam geboren of woont nu in Rotterdam'. Zulke mededelingen zijn waarschijnlijk wiskundig mogelijk, maar nu nog niet door Microsoft ontworpen en aan de specificatie toegevoegd.

Een andere functionaliteit die door Microsoft nog niet is toegevoegd, is het intrekken van eenmaal uitgegeven tokens. Als iemand zijn eNIK kwijtraakt of als blijkt dat bepaalde tokens om een andere reden niet meer geldig zijn, moeten deze door de overheid kunnen worden ingetrokken. Het is duidelijk dat het niet wenselijk is de geldigheid van

een token bij de overheid na te vragen, omdat dat een indicatie geeft van het soort interacties dat met de eNIK wordt ondernomen. Er is op dit moment nog geen oplossing voor dit probleem, al heeft Microsoft aangekondigd hier wel aan te werken [Microsoft, 2010].



Conclusie

Al met al vormt het programma van eisen van de eNIK een goede aanleiding om U-Prove wat uitgebreider onder de loep te nemen. Het systeem kent enkele privacygaranties die precies aansluiten bij de eisen zoals die door het ministerie, burgers en derde partijen worden geformuleerd. De functionaliteit die U-Prove biedt op het gebied van pseudo-identiteiten is een goede voorzet voor deze kaart: het in staat stellen van de burger om zijn eigen pseudo-identiteit te kiezen voor elke interactie met een derde partij ligt in het verlengde van het door Westin gestelde streven van 'privacy as control' [Westin, 1970]. Waarschijnlijk is de eis van het ministerie dat de kaart gesloten moet zijn bij uitgifte onnodig beperkend en een rem op verdere interessante toepassingen met tokens en attributen van derde partijen op de kaart. Wel is U-Prove op dit moment nog niet klaar om te worden gebruikt op de eNIK.

Vooral het gebrek aan een intrekmogelijkheid voor U-Prove tokens zal een belangrijke beperking zijn, maar ook het bieden van meer mogelijkheden voor complexere mededelingen zal uiteindelijk de privacy van de burger ten goede komen.

Mogelijkheid dynamische attributen wenselijk

Literatuur

Brands, S.A., *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy.* MIT Press, Cambridge, MA, USA, 2000.

Microsoft, U-Prove technology overview. 2010, Microsoft, 2010 Microsoft. Microsoft U-Prove technology overview. *https://connect.microsoft.com/site642/Downloads/DownloadDetails.aspx?DownloadID=26953*, ingezien op 4 februari 2011.

Rogaar, P., *Attributes and tokens in U-Prove: Interval proofs and use cases*, afstudeerscriptie Radboud Universiteit Nijmegen, 2011.

Mostowski, W., P. Vullers, 'Efficient U-Prove Implementation for Anonymous Credentials on Smart Cards', in *Proceedings of the 7th International ICST Conference on Security and Privacy in Communication Networks*, Springer-Verlag, Berlijn 2011. (te verschijnen)

Westin, A.F., *Privacy and freedom.* Atheneum, Amsterdam, 1970.

Eindnoten

[1] *https://connect.microsoft.com/content/content.aspx?contentid=12505&siteid=642.*

[2] *http://www.zurich.ibm.com/security/idemix/*

[3] *Het tonen van attributen met U-Prove gaat sneller naarmate er minder attributen verborgen blijven. Het computationeel intensieve werk bij het tonen komt voort uit het verbergen van de niet-getoonde attributen.*

ELEKTRICITEITSNETWERKEN: MEER EFFICIENCY VEREIST MEER INFORMATIE DELEN

EEN KLEINER ENERGIEPROBLEEM, MAAR EEN GROTERE UITDAGING VOOR INFORMATIEBEVEILIGING

E.G. Broenink M.Sc., Security Specialist bij TNO, gerben.broenink@tno.nl
Drs. K.A.Helmholt, Senior Consultant bij TNO, kristian.helmholt@tno.nl

Het opraken van de fossiele energiebronnen en het veranderende klimaat zijn twee maatschappij bedreigende ontwikkelingen die op het eerste gezicht niets met het beveiligen van informatie van doen hebben. Toch hebben ze gezorgd voor een maatschappelijke reactie in de vorm van de ontwikkeling van intelligente energienetwerken (smartgrids). Het is volgens ons hoog tijd dat informatiebeveiligers zich betrokken gaan voelen bij de keuzes in informatiedeling die overheden, bedrijven en burgers nu en in de komende jaren gaan maken.

Het delen van informatie tussen elektriciteitsleveranciers en hun klanten staat momenteel in de kinderschoenen. Een keer per jaar wordt het totale energiegebruik in de vorm van de gebruikte Joules ('Kilowattuur') gecommuniceerd. Dit gebruik vormt de basis van de elektriciteitsrekening. Dit model van verrekenen werkt al decennia, omdat het afrekenen binnen een kortere periode dan een jaar niet nodig is, om verschillende redenen. Een van deze redenen is dat de elektriciteitsprijzen (voor burgers) amper door het jaar heen veranderen. Er zijn wel verschillende tarieven voor de verschillende tijdstippen op de dag, zodat diegenen die de mogelijkheid hebben hun stroomverbruik naar de nacht te schuiven (wasmachines en wasdrogers en dergelijk) kunnen profiteren van een nachttarief. Het voordeel voor elektriciteitsleveranciers en netbeheerders is dat ze gebruikspieken van de dag kunnen afvlakken, zodat er overdag in totaal minder en meer verspreid geproduceerd kan worden.

Dat simpele model van informatiedeling voor verrekenen is maatschappelijk gezien inmiddels aan behoorlijke slijtage onderhevig. In de eerste plaats is het de klimaatverandering die maatschappelijk een 'druk tot registreren' lijkt te hebben geïnitieerd. Reductie van CO2-uitstoot heeft bij beleidsbepalers het primaat en er is al wetgeving ontwikkeld om CO2-verbruik te registeren en bonussen/malussen te plaatsen op vermindering/vermeerdering van uitstoot. Deze ontwikkeling zorgt op zichzelf niet voor de slijtage aan het verrekeningsmodel. Het is ook de groeiende schaarste van fossiele brandstoffen die andere vormen van verrekening lijkt te gaan vereisen. De schaarste lijkt (economisch) namelijk alleen te kunnen worden opgevangen met, ten eerste een mix van andere en bij voorkeur duurzame energiebronnen en ten tweede door een efficiënter gebruik van energie. Zowel het mixen als het efficiënter gebruik van energie hebben hun eigen effecten op het energienetwerk, en daardoor op het verrekeningsmodel en de informatiedeling. Efficiënter gebruiken betekent onder andere productie en consumptie van elektriciteit beter op elkaar afstemmen. Dat kan door het beter voorspellen van elektriciteitsverbruik en door het (ver)schuiven van productie en consumptie. Het mixen van energiebronnen heeft echter nog een ander effect. Deze duurzamere energiebronnen (zoals zonne-energie en windenergie) zijn namelijk moeilijker aan en uit te schakelen, en ook minder voorspelbaar. Dit alles moet door het energienetwerk worden opgevangen.

De 'slimme meter'

De 'slimme meter', zoals deze de afgelopen tijd in de politiek is besproken kan daarbij helpen. Deze slimme meter zal frequenter meterstanden doorgeven, die de netbeheerders een beter inzicht in het gebruik van het netwerk geven. De privacyconsequenties hiervan zijn inmiddels ook al breed uitgemeten in de verschillende media [Webwereld, 2009] [Security.nl, 2011] [FD.selections, 2011]. Voor het invullen van de nieuwe eisen aan het energienetwerk is er echter meer nodig dan alleen deze slimme meter. Voor het creeren van een hogere efficiëntie hebben

producenten betere voorspellingen nodig van het gebruik van hun consumenten. En het mixen van (nieuwe en duurzame) energiebronnen betekent momenteel dat er energiebronnen in de productie moeten gaan worden opgenomen met een slechtere voorspelbaarheid qua productie (zonne- en windenergie). Om dit op te lossen is er de wens tot meer flexibele en geplande afname. Ook hiervoor zijn betere voorspellingen van het gebruik van consumenten vereist. Daar komt nog eens de decentralisatie van elektriciteitsproductie bij. Het wordt economisch gezien aantrekkelijker om bijvoorbeeld zonnepanelen te plaatsen. Op zonnige dagen kunnen deze meer energie produceren dan er in huis wordt gebruikt, met als resultaat dat consumenten ineens producenten worden.

Dit is geen eenvoudige uitdaging voor netwerkbeheerders. Want op een elektriciteitsnetwerk moet altijd balans zijn. Het aanbod aan vermogen moet altijd gelijk zijn aan de vraag (er zit geen buffer in het netwerk). Het vinden van een balans tussen de productie en consumptie is een complex en kritisch proces. Als de productie te hoog is, stijgt het voltage op het netwerk waardoor apparatuur kan uitvallen of doorbranden, maar is de productie te laag dan kan apparatuur ook uitvallen. Hier komt bij dat productie-eenheden als een kolencentrale, kerncentrale en zonnepanelen niet zo maar een tandje lager kunnen worden geschakeld.

Daarom is beïnvloeding van de vraag ook een middel geworden voor die partijen die verantwoordelijk zijn voor de balans op het netwerk. Een concreet voorbeeld van beïnvloeding is het bieden van een vergoeding (korting) om de wasmachine op een later tijdstip aan te zetten.

Energienetwerk moet intelligenter worden

Welke oplossing ook gekozen wordt, het lijkt er op dat het energie/elektriciteitsnetwerk in elk geval intelligenter moet worden om de verschillende aanbieders en afnemers van elektriciteit van dienst te kunnen zijn en de energie heen en weer te kunnen transporteren, waarbij de productie en consumptie van energie zodanig wordt bijgehouden dat financiële prikkels mogelijk zijn. In Nederland is de tender 'Proeftuinen Intelligente Netten' net van start gegaan. Daar moet ervaring opgedaan worden met het afstemmen van vraag en aanbod in een netwerk dat meerdere soorten bronnen van duurzame aard heeft, of dit nu gebeurt door betere voorspelling of door beïnvloeding van de vraag.

De proeftuinen hoeven niet vanuit het niets te beginnen. Er zijn ondertussen in de wetenschap al verscheidene voorstellen voor implementaties van intelligente(re) netten (ook wel smartgrids) gedaan. De doelen die partijen met deze onderling – qua implementatie – soms sterk verschillende intelligente netten proberen te bereiken variëren nogal; van optimalisatie van efficiency, optimalisatie van gebruik van groene energie en optimalisatie van een mogelijk businessmodel van een eindgebruiker. Vanuit het oogpunt van informatiebeveiliging zijn er ook duidelijke verschillen qua informatiedeling. De keuze voor een bepaalde implementatie van een intelligent(er) net kan nogal wat consequenties hebben op het gebied van privacy en het beveiligen van informatie. Vanwege hun aard zijn dit ook keuzes met sterke implicaties voor de maatschappij. Informatiemacht is een steeds belangrijkere factor in het maatschappelijk bestel. Vanwege deze implicaties stellen wij dat deze keuzes goed moeten worden overwogen, wat vereist dat de alternatieven goed moeten kunnen worden vergeleken. In de rest van dit artikel presenteren we daarom een begrippenkader dat het mogelijk maakt keuzes op het gebied van het delen van informatie op intelligente netten te vergelijken in termen van consequenties. Zo kunnen overheden, bedrijven en burger(organisatie)s op een gestructureerde manier in gesprek komen over welke informatie zij waarom willen delen, en wat hiervan de consequenties zijn.

Verschillende keuzemogelijkheden

De basis van ons begrippenkader ligt in drie assen waarop in keuzes kan worden gevarieerd, waarbij een keuze op één as geen invloed heeft op een keuze op een andere as. Deze assen zijn gedefinieerd op basis van een uitgevoerde analyse op een aantal beschrijvingen van intelligente netten. In fig. 1 zijn deze assen grafisch weergegeven. Het delen van informatie vindt plaats op een bepaald detailniveau, met een bepaald aantal ontvangers en een bepaalde richting in de tijd. In de volgende paragrafen zal dit begrippenkader verder worden uitgewerkt. Een uitgebreidere uitwerking van dit begrippenkader is beschreven in [Helmholt e.a., 2011].

Om meer ervaring op te doen met mogelijkheden voor een intelligent energienetwerk is er in Nederland onderzoeksgeld beschikbaar gesteld om vijf tot tien proeftuinen te starten. In deze proeftuinen wordt het netwerk van een stadsdeel of wijk voorzien van ICT-oplossingen om het energiegebruik te verminderen, of efficiënter gebruik te maken van duurzame energiebronnen. Hierbij kunnen we denken aan netwerken voor elektriciteit, gas of warmte.
Uiteindelijk doel van deze proeftuinen is om praktijkervaring op te doen met de intelligente netten. Op basis van deze ervaring zijn we in de toekomst beter in staat deze technologie op een goede manier in te zetten. [Agentschapnl, 2011]

Fig. 1.

Detailniveau
Met detailniveau bedoelen we de keuze omtrent de hoeveelheid details die wordt gedeeld. Hierbinnen zijn er nog twee onderverdelingen te maken. Allereerst kan er sprake zijn van een hoge of lage frequentie bij het delen van informatie. Zo is een voorbeeld van een lage frequentie: *'Karel Jansen heeft 1875 kilowattuur gebruikt in 2010'*. Een voorbeeld van een hogere frequentie is: *'Karel Jansen heeft 0,5 kilowattuur gebruikt op 10 augustus 2011 tussen 14:30 en 14:45'*. Ten tweede kan er meer of minder detail zijn in termen van energiegebruikende apparatuur (bij een gelijke frequentie). Een voorbeeld van weinig detail: *'Karel Jansen heeft 1875 kilowattuur gebruikt in 2010.'* En van meer detail *'Karel Jansen's wasmachine heeft 300 kilowattuur gebruikt in 2010'*. Meer detail in apparatuur en in tijd (hogere frequentie) geeft meer beeld over de activiteiten van de afnemer en daarmee inzage in zijn privéleven.

Richting in tijd
Bij gelijkblijvend detailniveau kan er worden gevarieerd in de richting van de tijd. Het maakt wat betreft de privacy ook uit of de uit te wisselen informatie over de toekomst gaat, of over het verleden. En, als het over informatie uit het verleden gaat, maakt het uit of dit informatie over gisteren is, of informatie over vijf jaar geleden. Bij het maken van beleid voor intelligente netten moet een beslissing worden genomen met betrekking tot welk tijdsbestek er informatie moet worden uitgewisseld. In fig. 2 zijn deze keuzemogelijkheden weergegeven.

Ontvangers en hun doel
Bij gelijk detailniveau, gelijke richting in de tijd, kan er nog worden gevarieerd op de ontvangers en hun doel. Deze zijn van belang bij het maken van een keuze in het delen van informatie. Zo vinden de meeste gebruikers van energie het geen probleem dat hun energieleverancier hun gebruik kan inzien. Maar anders wordt het als de overheid het energiegebruik kan inzien. Een partij met wie de meeste gebruikers hun gebruik niet willen delen is een inbreker. Een inbreker zou de gebruiksgegevens namelijk kunnen gebruiken om af te leiden of iemand thuis is, en op basis van deze gegevens beslissen waar hij gaat inbreken.

In fig. 3 zien we een plaatje waarin deze situaties schematisch worden weergegeven. In het eerste plaatje zien we dat Karel Jansen zijn gegevens deelt met twee partijen, waarvan hij er een goed vertrouwt (groen) en een vertrouwt hij minder (oranje). In het tweede plaatje zien we dat Karel zijn gegevens deelt met een vertrouwde partij, en een niet vertrouwde partij (rood). Maar zonder dat Karel het weet speelt de vertrouwde partij zijn gegevens door aan een minder vertrouwde partij (oranje). In het laatste plaatje zien we dat Karel zijn gegevens deelt met vijf partijen die hij vertrouwt. Ondanks dat hij al deze partijen vertrouwt, is het wel de vraag of het wenselijk is dat zoveel partijen zijn gebruiksgegevens ontvangen.

Consequenties van keuzes
Het begrippenkader laat zien dat er veel kan worden gevarieerd. Die variatie heeft consequenties. Een keuze voor het wel of niet delen van een soort informatie maakt bijvoorbeeld bepaalde marktmodellen (on)mogelijk. We zien globaal drie categorieën: consequenties rond privacy, verrekening en balans op het netwerk.

Consequenties rond privacy
Als er gebruikersgegevens worden gedeeld, schaadt dat de privacy van de gebruiker. Ongeacht welke informatie er wordt gedeeld, er is altijd mogelijke schade. De grootte van de schade kan hierbij erg verschillen. Het delen van het geaggregeerde gebruik over het afgelopen jaar (weinig detail in de tijd) met alleen de energieleverancier (één ontvanger) heeft een relatief kleine impact op

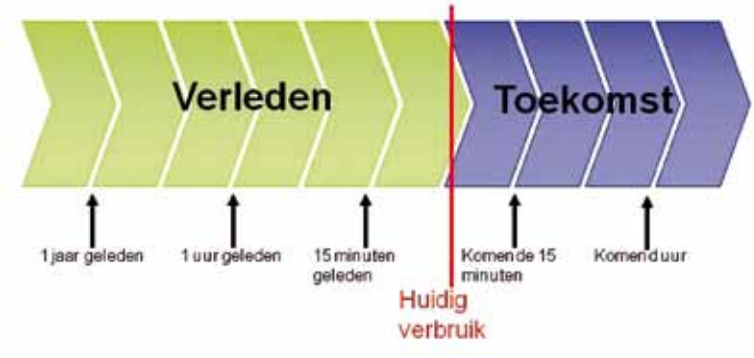


Fig. 2.

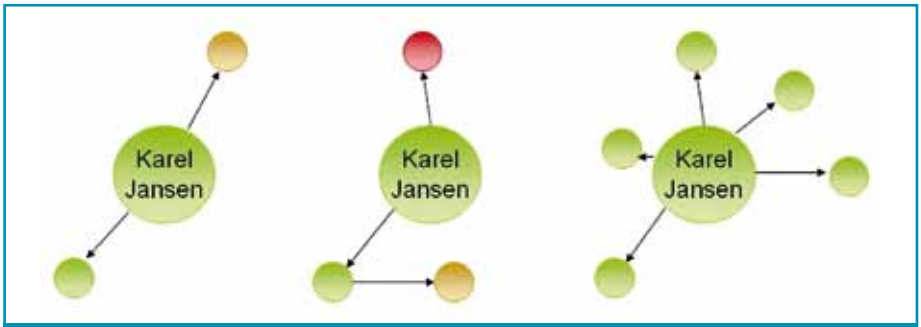


Fig. 3.

de privacy. Maar het iedere vijf minuten registreren van het gebruik (veel detail in de tijd) en dit meteen delen met meerdere partijen (meer ontvangers) maakt het eenvoudiger om het privéleven van een consument in kaart te brengen. Het is wel mogelijk om met behulp van technische oplossingen deze privacyimpact in te perken. Hierbij kan worden gedacht aan bijvoorbeeld cryptografie [Microsoft, 2010]. De mogelijkheden van deze technische oplossingen zijn echter beperkt. Hier ligt een belangrijke afweging: het minimaliseren van privacyimpact kan ten koste gaan van het maximaliseren van de efficiency van het netwerk.
De vraag is dan hoeveel we bereid zijn om te betalen voor onze privacy.

Consequenties rond verrekening
De energieleverancier en netbeheerder zijn verantwoordelijk voor het opstellen van de rekening voor de geleverde energie en transportdiensten. Om deze rekening te kunnen opstellen is het echter noodzakelijk dat de energieleverancier enige informatie heeft over het gebruik van de consument. In het meest eenvoudige model moet de energieleverancier het totaalgebruik van de consument over een periode (bijvoorbeeld. een jaar) weten, om zo een rekening te kunnen opstellen. Wanneer de energieleveranciers meer informatie krijgen, zijn andere soorten verrekening mogelijk. Zo kan een energieleverancier door middel van prijsdifferentiatie de consument aanmoedigen om het gebruik aan te passen. Denk aan het stimuleren van een gebruiker om minder energie af te nemen, of om zijn gebruik te verplaatsen naar de daluren. In beide gevallen bepalen de keuzes over de te delen informatie welke mogelijke prijsprikkels een energieleverancier en/of overheid kan geven om de consument aan te zetten tot ander gedrag.

Consequenties rond netbalans
Het balanceren van vraag en aanbod op een elektriciteitsnetwerk wordt moeilijker naar mate er meer 'onvoorspelbare' energieproducerende apparaten zijn, zoals zonnepanelen en windmolens. Hoe beter vraag en aanbod kunnen worden voorspeld, des te beter kan een stabiele netbalans worden gerealiseerd. De voorspellingen lijken te kunnen worden verbeterd als er meer informatie beschikbaar komt, met name als er informatie over gepland aanbod en gepland gebruik beschikbaar komt. Het niet delen van deze informatie maakt het moeilijk – wellicht onmogelijk – om tot goede voorspelling te komen, waardoor het moeilijker (lees: kostbaarder) wordt om tot een balans in het netwerk te komen, omdat er meer geïnvesteerd moet worden in materiaal en diensten die voor balans in het netwerk zorgen. Denk hierbij aan een uitgebreider energienetwerk, meer gas gestookte elektriciteitscentrales, enz.

Hoe maken we nu een keuze?
Allereerst zal er in Nederland meer ervaring moeten worden opgedaan in de proeftuinen met intelligente netten. Hierbij is het belangrijk om de consequenties van de verschillende mogelijke keuzes duidelijk te krijgen, zodat er goed kan worden vergeleken. Op basis van die ervaring en de ervaring die er elders internationaal in de komende jaren wordt opgedaan kan er door de energieleveranciers, maar ook door consumentenorganisaties en de overheid worden geëvalueerd. Het hier gepresenteerde begrippenkader kan hierbij een middel zijn om de verschillende keuzemogelijkheden te vergelijken. Uiteindelijk is het belangrijk dat er in Nederland door alle betrokken partijen een overwogen beslissing wordt genomen over de te nemen keuzes.

Nu weten we dat er vanuit de optiek van informatiedelen altijd een afweging tussen verschillende consequenties gemaakt zal moeten worden. Een optimale keuze bestaat niet. Wel stellen we dat er vanuit het doel van de te delen informatie moet worden geredeneerd. Het hangt er dan vanaf welk aspect zwaarder weegt. Dat zal op sommige punten betekenen dat er ergens moet worden ingeleverd om op andere punten winst te bereiken.

Er moet een keuze worden gemaakt

Literatuur

Agentschap, 2011, *Proeftuinregeling intelligente netten*, www.agentschapnl.nl/nl/programmas-regelingen/intelligente-netten

FD.selections, 2011, *Privacy bij slimme meter nog niet helemaal goed geregeld*, www.fdselections.nl/energie/Opinie/Energievisie/articleType/ArticleView/articleId/19392/Privacy-bij-slimme-meter-nog-niet-helemaal-goed-geregeld.aspx

K.A. Helmholt, E.G. Broenink, *"Degrees of Freedom in Information Sharing on a Greener and Smarter Grid"*, Energy 2011, pp 141-147, 2011

Microsoft, 2010, *Privacy-Preserving Smart Metering*, research.microsoft.com/apps/pubs/?id=141726

Security.nl, 2011, *Privacy slimme meter niet goed geregeld,* www.security.nl/artikel/36350/1/%22Privacy_slimme_meter_niet_goed_geregeld%22.html

Webwereld, 2009, *vijf domme dingen van slimme meters*, webwereld.nl/de-vijf/56792/vijf-domme-dingen-van-slimme-meters.html

REKENEN MET VERCIJFERDE DATA

Dr.ir. Thijs Veugen is sinds 1999 werkzaam als senior scientist bij TNO in de afdeling Information Security. Tevens werkt hij vanaf 2008 aan de TU Delft als senior researcher in de Multimedia Signal Processing groep. Zijn belangrijkste onderzoeksgebied is toepassingen van cryptografie.

Een nieuwe techniek om bestaande en nieuwe toepassingen 'privacy vriendelijk' te maken is gebaseerd op het concept 'rekenen met vercijferde data'. In dit artikel wordt dit mysterieuze idee uit de doeken gedaan en wordt de kracht ervan duidelijk gemaakt.

Het privacy-probleem ontstaat doordat sommige toepassingen gevoelige persoonlijke informatie nodig hebben. Om bijvoorbeeld op internet advies te vragen over de behandeling van een bepaalde ziekte zal je eerst moeten vertellen welke ziekte je precies hebt. En om bij bol.com advies te kunnen krijgen over boeken die je mogelijk interesseren, zal bol.com eerst moeten weten wat voor soort boeken jij zoal prettig vindt. Dat kan bol.com doen door een overzicht bij te houden van de boeken die je in het verleden hebt gekocht, of door bepaalde persoonlijke voorkeuren op te vragen die bol.com vervolgens vergelijkt met voorkeuren van andere gebruikers. Als iemand die qua voorkeuren op jou lijkt een bepaald boek leuk vindt, is de kans groot dat jij dat boek ook leuk vindt.
Zou het niet prettig zijn wanneer al die toepassingen je *wel* van nuttige informatie kunnen voorzien maar *zonder* dat ze al jouw persoonlijke informatie in handen krijgen? Voor de klanten is het een hele geruststelling om te weten dat hun privégegevens nooit in vreemde handen zullen vallen, en de provider hoeft zich ook niet meer druk te maken of hij wel zorgvuldig genoeg is omgegaan met de persoonlijke gegevens van zijn klanten.

Het is bekend dat je data kunt vercijferen om te voorkomen dat anderen bij die informatie kunnen. Tot nu toe betekende dat ook dat je die vercijferde data niet kunt gebruiken om nuttige dingen uit te rekenen zoals bijvoorbeeld een aanbeveling voor leuke boeken. Maar daar is nu een einde aan gekomen! Door nieuwe technieken als homomorfe encryptie, die verderop worden uitgelegd, blijkt het mogelijk te zijn om *en* data te vercijferen *en* er toch leuke dingen mee uit te rekenen als een medisch advies speciaal voor jouw ziekte of een boek aanbevolen krijgen waar je zelf nooit op was gekomen.

De voordelen van zekerheid
Er is natuurlijk wetgeving die voorschrijft hoe er met persoonlijke gegevens dient te worden omgegaan en tot op zekere hoogte zijn je gegevens daarmee ook veilig. In de praktijk blijken

Vercijferen van data.

er echter steeds meer meldingen te komen van gevoelige gegevens die om een of andere reden toch bij onbevoegden terecht zijn gekomen. Wat gebeurt er bijvoorbeeld met je gegevens wanneer een provider als bol.com failliet gaat of wordt overgenomen door een andere partij? Of wanneer iemand weet in te breken en de gegevens steelt, of een medewerker iets te onzorgvuldig met zijn laptop is omgegaan?

Om je met zekerheid te beschermen tegen alle mogelijke manieren waarop gevoelige data kan uitlekken is encryptie een goede oplossing. Wat er ook met de data gebeurt, je weet zeker dat jouw gevoelige data nooit op straat zal komen. Door die zekerheid ontstaan er ook nieuwe mogelijkheden. Waar het gaat om zeer gevoelige gegevens van bijvoorbeeld medische of concurrentiegevoelige aard, zijn gebruikers en organisaties zeer huiverig om deze voor bepaalde toepassingen beschikbaar te stellen. Wanneer ze echter de garantie krijgen dat er niets onrechtmatigs met die data kan gebeuren, zullen ze eerder geneigd zijn om deze te overhandigen zodat er tal van nieuwe toepassingen kunnen ontstaan. Denk bijvoorbeeld aan het kunnen uitbesteden van financiële bewerkingen van bedrijfsdata, het genereren van aanbevelingen gebruikmakende van profielen van verschillende organisaties, of het gebruiken van data van contacten in een sociaal netwerk om betere aanbevelingen te kunnen krijgen [CASoN2011].

Zodra je kunt rekenen met vercijferde data opent zich een wereld van toepassingen. Een bekende is om te kunnen zoeken in vercijferde data. Zo kun je toch selectief data opvragen die vercijferd bij een derde (of in de cloud) is opgeslagen, zonder alle data te hoeven uploaden, maar ook zonder dat de server weet om welke data het gaat en waarnaar je op zoek bent. Een ander, actueel voorbeeld is het gebruik van cookies in de internetwereld. Virtuele diensten slaan allerlei persoonlijke informatie op in cookies op de computers van gebruikers om hun dienst beter te kunnen aanbieden. Dit privacy-risico zou ondervangen kunnen worden door de cookies te vercijferen zonder dat het ten koste gaat van de dienstverlening.

Een nieuwe veelbelovende techniek

Het veilig kunnen rekenen met een aantal partijen samen is in de academische wereld al langer bekend als secure multiparty computation. Er zijn allerlei cryptografische protocollen bekend voor specifieke problemen, elk met hun eigen voor- en nadelen. Over het algemeen vragen dergelijke oplossingen echter een grote hoeveelheid rekenkracht en communicatie waardoor ze nog nauwelijks in de praktijk worden toegepast. Daar lijkt nu een einde aan te komen door de opkomst van *homomorfe encryptie*. Dat zijn encryptiesystemen die het mogelijk maken om bepaalde berekeningen te kunnen doen met vercijferde data zonder de tussenkomst van protocollen. Ook de Amerikaanse Defensie ziet het belang van deze techniek en heeft vijf miljoen dollar beschikbaar gesteld voor onderzoek [TheHN2011].
Onder andere via het COMMIT [COMMIT2011] programma, dat dit jaar is gestart, steekt de Nederlandse overheid veel geld in ICT-onderzoek. In een van de COMMIT-projecten, namelijk Trusted Healthcare Services (P15), worden expliciet technieken ontwikkeld om homomorfe encryptie praktisch toepasbaar te maken. In dit geval voor het gezondheidszorgdomein.
Dat betekent dat de komende vier jaar in Nederland hard kan worden gewerkt aan de doorontwikkeling van deze privacy-beschermende technieken.

Toepassing

Zoals gezegd is homomorfe encryptie een nieuwe techniek die het mogelijk maakt om te rekenen met vercijferde data. Het gaat te ver om hier uit te leggen hoe die asymmetrische encryptie precies werkt, maar stel bijvoorbeeld dat [x] de vercijfering voorstelt van bericht x, en [y] de vercijfering van bericht y. De belangrijkste eigenschap van homomorfe encryptie is dan dat je bijvoorbeeld de berichten x en y bij elkaar kunt optellen zonder ze te hoeven ontcijferen:

$$[x] * [y] = [x + y]$$

Door de cijferteksten [x] en [y] te vermenigvuldigen, krijg je de vercijfering van x + y. Encryptiesystemen met deze eigenschap worden *additief* homomorfe systemen genoemd. Op dezelfde manier zijn er ook *multiplicatief* homomorfe systemen waarmee je berichten met elkaar kunt vermenigvuldigen zonder ze te hoeven ontcijferen:

$$[x] * [y] = [x * y]$$

Het nadeel is dat een homomorf encryptiesysteem nooit beide eigenschappen tegelijk heeft. Het is ofwel additief homomorf, ofwel multiplicatief homomorf. Het kunnen rekenen met vercijferde data is dan beperkt tot optellen dan wel vermenigvuldigen. Om andersoortige rekenkundige bewerkingen te kunnen doen heb je weer cryptografische protocollen nodig en dat betekent interactie met de partij die in staat is om te ontcijferen.
Het ideale homomorfe encryptiesysteem kan berichten zowel optellen als vermenigvuldigen, en je kunt laten zien dat je daarmee alle mogelijke bewerkingen kunt uitvoeren die je maar wilt. Er wordt in de academische wereld momenteel gewerkt aan dergelijke systemen, die *volledig* homomorf worden genoemd, maar de eerste oplossingen vragen nog teveel rekenkracht.
Daarmee wordt dus ook duidelijk waar momenteel nog de schoen wringt. Homomorfe encryptie is namelijk een veelbelovende techniek om te kunnen rekenen met vercijferde data, maar in de praktijk ontkom je er nog niet aan om op een bepaald moment toch interactie te hebben met de partij die de decryptiesleutel heeft. Afhankelijk van de toepassing is dat de eigenaar van de data. Maar om gebruikers zoveel mogelijk te ontlasten kan het ook een tweede serviceprovider zijn die samen

met de eerste serviceprovider alle berekeningen uitvoert.
Een dergelijk model is te zien in fig. 1. Ter initiatie van de service sturen users hun vercijferde persoonlijke data naar een van de serviceproviders. Data richting serviceprovider 1 wordt vercijferd met de publieke sleutel van provider 2 en omgekeerd. De service providers, twee onafhankelijke organisaties, gaan via een protocol samen met die data rekenen zonder dat een van beide providers de data daadwerkelijk leert. Alle rekenkracht en communicatie concentreert zich tussen de twee providers. De users worden ontlast. Uiteindelijk wordt de output ter beschikking gesteld aan een van de partijen. In fig. 1 zijn de twee providers vergelijkbare rollen toegedicht. Het is echter ook mogelijk dat users alleen data naar serviceprovider 1 uploaden, en dan krijgt serviceprovider 2 meer een rol van onafhankelijke privacy serviceprovider die serviceprovider 1 helpt om op een privacy-vriendelijke manier diensten aan te bieden.

Voorbeelden van toepassingen met twee serviceproviders zijn:

- de Nederlandse overheid en de Duitse overheid die onderlinge databases van gezochte personen met een criminele achtergrond willen combineren om te kijken of er overeenkomsten tussen zitten;
- twee concurrerende aanbieders van diensten die userdata van de ander willen gebruiken om betere aanbevelingen te kunnen genereren;
- de overheid die gevoelige data van burgers ter beschikking stelt aan commerciële bedrijven die daar op een privacy-gevoelige manier waarde aan kunnen toevoegen;
- een provider van een sociaal netwerk gericht op bepaalde patiënten, die bij een content provider kan zoeken naar media die relevant kan zijn voor de patiënten.

Zoals gezegd heeft het ontbreken van volledig homomorfe encryptie tot gevolg dat af en toe intensieve cryptografische protocollen nodig zijn tussen twee onafhankelijke partijen. Dat kunnen de serviceprovider en de gebruiker zijn, maar wanneer de gebruiker intensieve berekeningen moet verrichten, gaat dat ten koste van de toepasbaarheid. Bovendien dragen ingewikkelde cryptografische protocollen die alleen door experts zijn te doorgronden doorgaans niet bij aan de transparantie richting gebruiker. Het model met twee serviceproviders biedt een mogelijkheid om die extra belasting niet bij de gebruiker neer te hoeven leggen. Wanneer de twee serviceproviders zouden samenwerken is het mogelijk om de gevoelige gebruikersdata te achterhalen, dus toepassing van dat model is voorlopig beperkt tot situaties waarbij de twee providers van nature niet geneigd zijn om informatie uit te wisselen maar toch het voordeel zien van samenwerking. Meer onderzoek is nodig om 'rekenen met vercijferde data' breder toepasbaar te maken en de benodigde hoeveelheid berekeningen en communicatie tot een minimum terug te brengen.

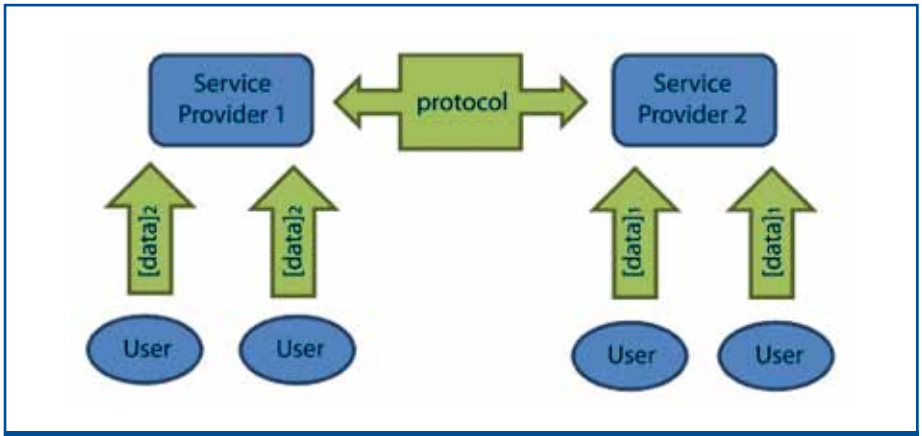


Fig. 1. Toepassing met twee service providers.

Conclusies

Door het toenemend aantal incidenten met gevoelige persoonlijke data groeit de behoefte aan privacybescherming. Er bestaat wetgeving die bedrijven dwingt om zorgvuldig met persoonlijke data om te gaan, maar bepaalde risico's lijken onvermijdelijk. Om zeker te zijn dat gevoelige data nooit uit zal lekken, zonder de kwaliteit van de dienstverlening aan te tasten, is rekenen met vercijferde data een veelbelovende techniek. Nieuwe toepassingen met zeer gevoelige data behoren dan tot de mogelijkheden.
Rekenen met vercijferde data is gebaseerd op een techniek die we homomorfe encryptie noemen. Deze veelbelovende techniek is ontstaan in de academische wereld en staat op het punt om zijn intrede te gaan maken in de hedendaagse praktijk. Bepaalde toepassingen met twee serviceproviders behoren al tot de mogelijkheden, maar omdat nog niet alle berekeningen met vercijferde data efficiënt kunnen worden gedaan, is er onderzoek nodig om de laatste stap richting toepassing te realiseren. De Nederlandse overheid erkent dit en investeert in de techniek door middel van het COMMIT-programma. Daar zal de toepassing worden toegesneden op de medische gezondheidszorg en zullen oplossingen worden bedacht om de transparantie richting gebruikers te verbeteren.

Referenties

CASoN, The International Conference on Computational Aspects of Social Networks, IEEE, *'Generating Private Recommendations in a Social Trust Network'*, Zekeriya Erkin, Thijs Veugen en Inald Lagendijk, isplab.tudelft.nl/content/generating-private-recommendations-social-trust-network, 2011.
COMMIT, www.commit-nl.nl/index.htm, 2011.
The Hosting News.com, DARPA invests 5 million towards solving homomorphic encrytion, www.thehostingnews.com/darpa-invests-5-million-towards-solving-homomorphic-encryption-17158.html, april 2011.

COLUMN

IK GEEF MIJN PRIVACY WEG, MAAR NIET VOOR NIETS!

Klakkeloos klikken. Klakkeloos tikken. In de online wereld geven wij onszelf bijna voor niets weg. Nog steeds klikken teveel mensen op allerlei nare links die ons worden voorgeschoteld. Vaak blijkt dan weer dat de sociale nieuwsgierige mens de zwakste schakel is. Scams die beloven dat je door [hier] te klikken kunt zien wie jouw Facebook-profiel het meest bekijkt, werken simpelweg omdat het een onweerstaanbaarheidsfactor in zich heeft. De mens in al haar ijdelheid wil graag weten wie naar hem kijkt. En in een klik en een zucht heeft de scam-artist jouw gegevens en trekt tegelijkertijd jouw vriendenlijst leeg. Twee vliegen in een klik.

Voor toegang tot een dienst, het gebruik van een vette nieuwe gadget of het kunnen bekijken van dat filmpje - zeg de laatste aflevering van die spannende serie die in Nederland nog niet is uitgezonden - tikken wij klakkeloos onze gegevens ergens in. Er zijn natuurlijk ook mensen die neptikken, maar het merendeel van de bevolking tikt nog steeds echt. Hoewel liegen iets zeer natuurlijks is en in de aard van de mens zit, blijken we online nog steeds zeer makkelijk ons 'echte zelf' in te tikken. Dat van dat liegen verzin ik overigens niet zelf, geïnteresseerden moeten er maar eens het werk van Genevieve Bell op naslaan.

Zijn de gevolgen reparabel? De gevolgen zijn inperkbaar, dat zeker. Als je dan toch zo nodig moest klikken (en zo gek is dat niet hoor), dan ging dat vaak gepaard met een 'toestemmingsklikje'. Je hebt de zogenaamde third party-app toegestaan contact te leggen met het Facebook-profiel (overigens geldt exact hetzelfde voor andere sociale sites). Die toestemming kan weer ingetrokken worden via de instellingen zodat verdere schade voorkomen wordt. Weggegeven gegevens blijven helaas gegeven. Dat is een feit wat toch nog steeds te weinig mensen zich lijken te beseffen. Je zou eens gebruik kunnen maken van de PIM om te kijken welke bedrijven wat van jou weten. Jaap-Henk Hoepman schreef er deze editie een mooi artikel over. Daarna kun je gebruikmaken van het recht op correctie en eventueel verwijdering. Mooie aanvullende rechten uit onze privacywet die helaas nog te weinig mensen kennen.

Als privacyrechtjurist ben ik zelf natuurlijk ook vaak bezig met denken over de sporen die ik achterlaat in de online wereld. Dat zijn er nogal wat. Ik ben vrij actief op verschillende sociale netwerksites en het is niet al te moeilijk om vrij veel over mij te weten te komen. Toch zijn er uiteraard veel dingen die ik niet prijsgeef. Althans… niet voor niets. Het werken aan deze privacyspecial, samen met veel andere auteurs, zette me aan het denken. Wat is ervoor nodig wil ik mijn privacy opgeven? En, hoeveel zou ik dan van mijzelf willen onthullen? Mogen mensen alles van mij weten? Wat is mijn prijs eigenlijk?

Voor een goed doel, bedacht ik me, zou ik best veel over mezelf willen prijsgeven. Maar ja, hoe doe je dat dan? Het is heel eenvoudig. U mag gaan bieden. Geld doneren. Aan een nog te bepalen goed doel. Uiteraard zal daar met behulp van het bestuur van het PvIB en de redactie met zorg over nagedacht worden. Twitter wordt het medium waarmee ik u op de hoogte zal houden. En waar mag u dan precies *voor* gaan bieden? Welnu, u mag mij alles vragen. **Ja, alles.** En dan bedoel ik dus echt dat geen vraag te gek is. Ik zal van de vijf hoogste bieders de vraag in alle openheid en eerlijkheid beantwoorden. Ik geef u mijn privacy, ik vertel u alles, maar dan alleen als u daar goed voor betaalt. Lex Borger, onze hoofdredacteur, zal er zorg voor dragen dat alles netjes verloopt en dat ook daadwerkelijk de – indien gewenst anonieme – vragenstellers voorzien worden van een eerlijk antwoord. Uiteraard te lezen hier op deze plaats in Informatiebeveiliging.

Misschien ten overvloede, maar ik blijf een privacydiva die zichzelf graag hoge doelen stelt. Al het geld dat u doneert moet bij elkaar opgeteld minstens 10.000 euro bedragen. Voor minder begint deze dame niet met het volledig prijsgeven van haar privacy. Bij een bedrag van 6000 euro beantwoord ik slechts 1 van de 5 vragen, voor 7000 euro 2, 8000 euro 3, 9000 euro 4 en voor 10.000 euro en meer worden alle 5 de vragen beantwoord. Hou mijn Twitter-account in de gaten voor het vervolg!

mr Rachel Marbus,
@RachelMarbus op Twitter

HET RECHT OP INZAGE IS EEN WASSEN NEUS. WAT NU?

Jaap-Henk Hoepman, Senior Scientist, TNO & Radboud Universiteit Nijmegen

Volgens de Wet bescherming persoonsgegevens (Wbp) heeft iedere burger het recht om inzage te krijgen in de persoonsgegevens die een organisatie over haar verwerkt. Tevens moet deze organisatie informatie geven over het doel van de verwerking, de herkomst van de persoonsgegevens, en een overzicht van organisaties waaraan deze gegevens eventueel zijn verstrekt. Recent heeft Bits of Freedom een tool gelanceerd waarmee burgers zo'n inzageverzoek eenvoudig kunnen genereren: de Privacy Inzage Machine (PIM)[1]

In het kader van het Privacy Seminar dat ik ieder voorjaar geef aan de Radboud Universiteit Nijmegen, heb ik mijn studenten begin 2011 gevraagd om bij een aantal organisaties gebruik te maken van dit recht. We hebben hiervoor een beta-versie van PIM gebruikt. Zelf heb ik dat ook gedaan.
Doel was om te kijken hoe organisaties met dergelijke inzageverzoeken omgaan. De conclusie is ontluisterend: dat doen ze beroerd. Het recht op inzage is in de praktijk een wassen neus.

Reageren op inzageverzoeken: de conclusie is ontluisterend, dat doen ze beroerd

We hebben de klantenservice van telecommunicatiebedrijven, verzekeringsmaatschappijen, webwinkels, supermarkten en dergelijke aangeschreven. De meerderheid (70% in deze beperkte steekproef) van de bedrijven en organisaties reageert simpelweg niet. Van de bedrijven en organisaties die wel reageren, kunnen we stellen dat de reactie zelden voldoet. Sommige bedrijven sturen geen brief maar bellen. Andere bedrijven sturen een e-mail, of een korte brief die niet ingaat op het verzoek maar enkel meedeelt: "Verder worden uw persoonsgegevens nooit vrijgegeven aan andere organisaties. U hoeft zich dus hierover geen zorgen te maken." We ontvingen ook een uitdraai van iets wat lijkt op een screenshot van een persooneelsadministratiesysteem. Daar staan wij niet in, inderdaad... De klantenservice van een ander bedrijf belt een student met de vraag of hij echt een inzageverzoek wil doen. De medewerker is al uren bezig met dit verzoek en nog steeds niet klaar.

De enige twee organisaties die het goed doen zijn de Gemeentelijke Basis Administratie (GBA) en Bol.com. Het antwoord van de GBA komt laat (na drie weken), maar bevat een uittreksel van alle gegevens die de GBA over de persoon in kwestie opgeslagen heeft, plus een overzicht van de gegevens die aan andere partijen zijn doorgegeven. Ook Bol.com reageert snel met een keurige brief met daarin alle gevraagde gegevens.

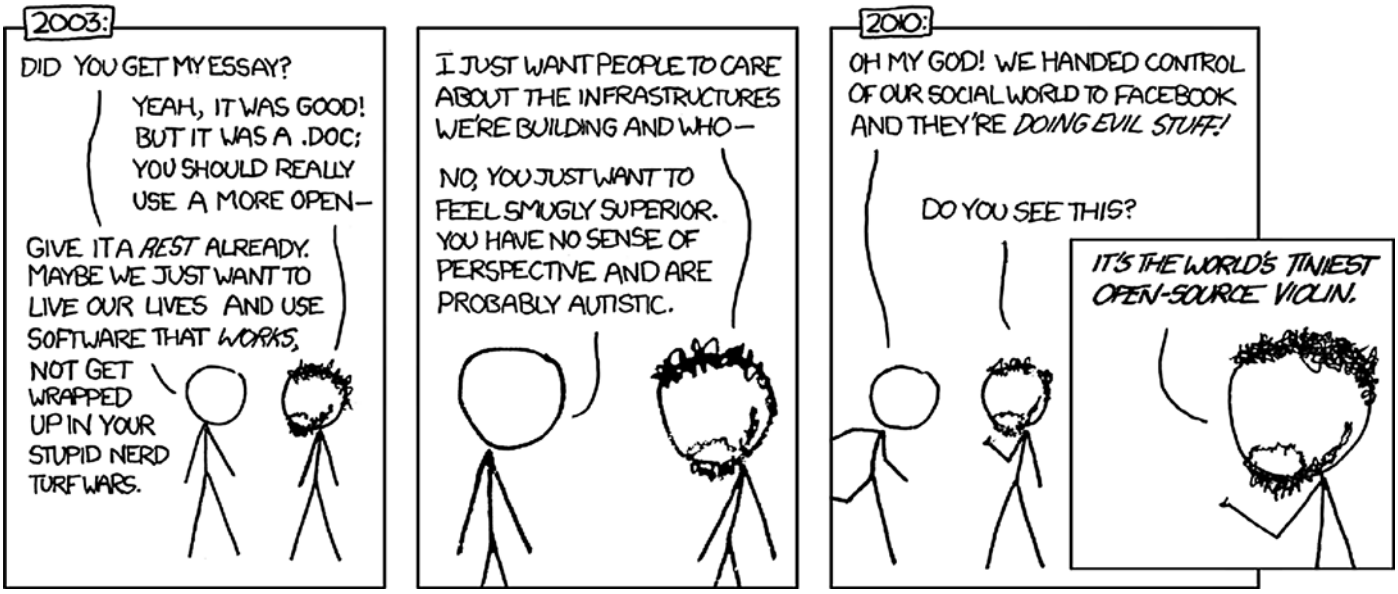
Kennelijk zijn er geen goede bedrijfsprocessen geïmplementeerd

Al met al een teleurstellend resultaat. Bedrijven zijn wettelijk verplicht binnen een redelijke termijn een verzoek tot inzage volledig te beantwoorden.
Waarom reageren ze dan zo onbeholpen? Dat kan liggen aan het feit dat bedrijven over het algemeen maar weinig inzageverzoeken ontvangen. Zo is bekend dat ook maar weinig mensen Google Dashboard raadplegen (om te kijken hoe Google omgaat met de persoonsgegevens die ze bewaart). En omdat ze maar weinig verzoeken tot inzage krijgen, hebben ze kennelijk geen goede bedrijfsprocessen geïmplementeerd om zo'n verzoek correct te beantwoorden.

Dat laatste is wel opmerkelijk, en eigenlijk ook wel zorgelijk, en onzorgvuldig. De PIM-tool van Bits of Freedom bevat alleen bedrijven die officieel hebben gemeld dat ze persoonsgegevens verwerken. Ook dit is een verplichting die voortvloeit uit de Wbp. Kennelijk melden bedrijven netjes de verwerking van persoonsgegevens, maar laten ze vervolgens na de noodzakelijke processen voor het verwerken van een inzageverzoek goed in te richten. Dan rijst toch de vraag of deze bedrijven überhaupt hebben nagedacht over de verwerking van persoonsgegevens. Weten ze wel precies welke persoonsgegevens ze allemaal verzamelen, en hoe en waar dat precies gebeurt?
Dit vergroot de kans op incidenten en privacyinbreuken van de klant. Immers, als je niet weet welke informatie je verzamelt, en waar je die opslaat, verwerkt en gebruikt, dan kun je die informatie ook niet afdoende beschermen.

Hoe deze situatie te veranderen?
Bedrijven zouden kunnen overgaan tot

[1] [https://pim.bof.nl/]



Randall Munroe - xkdc.com/743 (CC BY-NC 2.5)

het invoeren van een Enterprise Privacy Management Systeem (EPMS). Een eerste belangrijke stap daarbij is het vastleggen van het privacybeleid, in eerste instantie op een hoog niveau. Dit beleid wordt vervolgens uitgewerkt in gedetailleerde regels die voor elk type informatie aangeven welke operaties op die informatie mogen worden uitgevoerd, door wie, en onder welke condities. Daarnaast wordt geïnventariseerd binnen welke bedrijfsprocessen op dit moment persoonsgegevens worden verwerkt en of er wordt voldaan aan deze regels. Het EPMS kan dit deels automatisch doen, op basis van een formele beschrijving van deze processen. Ook wordt gecontroleerd of bepaalde noodzakelijke processen (zoals de mogelijkheid tot inzage) afdoende zijn geïmplementeerd. Vaak zullen IT-systemen moeten worden aangepast en moeten controls worden ingebouwd om naleving van de regels af te dwingen. Ook hierin kan het EPMS een belangrijke rol spelen, als centrale repository van het privacybeleid en de daaruit afgeleide regels.

Soms is het privacy management systeem (PMS) gecombineerd met het information security management systeem (ISMS) tot een geïntegreerd geheel. Dat kan kostenbesparend zijn, maar draagt ook een zeker risico in zich mee. Omdat ISMS'en al langer worden gebruikt, kan het er toe leiden dat privacy vooral in termen van security wordt gezien en geïmplementeerd. Of erger nog, dat privacy ondergeschikt wordt gemaakt aan security. Het moge duidelijk zijn dat privacy en security slechts deels overlappen qua doelstellingen en bijbehorende maatregelen.

Hebben deze bedrijven überhaupt nagedacht over de verwerking van persoonsgegevens?

Daarnaast zouden bedrijven ook online inzage in de persoonsgegevens van een klant kunnen bieden, zoals Google dat al deels met haar Dashboard doet, en zoals bepaalde webwinkels ook de aankoopgeschiedenis online tonen. Inzage wordt zo een primair proces. Voor consumenten is dit natuurlijk zeer gebruikersvriendelijk. Er schuilt hier echter wel een groot risico in. Ook kwaadwillenden hebben zo, in theorie, simpel toegang tot andermans persoonsgegevens. Zo raken we, qua privacy, van de regen in de drup.

Een dergelijke vorm van online inzage vraagt dus om een voldoende veilige vorm van authenticatie, om er zeker van te zijn dat het de klant zelf is die inzage in zijn gegevens vraagt. Gebruikersnaam en wachtwoord is hier niet altijd veilig genoeg voor. Denk bijvoorbeeld aan het Elektronisch Patiënten Dossier, financiële gegevens, of gegevens uit juridische dossiers. Voor inzage in dergelijke systemen is een sterkere vorm van authenticatie noodzakelijk. Een landelijke betrouwbare identiteitsinfrastructuur ontbreekt hiervoor op dit moment echter. DigiD is niet betrouwbaar genoeg, en systemen die op dit moment worden gebruikt voor internetbankieren zijn niet toepasbaar in andere sectoren.

Dit is meteen een interessant voorbeeld van het wellicht ironische feit dat soms een sterke vorm van authenticatie van *jouw* identiteit juist nodig is om je privacy te beschermen. De andere kant op ligt dat meer voor de hand. Een opsporingsambtenaar moet zich kunnen identificeren voordat je verplicht bent zelf je paspoort of rijbewijs te tonen. Sterke authenticatie van websites (door middel van TLS) is een ander voorbeeld van een maatregel die er voor bedoeld is om te voorkomen dat jouw persoonlijke gegevens in verkeerde handen vallen. Maar dat terzijde.

Soms is een sterke vorm van authenticatie juist nodig om privacy te beschermen

Volgend jaar testen we het recht op inzage nog een keer. Laten we er samen voor zorgen dat de bedrijven en organisaties in Nederland dan beter scoren.

"YOU HAVE ZERO PRIVACY ANYWAY, GET OVER IT."

Remco Bakker is sinds 1996 actief in de informatiebeveiliging en momenteel werkzaam als resource manager voor Cqure, detacheringsbedrijf voor IT Security professionals. Hij is bereikbaar via remco.bakker@cqure.nl.

Scott McNealy, de toenmalige CEO van Sun Microsystems deed deze uitspraak tijdens de introductie van Jini technology op 25 januari 1999. Deze uitspraak deed destijds veel stof opwaaien en er is veel over geschreven en gesproken. Commentaren varieerden van onbegrijpelijk tot onverantwoordelijk, maar ik heb destijds slechts weinigen horen zeggen dat hij er naast zat. Hardop althans...

Nu, in het kader van deze privacyspecial, is het wellicht een goed moment om nog eens bij zijn uitspraak stil te staan. Misschien begrepen we destijds nog niet de implicatie die het gebruik van het internet als carrier voor vrijwel al onze informatiestromen had, maar iemand als McNealy, wiens bedrijf als motto had 'The network is the computer' heeft dat ongetwijfeld voorzien. Meer waarschijnlijk lijkt mij, dat hij doelde op de feiten, zoals die ook toen al voorlagen. Ook destijds kocht ik boeken bij Amazon over security en kreeg ik aanbiedingen over van alles en nog wat, omdat de marketeers van Amazon mijn gegevens opsloegen en interpreteerden. Nee, ik heb nooit een boek over Nederland bij Amazon gekocht, maar mijn herkomst werd in ieder geval gebruikt, net als veel andere zaken. Waar McNealy echter de plank missloeg, is de houding ten opzichte van privacy. Zijn sneer op de RSA-conferentie richting zijn auditors die in februari 2006 een laptop kwijtraakten met daarop ook zijn social security nummer, was veelzeggend. Maar ook in Nederland heb ik in de afgelopen jaren veelzeggende reacties gehad over het onderwerp privacy en informatiebeveiliging. Wie herinnert zich nog, dat het RIVM in 2002 een Big Brotheraward in ontvangst mocht nemen omdat ze 1.4 miljoen bloedmonsters van kinderen hadden bewaard? Of dat in hetzelfde jaar de commissie MEVIS voorstelde om politie en justitie vergaande bevoegdheden te geven tot het vorderen van inlichtingen bij bedrijven en overheidsinstellingen?

> Omdat de marketeers van Amazon mijn gegevens opsloegen en interpreteerden

Hoewel iedere zichzelf respecterende professional de mantra C(onfidentaility) I(ntegrity) en A(vailabilty) kan opdreunen, is het nog maar twee jaar geleden dat ik als moderator van een discusssie over privacy met een select gezelschap van CISO's de discussie over privacy en informatiebeveiliging moest afsluiten met de conclusie, dat privacy niet het werkterrein van de CISO was. Op het eerste gezicht vreemd, maar bij nadere beschouwing wellicht toch begrijpelijk.

> Informatiebeveiliging vooral het domein van de cryptograaf

Naast een aanzet tot een definitie van privacy is het nuttig, om een korte blik op de historie van informatiebeveiliging te werpen. De privacy waar ik hier op doel, is de privacy die door de technologische ontwikkeling mede wordt vormgegeven. Zoals de opkomst van de brief heeft geleid tot het briefgeheim, zal ook de voortgaande digitalisering van onze maatschappij tot een nieuwe, verscherpte definitie van privacy moeten leiden. Eentje waarbij vooral de doelbestemming van de informatie, de opslag, de verwerking en het transport zodanig geregeld zijn, dat verder gebruik van de informatie niet mogelijk is.

World wide web

Toen ik in 1996 mijn entree in dit veld maakte, was informatiebeveiliging vooral het domein van de cryptograaf. Versleuteling van informatie was het hoogste goed, want de beveiliging van de mainframes waarop destijds de cruciale informatie werd bewaard, was zo goed geregeld (dacht men), dat er altijd voldoende tijd zou zijn om inbrekers te detecteren en gepaste maatregelen te nemen. Dat er intussen een woud van client servertoepassingen aan het groeien was en er zo iets in opkomst was als het world wide web, dat was aan velen voorbij gegaan. Het gevolg was, dat de mensen die begrepen hoe je een access control list op een router moest configureren ineens een leidende rol kregen, gevolgd door de bezorgde systeembeheerder die ontdekte, hoe eenvoudig de machines die aan hem waren toevertrouwd gecompromitteerd konden worden. Velen zullen zich nog de verhitte discussies over de onveiligheid van NT 4 kunnen herinneren en het dedain waarmee een ervaren UNIX-beheerder sprak over de beveiligingsmogelijkheden van het wintel-platform. Informatiebeveiliging

werd de kunst van het toegang verlenen, of platter gezegd, het verhinderen van ongewenste toegang. Daarnaast overspoelde e-mail als belangrijkste bedrijfscommunicatiemiddel de bureaus en schermen en wisten de kwaadwilligen al snel met behulp van virussen en andere malware veel van het beschikbare geld, aandacht en talent op te eisen. Privacy werd min of meer uitgekleed tot iets dat geregeld was, wanneer je de toegang tot informatie onder je voldoende afgeschermd was.

College Bescherming Persoonsgegevens

Ook de betrekkelijk lakse houding van de toezichthouder op dit gebied in die tijd, ofwel de lage financiële impact die een incident had, zal daarbij een rol hebben gespeeld. Helaas werd hierbij over het hoofd gezien, dat de informatie op de systemen zelf, nadat er toegang verkregen was, vaak in volle glorie door een ieder genoten kon worden. De vele incidenten die we de afgelopen jaren gekend hebben spreken wat dat betreft boekdelen. Zo is op de website van het College Bescherming Persoonsgegevens het volgende te lezen: *'Nederland behoort tot één van de Europese landen waar het slecht is gesteld met de bescherming van privacy. Het in toenemende mate tappen van telecommunicatieverkeer, het paspoort met biometrische gegevens en het delen en uitwisselen van gegevens maken dat Nederland samen met Zweden en het Verenigd Koninkrijk behoort tot de hekkensluiter van slechts presterende landen in Europa'* (mededelingen 9 november 2006).

Nu is het world wide web en het internetgebruik op zoveel plaatsen doorgedrongen en in zoveel technologie omarmd, dat het welhaast onmogelijk is om nog actief in de maatschappij te zijn, zonder. En daar ligt volgens mij ook de oorzaak van de veranderende houding ten opzichte van privacy. Privacy is namelijk een relatief nieuw begrip, niet alleen in onze digitale wereld, maar in onze maatschappij als geheel.

> Privacy is namelijk een relatief nieuw begrip

De ontwikkeling van het toilet is daar een mooi voorbeeld van. Lodewijk de XIVe ontving gasten zittend op zijn 'gemak', maar een toilet met riolering voor de massa kwam pas echt weer in ontwikkeling nadat in Engeland tienduizenden arbeiders overleden als gevolg van cholera. Of de gezondheid van de mensen of de gevolgen voor de productie hierbij het leidende motief is geweest, laat ik in het midden. Gesteld kan worden dat het grootschalige rampen geweest zijn, die verregaande veranderingen in het denken en regelgeving op hygiënisch gebied hebben bewerkstelligd. Privacy is wellicht ook zo'n gebied.

> Want als je niets te verbergen hebt…

Bestrijding van het kwaad

Na de begrijpelijke grootscheepse aantastingen van de grondrechten op het recht met rust gelaten te worden na de aanslagen op de Twin Towers in de Verenigde Staten in de vorm van de Patriot Act, leek het in eerste instantie zo dat de bestrijding van het grote kwaad van het terrorisme als een zegen voor de informatiebeveiliger kwam. Maar inderdaad op precies de manier, die ik hierboven al beschreef. Afschrikking, controle, maar niet de bescherming van de persoonlijke levenssfeer van de burger stonden voorop en in het verlengde daarvan bleven bedrijven en instanties druk doorgaan met het verzamelen van zoveel mogelijk informatie over klanten en burgers. Pas nu we beginnen te zien dat dit geen waarborg oplevert voor een veiliger (digitaal) bestaan, maar juist leidt tot schijnveiligheid, beginnen we de gevolgen van deze ramp ten volle te beseffen en komt privacy weer volop onder de aandacht. Het blijft echter een lastig onderwerp, want velen zullen betogen, dat in het algemeen belang, wij onze privacy zullen moeten opgeven. Want als je niets te verbergen hebt, dan heb je toch geen reden om te verhinderen dat er toegang tot je informatie, je wereld gezocht en gevonden wordt? Ga er maar aan staan als CISO, om die discussie aan te gaan in een wereld die met de dag onzekerder en onveiliger lijkt te worden. En dan ineens komt er toch een omslag in het denken. Begint de maatschappij, wij, zich te realiseren, dat al die informatie over ons, al die patronen, zoekgegevens, medische informatie, financiële gegevens, persoonlijke hobby's, voor- en afkeuren en zo meer persoonlijk zijn en horen te blijven. En in het verlengde daarvan komt ook de omslag in het denken van de CISO. Privacy komt hoog op de agenda te staan. We hebben dringend behoefte aan goede regels over wie, wat, waar met onze informatie, en informatie over ons doet en kunnen nu het voortouw nemen. En voor wie denkt, dat als je niets te verbergen hebt, je alles open kunt gooien heb ik een vraag. We accepteren dat er zaken misgaan, en dat er fouten worden gemaakt. Soms worden die bestraft, soms niet. Maar wil je serieus een (digitaal)leven, dat geen enkele fout meer toestaat, omdat alles genadeloos in de openbaarheid gebracht kan worden? Scott McNealy dacht misschien eerst van wel, maar kwam daar naderhand op terug. Wat mij betreft omarmen we de C van vertrouwelijkheid en zijn we als informatiebeveiligers de hoeders van de bescherming van de privacy.

> Informatiebeveiligers hoeders van de bescherming van de privacy

SOCIAL ENGINEERING EN PRIVACY

Ir Matthieu Paques CISSP CISA werkt als adviseur IT security bij KPMG IT Advisory. Hij houdt zich onder meer bezig met interne en externe security-testen, social engineering en specialistische beveiligingsonderzoeken. Hij geeft colleges en workshops met betrekking tot legal hacking en technische security-onderwerpen. Matthieu Paques is te bereiken via paques.matthieu@kpmg.nl

Tijdens een security-test maakt een adviseur gebruik van een zogenaamde keylogger (een soort mini USB-stick die tussen het toetsenbord en de pc wordt aangesloten) om hiermee inloggegevens van een medewerker te onderscheppen en daarmee toegang te krijgen tot het bedrijfsnetwerk. Wanneer de keylogger wordt uitgelezen, blijkt deze naast inloggegevens tot het netwerk, ook inloggegevens te bevatten van verschillende privé e-mailaccounts, enkele datingsites en zelfs de internetbankieromgeving van de medewerker (bijvangst). Hiernaast blijkt dat enkele privé e-mails getypt tijdens werktijd volledig op de keylogger zijn opgeslagen.

Doel van een security-test is veelal om vast te stellen of en in welke mate in beperkte tijd een aanvaller in staat is vertrouwelijke bedrijfsgegevens te verzamelen. Een dergelijke test kan beperkt zijn tot het gebruik van technische aanvalsmiddelen (ook wel een 'legal hack' genoemd) maar een tester kan ook gebruikmaken van bijvoorbeeld social engineeringtechnieken. Bij social engineering wordt gepoogd *medewerkers* in plaats van de techniek zo te manipuleren dat toegang wordt verkregen tot vertrouwelijke gegevens (of systemen). Verschillende van de schadelijkste security-incidenten zijn het resultaat van social engineering en social engineers. Niet hackers of crackers zijn volgens velen dan ook het grootste security-risico voor een organisatie.
Naast het verbeteren van de algehele security van een organisatie heeft een social engineeringtest een tweede belangrijk doel namelijk, het trainen en bewust maken van medewerkers van de technieken die social engineers kunnen gebruiken en hoe social engineeringaanvallen kunnen worden herkend en hoe hierop moet worden gereageerd. Doordat tijdens een social engineeringtest juist de medewerker het doelwit is, bestaat de kans dat de privacy van deze medewerker in het geding komt. De tester kan bijvoorbeeld ongewild in het bezit komen van allerlei privacy-gevoelige informatie zoals in bovenstaand voorbeeld.

Een aantal 'technieken' die een social engineer kan gebruiken zijn de volgende:

- een **band opbouwen** met het slachtoffer; mensen hebben de neiging ja te zeggen tegen personen die ze mogen;
- gebruik van (vermeende) **authoriteit/gezag**; mensen hebben de neiging verzoeken van hooggeplaatste personen sneller zonder vragen te stellen op te volgen;
- gebruik van **'herkenbare ' (vertrouwde) zaken**; mensen hebben de neiging het gedrag van collega's (of waarvan ze aannemen dat het collega's zijn doordat deze dezelfde stijl van kleding dragen, een (al dan niet gekopieerde) toegangsbadge, visitekaartjes, jargon, kennis van werkwijze of namen van informatiesystemen kennen) te volgen;
- het aanbieden van iets dat (verondersteld) zal leiden tot een **persoonlijk voordeel**.

Bij elk van deze genoemde technieken is *informatie* over het slachtoffer essentieel. Bij een social engineeringtest wordt daarom in de voorbereidende fase zoveel mogelijk informatie verzameld over relevante medewerkers van de te onderzoeken organisatie. Sociale media als Facebook, Hyves, Twitter zijn hierbij veelal een belangrijke informatiebron. Met deze informatie kan vervolgens een specifiek op de medewerker gerichte aanval worden uitgevoerd. Twittert de medewerker dat deze tennis speelt? Dan kan de social engineer hem (of haar) bijvoorbeeld 'namens de tennisbond' een gratis USB-stick als nieuwjaarsgeschenk sturen, uiteraard voorzien van de laatste malware. Wanneer de medewerker de USB-stick aansluit wordt zijn of haar systeem volledig gecompromitteerd. Alternatief kan de medewerker bijvoorbeeld via e-mail of telefoon worden benaderd om met een smoes meer (mogelijk privacy-gevoelige gegevens) los te krijgen.
In de praktijk blijkt, hoe meer informatie bekend is over relevante medewerkers, des te groter de kans op een (voor de tester) succesvolle aanval. Doordat de scheiding tussen werk en privé met het gebruik van ook sociale media op het werk met toenemende mate kleiner wordt, kan met het verzamelen van informatie mogelijk ook de privacy van de persoon in kwestie worden geschaad. De tester dient hier een goede afweging te maken welke informatie in het kader van het onderzoek wel en niet dient te worden verzameld. Enerzijds kan juist 'privé'-informatie

over een medewerker een cruciale rol spelen in een social engineeringaanval. Tijdens een 'echte' aanval zal een aanvaller ook niet schuwen deze informatie te gebruiken en kan het essentieel zijn een reëel beeld te krijgen van de daadwerkelijke risico's. Anderzijds dient te worden afgewogen in welke mate de mogelijke inbreuk op de privacy van het slachtoffer in kwestie opweegt tegen de belangen van het onderzoek en hoe deze inbreuk zo veel mogelijk kan worden beperkt (bijvoorbeeld door in alle gevallen anoniem te rapporteren). Een belangrijke rol speelt dan ook hoe de gebruiker zelf met de betreffende informatie omgaat. 'Privé' is immers niet voor iedereen hetzelfde. Wat de een als privé beschouwd, plaatst een ander rustig voor de hele wereld leesbaar op Facebook of Twitter. De vraag bij deze afweging is dan ook vooral niet *welke* informatie te gebruiken, maar meer *hoe en waar* deze informatie is verkregen.
Nadat tijdens een security-test toegang is verkregen tot de desktop van een van de systeembeheerders, blijkt de betreffende beheerder een map met enkele honderden megabytes aan persoonlijke bestanden te hebben. Enerzijds kan het handmatig doorzoeken van deze bestanden de privacy van de gebruiker schaden, anderzijds leert de ervaring dat gebruikers (en zeker systeembeheerders die tientallen wachtwoorden dienen te onthouden) deze vaak in een tekstbestand opslaan. Het achterhalen van deze wachtwoorden kan dan een waardevolle stap in het kader van de test zijn. Het geautomatiseerd doorzoeken van de map naar bestanden met bijvoorbeeld 'wachtwoord' of 'password' in het bestand kan dan een afweging van de tester zijn om zo aan beide tegemoet te komen.

> Bij social engineering is informatie over het slachtoffer essentieel

Wetgeving
Een ander relevant aspect waarmee de security-tester rekening dient te houden is de wetgeving. Er bestaat in Nederland geen algemene 'privacy wet'. De verschillende aspecten van de privacy worden geregeld in de volgende wetten:
de **Wet Bescherming Persoonsgegevens** (WBP), waarin is geregeld hoe persoonsgegevens mogen worden opgeslagen en verwerkt;
de **Wet Computercriminaliteit** en telecommunicatiewet. Hierin staan onder andere regels over aftappen en afluisteren;
de **Grondwet**, waar onder andere het briefgeheim in is geregeld.

In de **Wet Bescherming Persoonsgegevens** is vastgelegd dat persoonsgegevens alleen mogen worden opgeslagen en verwerkt als de betrokkene is geïnformeerd. De wet betreft echter 'geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.' En het is daarmee de vraag of deze op het (tijdelijk) verzamelen en verwerken van persoonsgegevens voor een social engineeringtest van toepassing is.

Regels met betrekking tot het aftappen en afluisteren van gegevens zijn opgenomen in de **Wet Computercriminaliteit**. Hieronder valt onder andere het aftappen van netwerkverkeer en telefoongesprekken. Ook het afluisteren van iemands voicemail valt onder aftappen. Er is volgens de wet alleen sprake van 'aftappen' als met een *technisch hulpmiddel* een kopie van het dataverkeer wordt gemaakt. Merk op dat ook het plaatsen van afluisterapparatuur (bijvoorbeeld een keylogger, verborgen microfoon of trojaans paard) al strafbaar is. Er hoeft dus niet al daadwerkelijk data te zijn onderschept.

De wet maakt een uitzondering voor het opvangen van signalen in de ether, dit is niet strafbaar tenzij je een 'bijzondere inspanning' moet leveren om de signalen te kunnen interpreteren (bijvoorbeeld decoderen). Het afluisteren van bijvoorbeeld draadloze DECT-telefoons is dus niet toegestaan.
Voor het afluisteren of opnemen van gesprekken tussen mensen (al dan niet telefonisch) zijn aanvullende regels in de wet opgenomen. In een besloten omgeving (woning) mag iemand die zelf geen deelneemt aan het gesprek dit gesprek niet opnemen. Daarbuiten mogen gesprekken alleen worden opgenomen indien dit van tevoren wordt aangekondigd. Deelnemers aan gesprekken mogen deze wel stiekem (laten) opnemen. Het is echter niet zo dat een rechtmatig gemaakte opname ook zomaar mag worden gepubliceerd.

Keyloggers waarmee toetsaanslagen kunnen worden onderschept.

In de **Grondwet** staan regels met betrekking tot het briefgeheim. Het briefgeheim is echter niet van toepassing is op e-mail en daarom over het algemeen niet relevant tijdens het uitvoeren van een security-test.

Filmen en fotograferen van mensen
Volgens het Wetboek van Strafrecht is filmen of fotograferen met een *aangebrachte camera* alleen toegestaan wanneer dat is aangekondigd. Dit geldt echter alleen voor publiektoegankelijke ruimtes (winkels, bioscopen en dergelijke) en op straat. Het Wetboek spreekt specifiek over *aangebrachte camera's*. Met andere woorden; camera's die permanent aanwezig zijn. Met een draagbare camera mag je dus wel onaangekondigd filmopnamen of foto's maken.

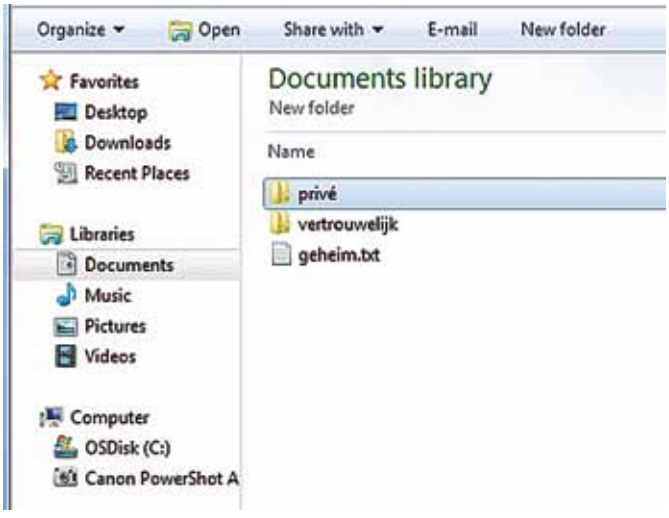
In besloten ruimtes (dus ook op het werk) mogen mensen niet zomaar worden gefilmd mits hier een 'zwaarwegend belang' is. Dit geldt voor zowel aangebrachte camera's als draagbare camera's. Voor het gebruik van (verborgen) spionagecamera's tijdens een security-test dient een belangenafweging te worden gemaakt tussen de inbreuk op de privacy van de betrokkene en het belang van de test. Bij voorkeur worden bij een dergelijke test ook personen niet (herkenbaar) in beeld gebracht en wordt bijvoorbeeld de camera gericht op het toetsenbord van de gebruiker zodat bijvoorbeeld alleen het intypen van het wachtwoord wordt opgenomen.
Ook voor film- en foto-opnamen geldt dat een rechtmatig gemaakte opname niet zomaar mag worden gepubliceerd. Wanneer de persoon herkenbaar aanwezig is kan dit een schending van het portretrecht betekenen. Publicatie mag dan alleen wanneer de privacy van de betreffende medewerker niet in gevaar komt.

Afspraken met werkgevers inzake het uitvoeren van een security-test
Wanneer een security-tester wordt ingehuurd door een bedrijf tekent het bedrijf over het algemeen een vrijwaringsverklaring (ookwel 'get out of jail free card') waarmee de tester wordt geautoriseerd bepaalde handelingen uit te voeren tijdens de test die normaal gesproken in strijd zijn met de wet (zoals het inbreken op computersystemen). De werkgever heeft echter over het algemeen niet zonder meer het recht om de tester toe te staan thuis telefoons van werknemers af te tappen, persoonlijke e-mails te lezen of op andere indringende wijze inbreuk te maken op de privacy van medewerkers.

Privacy van werknemers
Bij een security-test is het echter vooraf niet altijd vast te stellen of onderschepte data privédata van werknemers bevat. Door een vervaging van de grenzen tussen werk en privé regelen steeds meer werknemers allerlei privézaken tijdens werktijd en vanaf kantoor. Hetzelfde geldt voor het tijdens een test inbreken op een bedrijfs-pc. Mogelijk staan hier tevens privébestanden op. Het in aanraking komen met privébestanden tijdens een test is dan ook onvermijdelijk.

> Wat de een als privé beschouwt plaatst een ander rustig voor de hele wereld leesbaar op Facebook of Twitter

Werknemers delen zelf ook veel informatie. Wanneer je veel informatie deelt op profielsites als LinkedIn of Facebook vergroot je hiermee de kans dat je slachtoffer wordt van een social engineeringaanval. Waar je wellicht zou verwachten dat informatie die je deelt op bijvoorbeeld LinkedIn alleen zichtbaar is voor een selecte groep mensen (bijvoorbeeld je eigen netwerk) is dit niet altijd terecht. LinkedIn staat bijvoorbeeld search engines als Google toe je (automatisch gegenereerde) public profile-pagina te doorzoeken. Wanneer deze niet door de gebruiker handmatig wordt verwijderd, is via deze route evengoed allerlei profielinformatie zichtbaar. Vanuit dit oogpunt is het tevens af te raden LinkedIn of andere uitnodigingen van onbekenden te accepteren. Deze hebben na accepteren immers toegang tot alle informatie in je profiel waaronder alle relaties. Deze informatie maakt het de social engineer aanzienlijk makkelijk om je vertrouwen te wekken en informatie los te krijgen die je alleen met een bekende zou delen.
Een andere truc die zeer succesvol is gebleken is de volgende. Veel mensen hebben accounts op meerdere sociale media: Hyves, Facebook, LinkedIn enz. Wanneer je toegang wilt krijgen tot iemands profiel (bijvoorbeeld op Facebook) kan je je als



Werknemers slaan vaak ook privébestanden op bedrijfspc's op.

Dit lijkt een autosleutel, maar is in werkelijkheid een camera waarmee ongemerkt foto's en video's gemaakt kunnen worden.

een volkomen onbekende aanmelden en deze persoon een uitnodiging sturen. Wanneer deze persoon echter ook op een ander social medium aanwezig is, is het eenvoudiger om een van de vrienden (bijvoorbeeld op Hyves) van deze persoon te zoeken die *niet* op Facebook aanwezig is. Maak nu vervolgens een account aan onder naam van de vriend/vriendin van Hyves, kopieer enige noodzakelijke info en foto's, en het geselecteerde slachtoffer op Facebook zal je uitnodiging hartelijk aannemen en je toegang geven tot het volledige profiel. Sterker nog, wellicht dat via personal messages 'namens' de bekende nog wat verdere persoonlijke vragen kan stellen via 'persoonlijke' Facabook berichten … dag privacy.
Een interessant aspect van sociale media is de mogelijkheid anoniem te zijn en je als een ander voor te doen. Wanneer bijvoorbeeld het slachtoffer recentelijk is gescheiden of vrijgezel is geworden kan je een goeduitziende jonge dame zijn die op zoek is naar nieuwe vrienden. Combineer het feit dat je alles en iedereen kan zijn op social media met het feit dat de meeste mensen gewoonweg alles geloven maakt dit tot een interessante aanvalsmethode voor een social engineer.
Een andere interessante site om te noemen in dit kader is www.icanstalku.com. Deze site zoekt Twitter af naar gebruikers die foto's posten, genomen met hun smartphone. In deze foto's wordt mogelijk de GPS-locatie van de gebruiker opgeslagen, waarmee op het moment van posten de locatie van de gebruiker kan worden vastgesteld, mogelijk zonder dat de gebruiker zich hiervan bewust is. Voor een inbreker (of in dit geval social engineer) kan dit zeer waardevolle informatie zijn.
Dat medewerkers zich veelal niet bewust zijn van het onder valse voorwendselen verstrekken van privacygevoelige gegevens blijkt uit de hoge percentage reacties tijdens phishingonderzoeken. Bij een van deze onderzoeken konden medewerkers een van hun collega's nomineren voor de 'medewerker van de maand verkiezing'. In een online formulier konden medewerkers hun favoriete medewerker nomineren en aangeven waarom deze volgens hen een prijs zou moeten winnen. De applicatie was afgeschermd met gebruikersnaam en wachtwoord. Via e-mail werd een uitnodiging om deel te nemen aan deze verkiezing rondgestuurd. Van de medewerkers die de e-mail hadden geopend bleek ruim 60% hun (echte) gebruikersnaam en wachtwoord zonder aarzelen in te vullen op de website.

Informatie leidt tot informatie

Elk klein stukje informatie is waardevol voor een social engineeringaanval. Een onbelangrijke e-mail in het oud papier lijkt misschien op zichzelf niet waardevol, echter social engineering is een redundant proces waar elk stukje informatie weer wordt gebruikt om nieuwe informatie te verzamelen. Een e-mail geeft bijvoorbeeld informatie over hoe de e-mailadressen zijn opgebouwd. De social engineer kan nu vervolgens e-mail adressen van andere medewerkers 'raden' door namen van medewerkers die zijn verzameld op LinkedIn of Facebook te combineren met de informatie over de manier waarop de mailadressen worden opgebouwd. Vervolgens kan de aanvaller deze medewerkers een e-mail sturen vanaf een vervalst adres met dezelfde opbouw zodat het lijkt alsof deze vanaf een vertrouwd adres komen. Een social engineer kan zich bijvoorbeeld voordoen als een recruitment-agent, een medewerker van IT-support of van het ISP abuse team en de medewerker onder druk zetten vanwege 'geconstateerd ongepast surfgedrag'. Elk van deze scenario's kunnen leiden tot meer waardevolle informatie over het bedrijf en de betreffende medewerker zelf.
Een probleem is dat mensen zich vaak niet realiseren dat hun privégegevens gebruikt zijn en of dat ze slachtoffer zijn geworden van een social engineeringaanval. Wanneer ze dit wel merken is de kans groot dat ze dit niet melden uit angst voor represailles van de werkgever of zelfs maatregelen nemen om ontdekking te voorkomen en ze daarmee de social engineer feitelijk nog meer helpen. Vanuit een organisatie is het dus in het bijzonder aan te bevelen medewerkers die vermoeden slachtoffer te zijn geworden van een social engineeringaanval te stimuleren dit zo snel mogelijk te melden en hier goede procedures voor in te richten.
Een organisatie dient zich bewust te zijn dat wanneer een medewerker slachtoffer wordt van social engineering dit dient te worden gezien als het falen van processen en procedures en niet als het falen van het individu. Hoewel dit een belangrijk aspect is blijft de beste remedie het trainen van medewerkers om social engineering aanvallen te herkennen en bewust te maken terughoudend te zijn in het delen van persoonlijke gegevens.

IEDEREEN HEEFT IETS TE VERBERGEN

EN BEGRIJPT DAT EINDELIJK...

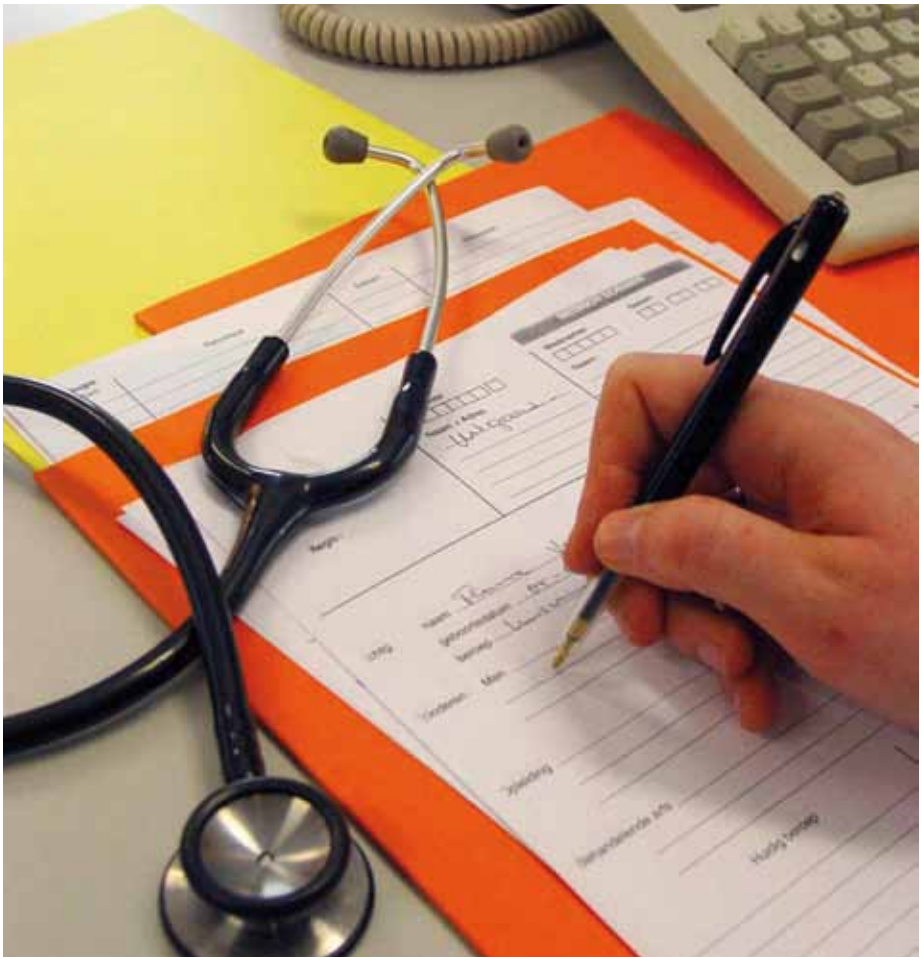
Bart de Koning (1967) is freelance journalist en spreker. Hij studeerde economie aan de Universiteit van Amsterdam. De Koning schreef onder andere voor Algemeen Dagblad, Quote, FemBusiness en HP/De Tijd. Van zijn hand verschenen bij Balans Operatie Blauw: weg met de bureaucratie bij de Nederlandse politie en Alles onder controle. De overheid houdt u in de gaten. Van dit boek verscheen in mei een geactualiseerde versie. Bart is te bereiken via Bart.de.Koning@planet.nl.

Privacy is binnen een paar jaar tijd van een obscuur onderwerp veranderd in voorpaginanieuws. Denk maar aan actuele dossiers zoals Google Streetview, Deep Packet Inspection door telecombedrijven, de opslag van vingerafdrukken, het Elektronisch Patiënten Dossier of winkeliers die beelden van inbrekers op internet zetten. Die maatschappelijke discussie over privacy is alleen maar toe te juichen, want door de voortschrijdende techniek zullen er nieuwe dilemma's op ons af blijven komen.

Dat was even schrikken voor de 'reaguurders' op GeenStijl, begin augustus. "Er komt een pro-criminelenwet aan. Het ministerie van Justitie sleutelt momenteel aan een wetsvoorstel dat de digitale schandpaal strafbaar maakt," zo schreef het weblog. Winkeliers die beelden van een overvaller of winkeldief op het internet zetten kunnen binnenkort een boete van 25 mille tegemoet zien. En dat alles onder politieke verantwoordelijkheid van staatssecretaris Fred Teeven. De redactie van GeenStijl en de reaguurders waren verbijsterd. Fred Teeven die het opneemt voor de privacy van criminelen? Dezelfde Fred Teeven die jarenlang in ieder interview over privacy riep: "Wie niets te verbergen heeft, hoeft nergens bang voor te zijn?" Dezelfde Fred Teeven die in een discussie met Alexander Pechtold had gezegd dat er wat hem betreft best méér privacybeperkende maatregelen mogen komen? Precies, die Fred Teeven. Ook het conservatieve blog De Dagelijkse Standaard had er geen goed woord voor over. Onder de kop "Teeven aan de iSchandpaal" beschuldigden ze de staatssecretaris van 'onduidelijke PvdA-speak'. Een zware beschuldiging in die kringen.
Een paar weken daarvoor, in juli, uitte Teeven kritiek op de afspraken die de Europese Unie en de Verenigde Staten hadden gemaakt over het uitwisselen van passagiersgegevens in het kader van de terrorismebestrijding. Hij vindt die regeling veel te ver gaan. De Amerikanen willen te veel gegevens hebben van Europese burgers en ze slaan die ook nog eens veel te lang op.

Even wennen: Teeven die het opneemt voor privacy

Het is voor vriend en vijand even wennen, Teeven die het genuanceerd opneemt voor privacy. Op de rechterflank van de VVD werd hij altijd zeer gewaardeerd om zijn bikkelharde aanpak van criminaliteit. Althans, tot voor kort. Onder privacy-voorvechters was hij altijd 'the man you love to hate'. Een debatavond over privacy was niet compleet zonder Fred Teeven in het panel. Hij was als geen ander in staat om met



een paar ongenuanceerde uitspraken de hele zaal op stang te jagen, zo heeft de schrijver van dit stuk persoonlijk mogen ondervinden.

De omslag

Het voortschrijdend inzicht van Teeven is typerend voor deze tijd. Een paar jaar geleden was privacy een onderwerp waar Nederlandse media nauwelijks aandacht aan besteedden. Na 9/11 stapelden politici de ene maatregel na de andere op elkaar in de strijd tegen het terrorisme. Denk aan het aanleggen van databanken, bestandskoppelingen, scanapparatuur, beveiligingscamera's, preventief fouilleren en de identificatieplicht. Protest was er nauwelijks, wie bezwaar maakte kreeg het verwijt kennelijk vóór terrorisme en misdaad te zijn. Ook buiten het veiligheidsdomein bestond er nauwelijks belangstelling voor privacy. Het Elektronisch Patiënten Dossier en de slimme elektriciteitsmeter zijn sprekende voorbeelden van technocratische projecten die onverstoorbaar doorgezet werden, zonder noemenswaardige politieke of maatschappelijke aandacht voor de zeer aanzienlijke privacybezwaren die eraan kleefden. Inmiddels is er een duidelijke omslag gekomen, waarvan Fred Teeven het meest opvallende en zichtbare voorbeeld is. De slimme elektriciteitsmeter, het Elektronisch Patiënten Dossier en de centrale opslag van vingerafdrukken van alle Nederlanders zijn de afgelopen tijd allemaal gesneuveld in het parlement. Het zijn stuk voor stuk dossiers waar de volksvertegenwoordiging een paar jaar geleden vrijwel geruisloos in meeging omdat privacy electoraal totaal niet interessant was. Nu buitelen parlementariërs over elkaar heen met maatregelen om consumenten te beschermen tegen opdringerige cookies en Deep Packet Inspection, het 'lezen' van e-mail en internetverkeer door providers. "Privacy is het nieuwe groen", kopte De Pers een tijdje geleden. Het is ineens hip geworden.

> Bezwaar? Dan kennelijk vóór terrorisme en misdaad

Nederland is een normaal land

Er is niet één eenduidige reden aan te wijzen voor die omslag in het denken over privacy in Nederland. Nederlanders waren van oudsher altijd nonchalanter over de bescherming van hun persoonlijke levenssfeer dan andere Europeanen. In Duitsland is bijvoorbeeld de herinnering aan de Stasi nog vers en hoefden politici niet aan te komen met dooddoeners als "wie niets te verbergen heeft, hoeft nergens bang voor te zijn". Voor de Stasi was geen detail te onbenullig om op te slaan en eventueel tegen mensen te gebruiken. Er was een fikse reeks schandalen, cyberfraude, datalekken en hacks voor nodig om de Nederlandse bevolking duidelijk te maken dat iedereéén dingen te verbergen heeft. Al was het maar je creditcardnummer en je pincode. Niemand wil dat zijn medisch dossier op straat komt te liggen. Of dat inbrekers van een afstand draadloos 'slimme' elektriciteitsmeters kunnen uitlezen en dus moeiteloos kunnen zien wie er in de straat wel en niet thuis zijn. De voortdurende publiciteit over beveiligingsproblemen rond de OV-chip maakten duidelijk dat ook grote prestigeprojecten van de overheid vaak knullig in elkaar zitten. Door al die privacyschandalen is Nederland op een normaal land gaan lijken, waarin burgers de plannen van hun overheid met wat meer gezond wantrouwen en scepsis bekijken.

> Er was een fikse reeks schandalen nodig

Verzamelen van data

Internationaal zorgde Wikileaks voor een enorme schok. Het liet zien hoe makkelijk het is geworden om in een klap enorme hoeveelheden data te kopiëren en te lekken, en hoe moeilijk het is om dat te voorkomen. Maar Wikileaks is veel meer dan een gigantisch lek, het maakt pijnlijk duidelijk wat voor fundamentele dilemma's het grootschalig verzamelen en opslaan van data met zich meebrengt. Hoe is het bijvoorbeeld mogelijk dat een gewone soldaat als Bradley Manning in een verre uithoek van Irak de beschikking had over zoveel vertrouwelijke gegevens uit zoveel verschillende bronnen? Het is een duidelijke schending van het bekende need-to-know-principe waar politie- en inlichtingendiensten vanouds mee werken. Mensen krijgen alleen de beschikking over die informatie die ze nodig hebben om hun werk te doen. Het is een gezondverstand-regel: wat

iemand niet weet, kan hij ook niet lekken. Ironisch genoeg was het een bewuste beslissing van de Amerikanen om die aloude regel na 9/11 flink op te rekken. Uit onderzoek na de aanslagen op de Twin Towers bleek dat de meeste kapers al in beeld waren bij Amerikaanse inlichtingendiensten, maar dat door bureaucratie, versnippering en ambtelijke stammenstrijd de puzzelstukjes nooit bij elkaar waren gelegd. Wilden de Amerikaanse inlichtingendiensten en strijdkrachten een volgende terroristische aanslag effectief voorkomen, dan moest de beschikbare informatie dus zo breed mogelijk worden verspreid. Vandaar dat een eenvoudige soldaat op divisieniveau vrijelijk over een zee aan vertrouwelijke gegevens kon beschikken.

Dat roept veel fundamentele vragen op, waar geen makkelijke antwoorden op zijn. Als het verzamelen en analyseren van vrijwel onbeperkte hoeveelheden data een van de belangrijkste instrumenten is in de strijd tegen terrorisme en misdaad, hoe gaan we dan om met die informatie? Nederlandse inlichtingendiensten en politiekorpsen hebben de afgelopen jaren een onverzadigbare honger naar meer data laten zien. In het rapport *Data voor daadkracht* signaleerden experts in 2007 al fijntjes dat de stijging van het aantal opgevraagde gegevens veel sterker is dan de stijging in het aantal opgehelderde misdrijven. Het is dus niet erg effectief: 'Door onvoldoende samenwerking worden naar alle waarschijnlijkheid verbanden over het hoofd gezien en kansen in de strijd tegen criminaliteit en terrorisme gemist.' Dat is dus hetzelfde probleem waar de Amerikanen vóór 9/11 ook mee worstelden. In 2010 trok de Inspectie Openbare Orde en Veiligheid snoeiharde conclusies over de automatisering bij de Nederlandse politie. Rechercheurs bleken cruciale informatie in schaduwsystemen te bewaren of bewust 'weg te schrijven' met een te hoog beveiligingsniveau, zodat collega's bij andere korpsen er niet bij kunnen. "Dit tast de kwaliteit van de opsporing en de handhaving aan en heeft daardoor gevolgen voor de effectiviteit van het politiewerk," concludeerde de Inspectie vorig jaar. Rechercheurs die informatie weghouden uit centrale databanken ondermijnen de effectiviteit ervan, maar, en dat moet ook gezegd, het is logisch dat ze vertrouwelijke informatie willen beschermen tegen Bradley Manning-achtige toestanden. En niet ten onrechte.

Privacy-problemen?

Dit zijn, zoals gezegd, heel wezenlijke dilemma's die voortdurend terugkeren. Een voorbeeld. In de discussie over de uitwisseling van passagiersgegevens begrijpen de Amerikanen werkelijk niet waarom de Europeanen zich zo'n zorgen maken over de privacy van de passagiers. Voor de Amerikaanse regering is het opslaan van de gegevens op zich geen probleem. Zij vinden dat er pas een privacy-probleem ontstaat op het moment dat die passagiersgegevens op straat komen te liggen, bijvoorbeeld na een hack of door toedoen van een klokkenluider à la Manning. Aangezien er nog nooit problemen van dien aard zijn geweest met de databank met passagiersgegevens, zijn er dus ook geen privacy-problemen. Dit is ook de boodschap die een Amerikaanse delegatie afgelopen juni bracht tijdens een rondreis langs Europese hoofdsteden om de geesten hier rijp te maken voor het uitwisselen van meer gegevens.

Lichtpunten

De pessimisten in het privacy-debat worden hier somber van. Zie je wel, het verzamelen van gegevens gaat gewoon door en het wordt steeds erger. De optimisten zien juist lichtpunten. Een paar jaar geleden voerde Washington antiterrorismemaatregelen gewoon in, desnoods zelfs zonder bondgenoten in te lichten. Nu reizen ze met een zware delegatie door Europa om hun beleid tot ver achter de komma toe te lichten. Dat is ook nodig, want zelfs houwdegens als Fred Teeven zijn tegenwoordig kritisch over privacy. Het debat over privacy is in een paar jaar tijd veel volwassener geworden. En dat is maar goed ook, want het zal in de nabije toekomst nog vaak moeten worden gevoerd. Nieuwe ontwikkelingen en nieuwe technieken (DNA, gezichtsherkenning, lichaamsscans) blijven nieuwe dilemma's oproepen. Oude dilemma's (informatie zoveel mogelijk verspreiden of juist niet) blijven steeds opnieuw opduiken. Dat privacy een belangrijk grondrecht is, is nu gelukkig wel overal doorgedrongen. En iedereen die dat grondrecht wil inperken moet er een héél goed verhaal bij hebben.

Het debat over privacy in een paar jaar tijd veel volwassener

2 - 3 NOV 2011 JAARBEURS UTRECHT

VAKBEURS, SEMINARS EN ONLINE MATCHMAKING VOOR IT-MANAGERS EN IT-PROFESSIONALS

IT SECURITY
INFOSECURITY.NL

Drie toonaangevende vakbeurzen onder één dak

infosecurity.nl NETHERLANDS

STORAGE EXPO

TOOLING EVENT

INFOSECURITY.NL 2011:
DÉ OPLOSSING VOOR AL UW SECURITY-VRAAGSTUKKEN

Bijblijven op uw vakgebied? Kom dan op 2 en/of 3 november naar dé vakbeurs over IT-security van Nederland.

- Ca. 100 exposanten met de laatste innovaties uit de branche
- Keynote sessies door o.a. Sophia Schwarz, Nederlands Instituut voor Forensische Psychiatrie (NIFP) (Pieter Baan Centrum)
- Uitgebreid seminarprogramma
- Case studies / solution sessions
- Ook toegang tot het gelijktijdige Storage Expo en het Tooling Event

Be secure. Be there. Op 2 en 3 november 2011 in Jaarbeurs Utrecht.

Gratis naar de beurs?
Meld u dan nu aan via www.infosecurity.nl!

DIRECT NAAR DE SITE?
SCAN DE QR-CODE:

Reed Exhibitions

vnu exhibitions europe

DE SOCIALE KRINGEN VAN GOOGLE+

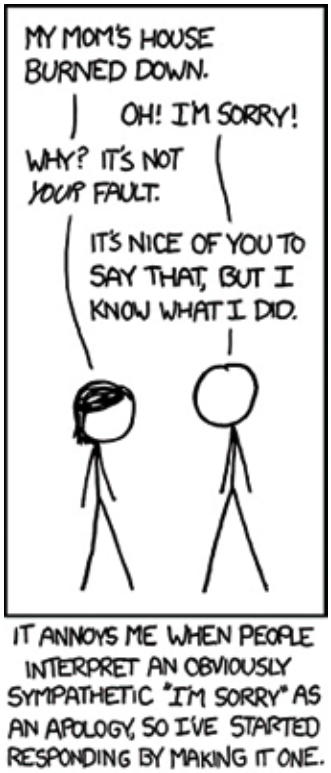
WINNENDE TROEF OF WAARDELOZE JOKER?

Wouter Steijn is promovendus aan de Tilburg Institute for Law, Technology and Society (TILT) van Tilburg University. Hij heeft zijn MSc behaald aan het Developmental Psychology department van de Universiteit Leiden. Op dit moment werkt hij aan een empirisch project dat deel uitmaakt van het programma 'Social Dimensions of Privacy'; een samenwerking tussen TILT en de Universiteit van Amsterdam (UVA).

Google's sociale netwerksite Google+ heeft in twee weken tijd al bijna 18 miljoen gebruikers vergaard. Een aantal waarvoor Facebook meer dan drie jaar nodig had. Facebook heeft op het moment wel een grote voorsprong met een totaal aantal leden van 750 miljoen gebruikers. Als er al iets uit deze cijfers is af te leiden, dan is het dat sociale netwerksites zeer populair zijn en dat Facebook er op het moment nog met kop en schouders boven uit steekt wat betreft het aantal leden.

Google+ is in alle opzichten 'the new kid on the block'. Het is pas enkele maanden oud en het heeft een troef waarmee het een marktaandeel bij Facebook probeert af te snoepen. Sinds de lancering promoot Google+ namelijk het eenvoudige gebruik van sociale kringen waarmee wordt tegemoetgekomen aan een veelgehoorde klacht over Facebook en de meeste andere sociaal netwerksites: privacy. Het gaat hier dan niet alleen om privacy in relatie tot identiteitsdiefstal, profilering, of het beschermen van gevoelige informatie zoals bankgegevens en woonadres, maar juist om het sociale aspect van privacy. Maar zijn de sociale kringen van Google+, die het mogelijk maken om je contacten op de site te verdelen op basis van sociale categorieën, nu werkelijk de oplossing voor deze vorm van privacy en zal dit gebruikers overtuigen om bij Facebook weg te gaan? Om deze vraag te kunnen bentwoorden, moeten we eerst kijken naar het wat het sociale aspect van privacy precies is.

Wat is het sociale aspect van privacy?
Het sociale aspect van privacy speelt een belangrijke rol in onze sociale interacties met anderen. In het leven komen we veel verschillende mensen tegen met wie wij een bepaalde relatie delen. Terwijl eigenlijk elke relatie uniek is, worden ze vaak gespecificeerd in termen van groepen die we tegelijkertijd tegenkomen. Bijvoorbeeld schoolvrienden, sportvrienden, collega's, en familie. Net zoals elke relatie met een ander persoon anders is, is onze identiteit verre van statisch. We passen ons aan aan de mensen die in de buurt zijn, of zoals Goffman (1959) het beschreef: 'elke persoon is een acteur die meerdere rollen speelt afhankelijk van de situatie'. De relatie die we met anderen hebben, beïnvloedt ons gedrag (Rachels, 1975).



From xkcd.com/918.

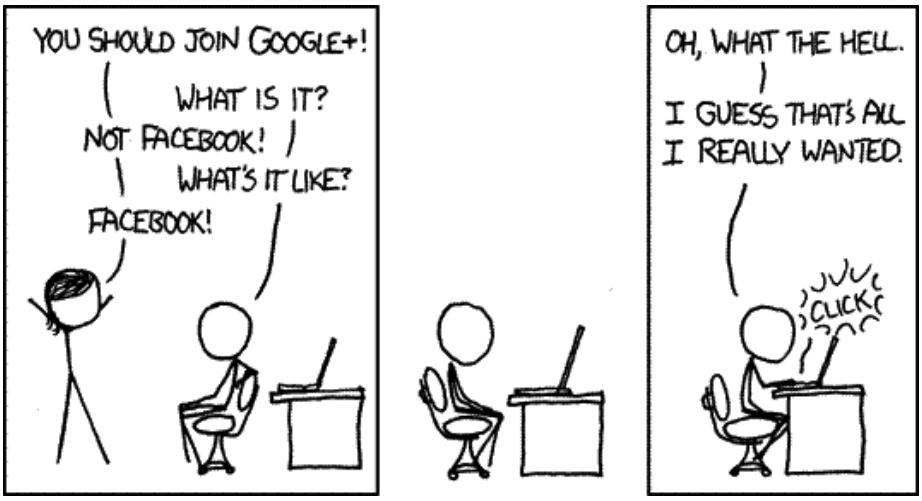
Over het algemeen, als een vrouw met haar zoon op stap is gedraagt ze zich als moeder, als ze samen met haar man is, is ze de echtgenote, op haar werk gedraagt ze zich als collega, en op stap met vriendinnen gedraagt ze zich weer anders. Op deze manier zorgen de verschillende rollen voor een versoepeling van de sociale interactie. Men kan een bepaalde verwachting hebben van hoe anderen zich gedragen. Hier komt ook privacy om de hoek kijken, want we vertellen onze partner andere dingen dan onze collega's en we willen ook niet dat collega's zich met familiezaken bemoeien. Gelukkig komen we mensen met wie we verschillende relaties hebben op andere momenten tegen. Zo komen we familie thuis tegen, collega's op het werk en groepen vrienden op diverse locaties. Hierdoor is het bijvoorbeeld voor een tiener mogelijk om zowel stoer te doen met vrienden als tegelijkertijd de brave kleinzoon van oma te zijn.

Het sociale aspect van privacy wordt bijna automatisch behouden tijdens offline interacties, simpelweg door de wijze waarop de wereld in elkaar steekt. Zo kan men maar op een enkele plek tegelijk zijn, en kan geluid maar een beperkte afstand afleggen en wordt door muren tegengehouden. Hierdoor zijn interacties met een be-

paalde groep relaties afgezonderd. Een schending van privacy is daardoor eerder uitzondering dan regel, in tegenstelling tot de situatie tijdens online interacties op sociale netwerksites.

Vervagende grenzen online

Interacties en het delen van informatie op sociale netwerksites verschilt wezenlijk van de offline situaties. Waar we offline onderscheid maken tussen veel verschillende sociale relaties, worden deze online vaak herleid tot een binaire functie. Of je bent een contact of niet. En terwijl je offline sociale relaties meestal apart van elkaar ontmoet, worden ze op sociale netwerksites op een hoop gegooid en kan er geen aparte rol voor ieder worden aangenomen. Op deze manier kunnen privacy-schendingen ontstaan omdat alle sociale relaties dezelfde toegang tot dezelfde informatie hebben, waar dit offline gescheiden en verschillend zou zijn. Dit sociale aspect van online privacy, krijgt in de media weinig aandacht en vaak is de berichtgeving vooral gericht op de geleden schade van de individuen. Een werknemer die ontslagen wordt omdat de baas toegang heeft tot uitspattingen gericht aan vrienden of een student die van school wordt gestuurd na beledigingen die normaal niet voorbij zijn vriendenkring zouden gaan, zijn goede voorbeelden van de vervagende grenzen online waarin bijna iedereen gelijke toegang heeft tot een individu. Sommige mensen geloven dat als we allemaal een gelijk beeld van elkaar hebben, dit alleen maar een goede ontwikkeling is.
Het 'twee gezichten hebben' of 'zich anders voordoen dan hij is' heeft vaak een negatieve toon en wordt vooral geassocieerd met bedriegers of mensen die iets te verbergen hebben. Online kunnen studenten in elk geval hun docenten niet meer zomaar beledigen. Toch heeft het sociale aspect van privacy zoals hier beschreven een zeer wezenlijke rol die voorbij gaat aan leugens en bedrog en is het hebben van 'twee gezichten' of zelfs meer, iets wat mensen



Randall Munroe - xkdc.com (CC BY-NC 2.5)

dagelijks gebruiken. Denk alleen maar aan hoe netjes je op je werk gedraagt om vervolgens thuis weer lekker de voeten op tafel te leggen. Onderzoek heeft aangetoond dat gebruikers van sociale netwerksites zich bewust zijn van de vervagende grenzen online en dat dit onwenselijk kan zijn (zie bijvpprbeeld Raynes-Goldie, 2010). Ze ergeren zich eraan dat sociale relaties zich mengen waardoor privé en werk, maar ook familie en vrienden moeilijker te scheiden zijn. Hoe moet dan de tiener online stoer overkomen op zijn vrienden zonder zijn oma te laten schrikken, als zowel oma als vrienden toegang tot het internet heeft? Als het aan de mensen van Google ligt zullen deze problemen in elk geval binnenkort weer verleden tijd zijn dankzij de sociale kringen van Google+.

De kringen van Google+

Bij de lancering van Google+ stonden de sociale kringen centraal. Met deze kringen kan men contacten indelen op basis van de relatie en zo bijvoorbeeld familie, vrienden en kennissen gescheiden houden om gericht informatie te kunnen delen. Dit zijn echter alleen maar de drie standaard kringen waarmee je begint. Je kunt nog extra kringen aanmaken voor bijvoorbeeld je collega's, teamgenoten, studievrienden, game-vrienden, of wie je maar wilt. Met een simpele sleepbeweging kan je je contacten in een of meerdere kringen plaatsen om vervolgens bij je berichten of foto's aan te geven welke kringen hier toegang tot hebben. Hiermee probeert Google+ weer een stap dichter bij het 'offline-gebruik' te komen. Door contacten in verschillende kringen te plaatsen kan men gericht boodschappen vermelden. Zo kan men foto's die alleen voor familie bestemd zijn aan familie laten zien en berichtjes die voor vrienden zijn weer alleen aan vrienden laten zien. Je oma kan dus niet meer bij de foto's die bedoeld zijn voor vrienden en je privacy en reputatie als brave kleinzoon is dus weer verzekerd.

Oud idee in een nieuw jasje

De sociale kringen van Google+ zijn geen compleet nieuw idee. Het wel of niet kunnen scheiden van verschillende sociale relaties speelt al langer mee met betrekking tot sociale netwerksites. Zo biedt Facebook ook de mogelijkheid aan om groepen maken en om contacten te onderscheiden. Waar het in Facebook echter moeilijk is om deze groepen te creëren, zit het bij Google+ zeer eenvoudig in elkaar. Hoe eenvoudig dit ook moge zijn, het onderverdelen van je sociale contacten in groepen steekt echter niet zo simpel in elkaar als wordt gesuggereerd. Voor elk contact moet dan namelijk worden overwogen of het een vriend is of alleen maar een collega. Doe ik alle familie samen of scheid ik verre familie? Maar wat dan van die neef waar ik goed mee kan opschieten bij familiebijeenkomsten,

doe ik hem dan als vriend? Offline gebeurt deze verdeling automatisch, online vergt dit voor elke contact een bewuste keuze. Een investering die veel gebruikers niet hebben willen maken op Facebook. Verder is het ook bijna onmogelijk om alle subtiliteiten die offline relaties hebben met technische opties te evenaren. Grimmelmann (2008) beargumenteerde dat zolang de fijne nuances van sociale relaties niet worden verwerkt in technologische opties, er altijd privacy-problemen zullen ontstaan.

Hoe mooi de sociale kringen er van Google+ dus ook uitzien, er is een grote kans dat ze maar minimaal worden gebruikt. Een dergelijk verdeling van groepen zal op zijn minst voorkomen dat collega's worden geconfronteerd met berichten van familie en familie wordt behoed voor foto's van de zaterdagavond. Maar het zal bij lange na niet in de buurt komen van de echte wereld. De vraag is of sociale netwerksitegebruikers hier überhaupt op zitten te wachten, want waarom doet het merendeel dit dan niet al op Facebook? Hiervoor moeten we kijken naar wat gebruikers nu eigenlijk willen van een dergelijke site.

Een stap terug?

Omwille van het argument waarom volgens mij mensen sociale netwerksites gebruiken, maak ik gebruik van een versimpelde tweedeling van communicatiemogelijkheden via internet. Het gericht communiceren via e-mail of instant messaging, en het massaal communiceren via sociale netwerksites zoals Facebook. Google+ lijkt zich op de niche tussen deze twee categorieën te richten. Met Gmail heeft Google al een mailprovider voor gerichte communicatie, maar het wil met Google+ niet zo massaal zijn zoals Facebook vanwege de geassocieerde privacy-problemen. Facebook begon oorspronkelijk ook met een doelgroep van alleen studenten, dit is echter uitgegroeid over de tijd en Facebook heeft dit zijn gang laten gaan, blijkbaar tevreden met het resultaat. Google+ gaat weer terug naar communicatie gericht op bepaalde categorieën, maar heeft zich niet beperkt tot een bepaalde categorie.

Deze stap terug, weg van de massale bereikbaarheid, is gemotiveerd door de hevige privacy-debatten die zijn ontstaan rondom massa sites zoals Facebook. Deze debatten zijn vaak zo gefocust op de negatieve consequenties van het gebruik van Facebook (ontslagen worden, beschamende foto's die online zijn gezet, of ouders die achter drugsgebruik komen), dat de pluspunten van het gebruik van Facebook worden vergeten. Als alle negativiteit uit de media echt een structureel probleem zou zijn, dan zou je verwachten dat deze sites niet zo populair blijven, of dat men allang gebruikmaakt van de opties die Facebook biedt om contacten gescheiden te houden.

De sociale dynamiek zoals eerder beschreven, is een veilige dynamiek maar zorgt er ook voor dat relatieontwikkelingen beperkt blijven. Met collega's heb je het vooral over werkgerelateerde onderwerpen, in de kroeg maak je de ene flauwe grap na de andere, en de persoonlijke onderwerpen bewaar je voor thuis bij je partner. Op sociale netwerksites verandert deze dynamiek omdat meerdere sociale relaties, tegelijkertijd worden bereikt. Dus nu kunnen collega's, kennissen en wildvreemden zien wat je normaal alleen met vrienden zou delen. Ja, dit kan leiden tot pijnlijke momenten zoals je baas die foto's van zaterdagavond ziet, maar het kan ook positief uitpakken. Als collega's en kennissen jou leren kennen zoals je normaal alleen aan vrienden laat zien, kunnen mogelijk banden versterken die anders nooit zouden zijn ontstaan. Denk aan neven die je normaal alleen bij familiebijeenkomsten ziet en die je beter leert kennen omdat je kan bijhouden wat ze doen, het ontdekken van gelijke interesses met een collega waar je het normaal op het werk niet over hebt, en het leren kennen van nieuwe vrienden die je anders nooit zou zijn tegengekomen. Deze mogelijke scenario's zullen verdwijnen met de introductie van de kringen van Google+.

Conclusie

Het is geen grote verrassing dat Google hoog heeft ingezet op privacy bij de lancering van Google+. De voorganger, Google Buzz, ontaardde in een privacy-ramp nadat er grote problemen ontstonden, onder andere omdat het gekoppeld was aan Gmail. Google lijkt de les te hebben geleerd en de kringen van Google+ zien er niet alleen mooi uit, maar zijn ook eenvoudig in gebruik. De sociale kringen van Google+ proberen het massale, zoals bij Facebook, in te tomen en weer wat privacy te creëren door het maken van sociale groepen te vereenvoudigen. Vooralsnog is echter het risico sterk aanwezig dat dit het kind samen met het badwater weggooit wat betreft sociale netwerksites. De kringen richten zich vooral op de negatieve consequenties van het gebruiken van sociale netwerksites. Toch blijven ook nu al mensen online gaan. Er zijn blijkbaar ook voordelen die tegen de mogelijke nadelen opwegen. Uiteindelijk hebben sociale netwerksites de internetgebruikers iets nieuws gegeven waarin de gebruiker centraal staat en in contact kan zijn met alle mensen die hij kent en zelfs die hij niet kent. Dit is misschien wel de grote aantrekkingskracht van deze sites, de mogelijkheid om dingen kunnen te delen, met iedereen. In dit geval zullen de kringen van Google+ geen troefkaart blijken te zijn, maar een waardeloze joker.

Literatuur

Goffman, E. (1959). *The presentation of self in everyday life*. Garden City: Doubleday.

Grimmelman, J. (2009). *Facebook and the social dynamics of privacy.* Iowa Law Review, 95(4).

Rachels, J. (1975). *Why privacy is important. Philosophy and Public Affairs*, 4(4), 323-333.

Raynes-Goldie, K. (2010). *Aliases, creeping, and wall cleaning: understanding privacy in the age of Facebook*. First Monday, 1(4).

WHAT'S UP MET WHATSAPP?

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

WhatsApp is in een razend tempo bezig om sms te vervangen. Waar gebruikers elkaar voorheen via het mobiele netwerk korte berichtjes stuurden, stappen smartphone-gebruikers en masse over op het versturen van berichten via de vaste databundel. Applicaties als WhatsApp communiceren via internet, waardoor een gebruiker naast de vaste kosten voor zijn databundel niet apart voor korte tekstberichten hoeft te betalen.

Providers zoals KPN maken zich zorgen over hun verdienmodel. De sms-berichten (ooit voor servicemonteurs geïntroduceerd en midden jaren 90 bij een aantal providers gratis) zorgden voor een stabiele inkomstenstroom. Gebruikers zien alleen voordelen. Een sms-verslaving hoeft nu immers niets extra's meer te kosten. Tenminste...
Als we de gebruikersvoorwaarden en het privacystatement van WhatsApp doorlezen zien we dat de app ons wel degelijk iets kost: het knaagt aan onze privacy.

WhatsApp stelt ons aanvankelijk gerust
"We do not use your phone number or e-mail address or other personally identifiable information to send commercial or marketing messages without your consent or except as part of a specific program or feature for which you will have the ability to opt-in or opt-out."
De aanbieder geeft vervolgens echter wel aan op verschillende manieren gegevens over ons te verzamelen, onder andere voor marketingdoeleinden. Als je het als primaire gebruiker geen probleem vindt om je persoonlijke gegevens met deze partij te delen dan is hier uiteraard niets mis mee. Hoewel je je als Europeaan wel dient te beseffen dat je gegevens conform het Amerikaans recht behandeld zullen worden. WhatsApp is van rechtswege niet voor gebruikers buiten de Verenigde Staten bedoeld.
"The WhatsApp Sites and Services are hosted in the United States and are intended for and directed to users in the United States. If you are a user accessing the WhatsApp Sites and Services from the European Union (...) you are transferring your personal information to the United States and you consent to that transfer."

Impact op je vrienden
Dat je als gebruiker zelf besluit je gegevens openbaar te maken of ze (zonder een safe harbor overeenkomst) te delen met een partij in de Verenigde Staten is natuurlijk volledig aan jezelf. Gebruikers dienen zich echter te beseffen dat WhatsApp ook gebruikmaakt van de gegevens in je adresboek.
WhatsApp stelt dat: "If another WhatsApp Services user has your phone number stored in their address book, they will be able see your status information."
De partij kan deze match vanzelfsprekend enkel maken indien het een kopie bezit van de contactpersonen van alle gebruikers. Zonder deze gegevens is het niet mogelijk om te controleren of iemand WhatsApp-gebruiker is en dus recht heeft op statusupdates.

Geen controle over eigen privacy
Door deze aanpak komt de privacy van een individu nog explicieter in de handen van derden te liggen. Niemand zal zijn vrienden vragen om zijn telefoonnummer te verwijderen om te voorkomen dat een applicatie als WhatsApp toegang krijgt tot zijn gegevens.
Het gros van de mensen denkt niet na bij de gevolgen van het gebruik van apps en zou je maar lastig vinden als je het ter sprake brengt. Daarnaast is het niet mogelijk om individuele contactpersonen te beschermen. Je geeft een app volledige toegang tot de contactgegevens, of je kiest ervoor de applicatie niet te gebruiken. Met als gevolg dat mensen massaal hun eigen privacy en die van hun vrienden opgeven voor toegang tot een ogenschijnlijk gratis applicatie. Iemand die waarde hecht aan zijn privacy zal zichzelf feitelijk in een sociaal isolement moet plaatsen om deze te beschermen.
Interessant is de vraag wie hier nou de fout in gaat? WhatsApp wijst gebruikers formeel op het feit dat de dienst juridisch alleen voor gebruik door Amerikanen bedoeld is. Je kunt van consumenten echter niet verwachten dat ze voordat ze privacy-gevoelige gegevens over hun vrienden delen WhatsApp benaderen voor afspraken over de bescherming ervan.
De ontwikkeling van sociale netwerken blijft dus vrolijk aan onze privacy knagen. Daar waar je bij Facebook of Hyves nog kunt kiezen om wel of niet mee te doen, zorgen smartphones ervoor dat je vrienden via het gebruik van apps feitelijk de keuze voor je maken. Zou privacy dan echt dood zijn?


CA
91716-0102

HET BURGERSERVICENUMMER EN DE RIJKSPAS

ZAAK NR. 11/2937 BESLU V134

Leon Kuunders is consultant bij Trusted-ID en is te bereiken via leon@trusted-id.eu.

Op maandag 29 augustus, 10:00 uur, diende de rechtszaak tussen de minister van Infrastructuur & Milieu versus het College bescherming persoonsgegevens. Onderwerp: het gebruik van het burgerservicenummer in het uitreikingsproces van de rijkspas. In de vorig jaar gepubliceerde privacyspecial van dit blad werd al op dit onderwerp ingegaan[1], nu diende dan eindelijk de rechtszaak[2] waarover ik in 2007 al een weddenschap afsloot voor een goede fles port.

Waar gaat het ook al weer over? Door de rijksoverheid wordt, mede in het kader van het programma Compacte Overheid, gewerkt aan het samenvoegen van allerlei ondersteunende faciliteiten. Zo is de overheid bezig om ministeries samen te voegen. Denk bijvoorbeeld aan het ministerie van Verkeer en Waterstaat dat is samengevoegd met het ministerie van VROM tot het ministerie van Infrastructuur en Milieu. Of de ministeries voor Economische Zaken en Landbouw, Natuurbeheer en Visserij, die samen nu het ministerie van Economische Zaken, Landbouw en Innovatie zijn. Hierbij worden ondersteunende diensten ondergebracht in domeinoverstijgende shared serviceorganisaties. Een voorbeeld van deze laatste is de afhandeling van personele zaken door P-Direkt en het beheer van facilitaire zaken door FMH, de Facilitair Management Holding, voorheen 4FM.

Een van de projecten die wordt gezien als voorwaarde voor het succes van deze interdepartementale samenwerkingsverbanden, is het programma Rijkspas. Met dit programma wordt beoogd te bereiken dat (beleids-) ambtenaren eenvoudig de facilitaire hulpmiddelen die in gebruik zijn door de rijksoverheid, kunnen inzetten voor hun werkzaamheden. Dit betekent met name eenvoudig toegang krijgen tot panden en ICT-systemen. Het normenkader dat door het programma Rijkspas is opgesteld schrijft dan ook het gebruik van specifieke technische hulpmiddelen (standaarden) voor. Doel is dus elke rijksoverheidmedewerker één pas te geven waardoor deze dankzij de daarop (gestapelde) functionaliteiten panden binnen kan lopen, kan inloggen op het netwerk, gebruik kan maken van follow-me printing, een digitale handtekening kan zetten en wellicht zelfs met het OV kan reizen met behulp van deze Rijkspas.

> Doel is dus elke rijksoverheidmedewerker één pas te geven

In het proces rondom het aanvragen en uitgeven van de Rijkspas worden de naamgegevens van de medewerker gecontroleerd met behulp van het Wettig Identiteitsdocument (WID) dat de medewerker daartoe overlegd. In het uitgifteproces bij het ministerie van Infrastructuur en Milieu werd daarnaast het burgerservicenummer (BSN) van de medewerker visueel gecontroleerd door de weergave ervan op het scherm te vergelijken met de weergave ervan in het WID.

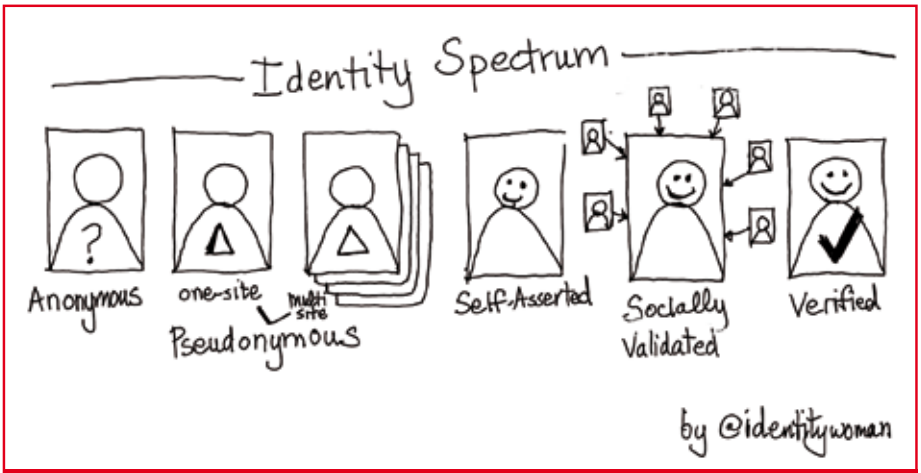
> Het gebruik van het persoonsnummer zou niet rechtmatig zijn

In een onderzoek uitgevoerd in begin 2010 door het CBP heeft het College daarop gereageerd met de eis dat het BSN wordt afgeschermd in het uitreikingsproces van de Rijkspas aangezien het gebruik van het persoonsnummer niet rechtmatig zou zijn. In de rechtszaak van 29 augustus werd het bezwaar van de minister (tevens direct als beroep bedoeld) op deze beslissing van het CBP door de bestuursrechter behandeld.

Wat is er gebeurd?

De behandeling van de Wet Algemene Bepalingen Burgerservicenummer (Wabb) heeft in zowel de Tweede als Eerste Kamer tot diverse vragen en amendementen geleid. Een kernpassage van de wet is te vinden in artikel 10, waarin de reikwijdte van het gebruik van het BSN wordt behandeld. Dit artikel luidt als volgt: '*Overheidsorganen kunnen bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun taak gebruikmaken van het burgerservicenummer, met inachtneming van hetgeen bij of krachtens dit hoofdstuk is bepaald.*' Een deel van de discussie gaat dan over 1) wat zijn overheidsorganen, en 2) wanneer voeren zij hun taak uit? Als derde werd door het CBP ingebracht dat het gebruik niet

noodzakelijk en daarom bovenmatig is (*subsidiariteitsbeginsel*).
Om dan met de eerste twee te beginnen; in de aanloop naar de rechtszaak is door beide partijen uitgebreid beargumenteerd waarom hun specifieke standpunten juist zijn. Ter zitting werden deze ten dele opnieuw ingebracht.
De minister zegt dat er sprake is van A- en B-overheidsorganen, waarbij inzake A-organen artikel 10 geen beperkende doelstelling heeft. Het CBP bestrijdt dat. Een A-orgaan is bijvoorbeeld een ministerie, een B-orgaan bijvoorbeeld een garagebedrijf tijdens het uitvoeren van een APK-keuring.
Het CBP zegt dat het uitgeven van een Rijkspas geen publiekrechtelijke taak is. De minister bestrijdt dat. De minister betoogt daar dat de bescherming (oftewel het uitvoeren van een juiste autorisatiebeslissing) van overheidsgebouwen en infrastructuur van evident (algemeen) belang is. In de pleitnota haalt zij dat met name aan door te verwijzen naar de bescherming van '*vitale objecten zoals sluizen en stormvloedkeringen, medewerkers en, niet in de laatste plaats, overheidsinformatie – informatie over burgers dus. [...] De bedrijfsvoering is daarmee een onlosmakelijk en integraal onderdeel van de (publieke) taakuitoefening. (2.10)*'
Over het derde wordt iets verderop in de pleitnota dit standpunt verder aangescherpt door te stellen: "*Het is dus van groot belang dat met de grootst mogelijke zekerheid rijksbreed maar één pas aan de juiste persoon wordt uitgereikt. Daarvoor is gebruik van het BSN – het enige uniek identificerende gegeven op een ID-bewijs – noodzakelijk als toetsingsinstrument. [...] de conclusie is getrokken – alle departementen hebben zich in het kader van de voorbereiding van de normenkaders voor de Rijkspas op dat standpunt gesteld – dat het noodzakelijk is eenmalig de identiteit en het 'recht' op een Rijkspas te controleren aan de hand van het BSN. (3.2)*"



Kaliya Young Hamlin - www.identitywoman.net/the-identity-spectrum.

Om haar taken goed uit te voeren heeft de minister dus een systeem nodig waarbij een Rijkspas terug te voeren is op een unieke persoon, en waarbij die persoon ook maar een Rijkspas mag hebben. Het BSN is daarvoor dan onmisbaar. Het gebruik ervan is dus noodzakelijk en dientengevolge niet bovenmatig, waarmee aan het subsidiariteitsbeginsel wordt voldaan.

Het CBP zegt dat het uitgeven van de Rijkspas geen publiekrechtelijke taak is

Het door de minister ingebrachte argument is feitelijk onjuist. Weliswaar zijn alle ministeries door het ministerie van BZK opgeroepen zich achter het standpunt van de minister te stellen en het BSN uit te vragen ten behoeve van de Rijkspas. Zie de memo Toepassen Normenkaders IdM, dd 14 juni 2011: '*In het kader van de beroepszaak is het van belang, dat de departementen de gekozen lijn voor het gebruik van het BSN in de bedrijfsvoering (zoals P-Direkt en Identitymanagement) blijven ondersteunen en daar niet van afwijken.*' Evenwel hebben niet alle ministeries daaraan gehoor gegeven. Onder andere het ministerie van EL&I heeft (inmiddels) duizenden Rijkspassen uitgegeven zonder daarvoor een visuele controle van het BSN uit te voeren. Tevens merk ik op dat het normenkader van de Rijkspas genuanceerder is op het punt van maximaal één pas mogen hebben. Dat schrijft voor dat een medewerker van de rijksoverheid maar één **actieve** rijkspas mag hebben. Met die toevoeging wordt ruimte gegeven aan het uitreiken van meerdere passen aan een en dezelfde persoon.
In de reactie van het CBP werd nadrukkelijk gewezen op het feit dat de WBP onverkort van toepassing is op de verwerking van het BSN, en dat de minister dus niet kan volstaan met het verwijzen naar enkel de Wabb. De toepassing van het subsidiariteitsbeginsel is dan met name van belang, omdat in het uitgifteproces van de Rijkspas '*de minister die identiteit al verifieert met behulp van een veelvoud aan persoonsgegevens (de achternaam, voornaam, overige initialen, voorvoegsels, geboortedatum en geslacht) [en dus] is gebruik van het BSN bovenmatig en niet noodzakelijk. (23)*'

Het CBP eist dat het BSN wordt afgeschermd bij uitreiking van de Rijkspas

De tweede ronde

Na de eerste ronde werd door de (vier) bestuursrechters specifieke vragen gesteld aan beide partijen. Na enig gesteggel over het verschil tussen A- en B-overheidsorganen en of daarmee wel of niet een beperking werd bedoeld in artikel 10 Wabb, ging men over tot het laatst genoemde punt: is het gebruik bovenmatig?

Het verweer van de minister, die in deze werd bijgestaan door enkele ter zitting aanwezige beleidsambtenaren, kwam er op neer dat met behulp van de genoemde identiteitsgegevens slechts in 98-99% van de gevallen zekerheid over de identiteit te verkrijgen is. Betoogd werd dat voor het goed functioneren van de Rijkspas 100% zekerheid noodzakelijk is. Door de rechtbank werd vervolgens gevraagd naar de statistische onderbouwing van dit argument: 'Over hoeveel medewerkers gaat het waarvoor het gebruik van het BSN bij de identiteitscontrole onmisbaar is?' Daar kwamen dus cijfers aan te pas, die een mooie inkijk geven in de grootte van het probleem. Van de 18.169 identiteiten in de identiteitenadministratie van het ministerie van I&M zijn er ongeveer 7.315 geslachtsnamen die slechts eenmaal voorkomen. Van de rest zijn er 368 waarbij zowel de achternaam als de voornaam hetzelfde is. En daarvan zijn er 15 waarbij ook de geboortedatum hetzelfde is.
Dat is 0,08%. Geëxtrapoleerd naar het servicegebied van de Rijkspas (volgens de minister maximaal 175.000 passen) zou dit betekenen dat ongeveer 140 medewerkers niet uniek identificeerbaar zouden zijn. Het cijfer van 0,08% maakte in ieder geval duidelijk dat met enkel gebruik van bekende identiteitsgegevens voor 99,92% zekerheid is te verkrijgen over de identiteit.
Een korte controle door de auteur laat in ieder geval zien dat voor een drietal andere departementen deze cijfers niet reproduceerbaar zijn. Daar is elke medewerker met behulp van voorletters, voornamen, voorvoegsels, geslachtsnaam, geslacht en geboortedatum uniek te identificeren.
Een van de rechters vroeg of bij de controle op de identiteit nog van andere kenmerken gebruik wordt gemaakt dan het persoonsnummer, en noemde vervolgens met name de *geboorteplaats en het geslacht*. Daarop werd door de aanwezige ambtenaren negatief gereageerd. De gedachtegang van de rechtbank lijkt daar dan te zijn dat er door het ministerie van I&M niet gezocht is naar een minder belastende werkwijze dan het gebruik van het BSN.

> Met de bekende identiteitsgegevens is voor 99,92% zekerheid te verkrijgen over de identiteit

> Door het ministerie lijkt niet gezocht te zijn naar een minder belastende werkwijze

De laatste ronde

De rechter doet binnen zes weken, dat is uiterlijk de tweede week van oktober, uitspraak. Een logische conclusie mag zijn dat het gebruik van het BSN voor de uitgifte van de Rijkspas vanwege het subsidiariteitsbeginsel niet zal worden toegestaan. Evenwel zei een wijs man eens dat er altijd vier kanten zijn aan een verhaal: dat van beide partijen, de waarheid en hetgeen werkelijk gebeurd is.
Hoe de rechtbank in deze dan ook beslist, is afwachten.
Ik vertrouw er op dat ik binnenkort een mooie fles port soldaat kan maken.

Referenties

[1] *Privacyspecial Informatiebeveiliging 2010 "Privacy en Identitymanagement", door Leon Kuunders*

[2] *http://webwereld.nl/nieuws/107739/minister---privacyschending--nodig-voor-rijkspas.html*

NASCHRIFT

Sneller dan gedacht deed de rechtbank op 7 september 2011 al uitspraak in deze zaak. En zoals te verwachten was geeft de rechter het College gelijk: de verwerking van het BSN ten behoeve van het facilitaire proces (i.c. de rijkspas) is niet toegestaan. Naar het oordeel van de rechter handelt de minister in strijd met de artikelen 8, 11 en 24 van de Wbp en artikel 10 van de Wabb. De rechter geeft aan dat de minister niet aannemelijk heeft gemaakt dat medewerkers van de rijksdienst niet te identificeren zijn met behulp van hun naamgegevens, geboortedatum en geslacht. Met andere woorden: het gebruik van het BSN voldoet niet aan het subsidiariteitsbeginsel.
Opvallend is verder de opmerking van de rechter dat de geschetste noodzaak voor het voorkomen van uitgifte van meerdere passen aan dezelfde medewerker , eerder te maken heeft met het inname proces van de rijkspas en niet met het uitgifteproces. Duidelijk is dan dat de rechter de door de minister opgestelde argumentatie onlogisch vindt.
Dit alles wijst uiteindelijk naar een probleem met de normenkaders voor de rijkspas. Die normenkaders, waarin bijvoorbeeld verplichte normen als NEN 1888 niet worden gevolgd, zijn niet precies en nauwkeurig genoeg om een succesvolle rijksbrede implementatie van de rijkspas te ondersteunen. Opgesteld vanuit de idee dat elk ministerie een eigen 'silo' is, wordt samenwerking en interoperabiliteit niet eens genoemd. Normen die voorschrijven hoe gegevens uit de Card Management Systemen kunnen worden gehaald en vervolgens gebruikt ter verbetering van het (gehele) proces en de kwaliteit, ontbreken volledig. Er is onduidelijkheid over gegevensdefinites en hun reikwijdtes, en de departementale implementaties van de Card Management Systemen laten dan ook een grote verscheidenheid zien.
Met de uitspraak van de rechter in de hand kan nu een begin worden gemaakt met het verbeteren van deze normenkaders, zodat rijksbreed gebruik van de rijkspas werkelijk mogelijk wordt.
Zonder BSN dan, dat wel.

ACHTER HET NIEUWS

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

GOOGLE+

Google+ is een interessant nieuw sociaal netwerk. Google heeft al eerder initiatieven ontplooid, denk aan Orkut, Buzz en Wave, maar Plus lijkt beter aan te slaan. Google heeft ook goed gekeken naar de sociale netwerkwereld en gebruikgemaakt van de slimmigheden van anderen en van wat ze zelf al goed doen: zoeken en vinden. En Google heeft op voorhand goed nagedacht over privacy. Het privacybeleid en de implementatie ervan lijken er beter uit te zien dan dat van bijvoorbeeld Facebook. Zo wordt gewerkt met circles van 'vrienden' waardoor de gebruiker veel beter zelf zijn informatiestromen kan beheren.
Maar Google heeft de gram van de identiteitenwereld over zich afgeroepen toen het profiel van Identity Woman werd geblokkeerd. Google stelt zich op het standpunt dat alleen echte namen gebruikt mogen worden in persoonsprofielen. Maar iedereen kent toch Identity Woman? Wat is het probleem? Ziet Google het goed? Of moet Kalya toch maar gewoon haar eigen naam gebruiken? En moeten we anonimiteit en pseudonimiteit ook tot de verworvenheden van het internet rekenen?

Lex Dunn:
Google+? Wa's dat nou weer? Een grotere uitvoering van Google (Big Mac, of VW Golf Plus)? Ik had er vaag wat over gehoord, maar aangezien ik geen Google diensten gebruik, zoals Gmail, ging het tot nu toe aan mij voorbij. Naar aanleiding van deze Achter het Nieuws toch maar eens gaan kijken wat het nou is. Het eerste wat mij opvalt als je naar de homepage van Google.nl gaat, is dat er dus niks te vinden is over Google+. Dan maar eens Google zelf proberen. Even slikken, slechts 12 miljard hits. Maar Google zou Google niet zijn als ze de zoekresultaten niet een beetje manipuleren. De eerste link verwijst naar plus.google.com. Had ik natuurlijk zelf kunnen bedenken ;-)
Ziet er uit als weer een social networking site, maar volgens André in zijn introductie voor deze rubriek is het toch echt wat anders en zou het met name wat privacy betreft een verbetering zijn. Ja ja, Google en privacy (of liever gezegd Eric Schmidt en zijn uitspraak dat we privacy maar moeten vergeten, behalve uiteraard als het die van hemzelf betreft).
Toch maar eens kijken in dat privacybeleid (die hele kleine lettertjes helemaal onder aan de pagina). Het begint al goed. Google verzamelt alles wat los en vast zit over uw acties en gedragingen binnen Google+. En om Google+ te gebruiken moet je een publiek Google-profiel hebben. Dus niet even op je gemak rondkijken, nee, de hele sociale networking-wereld weet gelijk dat je aan het snuffelen bent aan Google+ (heb ik dus maar niet gedaan). Dat profiel moet een naam bevatten, die je gebruikt voor alle Google-diensten. Geen woord over dat dit een echte naam moet zijn. En als dat een echte naam moet zijn, wat is dan een echte naam? De meeste mensen in ons vakgebied kennen mij als Lex Dunn, maar aan de hand van mijn geboortebewijs kan ik me sowieso nog onder minimaal drie anderen namen bekendmaken. En in Nederland mogen we als mannen tegenwoordig ook de naam van onze vrouw aannemen (lang leve de eMANcipatie!). Maar zou het voordeel hebben om de anonimiteit op internet op te geven? Enerzijds denk ik van wel. Maar hoe regelen we dan dat iedereen inderdaad met open vizier onder zijn eigen naam opereert? Anderzijds hoeft een bedrijf niet te weten wie ik ben als ik puur uit interesse even op hun website rondkijk. Als ik bij een Hema of Albert Heijn naar binnen ga, kan ik ook anoniem rondkijken en gewoon met contant geld zelfs wat kopen. Wat mij betreft loopt die discussie nog wel een tijd. Zelf ben ik er nog niet helemaal uit.

Rachel Marbus:
Ik heb het op verschillende plekken al geroepen: "if you don't have a Gmail-account, you don't exist". Ga maar na. Als beetje Google-minded persoon, maak je natuurlijk gebruik van Google Docs, Picassa, Latitude, Gmail, Gtalk en

nu ook van G+. Althans, als je Rachel heet. Het is gewoonweg te makkelijk om alles bij elkaar te hebben staan. De keerzijde van dat alles: voor Google besta je dus heel erg. Groots. Google weet waar ik ben, wat voor foto's ik heb, met wie ik vaak klets en met wie ik samen aan artikelen schrijf. Waarschijnlijk hebben ze ook gedeeltes van mijn proefschrift gelezen (staat netjes in Docs) want daarin beschrijf ik dat een stap voorwaarts richting meer privacy is om gebruikers de mogelijkheid te bieden zelf te bepalen met welk publiek ze welke informatie op welk moment willen delen. Door iets dergelijks als circles. Dat hebben ze in ieder geval goed begrepen bij Google. De gebruiker wil zelf meer controle over wat hij deelt en met wie. Een belangrijke stap voorwaarts dus in de wereld van de sociale netwerksites. Helaas blijft het vooralsnog wel bij dat ene aspect: het reguleren van privacy-opties tussen gebruikers onderling en de buitenwereld. Begrijp me niet verkeerd. Ik vind het prachtig hoe G+ is ingericht. Het enige wat nog steeds onveranderd is gebleven is de gebrekkige privacy van de gebruiker ten opzichte van de aanbieder van de dienst. Het zou Google sieren als ze ook hier een stoere stap voorwaarts nemen. Bijvoorbeeld door te starten met het schrappen van privacy invasieve bepalingen uit hun Algemene Voorwaarden. Zodat wij, de gebruikers, ook gewoon gebruik kunnen maken van onze pseudoniemen.

Andre Koot:
"Mijn naam is..." en dan volgt de naam van iemand waarvan een panel bij 'Wie van de 3' moest achterhalen welke individu bij die naam hoorde. Ik zou nu zeggen: bij welke persoon die identiteit hoort. Ik geloof namelijk heilig in het uitgangspunt dat een natuurlijk persoon, een fysiek individu, meerdere identiteiten heeft. En dan heb ik het een keer niet eens over mijn digitale identiteiten. Nee, ook in 'real life' heb ik meerdere identiteiten. Ik ben echtgenoot van, vader van, broer van, werknemer van, lid van, klant van... En elk van die identiteiten heeft een iets andere betekenis en invulling. De grootste gemene deler is dat de meeste van die identiteiten dezelfde voor- en achternaam kennen. Niet onlogisch omdat ook die ikken elkaar grotendeels overlappen. Maar soms is een echte naam niet noodzakelijk. Als ik een kilo suiker koop, dan speelt mijn werkelijke naam, mijn doopnaam, geen enkele rol. Sterker nog, die hou ik bewust erbuiten. Ik kies voor anonimiteit. Dus geen bonuskaart voor mij. Google en Facebook proberen in de digitale wereld hetzelfde trucje uit te halen. Los van de vraag of dat kan (hoe koppel je een echte naam van een fysieke identiteit aan een digitale identiteit?) speelt eerder nog de vraag waartoe? Wat is het belang van Google en Facebook? Die bedrijven leven natuurlijk van advertenties en hoe beter je de doelgroep kunt adresseren hoe beter. En als de digitale identiteit overeenkomt met een fysieke identiteit, dan is zo'n identiteit natuurlijk waardevoller voor adverteerders. Meer kans dat je de juiste attributen kunt valideren. Maar daar hebben wij als individuen niet veel aan, tenzij je prijs stelt op beter op jou toegesneden advertenties. Verplicht gebruik van een echte naam is dus geen win-win-situatie. Ik word daar niet beter van, sterker nog, ik kan niet anoniem zijn of een pseudoniem gebruiken. Ik verwacht dat er binnenkort nog wat meer gaat spelen. Advertenties zijn in de digitale wereld al betrekkelijk passend op de geadresseerde. Maar ik denk dat het aanbieden van diensten op het koppelvlak van de fysieke en de digitale wereld nog meer waarde zal gaan toevoegen. En aangezien Google en Facebook het gebruik van een echte naam eisen, zullen ze tot de eerste partijen behoren die daar munt uit gaan slaan. Ik denk dat we binnenkort ook buiten de browser meer van die bedrijven zullen gaan merken...

Maarten Hartsuijker:
Dat Google graag weet wie de echte eigenaar van een account is, is niet verwonderlijk. Google leeft van informatie en informatiesamenhang. En Google is groot geworden met het personaliseren van advertenties. Het is dan natuurlijk prettig om met al je diensten zo dicht mogelijk tegen de ware identiteit van je gebruiker aan te zitten en je platform wat dat betreft zo min mogelijk te vervuilen.

Of gebruikers met Google+ online betere privacybescherming krijgen betwijfel ik. De Circles van Google+ bieden gebruikers goede mogelijkheden om hun privacy naar de buitenwereld beter onder controle te houden. Maar gebruikers dienen zich wel te beseffen dat Google zich bij hun profielvorming niets van deze Circles hoeft aan te trekken. Met elk bericht dat je plaatst en elke relatie die je aanbrengt verrijk je het profiel dat Google met haar diensten zoals Search, Gmail en Analytics over je verzamelt. En als bedrijf geef je met elke 'Plus'-knop die je op je site plaatst een klein beetje informatie over het profiel van je bezoekers weg. Zo neemt de informatie die Google over onze interesses heeft steeds verder toe en neemt de controle die we over deze profilering hebben steeds verder af.

COLOFON

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

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

Redactieraad
Said El Aoufi (Metapoint)
Tom Bakker (Delta Lloyd)
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
Maarten Hartsuijker (ANWB)
Aart Jochem (GOVCERT.NL)
André Koot (Univé-VGZ-IZA-Trias)
Rachel Marbus (KPMG, IT Advisory)
Gerrit Post (G & I Beheer BV)

Advertentieacquisitie
e-mail: adverteren@pvib.nl

Vormgeving en druk
Van de Ridder Druk & Print, Nijkerk
www.vanderidder.nl

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

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

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

ISSN 1569-1063

OVERDRIJVEN WE NIET EEN BEETJE ?

Privacy, een begrip dat volgens mij nog niet langer dan twee decennia bestaat en dat ik meer en meer als overdreven ga beschouwen. Zo'n 20 jaar geleden werkte ik voor een ziekenfonds en binnen dat bedrijf was een plezierige en open sfeer. Iedereen was met iedereen begaan en vanuit dat uitgangspunt werd ook met elkaar omgegaan. Het was op een ochtend dat mijn secretaresse mij vroeg of ik veel napijn had gehad van de tandartsbehandeling van de week ervoor. Verbaasd keek ik haar aan en vroeg hoe zij wist wat de tandarts mij had aangedaan. Het antwoord werd eerlijk en zonder schroom gegeven. Ze had de declaratie van de tandarts ontvangen en zag wat mij was overkomen. Zij liep vervolgens weg zonder ook maar een idee te hebben wat haar mededeling bij mij had losgemaakt.

Een aantal maanden later werd door dezelfde secretaresse in de kantine omgeroepen van wie de auto met kenteken HD-HD-99 (volledig gefingeerd) was? Ik herkende het kenteken van mijn leaseauto en riep enthousiast: "van mij!" Daarop liep ze naar me toe en zei lachend dat ik niet te hard moest rijden en overhandigde mij een bekeuring van 35 gulden (toentertijd was het nog betaalbaar om een paar kilometer te hard te rijden).

Beide incidenten staan op zichzelf en zijn wellicht niet zo ernstig. Toch heb ik mijn directeur voorgesteld om de verwerking van de declaraties door een aantal medewerkers te laten doen die een geheimhoudingsverklaring zouden tekenen. Ook stelde ik voor de bekeuringen rechtstreeks naar mijn huisadres te laten sturen. Dit besluit viel als een bom en het resultaat was dat er enkele weken uiterst koel met mij werd omgegaan.

Als ik dit verhaal vertel op verjaardagen en andere partijen (ik ben een graag geziene gast met mijn anekdotes) wordt er vaak gereageerd met de dooddoener 'maakt mij niets uit want ik heb niets te verbergen' waarop ik altijd steevast vraag wat ze per maand verdienen. Het antwoord op die vraag heb ik nog nooit gekregen en als ik aangeef dat mijn secretaresse mij ook iedere maand mijn loonstrook overhandigde voelde ik iets meer begrip.

Dit was allemaal in de vorige eeuw en er is veel veranderd. Niet alleen in het bedrijf waar ik inmiddels niet meer werk maar ook in de maatschappij. Het gaat inmiddels al zover dat ik toch weer een aantal anekdotes wil vertellen die aangeven dat we volstrekt doorgeschoten zijn.

Laatst moest ik naar de notaris om iets te regelen. Hij vertelde mij tijdens ons gesprek dat hij toevallig de week ervoor een echtpaar aan zijn tafel had zitten. Beiden hadden een testament laten opstellen waarin zij aangaven dat in geval van overlijden alle bezittingen naar de partner zouden gaan. Na ondertekening van beider testamenten liepen zij hand in hand het kantoor uit. Een dag later zat de man wederom aan tafel en verzocht hij de notaris zijn testament te vernietigen. Inmiddels was mijn mond opengevallen en na mijn eerste verbazing te hebben weggeslikt vroeg ik de notaris of hij daar nog iets mee had gedaan. Zonder enige schroom gaf hij aan dat hij op basis van privacyregels er niets mee mocht doen. Ik voel vaak aan wanneer een discussie geen zin heeft en ook nu had ik dat weer goed aangevoeld. Hoofdschuddend verliet ik het kantoor van de notaris die privacy prevaleerde boven integriteit.

Als laatste voorbeeld wil ik graag de situatie van een familielid beschrijven. Door vervelende omstandigheden kon mijn familielid niet meer thuis worden verzorgd en zou hij worden opgenomen in een verpleeghuis. Treurig genoeg, maar uiteraard moet de administratie hieromtrent ook worden geregeld. Dus de gemeente moest op de hoogte worden gebracht van het feit dat mijn familielid in die gemeente zou komen te wonen. Natuurlijk even op de website van de gemeente gekeken of er langs elektronische weg mogelijkheden waren. Die waren er, maar dan alleen met het onvolprezen DiGiD, en die had mijn familielid niet. Een alternatief was om met een ID-kaart van mijzelf en een ID-kaart van mijn familielid naar het gemeentehuis te komen en dan alles te regelen. Ik heb 20 minuten tegen een alleraardigste ambtenaar van de bewuste gemeente aangesproken maar helaas kon ik haar niet overtuigen dat mijn familielid niet meer in staat was om mee te gaan naar haar balie. Een bijzondere genante vertoning, temeer omdat ik sterk het gevoel had over iemands persoonlijke leven te spreken wat hijzelf niet meer kon organiseren. De verhuizing kon niet worden doorgevoerd. Uiteindelijk heb ik een e-mail gezonden met een kopie van mijn ID en een kopie van het ID van mijn familielid en is de overschrijving blijkbaar gelukt. Tenminste, daar ga ik vanuit. Gelukkig zijn privacyregels niet altijd heel hard doorgevoerd en kan er schriftelijk meer dan een persoonlijk bezoek aan de balie van die aardige mevrouw.

Groeten Berry

Discover the next best thing since the introduction of FTP!

now also for
Lotus Notes &
Microsoft Outlook

BEFINE cryptshare®

- Easily send large files up to 2GB
- Confirmation of file download
- Simple and secure file transfer

CRYPSYS Data Security is de expert op het gebied van security oplossingen en distributeur van Cryptshare. Neem contact op via sales@crypsys.nl of via 018 362 44 44 voor een gratis evaluatie

CRYPSYS data security