03/2012

INFORMATIE BEVEILIGING

PvIB Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 3 - 2012

USER-MANAGED ACCESS: VEILIG ONLINE DATA DELEN

HET LEKKEN VAN DATA

XACML ALS STANDAARD VOOR AUTORISATIE

PI.LAB: SAMEN VOOR PRIVACY EN IDENTITEIT

SECURITY CAFÉ – MOBILE APP SECURITY

IMF
INTERNATIONAL MANAGEMENT FORUM

Certified ISO 27005 Risk Manager

Deze 3-daagse training leidt u op tot Certified Risk Manager op basis van de internationale standaard voor informatiebeveiligingsrisicomanagement ISO 27005

ISO International Organization for Standardization

In deze 3-daagse Certified Risk Manager training leert u de risico-elementen m.b.t. informatie te beheersen. Op basis van praktische oefeningen en case studies leert u een optimale risico-evaluatie uit te voeren en risico's in de tijd te beheren door vertrouwd te raken met hun levenscyclus. U leert de verschillende methoden van risico-evaluatie kennen, zoals CRAMM, EBIOS, MEHARI, OCTAVE en de Microsoft Security Risk Management Guide.

Schriftelijke cursus CISSP

Deze unieke Nederlandstalige schriftelijke CISSP cursus bereidt u voor op het officiële CISSP-examen van (ISC)2

U kunt u tevens aanmelden voor de (optionele) CISSP examentraining. Tijdens de examentraining wordt uitvoerig aandacht besteed aan het CISSP examen en wordt er intensief getraind met behulp van oefenexamenvragen.

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

EUROCLOUD EN VKA BEVORDEREN CLOUDCERTIFICATIE

Verdonck, Klooster & Associates (VKA) heeft zich als eerste onafhankelijke adviesbureau als partner aangesloten bij Stichting Eurocloud Nederland. In dit blad schreven we al eerder over de inspanningen van Eurocloud voor een veilige cloud en VKA kennen we vanuit het PvIB natuurlijk heel goed. Het partnerschap wil zich richten op het bevorderen van veilige en transparante cloud oplossingen. Er wordt binnen Eurocloud gewerkt aan een breed Europees gedragen certificeringsysteem voor IaaS, PaaS en SaaS oplossingen. VKA zal zich hierbij vooral richten op het lokaal bevorderen van dat certificeringsysteem, o.a. middels accreditaties.

VOORWOORD

Zo'n 25 jaar geleden heb ik mijn eerste forensisch onderzoek gedaan. In ons kantoor was er sprake van een lastig geval van voortdurende stalking. Dit was vóór deze term überhaupt was uitgevonden. De persoon in kwestie werd gepest met zeer vervelende boodschappen op zijn terminal, van een aard waarbij de dader crimineel vervolgd zou kunnen worden. In die dagen hingen we als bedrijf niet aan het internet, dus hadden we ook nog eens de wetenschap dat het wel iemand binnen het bedrijf moest zijn die dit veroorzaakte.

De methode die de dader gebruikte om opsporing te vermijden was een keten maken van pseudostations - dat was hoe we in die dagen een virtuele cliënt noemden. Van daaruit opende hij een sessie op een andere server, waar hij dan weer een nieuw pseudostation startte. Eigenlijk had hij dus een soort Tor netwerk opgezet. De sprongen raakten alle servers, productie en test, en overal werden wel gewoon log records weggeschreven. Bij het napluizen waren er wel wat uitdagingen; van een centraal verzamelpunt voor logs was geen sprake, en ook tijdsynchronisatie werd nog niet toegepast. Op testsystemen kon een log ook op ieder moment weggegooid worden.

Mijn onderzoek bestond dan ook uit het van server naar server gaan, de logs uitlezen, het tijdverschil tussen de twee servers bepalen en zo het spoor volgen. Na tien schillen afpellen ben je het aardig zat. Uiteindelijk bleek de bron een publiek opgestelde terminal te zijn die aan het directe zicht onttrokken was. Daarmee was er wel een vermoeden, maar geen bewijs. Dus er was sprake van een succesvol onderzoek, maar het resultaat bleef uit.

Vandaag de dag is forensisch onderzoek wel veranderd. Het volume van data is flink gegroeid; er zijn veel meer bronnen te raadplegen, we moeten ons druk maken over eventuele schendingen van privacy, over de integriteit van de verzamelde data en we moeten ons afvragen of we alles wel gevonden hebben. In een minionderzoek, gedaan in de PvIB LinkedIn groep, zien we dat het bewijzen van die integriteit wel als het meest belangrijke wordt gezien. Opvallend hierin ook is dat niemand het groeiend volume aan data aangegeven heeft als grootste zorg.

Oh, en voor wie het weten wil: de stalker is een korte tijd later wel gepakt. Uiteindelijk geeft zo iemand zich net te veel bloot.

Links:

http://www.linkedin.com/groupAnswers?viewQuestionAndAnswers=&discussionID=96827496&gid=133202

INHOUDSOPGAVE

"IK ZIE, IK ZIE, WAT VELEN NIET ZIEN": ADVANCED PERSISTANT THREATS

Christiaan Beek
Christiaan Beek is Principal Architect IR & Forensics bij McAfee Foundstone EMEA.
Hij is te bereiken via christiaan@securitybananas.com.

Inleiding

Het begrip APT heeft dezer dagen een hele nieuwe betekenis gekregen. De term refereert naar aanvallers die de middelen hebben om zichzelf ongeautoriseerde toegang tot specifieke bedrijfsnetwerken te verschaffen. Helaas wordt de term met grote regelmaat verkeerd gebruikt. Uit commerciële overwegingen wordt de term veelal in verband gebracht met alle nieuwe geavanceerde malware, terwijl het in 2006 door analisten van de Amerikaanse Luchtmacht in het leven is geroepen om de groep aanvallers die zich op specifieke bedrijven richten te onderscheiden van de rest.

Waar virusscanners vaak nog redelijk in staat zijn om reguliere malware te herkennen, kenmerken APT's zich vaak door lastig te detecteren malware. De hackers achter de APT's zijn zich veelal erg bewust van de detectiemogelijkheden van antivirusproducten en doen er daarom alles aan om niet herkend te worden. In dit artikel zal aan de hand van een praktijkcase een APT worden besproken en een aantal eerste handreikingen worden gegeven om een APT te kunnen opsporen.

Verkenning

Om een gerichte aanval te kunnen uitvoeren, gebruiken aanvallers allerlei technieken om zoveel mogelijk informatie te kunnen verzamelen over hun doel. In het verleden werd er vaak actief met tools gescand op de ict-omgeving van het doel om zodoende informatie omtrent de beveiligings-mechanismen of kwetsbaarheden te verzamelen. Dit soort acties zijn niet geheel zonder risico's, ze kunnen door firewalls/IDS/IPS sensors worden opgemerkt. De meeste bedrijven echter negeren deze meldingen omdat ze te veel alerts opleveren. Jammer, ze konden zo waardevol zijn tijdens correlatie van de diverse gebeurtenissen. Tegenwoordig is het veel makkelijker en veiliger om informatie over het doel in te winnen door een passieve scan uit te voeren. Met behulp van online en open-source tools kan de informatie worden verzameld met een relatief zeer kleine kans om gedetecteerd te worden. Data van sociale netwerken, wat vertelt de website, foto's van werknemers met GPS data erin etc. Een bron van informatie die, gecombineerd met de kennis en ervaring van de aanvallers, een succesvolle infiltratie kan opleveren.

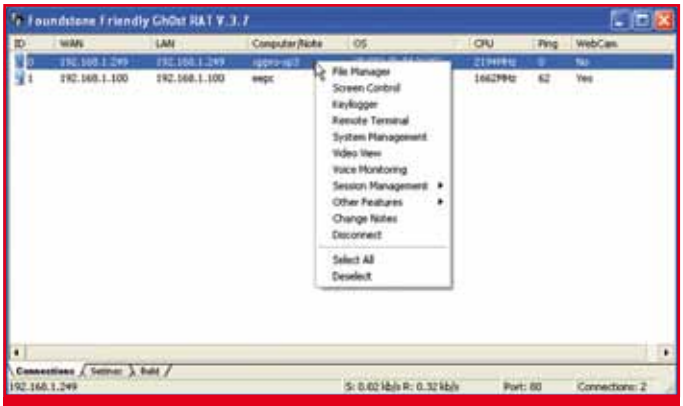
> APT vaak lastiger te detecteren dan normale malware

Praktijkvoorbeeld

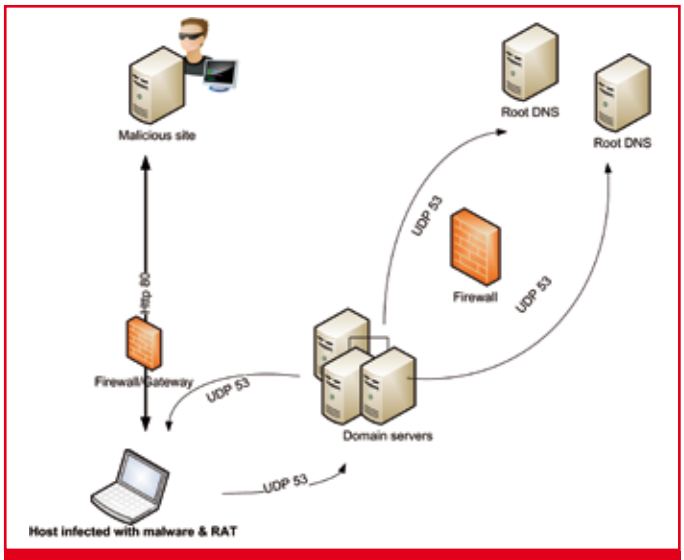
Een georganiseerde groep van aanvallers werd ingehuurd om de blauwdrukken van een specifiek organisatieonderdeel te bemachtigen. De groep begon met het profilen van het bedrijf: ip-adressen, e-mailadressen etc. Een belangrijke stap in de operatie is het achterhalen van informatie over de gebruikte software binnen het bedrijf. Een aantal e-mails werd verstuurd onder valse accounts om zodoende de 'reply e-mails' te onderzoeken. De headers leverden aardig wat informatie op en zo te zien gebruikte het bedrijf geen afwijkende spamfilter. Vervolgens werd met tooling de documenten van de website gehaald om daaruit de metadata te analyseren. Documenten bevatten vaak de gegevens omtrent wie het document heeft opgesteld, op welke share het is opgeslagen,

```
var jver = [0, 0, 0, 0], pdfver = [0, 0, 0, 0], flashver = [0, 0, 0, 0];
try {var PluginDetect = {handler : function (c, b, a){return function ()
{c(b,a)}
```

Afb. 1. Verkrijgen van software versie



Afb.2. Remote Access Tool



Afb.3. Verdacht verkeer

welke versie van het pakket is gebruikt etc. Uit de analyse blijkt welke versies van Microsoft Office, Adobe pakketten en welk besturingssysteem het meest gebruikt wordt. Op basis van deze informatie besluit de groep om de volgende aanval op te zetten: Een e-mail te versturen naar een grote groep van medewerkers met daarin een link naar een 'Java update'. Nadat een aantal gebruikers op deze link had geklikt werden ze zonder het te weten doorgelinkt naar een pagina die toebehoort aan de BlackHole exploit kit die door de groep speciaal was opgezet. Deze kit gebruikt diverse manieren om code te verbergen en zodoende het moeilijk te maken om gedetecteerd te worden. Deze pagina bevat een aantal scripts die de versie van Adobe/Java/Flash en het OS controleren. Op basis van deze informatie worden een aantal exploits uitgevoerd om de eerste toegang tot de systemen te proberen verkrijgen.

Voorzichtig bekijkt de groep welke systemen in handen zijn. De meeste systemen zijn minder van belang maar kunnen altijd nog gebruikt worden voor het geval de juiste systemen nog niet bereikt zijn. Bij een van de systemen blijkt het raak te zijn, deze blijkt eigendom te zijn van mogelijk een C-level medewerker. Door de vooraf verzamelde informatie te doorzoeken, komen ze erachter dat de persoon het hoofd van de onderzoeksafdeling is. Dat is een mooi success. Om langdurig toegang te kunnen hebben tot de machine, wordt een RAT (Remote Access Tool) gebruikt. Deze tool moet niet opgemerkt worden door de beveiligingsprogrammatuur of door de beveiligingslagen van de computer. De groep weet hoe bedrijven opereren en zorgt ervoor dat de communicatie tussen de RAT en hun servers verborgen wordt in het internetverkeer over TCP poort 80. Daarnaast wordt een mechanisme gebruikt dat dagelijks via DNS requests (UDP 53) zoekt naar de domeinen die opgezet zijn voor deze operatie. De RAT is voorzien van allerlei functionaliteiten waaronder het afluisteren van de gebruiker (voice monitoring) door de microfoon te activeren en het geluid op te nemen (zie figuur 2). Daarnaast zijn er nog vele functies ingebouwd met als doel zoveel mogelijk informatie te bemachtigen van het systeem waarop de tool is geïnstalleerd.

Analyse uitgaand DNS verkeer waardevol

Het bovenstaande scenario is helaas een dagelijkse werkelijkheid. Hoe is het mogelijk dat ondanks alle beveiligingsmaatregelen die getroffen waren, een kwaadaardig stuk software op de computer kon worden geïnstalleerd? Hoe werd het uiteindelijk gedetecteerd? Los van het feit om niet door anti-virus te worden gedetecteerd is het belangrijk om te weten dat bij een APT, mechanismen worden gebruikt om zo lang mogelijk ongedetecteerd te blijven op het netwerk en host. Zonder al te diep in te gaan op de techniek wordt op een host gebruik gemaakt van registerwaardes, geplande taken of scripts die ervoor zorgen dat de RAT ongemerkt blijft en een reboot overleeft. Daarbij wordt de hele trukendoos opengetrokken: het bestand wordt vermomd als driver, of men gebruikt een nep-versie van de prullenbak. Er zijn gevallen bekend waarbij de malware een eigen versleutelde partitie aanmaakt en van daaruit de controle uitoefent. Netwerkverkeer van de RAT wordt gemaskeerd en vaak verzonden over de reguliere internet poorten: 80 (http) en 443 (ssl).

Passieve infrastructuuranalyse hackers nauwelijks te detecteren

In het praktijkvoorbeeld werd er op een bepaald moment geconstateerd dat er veel uitgaand DNS verkeer plaatsvond, meer dan gemiddeld het geval was.

Inbreken via Acrobat, Java en Flash blijft populair

Door een tap in het netwerk te plaatsen werd uitgaand web en DNS verkeer afgevangen en bewaard voor analyse. Met behulp van speciale programma's werd het verkeer geanalyseerd op verdacht verkeer. Uit de analyse bleek dat er een aantal interne hosts vele requests per uur verstuurden naar een tweetal root-DNS servers in het buitenland (zie figuur 3).
In eerste instantie werd gedacht dat de domein-servers ook geïnfiltreerd waren, maar dat was niet het geval. De domeinservers waren zo geconfigureerd dat ze allemaal als interne DNS server konden worden gebruikt. Vervolgens stuurden zij de verzoeken door naar de twee DNS servers die werden gebruikt tijdens de APT aanval. De besmette hosts waren zo geconfigureerd dat ze ieder uur een aantal keer een DNS verzoek verstuurden om te achterhalen met welke sites ze op dat moment contact konden maken, om instructies te ontvangen, of om uit te zoeken naar waar de keylogger bestanden konden worden verstuurd. Om detectie van dit verkeer te voorkomen werd het ingepakt (een soort mechanisme als Winzip) en vervolgens dwars door de firewall en gateway heen verstuurd naar de sites die in handen waren van de APT groep. Door een regel aan te maken op de firewall om al het uitgaande DNS verkeer richting de twee buitenlandse Root DNS servers te blokkeren en te rapporteren, werden de besmette en geïnfiltreerde hosts opgespoord. De infiltratie was in dit geval mogelijk doordat een aantal functionaliteiten in de anti-virus software en web-gateway waren uitgeschakeld. Daarnaast werkte het update-beleid niet zorgvuldig en was de gebruikte Java versie kwetsbaar.

Tot Slot

Er bestaat geen alles-in-een oplossing of een product X om een onderneming tegen een APT te beschermen. Het is veelal een combinatie van techniek, processen en personeel. Update-beleid van third-party software, bewustzijn bij gebruikers en het monitoren van uitgaand verkeer zijn zo een aantal voorbeelden die ondersteund moeten worden door goede - en jaarlijks te herziene - procedures. De indicaties van een APT zijn vaak aanwezig in de diverse logbestanden of het netwerkverkeer. Echterdoor gebrek aan tijd/geld/kennis wordt er geen aandacht besteed aan een zorgvuldige correlatie van gegevens. Start eens met het monitoren van uitgaand DNS verkeer en analyseer of er 'Generieke' malware meldingen zijn in de anti-virus software; het kunnen de eerste indicatoren zijn van een APT of botnet infectie.

USER-MANAGED ACCESS: VEILIG ONLINE DATA DELEN

Cordny Nederkoorn is een software tester werkzaam bij Immune-IT, een softwaretestconsultancy-bedrijf met klanten in Nederland en België. Hij is per email bereikbaar via cclnederkoorn@hotmail.com

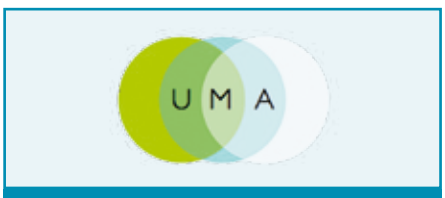
Cordny kwam met de UMAWG in aanraking bij de Cloud Identity Summit 2010 in Colorado, Verenigde Staten, waar hij een van de grondleggers van UMA, Eve Maler, ontmoette en gefascineerd werd door haar verhaal. Eve wilde graag een kwaliteitsslag maken met haar protocol en vroeg om hulp. Nu, anderhalf jaar later, heeft Cordny onder andere meegeholpen aan een interoperabiliteit testplan voor de implementaties van UMA bij verschillende organisaties en bedrijven.

Steeds meer mensen delen hun gegevens online. Met als gevolg dat de gedeelde data verspreid wordt over diverse sites. Hierdoor wordt het voor de data-eigenaar moeilijk te achterhalen wie waar toegang heeft tot zijn data. Data privacy en beveiliging zijn hierdoor in het geding. Hiervoor is nu een oplossing ontwikkeld: het *User-Managed Access* (UMA) protocol. UMA luidt een nieuw tijdperk in van User-centric Access control voor web-based applicaties zoals social networks, content-sharing portals en personal clouds. Dit artikel geeft een introductie tot UMA en haar online mogelijkheden.

UMA

De tijd die mensen online besteden is, zowel zakelijk als privé, toegenomen. Hierbij delen zij hun gegevens met derden, waarvan vaak niet duidelijk is wie er toegang tot hun gegevens heeft. Het User-Managed Access (UMA) protocol geeft de eindgebruiker de controle over haar online data.

Kantara Initiative
Een internationaal, open samenwerkingsverband van individuen uit de identity community, werkzaam in verschillende branches, die samenwerken aan oplossingen voor identity issues: interoperability & compliance testing (bv. SAML); identity assurance; beleid en wetgeving; eigenaarschap & aansprakelijkheid; privacy; UX & usability; cross community coordination; educatie; marketing; use cases en tools



Afb.1. UMA

UMA is ontworpen door een werkgroep van Kantara Initiative, de User-Managed Access Working Group (UMAWG). Kantara Initiative is een professionele organisatie, toegewijd aan het verbinden en harmoniseren van de identity-gemeenschap door middel van acties die meehelpen aan het veiligstellen van identity-based online interacties. Hierbij wordt misbruik van persoonlijke informatie voorkomen, zodat netwerken privacy-beschermend en betrouwbaar worden.

De UMAWG is ontstaan in 2009 nadat verschillende personen uit de identity community het mogelijk wilde maken dat een individu zelf de autorisatie kan beheren van de data die hij/zij wil delen tussen de online services. Daarnaast wilden zij een facilitatiecentrum vormen voor interoperabele implementaties van de te ontwerpen specificaties. De leden van de UMAWG, de UMAnitarians, ontwerpen de specificaties voor het UMA-protocol met de bedoeling de draft specificaties over te dragen als standaard aan de Internet Engineering Task Force (IETF). Een autorisatieprotocol maken en implementeren is lastig, maar door aan het begin van de specificaties al bezig te zijn met de testbaarheid ervan heeft dit voordelen tijdens de implementatie omdat van tevoren al goed is nagedacht over wat de mogelijke risico's bij implementatie zijn. De testbaarheid van het UMA-protocol is onderzocht door de specificatie om te zetten in pseudocode om te kijken of bepaalde stappen onvolledig of onvermeld zijn. Daarnaast is gekeken hoe in de specificatie is omgegaan met de verplichte (de 'MUSTs') en de optionele (de 'MAYs') stappen en/of eigenschappen. De testbevindingen hiervan gaven vaak verhitte discussies tijdens de wekelijkse UMA-teleconferences. Op een gegeven moment gingen de ontwerpers zelf ook pseudocode toepassen om zo mogelijke bevindingen voor te zijn. Deze kwaliteitsslag werd dus gemaakt, en toont aan dat een tester wel degelijk nut heeft bij de ontwikkeling van een specificatie.

> Vaak niet duidelijk wie toegang tot gegevens heeft

Stappen UMA

Nu we wat meer weten van UMA kunnen we ons wat meer verdiepen in haar eigenschappen.
UMA is gebouwd op het OAuth 2.0, een protocol, ontworpen om perso-

nen webservices te autoriseren voor het toegang krijgen tot de protected resources van een andere webservice.

OAuth 2.0
OAuth is een open standaard voor autorisatie. Gebruikers kunnen zo een programma/website toegang geven tot hun gegevens, zonder vermelding van gebruikersnaam en wachtwoord. In plaats daarvan wordt met tokens gewerkt die een bepaalde geldigheidsduur hebben en toegang verlenen aan slechts 1 type gegeven.

In vergelijking met OAuth 1.0 is OAuth 2.0 compleet nieuw, met meer nadruk op o.a. usability en performance.

Het grote verschil met van UMA met OAuth 2.0 is dat UMA de autorisatie-server (zie onder) bij een derde partij legt, die functioneert ten behoeve van de data-eigenaar.
UMA heeft een aantal specifieke deelnemers, die ik met een typische UMA use case zal illusteren: het verzenden van een online aangekocht boek.
De deelnemers worden vermeld met daarachter genoemd de rol van de deelnemer in het UMA-protocol.

Alice (UMA: de *authorizing user*) koopt een boek bij Books.com (UMA: de *requester*). Het adres van de klant staat in een online adressenboek AdresBoek (UMA: een *host*), waarbij de host toegang verleent op basis van een access policy gemaakt door bijvoorbeeld een Social Network zoals het fictieve SocialMe (UMA: *authorization Manager* / AM).

Alice heeft deze *access policy* bij SocialMe ingesteld. Dit betekent dat Alice zelf kan bepalen via SocialMe wie waar toegang heeft tot haar adres (UMA: *protected resource*).
Om aan dit proces te voldoen wordt het UMA-protocol doorlopen. Dit bestaat uit de volgende drie stappen: 'Bescherm de resource', 'Krijg Autorisatie' en 'Access de resource'.

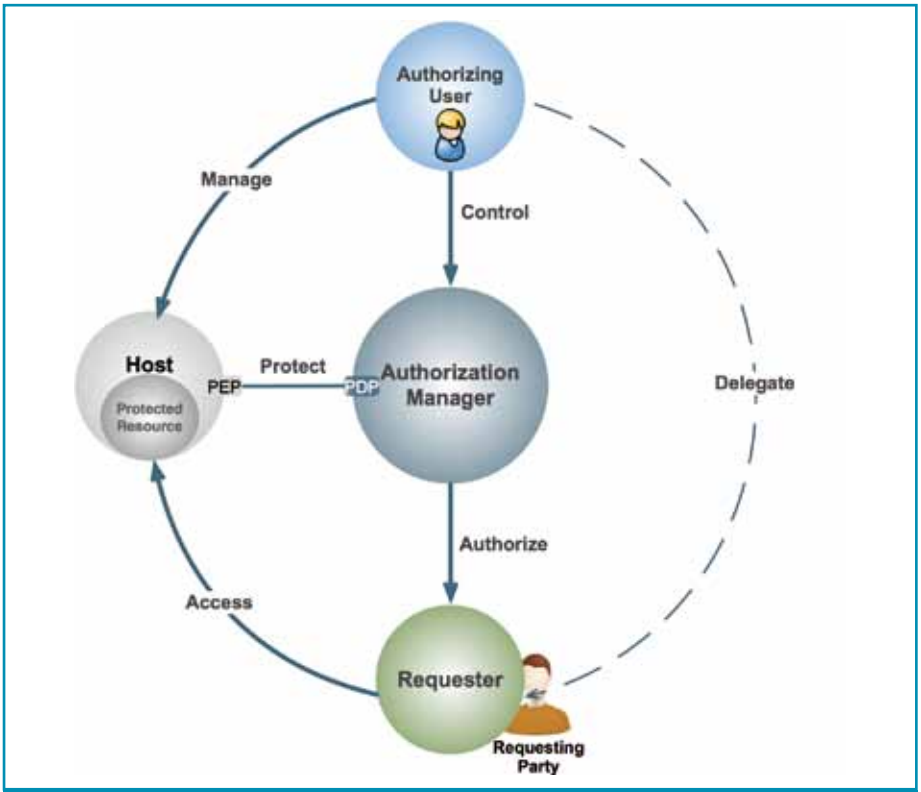
Een autorisatieprotocol maken en implementeren is lastig

Deze stappen zijn uitvoerig beschreven in het UMA Core Protocol, wat nog altijd aan verandering onderhevig is. Daarom worden nu de belangrijkste eigenschappen per stap besproken met behulp van het al besproken voorbeeld: het verzenden van een online gekocht boek.

>Bescherm de resource
Hierbij zijn de authorizing user Alice, de host AdresBoek en de Authorization Manager SocialMe betrokken.
Alice heeft AdresBoek gekozen voor het beheer van haar online resources.
AdresBoek heeft Alice geïntroduceerd aan SocialMe, door middel van een OAuth-interactie.
Hierbij heeft AdresBoek een access token van SocialMe gekregen. Via de protection API van SocialMe vertelt AdresBoek aan SocialMe welke resources (lees: adressen) een *access policy* hebben.
Daarnaast geeft, buiten het UMA-protocol om, Alice opdracht aan SocialMe welk toegangsbeleid moet worden toegewezen aan de betreffende adressen.

>Krijg autorisatie
Hierbij zijn de requester Books.com, host AdresBoek en AM SocialMe betrokken.
Bij deze stap wordt AdresBoek benaderd door Books.com (met de access token van SocialMe) om toegang te krijgen voor het door AdresBoek beheerde adres van Alice.
AdresBoek valideert de status van de token bij SocialMe en bij succesvolle validatie krijgt Books.com autorisatie om toegang te krijgen tot het adres van Alice.

>Toegang tot de resource
Hierbij krijgt, indien aan stap 1 en 2 is voldaan, Books.com toegang tot het adres van Alice, beheerd door Adres-



Afb.2. UMA players

Boek. Nu kan Books.com het door Alice gekochte boek naar haar opsturen.
Zoals al gezegd, een meer gedetailleerde beschrijving van de UMA-stappen kunt u vinden in het UMA Core Protocol dat te vinden is op de UMAWG-website. Let wel, UMA is nog steeds in ontwikkeling en de documentatie is aan verandering onderhevig.

Status UMA

In juni 2011 vond de officiële lancering plaats van het UMA-protocol: de publicatie van een draft recommendation voor het UMA-protocol en toevoeging ervan aan de IETF-standaarden.
Dankzij deze lancering en ondanks mogelijke toekomstige veranderingen, zijn UMAnitarians begonnen met het implementeren van UMA in online applicaties. De bekendste (en de oudste) is die van Newcastle University met het SMART project.

UMA is nog steeds in ontwikkeling

SMART staat voor Student-Managed Access to Online Resources, oftewel een online data access management system voor studenten in het Hoger Onderwijs.
Andere voorbeelden zijn een mobile location scenario (Fraunhofer Institute) en het Health Data Exchange-project hData (MITRE). Implementaties, gebaseerd op UMA, met actuele toepassingen. Tot op heden is er helaas nog geen Nederlandse implementatie bij de UMAWG bekend. Meer implementaties zijn te vinden op de UMAWG-website.
Zoals ik al zei in de introductie, meer mensen delen hun gegevens online. UMA stelt hen in staat de toegang tot hun data zelf te beheren, wat de online privacy en veiligheid van deze personen waarborgt.
UMA is in ontwikkeling en de UMAWG verwelkomt graag nieuwe (Nederlandse) UMAnitarians die mee willen werken aan nieuwe use cases, relaties met claims, interoperabiliteit met OpenID-Connect en implementaties van UMA. Wie wil er nou niet meewerken aan een veilig en privacygericht internet?

Verwijzingen

website UMAWG: http://kantarainitiative.org/confluence/display/uma/Home

website OAuth 2.0: http://oauth.net/2/

BLACK HAT EUROPE 2012

AMSTERDAM REVISITED

Lex Dunn CISSP ISSMP is Security Officer bij een grote, internationale ICT-dienstverlener. Hij is tevens voorzitter van de MSP-ISAC. Hij is bereikbaar via lex.dunn@capgemini.com.

Na twee jaar in Barcelona was het Black Hat Europe circus weer neergestreken in Amsterdam. Op 14, 15 en 16 maart was Krasnapolsky weer even het domein van de witte en zwarte hoeden. Hoe zit dat nu eigenlijk met "Black Hat" en "Black Hat Sessions"? Black Hat Europe is de Europese variant van de in Amerika al langer bekende Black Hat sessies (meestal in exotische plaatsen als Las Vegas ;-)). De Black Hat Sessions zijn een Nederlandse aangelegenheid en worden georganiseerd door Madison Ghurka, dit jaar op 4 april in de Reehorst in Ede (een verslag hiervan staat in het volgende nummer). In IB4 2010 en IB4 2011 vindt u verslagen van de eerdere Black Hat sessies in Barcelona.
Terug naar Krasnapolsky. De openingsspeech was voor Whitfield Diffie, bekend van de Diffie-Hellman key exchange, een van de grondslagen van de moderne cryptografie. Hij had het onder andere over "defense" versus "offense" en concludeerde dat je maar beter aan de "offense" kant kunt staan: als een aanval succesvol is ben je de held, doe je daarentegen "defense" dan wordt elke mislukking breed uitgemeten. Verder was de strekking van zijn betoog dat de huidige cryptografie voldoende beveiliging biedt, maar dat de vertrouwelijkheid steeds vaker door de "menselijke factor" wordt doorbroken (denk aan Bradley Manning, die WikiLeaks geheime US documenten toespeelde).
De drie dagen werden gevuld met zeer interessante en vaak ook erg technische sessies, in drie tracks. Een hoogtepunt (wat mij betreft):
U hebt een iPhone of Android toestel? En u heeft daar uw wachtwoorden/pincodes/credit card nummer in opgeslagen? Natuurlijk gebruik makend van zo'n handige "app", een "secure password manager" met "military-grade encryption"? Yeah, right! Niet dus. Onderzoek van een groot aantal vrij verkrijgbare, maar ook commerciële apps voor zowel iPhone als Android, door Andrey Belenko en Dmitry Sklyarov toonde tot hun verbijstering aan dat een aantal van deze apps niet eens de data te versleutelen, maar alleen het wachtwoord om de data in te zien! Bij de wel versleutelde data was het in veel gevallen erg makkelijk (lees: binnen enkele minuten) om middels "brute force" de data te ontsluiten.

Meer informatie is te vinden op de website van Black Hat: http://www.blackhat.com/html/bh-eu-12/bh-eu-12-home.html

GOING UP? SAFETY FIRST, THEN SEND YOUR DATA TO THE CLOUD

Joe Sturonis, CTO van PKWARE, schrijft over de risico's van informatie in de cloud. Wanneer bedrijfsinformatie aan de cloud wordt toevertrouwd is er maar één strategie dat een bedrijf kan toepassen om zich te verzekeren dat de vertrouwelijkheid en integriteit van die informatie geborgd is: vercijfer je informatie vóór je het aan de cloud toevertrouwd. Hierbij is het belangrijk om de vercijfering op bestandsniveau te doen, in plaats van vercijfering van het datakanaal.

By: Joe Sturonas. Joe Sturonas is Chief Technology Officer for PKWARE. PKWARE offers software solutions to critical IT problems, namely the explosive growth of data, the need to secure data, and the emergence of data in the cloud. He can be reached at Joe.sturonas@pkware.com.

As the proliferation of data continues to plague businesses, the pressure is on for companies to migrate away from their physical data centers usually on premise or within rented cages at large hosting providers. Cloud computing is being adopted at a rapid rate because it addresses not only the costs for physical space but also rising energy costs and mandates for more scalable IT services. Enterprises are drastically reducing their storage spend by using online storage solution providers to store massive amounts of data on third party servers. The trend of skyrocketing adoption rates for cloud computing is largely due to the more flexible on-demand IT resource capabilities, allowing anyone to capitalize on scalable storage solutions. According to IDC, public IT cloud services spending is expected to reach $72.9 Billion in 2015. Likewise, Gartner estimates that enterprises will spend $112 billion by 2015 cumulatively on cloud related technologies. The cloud is definitely calling, but even the most seasoned IT professionals debate, grapple and even get a bit intimidated by an otherwise simple term that has taken the world by storm.

Defining the Cloud

For professional collaboration and a more technical understanding, it is useful to standardize our definitions. Leveraging the Cloud Security Alliance [1] and published work of the scientists at the U.S. National Institute of Standards and Technology and their efforts around defining cloud computing [2] we find:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications, and services). Cloud computing is a disruptive technology that has the potential to enhance collaboration, agility, scaling, and availability, and provides the opportunities for cost reduction through optimized and efficient computing. The cloud model envisages a world where components can be rapidly orchestrated, provisioned, implemented and decommissioned and scaled up or down to provide an on-demand utility-like model of allocation and consumption."

> Any clouds are at high risk for loss, breach and exposure

If we explore even further, Cloud computing is often divided into three main service types: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). And by design, each impacts data control and governance in a slightly different manner. Since one of the most attractive features of cloud computing is efficiency afforded by economies of scale, the very inclusion of a blanket security protocol is perceived as restrictive and a possible deterrent to the masses.

> Cloud providers cannot help your damaged reputation

With IaaS, the customer may have full control of the actual server configuration granting them more risk management control over the environment and data. In fact, oftentimes IaaS or infrastructure Cloud environments will basically push all of the security protection onto the customer. In PaaS, the provider manages the hardware and underlying operating system but securing the applications developed against the platform and developing them securely belong to the consumer. With SaaS, both the platform and the infrastructure are fully managed by the cloud provider; security controls and their scope are negotiated into the contracts for

service. Amazon Web Services contract proves the necessity for security controls: it explicitly calls out encryption as an option for protecting "your Content", however Amazon does not provide it.

Lastly, the Cloud is generally categorized into three deployment models:

1. **Private cloud-** infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers.
2. **Public cloud-** infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
3. **Hybrid cloud-** infrastructure is a composition of two or more distinct cloud infrastructures. (Source: NIST)

With a more complete understanding, we can now highlight several significant benefits of cloud computing:

- Replacement of capital expenses with operating expenses
- Reduction in hardware costs
- Less required capacity
- Lower technology risk
- Increased productivity
- Improved user experience
- Overall impact on the environment improved

"For the foreseeable future, Cloud computing and storage will be the primary means to automate routine tasks and provision for the flexible delivery of content when and where it is needed. As organizations get swept up in the benefits, they should stay vigilant –private, public, hybrid, any clouds are at high risk for loss, breach and exposure if data isn't properly protected."
~Joe Sturonas, CTO, PKWARE

In Practice: Sending Server Data to the Cloud
Enterprises are constantly dealing with ever expanding unstructured data, where Network Attached Storage (NAS) ends up being a dumping ground for unstructured data. When unstructured enterprise data needs to be archived for compliance and regulatory concerns, data centers are looking to do that on the least expensive storage they can, as there are few performance requirements on archive data. A simpler, less expensive and more reliable way to archive server data would be to compress and encrypt the data on the server before sending to the cloud.

In Practice: Sending Mainframe Data to the Cloud
IBM Mainframe data is stored in a disk organization known as a Count-key-data (CKD) architecture, which gets its name from the record format, where the disk is addressable through Cylinder-Head-Record, unlike open systems disk architectures where they are based on organizing the disk into sectors or blocks. In other words, IBM Mainframe files are very structured and require the files to be pre-allocated on disk before data can be written; and the record lengths, block sizes and space need to be known when allocated. Mainframe data files can be saved on less expensive Cloud storage, but the mainframe data will lose the structure it had as a CKD file. If the archive data needs to be restored back on mainframe CKD storage, the file will need to be pre-allocated with very specific record size, block size, data set organization (type of mainframe file) and maximum space allocation. Then the data would need to be transformed back as a mainframe file. A much simpler, safer and more reliable way to archive mainframe data would be to compress and encrypt the data on the mainframe before archiving to the cloud.

Inevitable Risk
Every minute of every day presents the opportunity for a data mishap. A security breach, as well as lost, stolen or even compromised records triggers negative exposure that quickly equates to forfeited sales, legal fees, disclosure expenses and a host of remediation costs. The fallout can result in years of struggle to recoup reputation and repair a brand in the marketplace. Cloud providers do not want to be held liable for any issues related to your data loss. Best case, they will credit back your fees, but nothing can help a damaged reputation or customers who leave your organization when a data breach occurs.

While the cloud environment seems be to a holy grail for trends around data proliferation and massive storage needs; clouds present complex security issues and put critical corporate data, intellectual property, customer information, and PII (Personally Identifiable Information) in potential jeopardy. Enterprises forfeit security and governance control when data is handed over and cloud providers do not assume responsibility.

The recent cyber attacks and associated data breaches of Google and Epsilon (a leading marketing services firm) illustrate the need to incorporate an advanced risk and compliance plan that includes any third-party managed cloud environment. Clearly, the cloud often opens a Pandora's Box for unanticipated consequences.

Storing huge amounts of data on third party servers may mean instant online access and lower costs; however, that data is often comingled on shared

servers and exposed to users you don't know. If your Cloud storage provider encrypts your data but holds the key, anyone working for that Cloud storage provider can gain access to your data. That means the potential of your data be shared, sold, marketed to and profiled for someone else's gain.

Any data stored in dormant VMs lacks protection

Data also has to actually "get to" the cloud, which usually means leaving your trusted infrastructure and overcoming compounded transfer vulnerabilities as data moves to and from the cloud. Even the most unintended data breach could cost a company its reputation.

Potential Pitfalls

Transfer vulnerabilities - The potential for data breaches is multiplied as data travels to and from the cloud using various networks especially in highly mobile and distributed workforces.

Non-compliance penalties - Extended enterprises, partner networks and virtual machines are continuously scrutinized for compliance. All sensitive data must be protected with appropriate measures.

Storage expense - Companies are charged by the amount of data that is put into the cloud; therefore providers lack motivation to compress that data. Any compression by providers is deemed unreliable since encrypted data cannot be compressed.

VM control - Sensitive data that is transferred to an unprotected virtual machine (VM) will be exposed to users with access to the shared server. Any data stored in dormant VMs lacks protection when the operating system is not active or properly patched. VM sprawl wastes resources and creates unmonitored servers that could have access to sensitive data.

Provider holds the keys - Cloud agreements can address how internal folks at the vendor will be managing your data. Provisions can limit administrative access and grant who has hiring and oversight over those privileged administrators. If the data that is housed in the Cloud is, in fact, encrypted then the issue becomes more about who maintains the keys.

To summarize…

Security breaches will happen even for the most vigilant that do not encrypt their data.

Your company's reputation is at stake.

Security regulations are increasing.

The Cloud introduces new levels of risk.

Unsecure services, such as Dropbox, pose a security risk

Cloud providers have root access to all your unencrypted data in the cloud, and they are not your employees.

The only way to protect data in the cloud is if you encrypt the data and you maintain control of the private key.

CLOUD SECURITY BEST PRACTICES

Impact on security policies and procedures?

Your existing security policies and procedures need to be reviewed to evaluate the use of Cloud applications and storage. Some companies choose to shut off access to certain Cloud applications, some choose to implement application-stores to limit access to specific approved applications, and some do not attempt to curtail access at all. Shutting off access is not a popular option to your employees who are most likely already familiar with consumer type options, such as Dropbox. Your end-users have certain problems like transferring or sharing a large file too large for email that they know such services can solve.

Employees, internal team members and partners, may not have any idea of the risk of putting data in the Cloud insecurely. They probably have no idea that unsecure services, such as Dropbox, pose a security risk and may have sensitive company data stored there. You need to alert them to the data security risks of the Cloud and have them sign a security policy to that effect.

The regulatory standards issues that you deal with today in your own data center are just as important in the

Cloud. Compliance with PCI DSS, EU Privacy Act, Sarbanes-Oxley, and FIPS140-2, etc. are just as imperative. If you know that the data is encrypted before it goes into the Cloud, you may be compliant with any number of these regulations. Even if the Cloud vendor is hacked or someone uses an administrative password improperly, your data is impregnable at that location.

EVALUATING SECURITY SOLUTIONS FOR THE CLOUD

Encrypting your data and maintaining the keys yourself is considered by industry experts as the only way of making sure that no one can read your data, period. It doesn't matter if a privileged user has access to your data, they still can't decipher it.

According to Cloud Security Alliance's "The Security Guidance for Critical Areas of Focus in Cloud Computing" [3], one important way to increase data protection, confidentiality and integrity is to ensure that the data is protected in transit and at rest within the cloud using file-level encryption. It points out, "encryption offers the benefits of minimum reliance on the cloud service provider and lack of dependence on detection of operational failure."

Regulatory compliance counts in any cloud, any environment, any country, you must ensure your data is compliant with any regulation standards for your industry.

If there are assistants, executive and sales representatives who use different operating systems on different computing platforms and want to share that data securely inside or outside of the private or public cloud…then you need data-centric, file-level encryption that is portable across all.

Be sure to evaluate Data Location and Data Segregation as they relate to co-tenancy. Not only do you want to hold the key, but you want to encrypt all of your data so that your data, especially sensitive data (PII), is protected if comingled with other organization's data.

A Cloud security solution must also enable recovery and provide you with the ability to restore your data many years from now. To meet some regulatory compliance statutes you have to keep your data for seven, even 20 years.

Cloud providers might assure users that the communications from your browser to their servers are encrypted using TLS. That provides a level of protection of the data only as it travels through the Internet, but then data remains in the clear once it landed on their server.

> You will have to report a breach one day

Worry-free breach

Odds are you will have to report a breach one day. If that day comes, you want to announce that no data was compromised and minimize corporate liability both in dollars and reputation. With data-centric encryption where you hold the keys and the data is encrypted at the file level, no one can access that data. Therefore, you may not even have to report it as a breach and you don't really have to rely on all the remediation contractual issues…because essentially there was a breach but no data was lost.

So before you store sensitive data in the Cloud, make sure you encrypt that data. This insures that your data is safe and accessible to you and only you.

References:

Cloud Security Alliance: http://www.cloudsecurityalliance.org

U.S. National Institute of Standards and Technology: http://www.csrc.nist.gov

Cloud Security Alliance's "The Security Guidance for Critical Areas of Focus in Cloud Computing": https://cloudsecurityalliance.org/research/

COLUMN

PRIVACY DOOD? WAT EEN ONZIN

Boe-roepers zijn van alle tijden. Privacy-is-dood-roepers kom ik de laatste jaren ook steeds vaker tegen. Schermer riep het als stelling bij zijn proefschrift in 2007, Zuckerberg riep het in 2010, Rambam riep "Privacy is dead, get over it" in 2006, Schmidt riep het in vergelijkbare woorden in 2010 door te zeggen "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" en McNeally zei al in 1999 "You have zero privacy anyway". Ik zal u vertellen waarom al die heren ontzettend ongelijk hebben. Ze hebben er namelijk helemaal niets van begrepen. Maar dat geeft niet, iedereen heeft het recht om ongelijk te hebben. Zolang ze maar van uw en mijn grondrecht op privacy afblijven.

Maar waarom hebben die heren nu zo ontzettend ongelijk? Ten eerste omdat ze alleen maar naar bepaald gedrag kijken met betrekking tot informationele privacy om vervolgens op grond daarvan te oordelen dat privacy dood is. Informationele privacy gaat over de privacy van informatie over personen. Dit is slechts een gedeelte van het grondrecht op privacy. Het grondrecht op privacy omvat bijvoorbeeld ook de onschendbaarheid van het lichaam en het huis. Maar ook het briefgeheim en het recht om zonder onredelijke beperkingen te genieten van het gezinsleven. De dood van privacy slechts baseren op een aspect van het meeromvattende recht, lijkt mij een zeer gewaagde (en ook volledig incorrecte) aanname. Als privacy dood zou zijn, dan is het helemaal niet vreemd dat de postbode uw post al gelezen heeft voor hij bij u op de mat valt, dat uw voordeur altijd openstaat en dat het een ieder toegestaan is eens een kijkje te nemen in uw slaapkamer en dat uw werkgever van u mag verlangen dat u elke maand een uitgebreide medische test ondergaat (inclusief visitatie in alle lichaamsholtes, uitgevoerd door uw manager) waarbij de uitkomsten daarvan online gepubliceerd worden.

Ten tweede is de redenatie van dit soort boe-roepers zo lek als een mandje. Er schuilt een fundamentele fout in de logica gehanteerd door deze boe-roepers. Het gaat als volgt:

"U, beste gebruiker van de online wereld, zet alles online.
(Zelf geconstateerd feit niet gebaseerd op wetenschappelijk onderzoek)
Daarom is privacy dood.
(Daaruit een algemene conclusie trekken)
U heeft toch alles al weggegeven".
(De conclusie versterken door een ondersteunend argument aan te dragen)
Een van de fundamentele waarden achter het grondrecht op privacy is de autonomie van personen. Personen genieten de vrijheid om informatie over zichzelf te delen met anderen. De redenering dat de privacy dood is omdat personen gebruik maken van de autonomie die hen gegeven is, is absurd. Ik maak van mijn vrijheid gebruik en daarom wordt het grondrecht dat is ingegeven door deze autonomie de nietigheid in verklaard. Ziehier: de drogredenering gebaseerd op een aanname van niet bewezen feiten versterkt door een ondersteunend argument om het fatalistische van de situatie te bestempelen: "geef het nu maar op, er is niets tegenin te brengen". En dit staat dan nog even los van de vraag of al die mensen nu zomaar echt alles online zetten en of datgene wat ze daar dan neerzetten ook wel juist is. Ik wil de mensen die online liegen en onjuiste persoonsgegevens invullen liever niet de kost hoeven geven.

Ten derde: het begrip privacy is niet waardevast. Er bestaat geen definitie van privacy en een ieder die een poging daartoe waagt, zal zichzelf zien falen omdat hij achterhaald wordt door de feiten. Privacy is contextgevoelig, cultureel bepaald, flexibel van geest en gebonden aan temporele invloeden. Hoe privacy ingevuld wordt en wat wij daaronder verstaan is aan verandering onderhevig, het verschilt per plaats op de wereld en op welk moment in tijd wij ons bevinden. Wist u bijvoorbeeld dat het recht op lichamelijke integriteit pas in 1983 een plaats kreeg in onze grondwet? En dat daar echt letterlijk alleen het lichaam onder valt en niet de geest? Wist u dat het briefgeheim alleen papieren post omvat en dat een email daar dus niet onder valt? Wist u dat al in 1890 in de Verenigde Staten geopperd werd dat er een recht op privacy bestaat, maar dat er tot op de dag van vandaag geen grondrecht op privacy te vinden is in de Constitution?

Privacy is dood! Lang leve privacy!

mr. Rachel Marbus, @rachelmarbus op twitter

P.S. Ik neem namens het Platform voor Informatiebeveiliging deel aan het Nationale Privacy Debat op 11 juni in Den Haag. Komt u ook? www.nationaalprivacydebat.nl

HET LEKKEN VAN DATA

Johan Pater is als security consultant werkzaam bij KPN Corporate Market BV en heeft dit artikel op persoonlijke titel geschreven.

De Wet bescherming persoonsgegevens (Wbp) wordt aangepast met een meldplicht datalekken. Dit noodzaakt bedrijven en overheden zorgvuldiger met persoonsgegevens om te gaan, naast dat er reeds de algemene verplichting is om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. Maar wordt door deze meldplicht de beveiliging beter en wordt daarmee het lekken van data voorkomen? Welke organisaties moeten dit verplicht melden? En wat als het 'lek' niet wordt gemeld maar het op een andere manier bekend wordt? Kunnen er boetes worden opgelegd en door wie? En worden de meldingen betreffende datalekken openbaar gemaakt? Welke maatregelen kunnen organisaties nemen om datalekken te melden?

De beveiliging van informatie is tegenwoordig niet eenvoudig te noemen. Wet- en regelgeving is gecompliceerd en stelt eisen aan de beveiliging. Organisaties zijn qua informatie meer en meer van elkaar afhankelijk waardoor de grenzen van ICT-netwerken en verantwoordelijkheden lijken te vervagen. Daarnaast wordt de uitwisseling en opslag van informatie alleen maar omvangrijker en verandert de onderliggende techniek en het gebruik daarvan voortdurend. Het is dan ook niet eenvoudig om bescherming te bieden en te behouden. In het rapport[1] 'Cybersecurity beeld Nederland 2011', opgesteld door Govcert, nu het Nationaal Cyber Security Centrum (NCSC), worden digitale spionage en cybercrime als de grootste dreigingen voor Nederland genoemd. Dit blijkt ook wel als we terugkijken naar de security incidenten die zich hebben voorgedaan. Er zijn security incidenten geweest waarbij enorme hoeveelheden vertrouwelijke (persoons)gegevens zijn gelekt, organisaties niet meer konden werken of zelfs de staatsveiligheid in het geding kwam[2]. Wat hierbij vooral opviel was het aantal privacy incidenten en de hoeveelheid persoonsgegevens die op straat kwamen te liggen. Dat is merkwaardig omdat de bescherming van die persoonsgegevens voor veel organisaties belangrijk is omdat klanten en hun gegevens vaak het bestaansrecht zijn van een organisatie. Het respecteren van de privacy - en met name in relatie tot gegevens van klanten, burgers, medewerkers, bedrijven en partners - en het vertrouwelijk omgaan met en beschermen van die persoonsgegevens is dan ook ontzettend belangrijk. Het recht op privacy is vastgelegd in de Nederlandse grondwet en in het Europees Verdrag voor de Rechten van de Mens. Een onderdeel van het grondrecht op privacy gaat over de verwerking van persoonsgegevens hetgeen is uitgewerkt in de Wet bescherming persoonsgegevens (Wbp). Het kabinet wil dat organisaties het verlies, diefstal of misbruik van persoonsgegevens gaan melden. Hiervoor wordt de Wbp uitgebreid met een meldplicht datalekken. Wat betekent dat voor bedrijven en overheden en wordt hiermee ook het lekken van data opgelost?

De meldplicht datalekken

In december 2011 is het wetsvoorstel[3] voor aanpassing van de Wbp gepubliceerd. In dat wetsvoorstel staat dat bij het doorbreken van de beveiligingsmaatregelen, de verantwoordelijke organisatie die de persoonsgegevens verwerkt het College bescherming persoonsgegevens (Cbp) direct hierover moet informeren. De verantwoordelijke dient ook de betrokkenen wiens gegevens het betreft direct op de hoogte te brengen. Hierbij moet wel sprake zijn van nadelige gevolgen voor de privacy van die betrokkenen. Zij hoeven naar het oordeel van het Cbp niet te worden geïnformeerd indien er gepaste technische maatregelen zijn genomen waardoor de persoonsgegevens zijn versleuteld, of anderszins onbegrijpelijk zijn gemaakt voor eenieder die geen recht heeft op kennisname van de gegevens. Organi-

saties die een deel van hun ict hebben uitbesteed aan een dienstverlener dienen met de meldplicht rekening te houden in de bewerkersovereenkomst. Immers de dienstverlener heeft meestal toegang tot de data om hier een backup van te maken. Ook bij een dienstverlener kunnen immers lekken ontstaan. Hier dienen afspraken over te zijn gemaakt zodat bij een eventueel datalek de verantwoordelijke organisatie onmiddellijk wordt ingelicht door de dienstverlener zodat ze kan bepalen of er daadwerkelijk een datalekmelding moet worden gedaan. Daarbij kunnen de volgende vragen worden gesteld:

1. Is er een inbreuk geweest op de genomen beveiligingsmaatregelen? Zowel digitaal als fysiek kunnen er inbreuken op de beveiliging plaatsvinden. Een fysieke inbraak is relatief eenvoudig te constateren, maar een digitale inbraak vereist meestal een diepgaander onderzoek. Ook het verlies of diefstal van een smartphone of bijvoorbeeld laptop,usb stick of andere mediadrager zijn inbreuken op beveiligingsmaatregelen.
2. Zo ja: zijn er persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking? Dit moet zo objectief mogelijk worden beoordeeld want bij een fysieke inbraak kunnen ook usb sticks met persoonsgegevens zijn ontvreemd. Bij een digitale inbraak is analyse van de logfiles noodzakelijk om dit goed en objectief te kunnen bepalen.
3. Zo ja: is er een aanmerkelijk risico? Dit is niet eenvoudig omdat hier moet worden bepaald of er een aanzienlijk risico is dat die data is verloren of wordt misbruikt. Zo geeft het verlies van een mobiele telefoon of usb stick niet direct aanleiding om een melding te doen. Dit is afhankelijk van de aard van de inbreuk, de aard van de data die het betreft en het risico dat de betrokkenen lopen ingeval van zoekraken of onrechtmatige verwerking.

4. Zo ja: als het risico zich voordoet leidt dit dan tot nadelige gevolgen voor de persoonsgegevens of de persoonlijke levenssfeer van de betrokkene? Kortom, zijn er nadelige gevolgen voor de privacy van de betrokkenen? Dit is moeilijk te bepalen alhoewel het lekken van de hierboven genoemde voorbeelden hier meestal wel toe leidt.

Indien alle vragen met ja zijn beantwoord, dient men de datalekmelding bij het Cbp te doen. Zowel aan het Cbp als aan de betrokkenen dienen in ieder geval te worden gemeld:

- Aard van de inbreuk in een algemene omschrijving;
- Instanties waar meer informatie kan worden verkregen;
- Contactgegevens van de verantwoordelijke;
- En de aanbevolen maatregelen die de betrokkenen zelf kunnen nemen om de impact te beperken.

Daarnaast dient de melding aan het Cbp een beschrijving van het gebeuren te bevatten en de gevolgen voor de verwerking van de persoonsgegevens en de maatregelen die daarop zijn genomen of nog moeten worden genomen. Indien de verantwoordelijke organisatie niet voldoet aan deze meldplicht dan is het Cbp bevoegd om een bestuurlijke boete op te leggen van maximaal €200.000. De boete en eventuele negatieve media-aandacht, en daardoor mogelijke reputatieschade, heeft een grote impact op een organisatie. Dit betekent dat organisaties nog eens goed over privacy moeten nadenken en controleren of persoonsgegevens afdoende zijn beveiligd. Hopelijk worden organisaties door de dreiging van dergelijke boetes positief gestimuleerd om de beveiliging op orde te hebben en te houden om zodoende privacy incidenten te voorkomen.

Bijna alle organisaties die persoonsgegevens verwerken moeten aan het nieuwe artikel 34a voldoen. Alleen organisaties die aan de Wet financieel toezicht moeten voldoen zoals financiële instellingen hoeven niet aan het nieuwe artikel 34a in de Wbp te voldoen. In de Wet financieel toezicht is namelijk al een dergelijke meldplicht opgenomen. Het grote verschil is dat financiële instellingen een lek van persoonsgegevens niet aan de betrokkenen hoeven te melden omdat dit een te hoog risico betreft. Denk maar

aan de gevolgen indien mensen het vertrouwen in een bank verliezen en spaarders massaal hun geld van de bank halen. Aanbieders van elektronische communicatiediensten zoals telecomproviders dienen een datalekmelding straks ook bij het Cbp te doen. Deze aanbieders vallen onder de Telecomwet en deze wetgeving wordt daarvoor aangepast. Ook aan deze aanbieders kan het Cbp dan een maximale boete van €200.000 opleggen.

Melding openbaar of niet?

Volgens Bits Of Freedom[4] worden datalekmeldingen niet openbaar gemaakt. Uit het wetsvoorstel is niet duidelijk op te maken of alle datalekmeldingen openbaar toegankelijk zijn. Wel staat er een toelichting in het wetsvoorstel dat bij een vermoeden van strafbaar handelen het strafrechtelijk onderzoek kan vereisen dat een door de verdachte gevolgde unieke werkwijze niet publiekelijk bekend wordt gemaakt omdat dit het onderzoek zou hinderen. Vervolgens staat er in de toelichting dat de kennisgeving aan het Cbp zonodig ook geheel of gedeeltelijk vertrouwelijk kan worden gedaan. Er wordt daarbij niet vermeld dat de datalekmelding openbaar wordt gemaakt indien het onderzoek is afgerond. Terwijl dit volgens Bits of Freedom nu juist de transparantie ten goede zou komen. Maar wanneer is de melding transparant en leren organisaties daarvan? Is dat indien er een overzicht wordt gepubliceerd van organisaties die een datalek hadden en de gegevens die mogelijk hierbij betrokken zijn geraakt? Of is dat door publicatie van de details van inbraak en de daarbij benutte kwetsbaarheden met als gevolg dat die gegevens ook kunnen worden misbruikt? De ervaring leert dat er pas extra maatregelen worden genomen indien de schade al is geleden. Hier komen vaak hoge kosten bij kijken omdat de beveiliging achteraf snel moet worden ingeregeld. Het publiceren van een lijst met organisaties met datalekken zorgt waarschijnlijk niet voor een hogere bewustwording bij organisaties waardoor zij hun beveiliging onder de loep gaan nemen. Een andere en wellicht betere optie is dat het Cbp of het NCSC een analyse doet op de oorzaken van datalekken en hierop stuurt om organisaties hier bewust van te maken dit te verbeteren. Zo publiceert het NCSC regelmatig factsheets en whitepapers[5] over onderwerpen die belangrijk zijn voor de ICT-veiligheid en hieraan kunnen bijdragen.

Melding bij het Cbp?

Het wetsvoorstel stelt dat organisaties het Cbp moeten informeren inclusief de maatregelen die zijn of worden genomen om het lek te verhelpen. Het Cbp zal hierin dan vooral een administratieve taak hebben. Op de website tweakers.net[6] is te lezen dat de Nationaal Coördinator Terrorismebestrijding en Veiligheid, Erik Akerboom, voorstelt om het Nationaal Cyber Security Centrum (NCSC) de meldplicht voor datalekken op zich te laten nemen en dat zij daarmee de ontvanger worden van de meldingen. Volgens het artikel op tweakers.net moeten organisaties met datalekken deze dan melden bij het NCSC, dat vervolgens expertise kan leveren bij het oplossen ervan. Dit zou een goede aanvulling op de dienstverlening kunnen zijn. Maar volgens de NCSC[7] website zijn de primaire doelgroepen van het NCSC de rijksoverheid en de vitale sectoren. Het NCSC richt zich hierbij op incidenten die kunnen leiden tot grootschalige ICT-verstoring. Het NCSC zou dan alleen een rol kunnen hebben voor de genoemde doelgroepen. Een andere optie is dat de melding nog steeds bij het Cbp wordt gedaan maar dat gemelde lekken van organisaties met een relatie tot de vitale sector worden doorgegeven aan het NCSC. Meestal hebben deze organisaties namelijk al een relatie met het NCSC. Daarnaast is het zo dat het wetsvoorstel uitgaat van ongeveer 103.700 ondernemingen die hieronder gaan vallen. Hierbij wordt ingeschat dat er jaarlijks 66.000 datalekmeldingen worden gedaan bij het Cbp. Dat betekent dat er circa 180 meldingen per dag worden gedaan. Hierdoor kan het Cbp niet meer doen dan de melding ontvangen, registreren en bewaren. Natuurlijk leidt dit niet telkens tot een onderzoek, maar hoe het Cbp

dergelijke aantallen moet gaan afhandelen moet de praktijk gaan uitwijzen.

Beveiligingsinbreuken en maatregelen

In artikel 34a van het wetsvoorstel staat dat organisaties een overzicht moeten bijhouden van alle inbreuken op de beveiliging. Dit is inclusief de inbreuken die wel zijn geconstateerd maar niet zijn gemeld omdat er bijvoorbeeld geen persoonsgegevens bij betrokken waren. Achteraf zou dan kunnen worden beoordeeld of de inbreuk toch had moeten worden gemeld. Hierbij is niet vermeld hoe lang dit overzicht moet worden bewaard en wat dan de criteria zijn. Aan het Cbp moet onverwijld of ogenblikkelijk een beveiligingsinbreuk met verlies van persoonsgegevens worden gemeld. En indien de persoonsgegevens niet waren versleuteld of op een andere manier onbegrijpelijk waren gemaakt dan dienen ook de betrokkenen direct op de hoogte te worden gesteld van de inbreuk. Werknemers kunnen ook een oorzaak van een datalek zijn zoals door het verliezen van een smartphone of inbraak bij de werknemer thuis. Het is daarom voor een organisatie noodzakelijk dat gebruikers worden geïnstrueerd wat zij wel en niet moeten doen.

Ook is het handig als een organisatie de incidenten centraal registreert en vastlegt welke informatie hierbij betrokken is en om hoeveel gegevens het gaat. Hierdoor is een organisatie beter in staat om een datalekmelding bij het Cbp te doen. De betrokkenen, wiens gegevens zijn gelekt, hoeven niet te worden geïnformeerd indien de informatie is versleuteld of op een andere wijze onbegrijpelijk is gemaakt. Dus een maatregel die bijna altijd kan worden genomen is het versleutelen van de communicatiekanalen, wachtwoorden en informatie op mobiele datadragers zoals laptops, harde schijven, backup tapes, geheugensticks/kaarten en smartphones. Hierdoor zijn bij een eventueel lek de bedrijfs- en of persoonsgegevens niet meer leesbaar waardoor de impact lager wordt. Uiteraard dient de versleuteling niet eenvoudig achterhaalbaar te zijn. Dit kan men oplossen door gebruik te maken van versleutel algoritmes met voldoende keylengte[8]. Maar hoe kunnen organisaties inbreuken signaleren op de genomen beveiligingsmaatregelen? Organisaties moeten dan de gebeurtenissen op het netwerk en in applicaties gaan vastleggen. Vervolgens dienen deze gebeurtenissen regelmatig te worden gecontroleerd. Het is voor de meeste organisaties bijna onmogelijk om alle gebeurtenissen handmatig te analyseren. Dit kan alleen maar automatisch worden gedaan waarbij verbanden worden gelegd en prioriteiten aan gebeurtenissen kunnen worden gesteld. Hierdoor kunnen inbreuken eerder worden 'gezien' en kan sneller een eventuele melding na analyse worden gedaan. Daardoor kan de impact van een datalek worden verlaagd voor zowel de organisatie als de betrokkenen.

Vertrouwen in een meldplicht datalekken?

Vertrouwen komt te voet en gaat te paard is het gezegde. Door slechte communicatie of zelfs het ontbreken van communicatie kan het vertrouwen worden geschaad. Een meldplicht datalekken kan een eventueel geschonden vertrouwen weer langzaam herstellen door transparantie na te streven en een beter inzicht in risico's te geven. Hierdoor kunnen personen die worden getroffen de noodzakelijke maatregelen nemen zoals het blokkeren van hun creditcard of het wijzigen van hun wachtwoord. Het zou natuurlijk beter zijn als organisaties (meer) preventieve maatregelen nemen en men hoopt door deze meldplicht dat organisaties dat gaan doen. Toch is het voor de meeste personen handig om te horen wat ze kunnen doen indien hun gegevens op straat liggen. Bedrijven geven hiermee te kennen dat zij ook hun verantwoordelijkheid serieus nemen. De aanpassing van de Wbp met een meldplicht datalekken kan hier zeker een bijdrage aan leveren en indien de meldingen ook openbaar worden, kunnen, tot een bepaalde hoogte, de consequenties ook echt zichtbaar worden.

(Endnotes)

[1] *Cybersecuritybeeld Nederland 2011, www.nctb.nl/Images/cybersecuritybeeld-nederland_tcm91-397524.pdf*

[2] *Staatsveiligheid in geding door ict, www.nos.nl/artikel/272836-staatsveiligheid-in-geding-door-ict.html [bijgewerkt tot 15 september 2011]*

[3] *Internetconsultantie december 2011, www.internetconsultatie.nl/camerabeelden/document/467*

[4] *Zenger R. Wetsvoorstel meldplicht datalekken. Eindelijk! 2011, www.bof.nl/2011/12/22/wetsvoorstel-meldplicht-datalekken-eindelijk/*

[5] *NCSC whitepapers, www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers*

[6] *Schellevis J. 'Cyber Security Centrum' opent deuren 2011, tweakers.net/nieuws/79317/cyber-security-centrum-opent-deuren.html*

[7] *www.ncsc.nl/actueel/veel-gestelde-vragen.html*

[8] *www.keylength.com*

XACML ALS STANDAARD VOOR AUTORISATIE

Rémon Sinnema

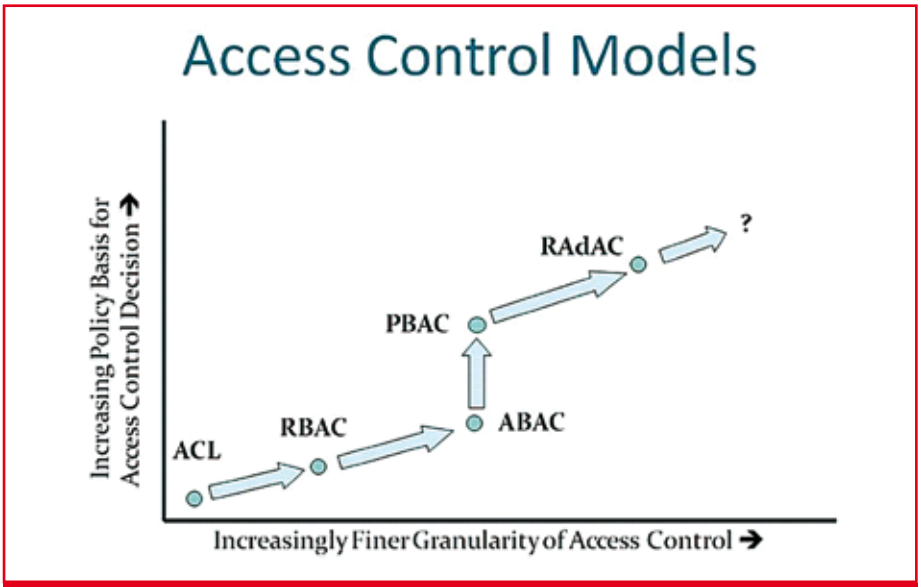
Rémon werkt als Consultant Software Engineer bij het XML R&D center van EMC in Rotterdam aan de opvolger van EMC Documentum: een Plaform as a Service op basis van de native XML database EMC Documentum xDB. Zijn specialisatie is access control en daarom is hij ook lid van de XACML Technical Committee. Volg hem online: @sinnema313, http://nl.linkedin.com/in/sinnema313, http://sinnema313.wordpress.com.

Autorisatiemodellen

Voor autorisatie zijn verschillende modellen in omloop. We kennen natuurlijk allemaal *Access Control Lists* (ACLs) en *Role Based Access Control* (RBAC). Beide modellen hebben zo hun beperkingen: ACLs zijn moeilijk te onderhouden en rollen zijn vaak niet fijnmazig genoeg.

Vanwege deze nadelen wordt tegenwoordig steeds vaker *Attribute Based Access Control* (ABAC) toegepast. ABAC is volledig gebaseerd op attributen en sluit dus nauw aan bij andere componenten in het IAM landschap.

ABAC
ABAC is volledig gebaseerd op attributen, eigenschappen van personen, documenten, etc. Dit sluit dus nauw aan bij andere (nieuwe) componenten in het IAM landschap, zoals Identity Providers die claims mbt attributen aanleveren.



Trends in autorisatiemodellen zoals geïdentificeerd door NIST

Alle attributen die voor autorisatie van belang zijn, kunnen worden gebruikt in ABAC beleidsregels: attributen over het *subject* (gebruiker, organisatie, applicatie, rollen, etc.), de *resource* (bestand, database record, etc.), de *action* (lezen, schrijven, verwijderen, etc.) en de *environment* (device, locatie, datum/tijd, etc.). Met name dat laatste maakt het mogelijk ook de context in acht te nemen in de beleidsregels. Men kan bijvoorbeeld alleen leesrechten toekennen aan iemand die via een mobiele telefoon toegang vraagt tot een document, terwijl diezelfde persoon ook schrijfrechten krijgt als hij werkt vanaf z'n vertrouwde bedrijfsdesktopcomputer die in het bedrijfsnetwerk hangt.

Steeds fijnmaziger autorisatiemodellen

ABAC past in een door NIST beschreven trend naar steeds fijnmaziger en meer op beleid gebaseerde autorisatiemodellen. Men kan nog een stapje verder gaan naar *Policy Based Access Control* (PBAC). Dit is niet fundamenteel anders dan ABAC, maar nu worden de te gebruiken attributen geharmoniseerd over meerdere applicaties, departementen of zelfs organisaties heen. Nog geavanceerder is *Risk-Adaptive Access Control* (RAdAC). Hierbij houden beleidsregels ook rekening met dynamische risiconiveaus. Men kan bijvoorbeeld automatisch tijdelijk schrijfrechten wegnemen als wordt vermoed dat er een indringer op het netwerk actief is.

XACML
Het goede nieuws is dat al de hiervoor beschreven autorisatiemodellen met één standaard te implementeren zijn: *eXtensible Access Control Markup Language* (XACML). Deze standaard wordt ontwikkeld door de *Organization for the Advancement of Structured Information Standards* (OASIS). Het is een open standaard, dus vrijelijk en gratis te lezen en implementeren.

De XACML specificatie bestaat uit drie delen: een architectuur voor autorisa-

tiecomponenten, een gestructureerde taal voor het vastleggen van beleidsregels en een protocol voor het uitwisselen van autorisatieberichten.

Daarnaast zijn er zogenaamde *profielen*, optionele uitbreidingen op de specificatie. Zo zijn er onder meer profielen voor RBAC en voor het delegeren van administratieve bevoegdheden (waardoor migratie van traditionele op RBAC gebaseerde systemen vereenvoudigd wordt). Sommige van die profielen zijn niets meer dan afspraken over welke attributen te gebruiken en welke waarden die mogen hebben. Dit is dus een harmonisatie in de zin van PBAC. Een voorbeeld is het 'Intellectual Property Control' (IPC) profiel dat momenteel ontwikkeld wordt.

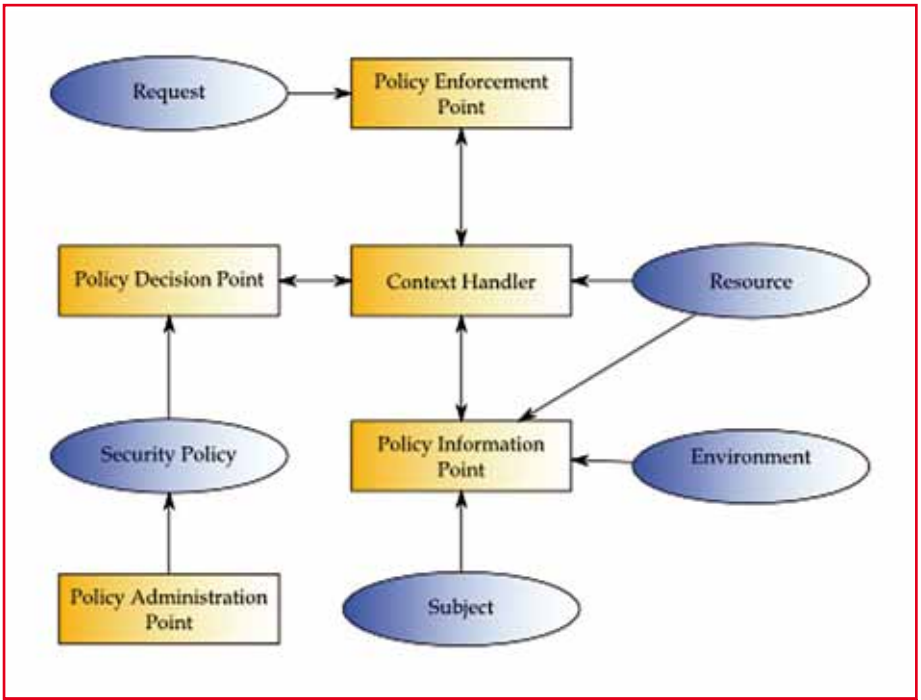
De XACML Technical Committee, die de specificatie ontwikkelt, werd gevormd in 2001 en versie 1.0 van XACML werd een OASIS standaard in 2003. We praten dus over een volwassen standaard met een behoorlijke historie.

Versie 2.0 van de specificatie is de huidige OASIS standaard. Deze specificatie dateert uit 2005. Een OASIS specificatie wordt pas een standaard als er minstens drie verschillende implementaties bekend gemaakt zijn. Er zijn dus inmiddels voldoende alternatieven voorhanden om niet aan één leverancier vast te zitten. Dat de verschillende implementaties ook in de praktijk prima gegevens kunnen uitwisselen, is bewezen op de RSA conferentie van 2008, toen meerdere partijen een zogenaamde interop hielden op het gebied van de gezondheidszorg.

Inmiddels wordt de laatste hand gelegd aan versie 3.0. Er zijn twee implementaties officieel bekend gemaakt en tijdens de RSA conferentie van dit jaar hebben vijf partijen opnieuw een interop gehouden, ditmaal op basis van het IPC profiel.

Architectuur

XACML volgt het ISO/IEC 10181-3 Access Control Framework. Dit raamwerk kent



Afb.2. XACML architectuur

twee belangrijke componenten: de Access Decision Function (ADF) neemt autorisatiebeslissingen en de Access Enforcement Function (AEF) verleent wel of geen toegang tot resources op basis van beslissingen van de ADF.

In XACML heten deze componenten respectievelijk Policy Decision Point (PDP) en Policy Enforcement Point (PEP). Daarnaast kent XACML nog de Policy Administration Point (PAP), waarmee men beleidsregels kan definiëren en de Policy Information Point (PIP) die een bron van waarden voor attributen is. De Context Handler is tenslotte de component die de andere componenten met elkaar verbindt.

De XACML specificatie bestaat uit drie delen

In een op XACML gebaseerd systeem verloopt autorisatie als volgt:
De PEP onderschept een poging om een bewaakte resource te benaderen.
De PEP stuurt een autorisatieverzoek naar de Context Handler.
De Context Handler zet dit verzoek om in een request in XACML formaat en voegt eventueel informatie toe in de vorm van attributen. Deze informatie kan aangeleverd worden door één of meerdere PIPs. Optioneel kan ook (een weergave van) de inhoud van de resource (in XML-vorm) toegevoegd worden.
De Context Handler stuurt het XACML request naar de PDP.
De PDP vergelijkt het request met de beleidsregels die via de PAP beschikbaar gemaakt zijn. Eventueel kan de PDP de Context Handler om meer attributen vragen als die wel in de beleidsregels staan, maar niet in het request.
De PDP neemt een beslissing en stuurt die terug naar de Context Handler.
De Context Handler antwoordt de PEP in een formaat dat de PEP begrijpt.
De PEP verleent wel of niet toegang op basis van de beslissing van de PDP.

Deze architectuur heeft twee voordelen. Ten eerste bestaat het uit componenten waarvan sommige onafhankelijk zijn van de applicatie, zoals de PDP, PAP en PIP. Deze componenten kunnen dus hergebruikt worden in meerdere applicaties en aangekocht worden van gespecialiseerde leveranciers.

Het tweede voordeel is dat beleidsregels onafhankelijk van de applicatie

gedefinieerd worden, zodat men die hergebruikt in verschillende applicaties. Dit brengt niet alleen lagere kosten en een kortere doorlooptijd met zich mee, maar biedt daarnaast veel betere mogelijkheden om de regels consistent te houden over applicaties heen.

Taal

De XACML taal voor beleidsregels is gebaseerd op XML. Op het laagste niveau in deze taal staan de regels. Een *regel* definieert in een zogenaamd *target* op welke combinatie van subject, resource, action en environment de policy van toepassing is. Dat gaat via relatief simpele vergelijkingen van waarden van attributen. Voor complexere gevallen kan een regel een *conditie* hebben. Hierin kan een expressieve taal gebruikt worden, waarin vele functies tot de beschikking staan. Tenslotte heeft een regel een *effect*, dat aangeeft of toegang wel of niet verleend moet worden als de regel van toepassing is.

XACML volgt het ISO/IEC 10181-3 Access Control Framework

Regels kunnen niet op zichzelf staan; ze moeten altijd onderdeel zijn van een *policy*. Een policy combineert een aantal regels tot een samenhangend geheel. Een policy kan ook een target hebben. In dat geval wordt het gecombineerd met het target van de regels die het bevat. Op deze manier kan herhaling voorkomen worden.

Policies kunnen zelf ook weer als bouwstenen dienen door ze op te nemen in *policy sets*. Een policy set mag ook weer een target hebben en kan meerdere policies en ook policy sets bevatten.

Het target in een regel, policy of policy set is bedoeld als een eerste filter dat de PDP gebruikt om te bepalen welke regels van toepassing zijn op een autorisatieverzoek. Hierbij worden attributen als gelijk beschouwd als hun categorie (subject, resource, action, environment), ID, data type en uitgever overeenkomen. Sommige XACML implementaties hebben speciale optimalisaties om via een target snel in te zoomen op de van toepassing zijnde regels. Condities zijn in het algemeen moeilijker te optimaliseren.

Het kan natuurlijk voorkomen dat op een bepaald autorisatieverzoek meerdere regels van toepassing zijn. De XACML specificatie voorziet in conflictoplossing via zogenaamde *combineeralgoritmen*. Er zijn combineeralgoritmen voor policies om effecten te combineren tot één antwoord en voor policy sets om de antwoorden van meerdere policies te reduceren tot één eindantwoord. Voorbeelden van combineeralgoritmen zijn *deny-overrides* (dat altijd voorrang geeft aan het verbieden van toegang) en *permit-overrides* (dat juist voorrang geeft aan het verlenen van toegang).

De X in XACML staat niet voor niets voor eXtensible

Een antwoord in XACML kan meer zijn dan slechts het wel of niet toegang verlenen (Permit/Deny). Er zijn namelijk nog twee situaties denkbaar die afgehandeld moeten worden: het kan zijn dat er helemaal geen regels van toepassing zijn op het verzoek (NotApplicable) en er kunnen fouten zitten in de regels of attributen ontbreken (Indeterminate). De PDP zal één van deze antwoorden teruggeven en het is dan aan de PEP om te bepalen of men toegang verleent of niet. Er zijn dus meerdere implementaties van een PEPs mogelijk. Men spreekt in dit verband van bijvoorbeeld een deny biased PEP (verleen alleen toegang als Permit het antwoord is) of een permit biased PEP (verleen toegang tenzij het antwoord Deny is).

Met het wel of niet verlenen van toegang zijn we er echter nog niet. Soms willen we bijvoorbeeld alleen toegang verlenen als dat ook gelogd wordt, zodat we kunnen controleren dat er geen misbruik van bevoegdheden gemaakt wordt. Een arts op de spoedeisende hulp moet bijvoorbeeld inzage kunnen hebben in medische gegevens van patiënten die normaal gesproken niet bij haar onder behandeling zijn. Andere acties die we zouden willen kunnen uitvoeren zijn het versturen van een email naar een manager, of het tonen van een waarschuwing op het scherm.

XACML implementeert deze functionaliteit via *obligations* die bij beleidsregels vastgelegd kunnen worden. Op het moment dat de beslissing van

Afb.3. Elementen van de autorisatietaal

de PDP gebaseerd is op zo'n regel, zal de PDP met het antwoord ook de obligation teruggeven. De PEP mag dan alleen toegang verlenen indien het de obligation kan uitvoeren. Een mildere variant is het *advice*, dat in principe hetzelfde werkt, maar dat door de PEP genegeerd mag worden als die het niet begrijpt. Zowel obligations als advice zijn optionele onderdelen van de specificatie, dus niet iedere XACML implementatie hoeft ze te ondersteunen. De specificatie laat ook de acties die de obligations/advice voorstellen open, zoals loggen, etc. De makers van het autorisatiebeleid zullen dit dus moeten afstemmen met de PEP implementatie.

Uitbreidbaarheid

De X in XACML staat niet voor niets voor eXtensible: er zijn meerdere punten waarop een op XACML gebaseerd systeem uitgebreid kan worden. Natuurlijk kunnen nieuwe attribuut IDs toegevoegd worden. Hiervoor is alleen nodig dat een PIP een waarde voor het nieuwe attribuut kan leveren. Sinds versie 3.0 kunnen zelfs nieuwe categorieën bedacht worden, naast subject, resource, action en environment.

Verder kunnen er nog nieuwe data types geïntroduceerd worden. Dit vereist meestal wel een aanpassing in de PDP, zodat men attributen op een correcte manier kan vergelijken. Ook kunnen nieuwe functies beschikbaar gemaakt worden voor gebruik in condities en verzint men mogelijk nieuwe combineeralgoritmen.

Al deze flexibiliteit maakt het zeer onwaarschijnlijk dat men in de praktijk vastloopt met autorisatiebeleid dat niet in XACML uit te drukken is.

Conclusie

XACML wordt zonder enige twijfel de nieuwe *de facto* standaard op het gebied van autorisatie. Het is een open, volwassen standaard, ondersteund door meerdere leveranciers, en die mee kan groeien met elk evoluerend autorisatiebeleid. De flexibele architectuur maakt het mogelijk XACML in te zetten in uiteenlopende situaties, van embedded in een enkele applicatie tot Authorization as a Service (AzaaS).

Wilt u meer weten over XACML in de praktijk, geef u dan op voor het seminar XACML praktijk ervaringen op donderdag 26 april te Utrecht dat PvIB organiseert in samenwerking met PIMN en CSA NL. Leden van PvIB krijgen €50 korting.

Meer info over het XACML seminar op http://xacml.eventbrite.com/

Referenties

NIST overzicht van autorisatiemodellen
http://csrc.nist.gov/news_events/privilege-management-workshop/PvM-Model-Survey-Aug26-2009.pdf

ISO/IEC 10181-3:1996 Access Control Framework
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18199

XACML Technical Committee (met links naar specificaties)
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

PI.LAB: SAMEN VOOR PRIVACY EN IDENTITEIT

BUNDELING VAN KRACHTEN IN NIEUW LAB

Ronald Leenes

Ronald Leenes is hoogleraar regulering door technologie aan Tilburg University en wetenschappelijk directeur van PI.lab. Hij is via email bereikbaar op ronald.leenes@pilab.nl

In rap tempo zijn we de afgelopen twee decennia de informatiemaatschappij ingerold. Informatie is een belangrijke grondstof geworden terwijl de uitdrukking 'kennis is macht' meer dan ooit waar blijkt. Persoonsgegevens vormen in dit licht een belangrijke en omvangrijke categorie gegevens. Zeker wanneer we de definitie volgen van de Europese dataprotectieregelgeving: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Dienstverlening vindt in toenemende mate gepersonaliseerd plaats en 'gratis' online diensten worden gefinancierd door het aanbieden van gerichte advertenties die slechts mogelijk zijn door de statistische verwerking van persoonsgegevens via profielen. Door een ruimhartige interpretatie van identificatie door de Artikel 29 werkgroep[1], valt profileren en behavioural advertising onder de verwerking van persoonsgegevens omdat daarbij gebruik wordt gemaakt van cookies en IP adressen van de gebruikers.

Christian van 't Hof, dagvoorzitter.

De verwerking van persoonsgegevens maakt het mogelijk diensten te ontwikkelen die zijn toegesneden op de wensen van individuele gebruikers. Tegelijkertijd werpen dergelijke diensten onvermijdelijk privacy vragen op. Te meer omdat de gegevens niet eenmalig worden gebruikt, maar in meer en meer gegevensbestanden worden opgeslagen, hergebruikt en uitgewisseld. Doordat de aard, reikwijdte en arrangementen van dienstverlening continue veranderen – denk aan de snelle opkomst van social media zoals Facebook en Twitter, en cloud computing –, is niet altijd even duidelijk wat de privacy implicaties zijn van nieuwe diensten en de immer groeiende datahonger van organisaties.

'. . . het moet gewoon werken'

De informatiemaatschappij is volledig afhankelijk van moderne ICT. De technische ruggegraat, het internet, is gedateerd en essentiële kenmerken reflecteren een ander tijdperk. Het 'rode gevaar' vormde weliswaar de achtergrond voor de ontwikkeling van het internet, maar de 'bad guys' bevonden zich kennelijk niet online. Een identiteitsinfrastructuur werd niet nodig geacht. Apparaten kunnen weliswaar met elkaar communiceren (via IP adressen), maar wie er schuil gaat achter de apparatuur is niet duidelijk. Hierdoor heeft het internet er de schijn van te staan voor anonieme communicatie en interactie. Dat is, zo weten we ondertussen, niet waar. Via intelligente koppelingen worden we, al dan niet bij naam, gekend door tal van online dienstverleners. Onder normale omstandigheden opereren we daardoor in

een soort schemergebied, onze handelingen lijken anoniem of pseudoniem, maar zijn dat ook weer niet helemaal. Wanneer we daarentegen onder onze echte identiteit willen opereren omdat we belangrijke transacties online willen verrichten (zoals zaken waarvoor een handtekening of akte noodzakelijk is) dan is dat eveneens niet goed mogelijk. We hebben geen betrouwbare elektronische identiteit die universeel bruikbaar is. Voor deelterreinen, zoals online bankieren bestaan betrekkelijk betrouwbare e-identiteiten, maar die hebben een beperkt toepassingsbereik; probeer maar eens met je bankpasje plus randomreader belastingaangifte te doen. Met andere woorden, we kunnen online noch anoniem of pseudoniem handelen wanneer we dat willen, noch kunnen we betrouwbaar geïdentificeerd handelen.

Langs het hele spectrum zien we vervolgens problemen. Er vindt bijvoorbeeld heimelijke monitoring plaats (profilering) en er worden bij online interacties veel meer persoonsgegevens gevraagd dan strikt noodzakelijk voor de betreffende dienst. Ook zijn allerhande diensten niet mogelijk omdat de identiteit van de gebruiker niet deugdelijk kan worden vastgesteld. Dit heeft e-government bijvoorbeeld lang vertraagd.

Hoe identiteit vaststellen op internet

In de afgelopen vijftien jaar zijn er vele technische en organisatorische deeloplossingen voor deze problemen ontwikkeld door technologie-ontwikkelaars, bedrijven en overheden. Ze zijn incompatibel, zowel technisch als juridisch; bankidentiteiten zijn niet bruikbaar buiten bankieren en de DigiD mag niet worden gebruikt in de private sector. Daarnaast wordt privacybescherming doorgaans niet meegenomen als ontwerpeis.

Een gevolg van deze gebrekkige identiteitsinfrastructuur is dat er veel meer informatie wordt verzameld dan strikt noodzakelijk is voor de meeste (online) dienstverlening. Aangezien deze informatie ook bewaard blijft introduceert dit ook beveiligingsrisico's. Dat het niet alleen risico's betreft, maar met regelmaat tot grotere problemen in de vorm van datalekken leidt wordt wekelijks geïllustreerd in de pers. Te veel persoonsgegevens verwerken is niet alleen onwenselijk vanuit de daarmee samenhangende beveiligingsrisico's en de inbreuk die verder gebruik op de privacy van betrokkenen betekent, maar in veel gevallen ook onnodig.

Mireille Hildebrandt.

Op internationaal vlak springen grote internationale spelers, zoals Google, Facebook, Amazon en Apple in het gat in de identiteitsinfrastructuur. De grote sociale netwerk- en contentaanbieders zijn gaan opereren als identity providers voor derden. Dat is een logische stap en zowel de identity provider als de relying parties hebben er baat bij. Voor de identity provider zorgt dit voor verdere lock-in, meer kennis over wat hun gebruikers doen en additionele inkomsten uit advertenties die kunnen worden geplaatst bij de relying parties. De relying party krijgt gevalideerde gebruikers en kan mogelijk gebruik maken van de kennis die de identity provider heeft van haar gebruikers. Voor de eindgebruiker levert de mogelijkheid om op tal van plaatsen in te loggen met een Facebook account gemak op. Het lijkt winst voor alle partijen, maar de eindgebruiker trekt aan het kortere eind; haar gedrag wordt meer en meer een open boek voor Facebook. De eindgebruiker is geen klant, maar het product dat wordt verkocht en dat hoeft uiteindelijk niet in het voordeel van de eindgebruiker te zijn. Daarnaast hebben organisaties zoals als Facebook en Google een internet-achtige schaalgrootte bereikt, maar staan ze anders dan het internet onder controle van 1 partij. Je kunt je afvragen wat dit gaat betekenen voor de openheid en governance van de publieke communicatie-infrastructuur.

Er zullen alternatieven met een breed toepassingsbereik voor dergelijke private identiteitsdiensten moeten worden ontwikkeld, waarbij privacy bescherming van het individu een centrale plaats moet innemen, naast gebruiksgemak, veiligheid, en kostenbeheersing. Moderne cryptografie is hierbij onontbeerlijk. Sinds het midden van de jaren 80 zijn er cryptografische technieken die vertrouwen in de informatiemaatschappij kunnen creëren

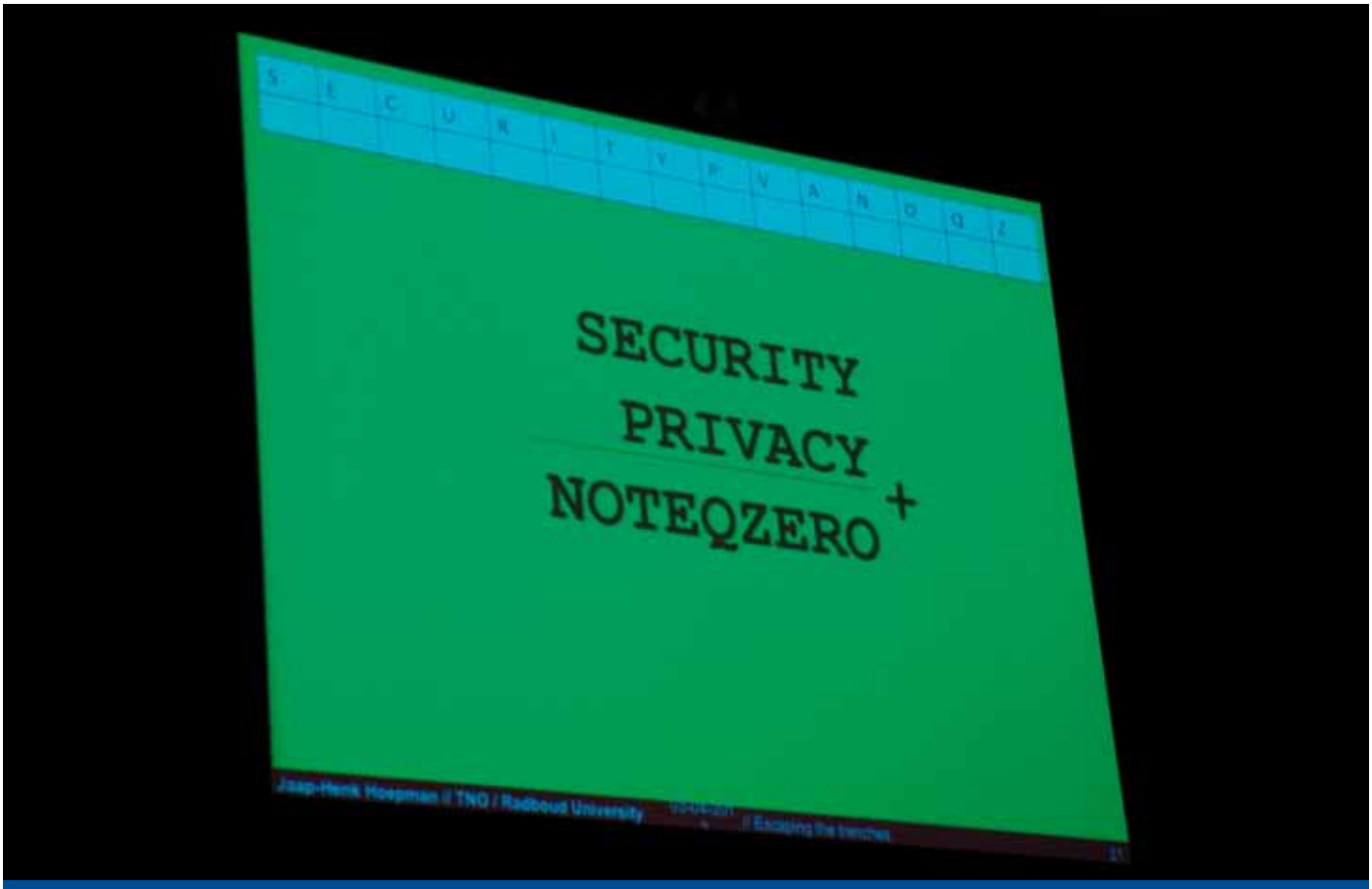
met inachtneming van de privacy van betrokkenen. Anonymous credentials (zie bijv. Camenisch & Lysyanskaya 2011; Brands 2000; Batina et al. 2010) maken het bijvoorbeeld mogelijk om bepaalde eigenschappen van de aanbieder via een zogenaamde credential te bewijzen zonder daarbij onnodig persoonsgegevens te lekken. Dit maakt het bijvoorbeeld mogelijk om te bewijzen dat je ouder bent dan 18, zonder je geboortedatum te tonen. Cryptografie maakt het ook mogelijk om 'revocable pseudonymity' te realiseren, pseudonimiteit die in gevallen van misbruik kan worden opgeheven (zie bijv. Galindo & Hoepman 2011). Dit soort technieken laten zien dat privacy en veiligheid niet op gespannen voet hoeven te staan en zelfs goed samen kunnen gaan.

In wetenschap en praktijk wordt in toenemende mate gezien dat privacy en identiteit met elkaar verbonden zijn. Philip Agre en Marc Rotenberg (1997) hebben de relatie tussen de twee aardig aangegeven met hun bekend geworden definitie 'the right to privacy is the freedom from unreasonable constraints on the construction of one's own identity'. Deze definitie legt mooi een verband tussen negatieve vrijheid (liberty), "the freedom from", en positieve vrijheid (identity-building), "the freedom to" (Hildbrandt 2006). Ook laat het mooi zien dat privacy niet absoluut is; er is ruimte voor redelijke inperkingen.

Identiteit en privacy zijn meervoudige, complexe en evoluerende concepten die in het licht van de zich ontwikkelende informatiemaatschappij beschouwing vanuit verschillende disciplines vereisen.

Privacy en identiteit gaan altijd samen

In de loop van de tijd heeft identiteit zich ontwikkeld van vrijwel afwezig – middeleeuwers onderscheidden zich nauwelijks van elkaar –, via aandacht voor onderlinge verschillen tussen mensen tot expliciete en publieke constructie en vertoning van de eigen identiteit (denk aan profielen op online sociale netwerken). Identiteitsmanagement is daarmee niet alleen een technische aangelegenheid – het beheren van online accounts met de focus op identificatie, authenticatie en autorisatie. De meer sociale/filosofische kant raakt steeds meer verweven met deze technische benadering. Memoreer de hierboven geschetste ontwikkeling van Facebook richting identiteitsprovider. Facebook probeert juist de kennis die zij hebben over hun gebruikers te kapitaliseren in een context die in eerste instantie niets anders lijkt te zijn dan accountbeheer. Identiteit beschouwd vanuit een bredere context betekent onderkennen dat mensen meerdere deelidentiteiten hebben om uiting te kunnen geven aan de verschillende rollen die ze in het maatschappelijke leven spelen (wetenschapper, echtgenoot, vader, aanvaller in het basketbalteam). Bij die verschillende rollen horen verschillende regels en worden, in informatietermen, verschillende attributen of eigenschappen getoond. Het gescheiden houden van de ver-



Illustratie van Jaap-Henk Hoepman.

Forumdiscussie.

schillende soorten publiek is belangrijk omdat informatie in de verkeerde context geloofwaardig functioneren in die rol kan verstoren (Goffman 1956; Nissenbaum 2009). Bij de ontwikkeling van identiteitsmanagementsystemen zal daar rekening mee moeten worden gehouden. Dat gebeurt lang niet altijd. Zo kennen we in de publieke sector het Burgerservicenummer (BSN) voor interacties met de overheid. Kan dat nummer ook worden gebruikt wanneer een individu niet als burger, maar als vertegenwoordiger van een bedrijf opereert? Burger en ondernemer of vertegenwoordiger van een onderneming zijn verschillende rollen. Los van de vraag of het BSN juridisch gebruikt mag worden in een privaatrechtelijke context (het antwoord daarop is een helder "nee!"), is dit vanuit het eerder geschetste perspectief op identiteit sowieso geen goed idee.

Beschouwen vanuit verschillende perspectieven

Ook privacy vergt aandacht vanuit verschillende perspectieven. Vanuit technisch perspectief raakt privacy aan beveiliging. Maar minstens zo belangrijk is de juridische dimensie. We moeten opereren binnen een immer complexer wordend juridisch raamwerk dat door technische ontwikkelingen onder constante druk staat, zeker omdat dit raamwerk meerdere doelen dient: de bescherming van persoonsgegevens en de bevordering van het vrije verkeer van informatie. Aangezien regelgeving beoogt rechtszekerheid te bieden en aanpassing bovendien tijdrovend is, moeten juridisch alle zeilen bijgezet worden om de informatiemaatschappij in goede banen te leiden en te stimuleren. Nieuwe technische ontwikkelingen worden daarom zo veel mogelijk binnen de bestaande kaders geplaatst (een voorbeeld daarvan is 'cookies' onder het begrip 'equipment' scharen door de eerder genoemde Art. 29 werkgroep) en wordt geprobeerd regelgeving zo veel mogelijk technologieneutraal te formuleren (bijv. "geautomatiseerde verwerking"). Ook is het noodzakelijk om te doorgronden wat we nu eigenlijk bedoelen met privacy (bescherming). Privacy heeft meer en meer betrekking op informationele privacy in plaats van op de andere dimensies, zoals lichamelijke integriteit of huisrecht. Wanneer we vervolgens zien dat – met name jongeren – vrijwel onbeschaamd allerhande persoonlijke details op sociale netwerken uitdragen, kunnen we ons vervolgens de vraag stellen of informationele privacy nog wel bestaat (waarop volgens ons het antwoord "ja" is). Desalniettemin lijkt het belang van privacy op individueel niveau te verschuiven. Privacy heeft ook een sociale persoonsoverstijgende maatschappelijke waarde: een maatschappij waarin privacy sterk wordt ondermijnd (denk aan het voormalige Oostblok) is niet de maatschappij waarin wij willen leven. Daarom zullen we bepaalde privacy waarborgen moeten inbakken in de technologie en regulering om het individu te beschermen tegen zichzelf. Wanneer de verschillende perspectieven op privacy en identiteit onvoldoende in ogenschouw worden genomen ontstaan risico's en brokken die verdere ontplooiing van de informatiemaatschappij in de weg staan of vertragen. In de afgelopen jaren hebben we daarvan verschillende voorbeelden kunnen zien. Het Elektronisch Patiënten Dossier, de OV-chipkaart, de Slimme Meter, rekeningrijden en RFID chips zijn voorbeelden van grote projecten waarin veiligheid, privacy en identiteitsvraagstukken zijn onderschat of niet handig zijn aangepakt waardoor potentieel goede ideeën in de koelkast zijn verdwenen.

PI.lab met zes onderzoekslijnen

Om de hier bepleite multidisciplinaire aandacht voor (online) privacy en identiteit concreet vorm te geven en bij te dragen aan de ontwikkeling van betere IT toepassingen is begin 2012 het Privacy & Identity Lab (PI.lab) van start gegaan. In PI.lab werken zo'n 25 onderzoekers vanuit Tilburg University (via het 'Tilburg Institute for Law, Technology, and society (TILT)'), de Radboud Universiteit (middels het 'Institute of Computer and Information Science'), TNO (met name de afdelingen 'Information Security' en 'Strategies for the Information Society') en SIDN (het bedrijf achter .nl) samen. Het lab brengt bestaand onderzoek van de partners bij elkaar en ontwikkelt nieuw onderzoek – zowel fundamenteel (o.m. PhD onderzoek) als toegepast (contractonderzoek). Het samenwerkingsverband is uniek omdat het de technische, juridische, organisa-

torisch en socio-economische aspecten van privacy en identiteit integraal onderzoekt en aanpakt. Het lab bouwt wetenschappelijke kennis op, doet actief mee aan nationale en internationale onderzoeksactiviteiten en programma's en ontwikkelt (prototypes van) praktische toepassingen. Een gerichte valorisatiestrategie draagt er toe bij dat de kennis niet op de plank blijft liggen maar daadwerkelijk benut gaat worden. Daartoe zullen onder meer een jaarlijks te organiseren conferentie, kennisseminars, een publicatiereeks en concrete op de markt gerichte onderzoeks- en implementatieactiviteiten bijdragen.

Netwerken tijdens PI Lab event.

Het onderzoek van PI.lab zal in eerste instantie worden georganiseerd langs een zestal onderzoekslijnen waarin telkens meerdere onderzoekers samenwerken:

- privacy in infrastructuren: smart grid, road pricing, location based e-ticketing,.
- privacy door middel van techno-regulering: privacy by design, revocable privacy, compliance engineering, juridische bescherming door technologie
- monitoring en profiling: behavioural targeting, do-not-track, deep packet inspection, juridische aspecten van profiling en datamining, (internet) taps in opsporing en handhaving
- identiteit, digital persons, eID, IDM: digitale dossiers (EPD, EKD etc), identity online, privacy-enhancing identity management, anonymous credentials
- privacy en identity in the Internet of Things; thema's: ambient intelligence, smart devices
- right to be forgotten: het 'nieuwe' recht om vergeten te worden zoals voorgesteld in de (draft) General Data Protection Regulation

De plannen van het lab zijn op 3 april gepresenteerd tijdens het openingscongres. Meer informatie over PI.lab is te vinden op de website www.pilab.nl.

Wouter Steijn.

Literatuurverwijzingen:

Philip Agre and M. Rotenberg, 1997, Technology and privacy: the new landscape, Cambridge, Mass.: MIT Press.

L. Batina, J.-H. Hoepman, B. Jacobs, W. Mostowski, and P. Vullers. Developing Efficient Blinded Attribute Certificates on Smart Cards via Pairings. In 9th IFIP Int. Smart Card Research and Advanced Application Conference (CARDIS), pages 209-222, Passau, Germany, April 2010.

Stefan Brands. Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. Number ISBN 0-262-02491-8. MIT Press, 1st edition, 2000.

Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Birgit Pfitzmann, editor, EUROCRYPT, volume 2045 of Lecture Notes in Computer Science, pages 93–118. Springer, 2001.

D. Galindo and J.-H. Hoepman. Non-interactive Distributed Encryption: A New Primitive for Revocable Privacy. In Workshop on Privacy in the Electronic Society (WPES), Chicago, IL, USA, October 2011. (to appear).

Erving Goffman, 1956, The presentation of self in everyday life, Edinburgh: University of Edinburgh.

Mireille Hildebrandt, 2006, Privacy and Identity, In: Privacy and the Criminal Law (eds Claes, E., Duff, A. and Gutwirth, S.), pp. 43-58. Intersentia, Antwerpen - Oxford.

Helen Nissenbaum, 2009, Privacy in Context: Technology, Policy, and the Integrity of Social Life, Palo Alto, CA: Stanford University Press.

Endnotes

[1] De Artikel 29 werkgroep adviseert over de interpretatie van de Data Protectie Richtlijn 95/46/EC en bestaat uit vertegenwoordigers van de data protectie autoriteiten uit de verschillende EU lidstaten.

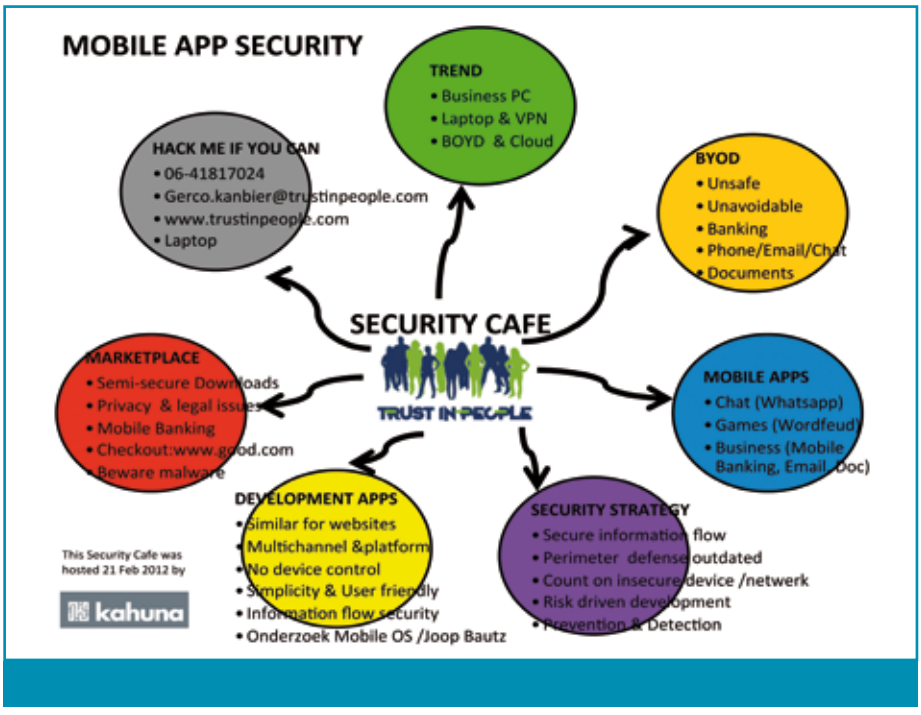
Foto's gemaakt door Arnold Roosendaal en Martin Pekárek (PI-lab)

VERSLAG

SECURITY CAFÉ – MOBILE APP SECURITY

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

Vier maal per jaar organiseert Trust in People het Security Café. De laatste editie, van 21 februari 2012, werd bij Kahuna te Amersfoort georganiseerd. Op LinkedIn hadden de inmiddels 550 leden van de groep voor het onderwerp "Mobile App Security" gestemd. Hiervoor was er een panel met twee experts uitgenodigd, bestaande uit: Martin de Vries, Security officer bij Rabobank International voor alle direct banken in het buitenland en John Grüter, organisatie adviseur bij Digital Knowledge. Hier volgt een impressie van de panelpresentaties en –discussie:
Enkele jaren geleden – zeg tien jaar – kreeg je nog een standaard beveiligde PC waarmee je toegang kreeg tot het bedrijfsnetwerk. De PC werd al snel vervangen door de laptop, zodat je thuis met een beveiligde VPN verbinding ook het bedrijfsnetwerk kon bereiken. Onvermijdelijk is nu Bring Your Own Device (BYOD) en werken in de cloud, waarbij het apparaat onder controle staat van de gebruiker en vanuit bedrijfsperspectief per definitie als onveilig moet worden beschouwd.
Hoe zorgen wij ervoor dat de risico's van bedrijfsinformatie op uiteenlopende apparaten tot een minimum beperkt blijft, zonder dat dit ten koste gaat van gebruikersgemak en/of functionaliteit? Dat is de inzet van dit Security Café.
Bij mobiele apps denken veel mensen aan Whatsapp, Wordfeud en Mobiel Bankieren. Deze applicaties staan representatief voor respectievelijke functie communicatie, games en zakelijke toepassingen, die zowel privé als zakelijk door elkaar lopen en toegankelijk zijn via pc, laptop, tablet en/of smartphone. Als bedrijf moet je daarom je security strategy geschikt maken voor informatiestromen die interactie hebben met de buitenwereld. Hierbij moeten de risico's zoveel mogelijk worden beperkt, met zo min mogelijke impact op het gebruikersgemak en/of functionaliteit. Mede door detective maatregelen en restricties op transacties is mobiel bankieren succesvol en relatief veilig, ondanks de mogelijkheid van onveilige apparaten. Banken lopen nu met een mobiele app voor dit belangrijke bedrijfsproces voorop in de ontwikkeling van mobile applications.
Op een marketplace kun je apps downloaden. Apple kent daarin een gesloten aanpak en accepteert alleen mobiele apps na controle; Google is daarentegen open en accepteert alle applicaties en gooit een app eruit als er specifieke klachten zijn. Natuurlijk zijn er voldoende geaccepteerde apps die onder water gewoon malware of een trojan zijn.
De ontwikkeling en het testen van een mobiele applicatie is vergelijkbaar in aanpak met een gewone website, waarbij je wel extra rekening houdt met de beperkingen van kleinere mobiele apparaten en het mobiele platform waarop het moet draaien. De opzet van het mobiele platform en het sandbox-principe per mobiele applicatie, levert relatief weinig security risico's op. Echter, vele mobiele applicaties vragen gewoon toestemming van de gebruiker om toegang te krijgen tot alle privé- en bedrijfsinformatie dat elders opgeslagen is in het apparaat. Daarnaast wordt de meeste informatie, die verwerkt is via een app, opgeslagen in het buitenland en daar gelden andere juridische regels dan in Nederland.
Om die reden is het goed voor bedrijven na te denken hoe bedrijfscontacten, email en documenten beschermd kunnen worden op onveilige apparaten. Een aantal bedrijven experimenteren momenteel met www.good.com om documenten en email in een soort veilige mobiele app aan de bieden, zodat de vertrouwelijkheid van deze informatie stromen ook geborgd kunnen worden. Ook kun je denken aan een "business cloud", waarin kantoor automatisering en/of ERP in de cloud draait en download van bedrijfsinformatie niet nodig is. Tot slot is er ook een strategie mogelijk waarbij je een Mobile Device Management systeem optuigt om jouw bedrijfs-app te distribueren en op afstand te beheren voor een heterogene omgeving.



Links:

www.trustinpeople.com/security_cafe.php

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.

Inleidende tekst door Aart Jochem: "Met je vinger in de firewall."
Er is geen houden aan: de een na de andere database met persoonsgegevens wordt gepubliceerd op Pastebin, het publieke uithangbord voor van alles en nog wat op internet. De oogst van afgelopen maanden bevatte ondermeer een datingsite, een biermerk, diverse webshops, een grote pornosite en een site van slachtoffers van een misdrijf. Ook worden datalekken regelmatig gemeld zonder dat de data gepubliceerd wordt. Achter het Nieuws vroeg zich af of dit nu vaker voorkomt dan "vroegâh" en hoe het komt dat al die gegevens lekken. Is er iets aan te doen om het te stoppen en waar is Hans Brinkers als je hem nodig hebt?"

Maarten Hartsuijker
"De rest van de gegevens publiceer ik niet, want die ga ik verkopen". Zo besloot de hacker van de Philips microsites zijn publicatie van een paar honderd van de 200.000 e-mailadressen en telefoonnummers van Philips klanten en medewerkers. Ondanks dat de stortvloed aan publiciteit wellicht suggereert dat er hier sprake is van een nieuwe trend, zijn lekke websites niet nieuw. Als ethisch hacker constateer ik dat de resultaten van website penetratietesten nog grotendeels hetzelfde zijn als een decennium geleden.

Wat wel nieuw is, is dat hackers steeds meer in de openbaarheid treden. Soms om een politiek statement te maken, soms om oprecht kwetsbaarheden aan de kaak te stellen, soms om op te scheppen tegen vriendjes en soms gewoon voor zelfpromotie en omdat het leuke pers oplevert.

Interessant is het om je af te vragen wat erger is: gevoelige informatie die in alle stilte wordt gestolen, of veel publiciteit rondom hacks die ertoe leidt dat we ons allemaal bewuster zijn van de noodzaak om gegevens te beschermen. Wat het antwoord ook is, ik hoop dat het laatste effect in elk geval niet uitblijft. Als we deze trend als website-eigenaren willen doorbreken zullen we beveiligingsaandachtspunten meer structureel op moeten nemen in onze selectiecriteria, onze ontwerpen en onze testplannen. Geef duidelijk aan wat je van een leverancier of ontwikkelaar verwacht en controleer hier achteraf ook op, al is het maar steekproefsgewijs. Vaak ontbreekt deze beveiligingsaandacht en zijn we als afnemers al lang blij als de langverwachte website eindelijk werkt.

Tom Bakker
Ik ben niet verbaasd dat het slecht gesteld is met de beveiliging van websites. Dat is niets nieuws. Wat me echter wel verbaast is de omvang.
De datalekken vliegen je de laatste tijd om de oren. Het lijkt dus een structureel probleem.
Ik heb wel eens een vakgenoot, die in het onderwijs zit, horen vertellen dat IT opleidingen nauwelijks aandacht schenken aan beveiligingsaspecten van IT en webdesign in het bijzonder. Ik weet niet of dat altijd waar is maar mijn ervaring is ook dat veel ontwikkelaars (en de opdrachtgever) meer geïnteresseerd zijn in functionaliteit en 'geliktheid' van de website. Niet zo lang geleden wel eens met webontwikkelaars gepraat. Zij hadden nog nooit van OWASP gehoord. Soms zijn de meest basale zaken geen eens geregeld (OWASP top tien?). Ik heb leveranciers er wel eens op aangesproken als een lek(je) is ontdekt. De reactie is vaak flauw, zo van dat 'het niets voorstelt want er worden geen persoonsgegevens verwerkt'. Men vergeet dat websites naast lekken van gegevens ook wel op andere manieren misbruikt kunnen worden (spam). Dan heb je in ieder geval wel reputatieschade.
Informatiebeveiliging is wat mij betreft gewoon een kwaliteitsaspect, net zo goed als gebruikersvriendelijkheid, performance etc. Ook dat is niets nieuws. Denk aan de aloude ISO 9126 norm. Na een incident zal het gat meestal wel gedicht worden. Je vraagt je dan af of het niet meteen goed had gekund. Elke ontwikkelaar weet dat latere aanpassingen een veelvoud kost dan met het meenemen in het begin van het ontwikkeltraject. Dus security by design.
We zullen toch meer eisen moeten stellen aan leveranciers en ontwikkelaars. Meer pentesten bijvoorbeeld. Maar beter is het bij de bron aan te pakken door bij het ontwerp de beveiligingsaspecten te toetsen. En vooral bij de opleidingen meer aandacht te schenken aan veilige websites.

Lex Borger
We hebben zeker meer lekken dan vroeger. Maar we hebben ook veel meer informatie dan vroeger om te lekken. Daar waar twintig jaar geleden de kunst nog was om te weten waar de schaarse informatie te halen was, is er nu zoveel data te krijgen dat je goed moet filteren om de juiste informatie over te houden. Daar heeft iedereen last van, ook de instanties die persoonsgegevens verwerken - als we ons even tot persoonsgegevens beperken. Ik denk zelfs dat men relatief goed werk levert. De aanwas van data gaat sneller dan de aanwas van lekken.
En waarom wordt gelekte informatie niet meer gepubliceerd? Het is kennelijk niet meer de moeite waard of men houdt het achter om het mogelijk te verkopen. Dit is de twilight zone tussen de script kiddie en de organized crime.
Maar een ding is zeker: er zijn zoveel mogelijkheden om in te breken dat we weten dat preventie ervan altijd wel ergens te kort zal schieten.
Hans Brinkers - Een Amerikaans/Nederlands icoon. Ik denk dat de vraag waar hij is niet de juiste is om te stellen. Maar het is een goede vergelijking in de zin dat naast goede preventie vroege detectie van het falen ervan cruciaal is. En ook duidelijk uit het verhaal van de zilveren schaatsen: weten hoe je de repressie uitvoert is ook belangrijk. Toch zie ik om mij heen nog vaak een maniakale focus op preventie en preventie alleen. Goede monitoring is niet weggelegd voor security, laat staan analyse van resultaten, alerting en incident response.
Maar is informatie dan niet al gelekt ten tijde van het incident? Ja, als er maar één dijk is wel. Maar wij polderaars weten al eeuwen dat goede dingen in drieën komen: de waker, slaper en dromer. Dat geeft je twee kansen tot detectie en repressie voordat jouw persoonsgegevens lekken. Het wordt tijd dat we beveiliging echt op die manier gaan aanvliegen.

(Advertorial)

DNV EN DE CERTIFICERINGSMARKT

Een redacteur van Informatiebeveiliging bezocht onlangs de Zorg & ICT Beurs en raakte in gesprek met DNV. DNV Business Assurance is een belangrijke speler in de certificeringsmarkt. Als certificerende instelling certificeert en traint DNV volgens (inter)nationale- en brancheSpecifieke normen en standaarden op gebieden als o.a. kwaliteit, veiligheid, duurzaamheid, arbo, voedselveiligheid en informatiebeveiliging.
We vroegen Mike Wetters, lead auditor informatiebeveiliging van DNV Business Assurance, naar de norm NEN 7510. Wetters: "De norm NEN 7510 is een afgeleide van ISO 27001 en toegesneden op informatiebeveiliging in de zorg. Deze norm is specifiek bedoeld voor instellingen in de zorgsector om de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie ten behoeve van verantwoorde zorg voor patiënten te waarborgen. Naast het borgen van informatiebeveiliging moeten de informatiebeveiligingsmaatregelen volgens de norm zo zijn ingericht dat ze zijn te controleren. NEN 7510 kan worden gezien als een kader waarbinnen iedere proceseigenaar relevant geachte informatie voor het proces kan specificeren, inclusief bijbehorende maatregelen. De norm dekt het hele gebied van informatiebeveiliging en blijft dus niet beperkt tot technische specificaties maar geeft ook richting aan de organisatie en het menselijk handelen. Bij informatiebeveiliging, ongeacht welke branche het betreft, gaat het om 70% menselijk handelen en 30% ICT systemen."

Wetters vertelt over de proefaudits die DNV Business Assurance verzorgt voor bedrijven en organisaties. "Zo'n proefaudit is geschikt voor elke organisatie die wil starten met het opzetten en implementeren van een ISMS (information security management system). Men krijgt dan een overzicht van de al aanwezige elementen van een ISMS en inzicht in hoeverre dit correct is geïmplementeerd. Een goede graadmeter of de organisatie klaar is voor een externe NEN 7510 of ISO 27001 audit."

DNV Business Assurance ontwikkelde de whitepaper 'In 10 stappen starten met informatiebeveiliging volgens NEN 7510 of ISO 27001'.

De whitepaper is te downloaden via www.dnvba.nl/whitepaper.

(www.dnvba.nl/informatiebeveiliging)

ARTIKEL VAN HET JAAR 2011

Leo van Koppen, voorzitter van de jury.
Leo is te bereiken via l.c.m.vankoppen@hhs.nl

Bij publicatie van deze uitgave zal de prijsuitreiking voor het artikel van het jaar 2011 net geschied zijn. Deze vond plaats op de ledenvergadering van 26 April.

Allereerst de uitslag:

auteur	titel	thema	
Schimmel, P	Succesvolle integriteitsbeheersing door beïnvloeden menselijk handelen	menselijke factor	1
Veen, M. van,	De volgende stap in applicatiebeveiligingsonderzoeken	applicatie beveiliging	2
Roosendaal, A.	Facebook volgt iedere internetgebruiker: like this!	social media/ privacy	3

De beweegredenen van de jury in het kort:
P. Schimmel: Boeiend artikel over een essentieel aspect van het vakgebied: integriteit van mensen, dat een breed publiek zal aanspreken. Nieuwe invalshoeken worden getoond en uitstekend uitgewerkt. In essentie toepasbaar in een breed scala van organisaties en functies.
M. van Veen: Applicatiebeveiliging is de achilleshiel van IT-beveiliging en mede daarom verdient dit artikel alle waardering en is een must read voor alle software engineers, omdat het applicatiebeveiliging daarmee inderdaad naar een hoger niveau kan brengen. Overigens ook zeer leesbaar voor niet software engineers.
A. Roosendaal: In een uitstekend opgebouwd artikel wordt bij de conclusie duidelijk dat Facebook onontkoombaar is. Op heldere wijze worden de slimme technieken die Facebook toepast uitgelegd. Het leest als een thriller, want langzaamaan sluit het net zich om het slachtoffer, gebruiker van Facebook of niet.
In de volgende uitgave van Informatiebeveiliging wordt het volledige juryrapport geplaatst, met een verslag van de uitreiking van de prijs.

COLOFON

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

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

Redactieraad
Tom Bakker
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;
of neem contact op met MOS (Motivation Office Support)
T (033) 247 34 00
ibmagazine@pvib.nl

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

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

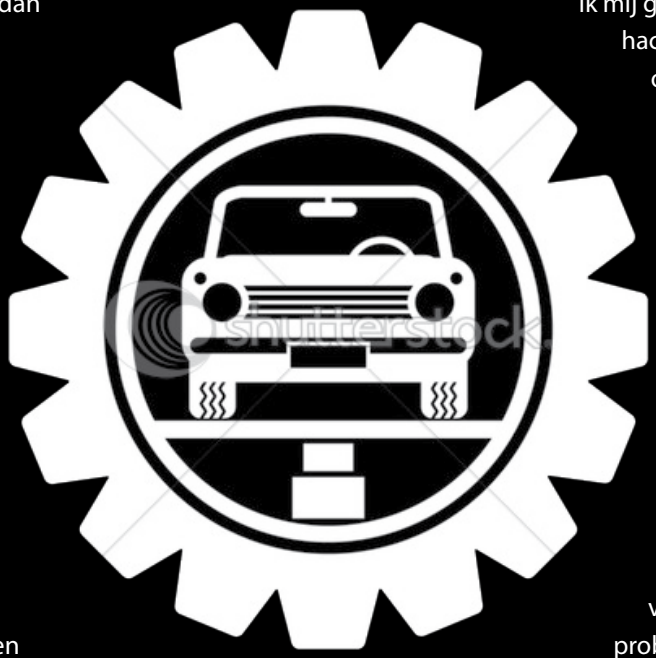
Abonnementen 2012
De abonnementsprijs bedraagt 115 euro per jaar (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

STORENDE ONDERHOUDSACHTERSTAND

Kortgeleden ging mijn auto naar de garage voor een reguliere onderhoudsbeurt. Inmiddels is de rekening op de deurmat gevallen en valt het toch weer tegen maar met de wetenschap dat een goed onderhouden auto vele malen betrouwbaarder is dan een auto met onderhoudsachterstand. Omdat ik zowel overdag als in de nacht in weer en wind over de Nederlandse wegen rijd is een betrouwbare auto mij dan ook wel wat waard. Ik open de website van het telebankieren van mijn bank maar daar wordt aangegeven dat "de dienst tijdelijk niet beschikbaar is". Geen probleem doe ik het over een uurtje wel. Even op nu.nl kijken en daar valt mij het bericht op dat dit reeds de 3e dag is dat er geen betalingen verricht kunnen worden.
Ik neem mijn peinshouding aan en vraag mij af hoe de reactie binnen ons bedrijf zou zijn als onze klanten 3 dagen geen connectie kunnen maken met onze databases. Ik denk dat de sfeer binnen ons bedrijf niet optimaal zou zijn (ik druk mij voorzichtig uit). Ik lees verder en zie dat er wederom een grote stroomstoring bezig is en dat de elektriciteitleverancier geen idee heeft hoelang dat allemaal nog zal duren. Mijn peinshouding wordt nog eens geïntensiveerd en ik zoek op google eens naar stroomstoringen; uit het aantal hits blijkt wel dat het blijkbaar niet meer vanzelfsprekend is dat er stroom op je stopcontacten staat. Inmiddels ben ik echt gaan peinzen en komen er ineens allerlei berichten in mij op van de afgelopen periode.
Grote dagenlange storing in het netwerk van BlackBerry. Uiteindelijk bleek dit probleem veroorzaakt door een server in London. Een server in London zorgt ervoor dat het hele BlackBerry netwerk plat ligt, één server zorgt voor problemen bij honderdduizenden gebruikers. Langdurige en veelvuldige storingen bij mobiele telefonie providers, hoe kan dat nou? Maandelijks minimaal 20 euro incasseren en dan onderuit gaat door een relais die doorgebrand is? Een onderdeel van maximaal 50 euro zorgt voor uitval van de telefonie bij tienduizenden bellers? Deze storingen zijn ook heel duidelijk te herkennen voor klanten, of je kunt elektronisch betalen of niet, Je telefoon doet het wel of hij doet het niet. Je scheerapparaat heeft wel of geen stroom.



Zorgelijker vind ik het feit dat ik niet altijd door heb of de door mij geregistreerde persoonsgegevens wel of niet veilig liggen opgeslagen. Ik kan niet herkennen of ze wel of niet gekopieerd zijn door hackers, dat geeft de bewaarder van de data ook de ruimte om het maar even stil te houden. Wat niet weet wat niet deert, schijnt het credo te zijn. In een van mijn eerdere columns geef ik ook aan dat ik mij geen zorgen maak om de bekende hacks maar vooral om de nog niet ontdekte hacks. KPN komt ermee weg om een dagenlange telefoniestoring te verklaren met een relais van 50 euro, ze komen er blijkbaar ook mee weg een hack langere periode te verzwijgen. Wat de KPN vergeet is dat het mijn persoonsdata zijn, die zijn van mij en de KPN moet deze beschermen want zij willen ze hebben om een verhuizing te kunnen effectueren. Een korte analyse van de veroorzakers van deze problemen? Om de aandeelhouders tevreden te houden en de winstcijfers niet teveel onder druk te laten zetten onderhouden we onze spullen niet. We voeren de noodzakelijke updates niet uit en we laten alle telefonie over dat ene relais lopen. Als die stuk gaat dan vervangen we hem wel, als we hem niet in voorraad hebben dan bestellen we dat relais eerst. Dubbel uitvoeren? Weet je wel wat dat kost?
Jammer genoeg gaat deze verkeerde bezuiniging ook de grens over. In Frankrijk gaan ze nog grover te werk. Een kerncentrale kan best 60 jaar mee in plaats van de 40 jaar waarop ze gebouwd zijn. Over 10 jaar bereiken 22 van de 58 reactoren de respectabele leeftijd van 40 jaar. Ook zij mogen dan nog niet met pensioen. Ze moeten nog een jaartje of 20 door, en wij maar zeuren dat onze pensioen gerechtigde leeftijd van 65 naar 67 gaat. We kunnen best nog wel even door met Windows Explorer 6, hij doet het toch nog? Hoezo een nieuwe werkplek? Wat is er mis met je oude werkplek met Windows XP? Een upgrade van onze CV ketel? Onzin, het is toch lekker warm?
Peinzend kijk ik naar de rekening die ik van mijn garage mocht ontvangen, ik zal het geld wel even pinnen en het bij mijn garage langsbrengen, tenminste als de geldautomaat nog werkt.

Groetjes, Berry

SOPHOS

simple + secure

Individually great, altogether – better

Security products that cover every aspect of your business, individually great, but if you put them altogether – they're even better.

endpoint | web | e-mail | encryption | mobile | network

distributeur: CRYPSYS Data Security | 0183 - 62 44 44 | sales@crypsys.nl | www.crypsys.nl