07/2011

INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 7- 2011

PKI, GEEN MYSTERIE EN ZEKER GEEN MAGIE

SECURITY AWARENESS

ING'S ROLE BASED ACCESS CONTROL IS ROBUUST

DENIAL OF SERVICE AANVALLEN

HET DIGINOTAR-DRAMA IN TWEETS

FOX-IT

for a more secure society

Protecting secrets

Fighting cybercrime

Finding digital evidence

Innovating internet interception

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

VOORWOORD

In mijn eerste voorwoord heb ik mij gewaagd aan een aantal voorspellingen. Nu we een heel eind verder zijn in een tumultueus jaar lijkt het me een goed moment om een tussenstand op te nemen:

Ik dacht dat we dit jaar niet weer een aanval à la Stuxnet zouden zien. Wat ik toen voor ogen had was een aanval met meerdere 'zero-days', Stuxnet had er vier. Dit vond ik het meest opmerkelijke aspect van de succesvolle verspreidingsstrategie van deze worm. Het is echter niet zo dat een volgende Stuxnet wederom zo zou moeten leunen op zero-days. Alleen in dit geval is een heel andere route uitgestippeld om binnen te dringen. Het feit dat we zo gek zijn om honderden root-certificaten (bijna) blind te vertrouwen in iedere computer die aan internet verbonden is, is echt te gek voor woorden als je erover nadenkt. Dat is misschien wel een van de belangrijkste lessen die we mogen trekken uit de geschiedenis van malware. We lopen als beveiligers telkens een stap achter op de hackers, die weer iedere keer een nieuwe dosis creativiteit tonen. Ik erken nu dan ook dat de DigiNotar-hack als een waardige opvolger gezien mag worden. Wereldwijd is het groots in het nieuws geweest. Ook buiten de beveiligingskringen of zelfs buiten de IT. Dat, gecombineerd met het faillissement van DigiNotar en de dreiging dat meerdere CA's al 'owned' zijn, maakt dit een cyberaanval van het hoogste kaliber. En het is nog niet afgelopen. Voorspelling 1: NIET uitgekomen.

Ik dacht dat we dit jaar een publieke aanval op het gsm-verkeer zouden zien. Tot zover is het rustig op dit front. Of het heeft nog niet plaatsgevonden, of we hebben er nog niets van gemerkt. Het blijft dus zo dat gsm theoretisch lek is, maar praktisch is dat nog niet gebleken. Hier zie ik de zwakte van mijn voorspelling. Het zou zomaar kunnen dat ergens een partij al helemaal onder de aanval staat van een advanced persistent threat, waarbij gsm-verkeer een belangrijke rol speelt, maar daarmee is het nog niet publieke kennis. Wellicht hebben de telecombedrijven hier nog een kans om de aanvalsgolf voor te blijven. Alhoewel, ik ben in dat geval toch bang dat we weer zoveel compatibiliteit moeten inbouwen met oude infrastructuur dat een aanval nog steeds mogelijk blijft, ook al zijn de protocollen verbeterd. Voorspelling 2: te vroeg voor een uitslag.

En mijn laatste onderwerp: een malwareplaag op het iOS- of Android-platform. Ik wil denken dat Zeus in the mobile (ZITM) zich hiervoor kwalificeert. Het is niet echt breed uitgemeten in alle pers, maar het heeft onder de beveiligers best wel wat losgemaakt. Het concept van sms als sterk authenticatiemiddel, omdat het door middel van een ander kanaal wordt verstuurd en ontvangen, is in de laatste tien jaar compleet onderuit gehaald door de opkomst van de smartphone. Nu kan ZITM transparant sms-berichten afvangen, en het is geen theoretische aanval meer. Al moet ik toegeven dat de omvang vooralsnog beperkt is en je voor een 'plaag' je meer 'last' mag verwachten. Voorspelling 3: een mager 'wel uitgekomen'.

Ik scoor voorlopig nog niet best als visionair, ik kan mijn huidige baan beter nog maar even aanhouden. Ik wacht nog even twee uitgaven voordat ik mezelf gewonnen geef en ik begin alvast na te denken over voorspellingen voor 2012. Ik zie dat het vakgebied informatiebeveiliging in ieder geval meer in de belangstelling staat dan in voorgaande jaren en aan verandering onderhevig is. Ik wil die beweging graag volgen met dit blad.

INHOUDSOPGAVE

Voorwoord 3

PKI, geen mysterie en zeker geen magie 4

Column: Technodwang 9

Security Awareness 10

ING's Role Based Access Control is robuust 14

Denial of Service aanvallen – Deel 1 20

Boekbespreking: De Macht van Michael Bellinger 23

Het DigiNotar-drama 25

Achter het nieuws 26

Geslaagd Security Congres van PvIB, NOREA & ISACA 28

Joop Bautz Information Security Award 29

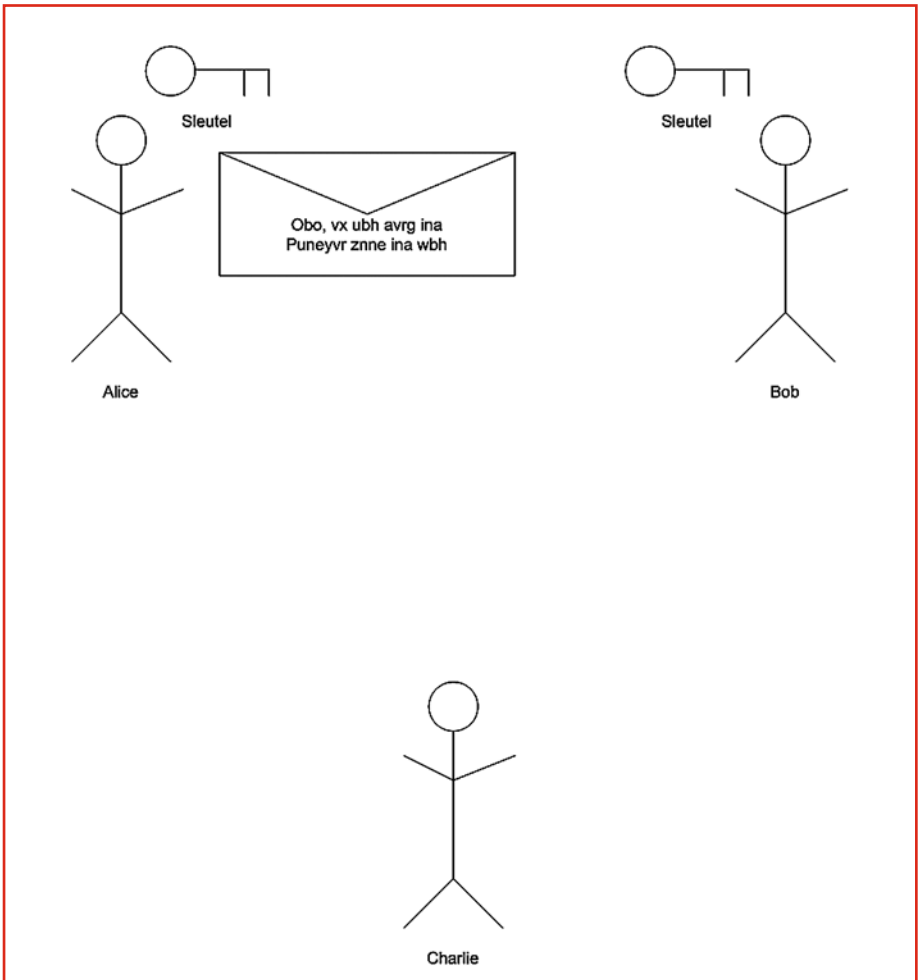
Column Berry: 'Gelukkig is er niets gebeurd...' 31

PKI, GEEN MYSTERIE EN ZEKER GEEN MAGIE

Shaun is werkzaam als freelance technical writer. Hij is bekend bij de redactie. Reacties graag via de redactie.

Door de recente ontwikkelingen bij DigiNotar en GlobalSign en daarvoor bij Comodo staan certificaten ruim in de belangstelling. Zelfs het acht uur journaal en de kranten berichtten erover, maar wat is nu eigenlijk een certificaat of een CA? Wat is PKI voor een beest en hoe doet het wat het moet doen en waarom is de inbraak bij DigiNotar nu eigenlijk zo belangrijk? We mogen ervan uitgaan dat de meeste lezers van dit blad enige kennis van PKI hebben. Toch willen we in dit artikel vanuit de basis (nogmaals) proberen uit te leggen wat PKI is en waarom de inbraak bij DigiNotar voor iedereen slecht nieuws is.

PKI staat voor Public Key Infrastructure, een infrastructuur voor publieke sleutels dus. Maar waarom zijn deze publieke sleutels nu zo belangrijk en waarom is er een infrastructuur voor nodig? Om die vraag te beantwoorden moeten we eerst teruggaan naar de basis van cryptografie.



Symmetrische versleuteling.

Symmetrische encryptie

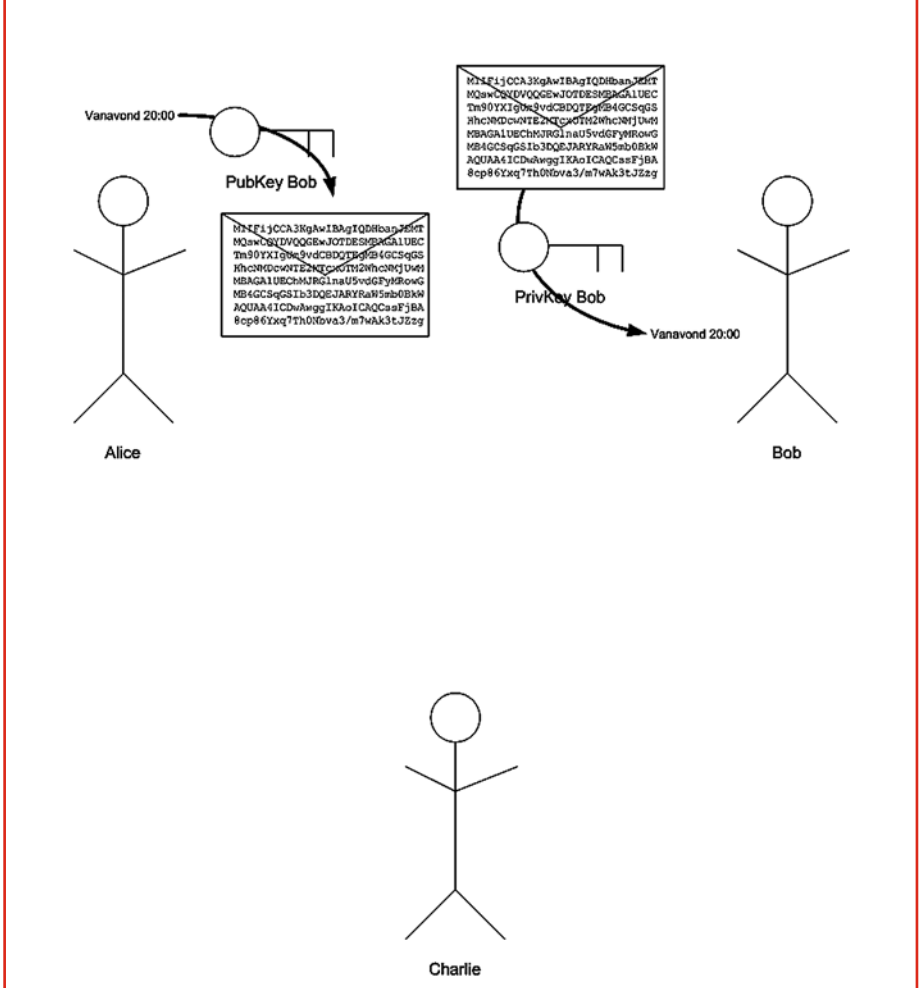
De eenvoudigste vorm van cryptografie is symmetrische encryptie. Bij symmetrische encryptie wordt er gebruikgemaakt van een afspraak. Bijvoorbeeld vervang elke letter in het alfabet door de letter die 13 posities verder of terug staat [1)]. Deze afspraak heet de sleutel (key). Als Alice een bericht naar Bob wil sturen zonder dat Charlie het leest, dan verandert zij de tekst van het bericht (plaintext) met behulp van de sleutel in een gecodeerd bericht (ciphertext) die zij naar Bob kan sturen zonder dat Charlie het kan lezen. Bob kan deze ciphertext met dezelfde sleutel weer omvormen naar plaintext en zo het bericht lezen.

Het nadeel van deze encryptie is dat Alice en Bob de sleutel moeten uitwisselen zonder dat deze in handen van Charlie valt. Symmetrische encryptie werkt dus alleen als er naast het gecodeerde communicatiekanaal nog een ander, vertrouwd kanaal bestaat.

Waarom is de inbraak bij DigiNotar voor iedereen slecht nieuws?

Asymmetrische encryptie

Bij asymmetrische encryptie wordt er niet één sleutel gegenereerd, maar een sleutelpaar, bestaande uit een publiek deel (public key) en een privaat deel (private key). Deze twee sleutels worden (via een cartografische berekening [2)]) zo gekozen dat zij complementair aan elkaar zijn. Dat wil zeggen, alles wat met de public key versleuteld is kan uitsluitend met de private key worden ontsleuteld en omgekeerd. Dus, indien Alice een bericht aan bob wilt sturen, dan kan zij met behulp van Bob's public key haar bericht omzetten van plaintext naar ciphertext. Alleen Bob kan met zijn private key deze ciphertext weer leesbaar maken.



Asymmetrische versleuteling.

ook wel een Man-in-the-Middle-attack genoemd.

Digitale handtekening

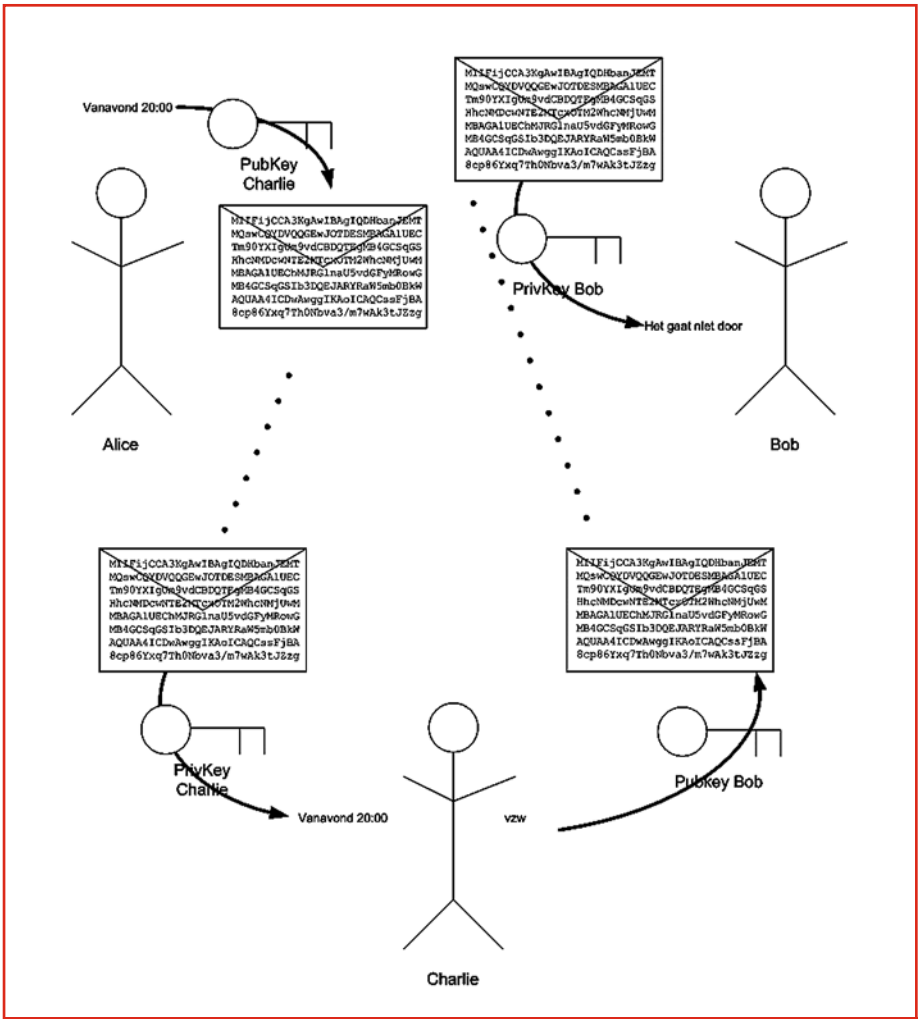
Asymmetrische cryptografie kan ook worden gebruikt om de authenticiteit van een bericht aan te tonen. Hierbij wordt gebruikgemaakt van het feit dat wat met de private key is versleuteld, met de public key ontsleuteld kan worden. Stel dat Alice bij het versturen van haar bericht, ook een kopie van het bericht meestuurt dat is versleuteld met haar private key. Bob weet zeker dat als het bericht en het versleutelde bericht overeenkomen, het bericht daadwerkelijk van Alice afkomt. Zij is immers de enige die het bericht kon versleutelen met de private key. Omdat het twee keer versturen en versleutelen van berichten veel processorkracht kost, wordt in plaats van een versleutelde kopie van het bericht, een versleutelde kopie van de hash[3)] van het bericht bijgesloten.

Asymmetrische encryptie heeft als voordeel dat Bob zijn public key niet tegen afluisteren hoeft te beschermen, deze kan immers niet worden gebruikt om de berichten tussen Alice en Bob af te luisteren dat kan namelijk alleen met de private key van Bob.

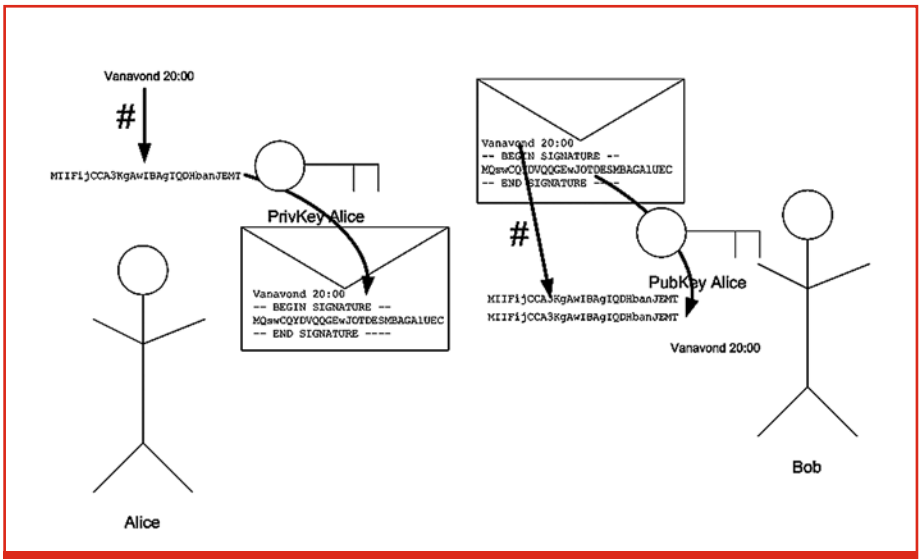
Man-in-the-Middle

Het is voor Alice echter wel enorm belangrijk te weten dat de public key van Bob ook daadwerkelijk de public key van Bob is. Indien Charlie Alice weet te overtuigen dat de de public key van Charlie de public key van Bob is, dan kan hij de communicatie afluisteren en zelfs veranderen zonder dat dit voor Alice of Bob zichtbaar is.

Alice encrypt haar bericht met de public key van Charlie, denkende dat dit de public key van Bob is. Charlie onderschept het bericht, decrypt het met zijn eigen private key, leest het bericht en encrypt het vervolgens met de echte public key van Bob. Bob ontvangt het bericht en kan het met zijn eigen private key decrypten. Deze aanval wordt



Man-in-the-Middle m.b.v. certificaten.



Digitale handtekening.

Bob weet in dit voorbeeld dus zeker dat het bericht afkomstig is van Alice, omdat hij de public key van Alice heeft. Ook hier is het weer van wezenlijk belang dat Bob zekerheid heeft dat de public key van Alice ook daadwerkelijk de public key van Alice is.

Vertrouwenspersoon

In dit beperkte voorbeeld is het voor Alice en Bob nog te doen om sleutels uit te wisselen en zo zeker te zijn over welke identiteit bij welke sleutel hoort. Maar naar mate de populatie groeit wordt dit steeds moeilijker. Dit is op te lossen door het inroepen van een vertrouwenspersoon, de zogeheten TTP (Trusted Third Party). De rol van deze TTP is het vaststellen van de identiteit van een persoon en het koppelen van deze identiteit aan een public key.

Certificaat

Stel, Alice bezoekt Trent, een TTP, en bewijst haar identiteit aan Trent. Trent kan nu een document maken met daarin een beschrijving van de identiteit van Alice en een kopie van haar public key. Zo'n elektronisch identiteitsdocument noemen we een certificaat[4]. Een certificaat bevat onder andere de zogenaamde Common Name (CN) van het Subject (de persoon waarvan de identiteit is vastgesteld) en de CA (Certificate Authority, de TTP de het certificaat heeft verstrekt) en de public key van het Subject.

Stel dat Bob een bericht binnenkrijgt dat bestaat uit de volgende onderdelen:

- het bericht;
- een digitale handtekening van het bericht;
- het certificaat van de verzender.

Bob kan nu:

- de identiteit van de verzender vaststellen aan de hand van de CN in het certificaat;
- de echtheid van het bericht vaststellen aan de hand van de handtekening van het bericht en de public key van het certificaat;
- de echtheid van het certificaat vaststellen aan de hand van de handtekening van het certificaat en de public key van de CA.

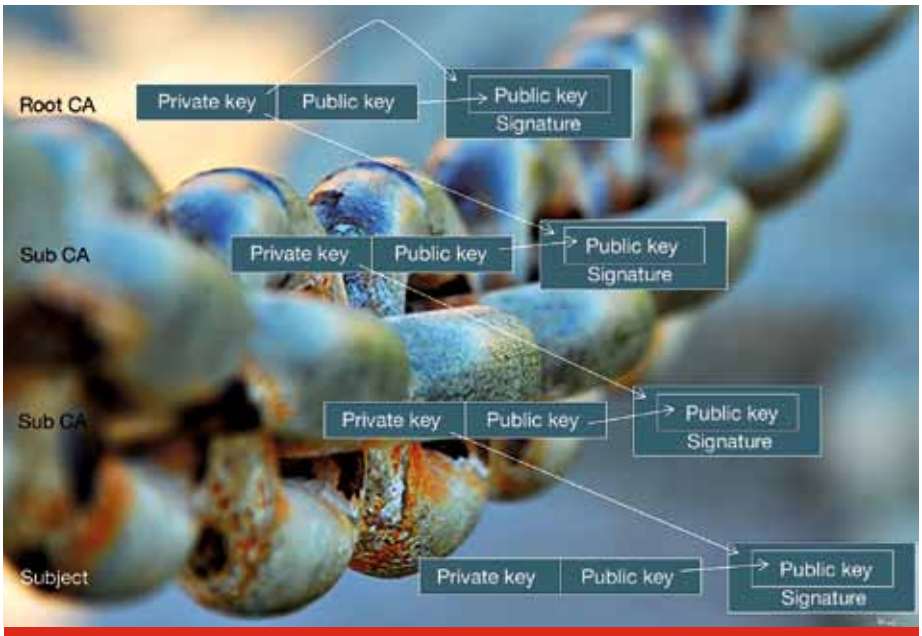
Vertrouwensketen

Een CA verspreidt zijn public key vaak ook in een door hemzelf getekend certificaat, een zogenaamd self signed certificate. Hierdoor ontstaat een vertrouwensketen (chain of trust).
Vanuit praktische overwegingen worden identiteiten niet altijd rechtstreeks door een zogenaamde root CA getekend, maar door een sub (ook wel intermediate) CA. Zo had PKI overheid een Sub-CA die beheerd werd door DigiNotar. Hierdoor hoefde de overheid niet zelf alle 'PKI-Overheid'-certificaten uit te geven, maar kon ze dit werk uitbesteden aan derden.[5]

Het volle vertrouwen?

In een PKI-infrastructuur worden de Root CA's voor de volle 100% vertrouwd. Zij mogen dus certificaten uitgeven voor alle doeleinden en voor iedere identiteit. Dit staat in sterk contrast tot wat wij gewend zijn bij bijvoorbeeld de uitgifte van paspoorten. De Nederlandse overheid mag immers nooit Amerikaanse paspoorten uitgeven.

In de PKI worden de Root CA's voor 100% vertrouwd



Vertrouwensboom Certificate Authorities.

X.509 bevat wel mechanismen om beperkingen op te leggen aan de uitgifte van certificaten, maar deze mechanismen kunnen alleen worden gebruikt om de mogelijkheden van de door de CA uitgegeven certificaten te beperken. Zo kan een CA bijvoorbeeld voorkomen dat je met een simpel SSL-certificaat zelf nieuwe certificaten kunt ondertekenen.

De voorwaarden waaronder een CA certificaten verstrekt en de garanties die CA's voor hun werk verlenen zijn ook per CA verschillende. Zo verstrekt een CA die zogenaamde 'domain validated'-certificaten verstrekt, deze op basis van de gegevens die zijn vastgelegd in de domeinregistratiedatabase en het feit dat de aanvrager kan reageren op een mail verstuurd naar een in deze database genoemd e-mailadres. Voor een 'organisation validated'-certificaat moet echter ook de identiteit van de aanvragende organisatie worden vastgesteld.

Deze verschillen staat omschreven in de CSP (Certificate Signing Policy). Voor eindgebruikers zijn de verschillen, met uitzondering van EV-certificaten waarbij de adresbalk groen kleurt, echter nauwelijks zichtbaar.

> Er zijn ruim 200 CA's die door de browser worden vertrouwd

PKI in uw browser

Iedereen die internet gebruikt, gebruikt al PKI. Elke keer als u een beveiligde site bezoekt, wordt zonder dat u dat merkt, een aantal acties uitgevoerd:

- het certificaat van de site wordt opgehaald;
- er wordt gecontroleerd of het certificaat ondertekend is door een, door de browser, vertrouwde CA of dat de keten van certificaten eindigt in een certificaat van een vertrouwde CA;
- van alle certificaten wordt gecontroleerd of de geldigheidsdatum in orde is;
- van alle certificaten wordt gecontroleerd of deze niet op een online intrekkingslijst staan;
- er wordt gecontroleerd of de webserver wel over de juiste private key beschikt.

Hoeveel CA's zijn er?

Het Microsoft Root CA program onderkende in 2009 104 organisaties. Deze 104 organisaties beheerden in totaal 285 CA's. Toen ik in mei 2010 het aantal root CA's in mijn Firefox-browser telde, kwam ik op een totaal van 216 CA's. Er zijn dus ruim 200 CA's die door een browser, en dus impliciet door de gebruiker van de browser, worden vertrouwd. Iedere CA, voor de volle 100%, voor iedere claim die ze in hun certificaten maken. Over wie hier toezicht op houdt en op welke manier dit toezicht wordt ingevuld leest u in een volgend artikel meer.

De zwakste schakel

De inbraak bij DigiNotar laat zien dat het CA-systeem zo sterk is als zijn zwakste schakel, in dit geval DigiNotar.

De zwakste schakel.

De DigiNotar-inbraak is, bij het grote publiek, onder de aandacht gekomen doordat het internetgebruikers in Iran opviel dat bij het bezoeken van, met SSL beveiligde, Google-sites gebruikgemaakt werd van een door DigiNotar uitgegeven certificaat voor *.google.com[6]. Waarschijnlijk met als doel de communicatie tussen de gebruiker en Google af te luisteren of te manipuleren. De werkwijze was vermoedelijk om het Google-verkeer via een met een namaakcertificaat vermomde proxyserver te laten lopen. De gebruikers zien een vertrouwd *.Google.com-certificaat en hebben niet door dat er iets mis is. Zo'n werkwijze is in dergelijke landen met door de overheid gereguleerde ISP's natuurlijk goed te realiseren. In dit geval is de proxy server de Charlie uit onze plaatjes. Wat voor google.com kan, kan ook voor andere domeinen. Een Man-in-the-Middle-attack is mogelijk tegen iedere site, ongeacht welke certificaten of CA de site zelf gebruikt.

DANE, Perspectives en Convergence

Dane staat voor DNS-based Authentication of Named Entities. DANE is een protocol waarmee aanvullende informatie ten behoeve van het identificeren van bijvoorbeeld websites in DNS geraadpleegd kan worden. Via DANE is het voor een beheerder bijvoorbeeld mogelijk het serienummer of de fingerprint van zijn certificaat vast te leggen of vast te leggen dat zijn site uitsluitend gebruikmaakt van certificaten van een enkele CA. Hiermee wordt de controle voor een belangrijk deel teruggegeven aan de beheerder. Voor de werking van DANE is de betrouwbaarheid van DNS-gegevens van levensbelang. Daarom is invoering DNSSEC een voorwaarde voor DANE.
Perspectives en Convergence zijn beide systemen die proberen de 'echtheid' van SSL-certificaten via een andere methode dan het PKI-systeem vast te stellen. Beide systemen maken gebruik van zogenaamde notaries. Indien de browser een met SSL beveiligde site bezoekt, dan biedt deze de gegevens van het certificaat ter controle bij de notaries aan. Deze notaries vergelijken de gegevens met het door henzelf opgehaalde certificaat en geven vervolgens een resultaat, goed/niet goed, terug aan de browser. Indien voldoende notaries een positief resultaat geven vertrouwt de browser de site.

Conclusie

Het huidige PKI-systeem is door zijn uitgestrektheid en het onbeperkte vertrouwen in de CA's zo fragiel geworden, dat een beveiligingsprobleem bij één CA, in dit geval DigiNotar, in een klap het vertrouwen in alle SSL-verbindingen ondermijnt totdat het vertrouwen in de 'foute' CA wordt opgezegd. Hoewel het PKI-systeem zijn diensten heeft bewezen en nog steeds bewijst, is het inmiddels duidelijk aan het worden dat het niet geschikt is voor de schaal waarop het nu op het internet wordt toegepast. Het is voor de periode tussen 10 juli 2011 en het intrekken van de DigiNotar-certificaten onmogelijk te garanderen dat welke SSL-verbinding dan ook veilig is geweest. Het internet is toe aan alternatieven als DANE, Perspectives of Convergence[7], maar tot deze breed geaccepteerd zijn zullen we vooral onze CA's (en RA's[8]) in de gaten moeten houden.

We zullen onze CA's in de gaten moeten houden

Eindnoten

[1] Dit algoritme is bekend als ROT13, zie http://nl.wikipedia.org/wiki/Rot13

[2] Een voorbeeld hiervan is het RSA-algoritme. Zie http://nl.wikipedia.org/wiki/RSA (cryptografie)

[3] Een hash is een unieke code die als het ware de vingerafdruk van het bericht is. Het is praktisch onmogelijk twee berichten te fabriceren met een gelijke hash. Deze code wordt berekend met een hashing algoritme zoals bijvoorbeeld het SHA-algoritme. Zie http://nl.wikipedia.org/wiki/SHA-familie

[4] De exacte specificatie van digitale certificaten is beschreven in de X.509-standaard. Zie http://en.wikipedia.org/wiki/X.509

[5] Image: Don't Chain Me Down, a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from intherough's photostream

*[6] Het is in X.509 toegestaan zogenaamde wildcards voor delen van de Common Name te gebruiken. Volgens de standaard is een certificaat voor * voor alle websites geldig en een certificaat voor *.*.com voor alle .com certificaten. Gelukkig worden deze ruimtepatronen door moderne browsers niet meer ondersteund.*

[7] Zie: https://datatracker.ietf.org/wg/dane/, http://www.networknotary.org/firefox.html en http://convergence.io/

[8] RA staat voor registration autoristy. Een CA kan een gedeelte van zijn registratieproces delegeren aan een RA. Deze zorgt dan voor de registratie en validatie van de gegevens van de aanvragende partij en verzorgt de aanvraag van het certificaat bij de CA. De CA vertrouwt op de identiteitscontrole van de RA en levert vervolgens het certificaat.

COLUMN

TECHNODWANG

HOE ONLINE AANBIEDERS JOUW LEVEN BESTUREN

Met veel bombarie en tamtam stapt Zuckerberg op het podium. Hij kondigt aan dat hij mijn leven gaat indexeren. Alles netjes onder elkaar gaat zetten. Echt, alles wat ik ooit meemaakte mooi en inzichtelijk voor de hele wereld. Hij gaat ook voor mij bepalen wat de meest belangrijke zaken uit dat leven van mij zijn geweest. Daar weet Facebook natuurlijk alles van. Die snapt wat belangrijk is en kan die beslissing ook best voor me maken. En ze noemen het Timeline. Facebook gaat de profielen van gebruikers opnieuw inrichten, alles wat je in de loop van de jaren aan informatie hebt toegevoegd (of wat anderen over jou hebben verteld) wordt onder elkaar gezet en per jaar aanklikbaar.

"From now on, you can discover all the things people have done in their life!".

Daarnaast gaat Facebook wat veranderen betreffende de apps die je via het sociale netwerk gebruikt. Stel, je leest een online tijdschrift en luistert naar muziek via een dienst als Spotify (die je ook toegang hebt verleend tot jouw profiel doordat je akkoord bent gegaan met de Algemene Voorwaarden). Je bladert wat door verschillende artikelen heen (je swipet natuurlijk, bladeren is wel erg offline), soms kom je wat interessants tegen, maar vaak ook niet. Wat je niet weet, is dat op datzelfde moment de app al aan al jouw vrienden op Facebook heeft verteld wat je allemaal aan het lezen bent en welke muziek jou daarbij heeft begeleid. Dat verschijnt in een livestream op Facebook. Ook als je al bent uitgelogd. Deze livestream vertoont zeer veel kenmerken van het eerder door Facebook gelanceerde Beacon. Een feature die Facebook heeft moeten cancellen vanwege privacy issues en een rechtszaak die door vele gebruikers tegen de dienst was aangespannen. Of deze nieuwe livestream met gegevens van gebruikers het gaat overleven, is dus nog maar zeer de vraag.

Ik ben redelijk optimistisch ingesteld. Maar van deze wijzigingen in de functionaliteit van Facebook krijg ik echt kippenvel. En dan niet op een goede manier. Nog maar een paar columns terug vertelde ik dat ik naar Facebook was verhuisd vanwege de mogelijkheden om meer privacygericht mijn leven te delen met vrienden en familie. (Dat was overigens voordat Google+ in beta ging…). Het is wel wat bewerkelijk, want je moet telkens in de gaten blijven houden of Facebook niet stiekem weer wat verandert in de functionaliteit. Dat doen ze namelijk zeer regelmatig en meestal staat er dan weer wat open en deel je ineens, zonder het te beseffen, heel veel met heel veel mensen. Technodwang noem ik dat. Aanbieders van online diensten die telkens weer wat veranderen in de functionaliteit van de aangeboden dienst waardoor je gedwongen wordt een bepaalde richting op te gaan en de keuze om daarvan af te wijken in bijna alle gevallen ontbreekt.

Het dwingen door middel van technologie is niet nieuw. Het bestaat al geruime tijd en wordt ook wel begrepen als het reguleren van mensen, het sturen van gedrag. Reguleren hoeft niet per se een negatief gevolg te hebben, een duwtje in de juiste richting kan zeer goed uitpakken indien daaraan de juiste redenen ten grondslag liggen en dit beargumenteerd wordt gedaan. Het sturen van gedrag door middel van technologie heeft echter ook een aantal minder positieve kanten. Ten eerste is het vaak absoluut, hetgeen wil zeggen dat er geen keuze is voor de gebruiker om deze dwang te negeren. Ten tweede, de redenen die erachter liggen, willen nog wel eens niet transparant zijn voor de gebruiker. Ten derde ontstaan er soms neveneffecten wat betreft de privacy van personen die tevoren niet waren voorzien en die daardoor vaak achteraf gerepareerd moeten worden.

Sociale netwerksites zoals onder meer Facebook maken vaak gebruik van deze technodwang. Telkens verandert er iets zonder dat gebruikers dat in de gaten hebben. De werelden zijn er ook zo op ingericht dat we ons onder vrienden wanen hetgeen ons een veilig gevoel geeft. Daardoor laten we meer van onszelf zien en het is uiteraard de bedoeling dat we zoveel mogelijk delen met zoveel mogelijk vrienden en vrienden van vrienden van vrienden. Openheid en delen zijn daarbij de sleutelwoorden. Technodwang kan ook op een andere manier worden toegepast als duwtje in de juiste richting. Google+ bijvoorbeeld maakt gebruik van technodwang door de defaultinstellingen van de sociale netwerksite op volledig gesloten te zetten. Als je bijvoorbeeld de app voor iPhone installeert, deel je alleen zaken met jezelf. Je moet daarom actief personen en/of groepen toevoegen waarmee je gegevens wilt delen. Ik zou graag zien dat meer aanbieders van deze vorm van technodwang gebruikmaken. Zo kun je namelijk ook sturen naar meer veiligheid en meer privacy.

mr Rachel Marbus
@RachelMarbus op Twitter

SECURITY AWARENESS

IT SECURITY AWARENESS TRAINING BINNEN GROTE RETAILORGANISATIES

Menno Borst is onafhankelijk IT Risk Manager betrokken bij de afdeling Risk Management van verschillende retailorganisaties waaronder de Bijenkorf, HEMA, V&D, Hunkemöller en Praxis. Binnen zijn aandachtsgebied valt onder meer het aandragen en opstellen van informatiebeveiligingsbeleid, bijbehorende maatregelen en procedures, en het uitvoeren van IT audits als vorm van toetsing op het geïmplementeerde beleid. Hij is bereikbaar via menno.borst@iRiskiT.nl.

Training binnen retailorganisaties kent dezelfde uitgangspunten als die van elke willekeurige organisatie. Het betreft ook hier de uitdaging om medewerkers op een zo toegankelijk mogelijke manier te informeren over het geldende beleid, de opgestelde procedures en toegepaste technieken. De maatregelen die zijn geïmplementeerd om de opgestelde richtlijnen te borgen kun je terugvinden binnen het management van de operationele organisatie en de technische systemen van elke retailer.

In 2007 werd onder de toenmalige leiding van Maxeda Holding Nederland besloten tot het implementeren van een IT Control Framework dat toeziet op het naleven van het informatiebeveiligingsbeleid van de verschillende retailers. Dit beleid is van toepassing op alle werkmaatschappijen onder de vlag van de Maxeda-groep te weten: HEMA, V&D, de Bijenkorf, DoItYourself (bestaande uit Formido, Praxis, Brico, Brico Plan IT), Schaap -/- Citroen, Claudia Sträter, Hunkemöller en M&S mode. Tot aan 2010 is er veel tijd geïnvesteerd om de verschillende opgestelde maatregelen geïmplementeerd te krijgen binnen het management van de operationele processen en daaraan verbonden technische systemen van de retailers. Uit verschillende interne IT-audits kwam steeds duidelijker naar voren dat de security awareness bij de mensen die betrokken waren bij deze implementaties steeds verder toenam. Echter, verschillende security- incidenten toonden aan dat de grootste uitdaging kwam te liggen bij de medewerkers die niet direct betrokken waren bij deze implementaties en die zich onvoldoende bewust waren van de opgestelde richtlijnen. Deze groep bleek groot van omvang, snel wisselend en zeer divers vanuit allerlei aspecten zoals opleiding, interesse, vakgebied, culturele achtergrond, enz.

'Diefstal-cultuur' bij retailers

Binnen de retailers is voor het opstellen van een IT-security awareness-programma gebruikgemaakt van reeds bestaande processen voor het informeren en opleiden van medewerkers. Het was tijdens deze inventarisatie van de bestaande processen dat we erachter kwamen dat medewerkers van retailorganisaties een groot bewustzijn hebben voor beveiliging, vanwege de constante aandacht voor diefstal in de winkels. Het is deze diefstalcultuur die als klassiek kan worden omschreven binnen retailers. Immers, de verdienste (of eigenlijk het voorkomen van verlies) van goede beveiliging leidt direct tot betere financiële resultaten. Deze klassieke (en bij iedere medewerker bekende) diefstalcultuur zal een belangrijke rol spelen in het totale IT-security-programma.
Het eerste proces is het opstellen van een passend programma voor de beveiligingstraining. Zowel de Bijenkorf als V&D zijn op dit moment bezig met het opstellen van dit trainingsprogramma. Nadat het programma is opgesteld gaat men de te ontwikkelen materialen ontwerpen. Het is dit proces waarin de DoItYourself (DIY)-groep zich op dit moment begeeft. Zodra de verschillende materialen gereed zijn, is het van belang om de juiste invulling aan deze materialen te geven. Specifiek voor retail zal men moeten zoeken naar een e-learning-omgeving vanwege het groot aantal medewerkers en hun verschillende locaties in Nederland en daarbuiten.

Gebruik het NIST 800-50-model

Voor de theoretische ondersteuning van het IT-security-programma maken we gebruik van het NIST 800-50-model. Dit model zal de rode draad zijn binnen dit artikel. De keuze voor dit model is gebaseerd op de *lifecycle*-insteek van:

a) ontwerp;
b) ontwikkeling;
c) implementatie;
d) evaluatie.

Eerdere geleerde lessen op het gebied van eenmalige ontwikkeling van trainingen op gebied van IT-security voorzien onvoldoende in de constante verandering binnen de IT. Denk hierbij aan veranderingen op het gebied van

E-commerce, social media, cloud computing en privacy.
Tijdens het ontwerp van het IT-security-programma is bewust gekozen voor een afwijking van het NIST-model voor wat betreft de verantwoordelijkheid van het totale programma. Binnen elke retailer is een separate afdeling Risk Management opgericht die toeziet op zowel de operationele risico's als de IT specifieke risico's. In plaats van de CIO (of IT-managers) deze verantwoordelijkheid te geven is gekozen voor het hoofd Risk Management. Wij geloven met deze aanpak dat juist de IT-afdeling nog objectiever aandacht zal besteden aan de specifieke vereisten op het gebied van IT-security. Immers, de controle op dit programma ligt niet bij hen. De scope van het IT-security-programma is gericht op alleen de onderste laag binnen het NIST-model te weten 'awareness' van alle medewerkers. Omdat bij 'awareness' weinig activiteit van medewerkers wordt gevraagd, zullen er in de beveiligingstraining toch onderdelen van de andere lagen hun weg vinden. Echter, wel met de juiste pragmatiek in het achterhoofd. Vanuit het NIST-model wordt geadviseerd om de gebruikte middelen en materialen binnen de 'awareness' in te zetten bij de training. Dit laatste is door ons als zodanig toegepast door de IT-security flyers voor medewerkers, de aanwezige communicatie (onder andere posters) met '10 geboden van security', bewustwording rondom 3e partijen, PCI-DSS Credit Card-beveiligingscommunicatie, interne Code of Conduct en dergelijke, onderdeel te laten zijn van de beveiligingstraining.

NIST-organisatie
NIST staat voor het National Institute of Standards and Technology. Deze organisatie is in 1901 opgericht in Amerika onder de vlag van het US department of Commerce. Het NIST heeft als doelstelling om in samenwerking met het bedrijfsleven voor nieuwe technologie de bijbehorende maatregelen en standaarden te ontwikkelen ter verbetering van de economische veiligheid en de kwaliteit van het leven.

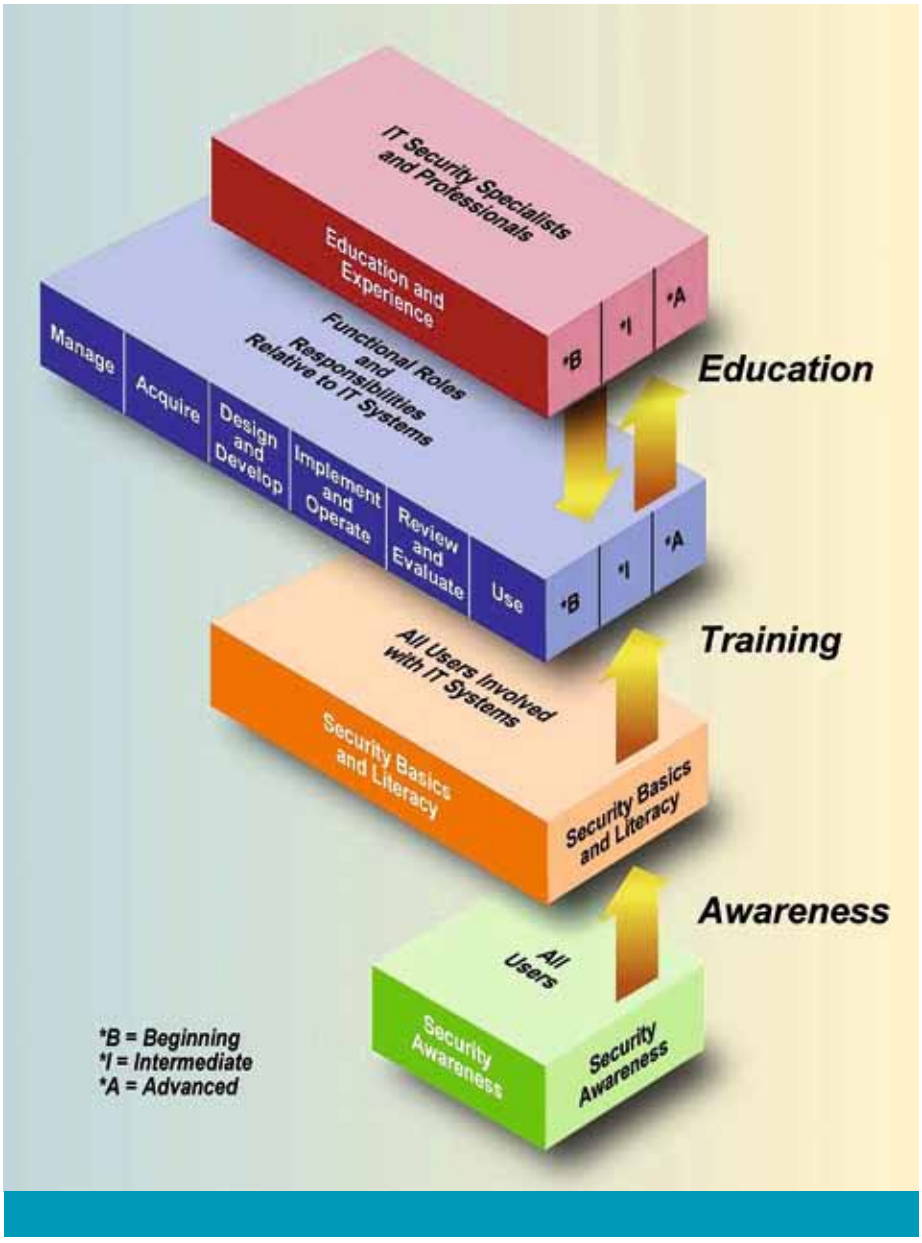
NIST 800-50-model
Het model 800-50 is ontwikkeld om binnen organisaties een IT-security awareness-programma te ontwikkelen en te onderhouden. Er bestaat een gelaagdheid (continuüm) in de aanpak te weten:

- creëren van bewustwording (awareness);
- ontwikkelen van trainingen (training);
- evolueren in opleidingen (education).

Awareness-fase
Deze fase richt zich primair op het bekendmaken van medewerkers met IT-security. Het is ontwikkeld om medewerkers de IT-security-risico's te laten herkennen en daarbij hun reactie te kunnen geven.

Training
De training heeft een hoger ambitieniveau met als doel de medewerker ook daadwerkelijk de benodigde vaardigheden en competenties bij te brengen. Deze vaardigheden en competenties hebben betrekking op hun directe of indirecte betrokkenheid met IT-security-risico's binnen hun werkzaamheden. Een concreet voorbeeld hierbij zijn system operators op IT-systemen.

Educatie
De educatiefase wordt gezien als hoogste volwassenheid binnen het



NIST-model. Deze fase draagt bij aan het beheren van een centraal kennisnetwerk op het gebied van IT-security-risico's. In dit kennisnetwerk komen alle verschillende vaardigheden en competenties bij elkaar waardoor het mogelijk wordt pro-actief te reageren op IT-security-risico's.

Voor de ontwikkeling van de IT-beveiligingstraining was het van belang om de huidige mentaliteit (of strategie) van de retailer duidelijk voor ogen te houden.

Hou rekening met de bedrijfscultuur

Er is een retailer veel aan gelegen om snel in te kunnen springen op de behoeften van zijn klanten. Dit vereist een enorme flexibiliteit en servicegerichtheid van de organisatie en haar medewerkers. Vanuit het informatiebeveiligingsbeleid waren we de afgelopen jaren al een aantal keer tegen deze 'beperking' vanuit IT-Security aangelopen. Immers, de klant komt eerst en dan pas de beveiliging. Inhoudelijk is altijd gekozen voor een goede volwassenheid van de geïmplementeerde maatregelen. Hiervan zal binnen de training niet worden afgeweken. Echter, de wijze van training zal wel voldoende flexibel moeten zijn voor een goede acceptatie. Specifiek wordt dan ook nagedacht om de medewerkers door middel van e-learning vanaf verschillende locaties (winkel, hoofdkantoor, distributiecentrum, thuis) de training te laten volgen.
In de afstemming naar de medewerkers is gekozen om dit via het huidige proces van personeelsmanagement te laten verlopen. Immers, deze processen zijn binnen retailers de afgelopen jaren geprofessionaliseerd en bereiken de juiste medewerkers op het goede moment met de juiste prioriteit. Vanuit het hoofdkantoor zullen de juiste materialen worden ontwikkeld en aangeboden aan de verschillende winkels (warenhuizen).

Gebruik staande organisatie

Er is bewust voor deze servicegerichte aanpak gekozen, omdat die het best aansluit bij de huidige mentaliteit. Het NIST-model biedt overigens ook mogelijkheden om dit decentraal aan te pakken.

Onderwerpen die naar voren komen in de training zijn geselecteerd aan de hand van de 'key'controls binnen het IT Control Framework. Deze aanpak komt voort uit de Risk Management-cultuur binnen deze retailers, de meest risicovolle onderwerpen eerst! Voor de beveiligingstraining van de DIY zijn nu de volgende onderwerpen geselecteerd:

a) toepassen van wachtwoorden;
b) gebruik van internet & e-mail;
c) social engineering;
d) toegangscontrole (incl. uitgangscontrole);
e) e-mailgebruik (onbekende mails, gebruik attachments, enz).

Vragen die nu nog uitstaan hebben met name betrekking op de verder 'in house'-ontwikkeling of het kopen van 'off the shelf'-trainingen behorend bij de hiervoor genoemde onderwerpen.

Zoals reeds eerder vermeld zal de implementatie van de IT-beveiligingstraining primair worden gecoördineerd door de personeelsafdeling van de verschillende retailers. Het is de afdeling Risk Management die het ontwikkelde trainingsprogramma voor 'funding' langs

de board van de retailer moet leiden om aldaar goedkeuring te verkrijgen. De gehele communicatie rondom trainingsprogramma's aan medewerkers in het algemeen wordt centraal op het hoofdkantoor van de retailers voorbereid. Personeelszaken zal specifiek voor dit trainingsprogramma de communicatie regelen richting de verschillende regio- of landmanagers voor wat betreft de planning, omvang en participatie van de medewerkers, methode van training door middel van e-learning en het beloningsmechanisme bij afronding training. Alle medewerkers zullen centraal worden geïnformeerd over hun individuele participatie in het e-learning programma. Dit zal plaatsvinden nadat het overgrote deel van de medewerkers via hun eigen managers is ingelicht. Het betreft hier de initiële start van de IT-beveiligingstraining. Doordat elke retailer te maken heeft met natuurlijk verloop van medewerkers ligt het in de lijn der verwachting dat we ook alle nieuwe en tijdelijke medewerkers van de retailers via personeelszaken laten informeren over het e-learning-programma specifiek voor de IT-beveiligingstraining.

De huidige voorkeur voor e-learning is ingegeven door de het grote gebruiksgemak hiervan. E-learning biedt de mogelijkheid om te voldoen aan het vereiste om vanuit verschillende locaties de betreffende training te volgen. Daarnaast is een dergelijk trainingsprogramma eenvoudig schaalbaar voor grotere groepen medewerkers. Het biedt zelfs mogelijkheden om voor bepaalde groepen medewerkers (zoals caissières, vakkenvullers, logistiek, IT-helpdesk, enz.) verschillende onderwerpen verder uit te lichten. Verder maakt e-learning het ook mogelijk om de individuele medewerkers te volgen in hun ontwikkeling en te sturen op hun verantwoordelijkheden voor wat betreft het afronden van de training of het ontwikkelen van extra training gezien hun prestaties. Heel specifiek voor afdelingen met een verhoogd risicoprofiel (denk aan: IT-afdeling, Call Center, Financiële administratie hoofdkantoor) zullen awareness-trainingen met een begeleider meer worden gebruikt. Met deze variant kan nog beter worden ingesprongen op vragen die, vanuit de trainingsonderwerpen, direct naar voren komen. Deze kennis kan later worden gebruikt tijdens de evaluatiefase van het trainingsprogramma.

Op dit moment verkeert nog geen enkele retailer uit dit verhaal in de evaluatiefase van de IT-beveiligingstraining. Het hier beschreven stuk is dan ook gebaseerd op eerdere ervaringen van retailers met andere grote trainingsprogramma's van onderwerpen als Hygiëne of Brand en Veiligheid. Standaard zal er gebruikgemaakt worden van evaluatieformulieren die naar de verschillende regio- en landenmanagers worden verstuurd. Bij de awareness-training met begeleider zullen er groepsmatige evaluaties worden toegepast alsmede de feedback van de betreffende begeleider. Risk Management zal zelfstandig uit het e-learning deel informatie filteren op het gebied van voortgang, participatie, gemiddelde score per onderwerp, doorlooptijden, enz. In combinatie met vooraf opgestelde succesfactoren draagt dit bij aan het tot stand komen van wijzigingen aan de IT-beveiligingstraining. Enkele van deze succesfactoren zijn:
het verlagen van het aantal security-incidenten;
de minimale medewerkerparticipatie aan de training;
compliancy aan externe & interne richtlijnen;
het adresseren van nieuwe technologie binnen de retail (zoals bodyscanners, virtuele kassa's, smartphone scanner apps, near field communication, enz.).

Deze wijzigingen zullen bijdragen aan het continu proces om de IT-security awareness van de medewerker op het huidige volwassenheidsniveau te handhaven. Iets wat in de huidige tijd van technologische ontwikkelingen, die elkaar in rap tempo opvolgen, een uitdaging op zich mag heten!

Links:

NIST 800-50: *Building an Information Technology Security Awareness and Training Program* is hier te downloaden: csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Windows security awareness program material: technet.microsoft.com/en-us/security/cc165442.aspx

E-learning demonstratie: www.inspiredelearning.com/sat/demos.htm

ING'S ROLE BASED ACCESS CONTROL IS ROBUUST

Marco Koelmans (CISSP, CISA, CISM) is zelfstandig, onafhankelijk Informatiebeveiliging Consultant en eigenaar van Xellentis. Marco is te bereiken op mkoelmans@xellentis.nl.

Henk Keller, hoofd Role Control Centre, ING.

Veel organisaties worstelen nog steeds met de implementatie van Role Based Access Control. De ING is sinds 2005 bezig om RBAC te implementeren. Na een onderzoek van Forrester werd de ING beloond met de op een na hoogste waardering: 'robuust', met de opmerking dat als ze de laatste verificaties zouden inrichten en automatiseren, ze de hoogste rating: ' best of class' zouden krijgen. Hoe heeft de ING de implementatie van RBAC aangevlogen en wat kunnen we van ze leren? Een interview met Henk Keller, hoofd Role Control Centre bij de ING geeft een interessant kijkje in de keuken van een grote organisatie die RBAC met succes implementeert.

Wij zijn in 2005 begonnen met de implementatie van RBAC. Daar was een aantal drijfveren voor. De minst mooie is dat er op dat moment een Hype was rondom RBAC. Ook binnen onze organisatie hoorde het management daarvan en de betreffende managers wilden daardoor ook RBAC binnen de ING implementeren. Daarnaast was er bij de business een sterke behoefte aan een vereenvoudigd aanvraagproces. Er waren audit-punten op het gebied van user accessmanagement waarbij het de toezichthouders opviel dat er verbeterpunten waren op dat vlak. Tenslotte kwam de Sarbanes Oxley regelgeving voor die bedrijven die aan de Amerikaanse beurs genoteerd staan. ING moest daaraan voldoen. Dit waren allemaal zaken die de aandacht voor RBAC verhoogden en daardoor de implementatie mede mogelijk maakten. Naast natuurlijk kennis, ervaring en tooling.

> ING werd door Forrester beloond met de waardering 'robuust'

We begonnen op het mainframe eind jaren 80 al volgens een hiërarchisch rollenmodel. Dat wil zeggen dat de rollen de hiërarchische structuur van de organisatie volgden. We kwamen er al snel achter dat dat problemen oplevert bij een organisatie die veel reorganiseert. Het vergt ontzettend veel onderhoud op de rollen bij elke reorganisatie. Daarbij moest men heel goed de rechten van de hiërarchie in de gaten houden. Je kunt je immers voorstellen dat de rechten die voor iedereen binnen een bedrijfsonderdeel gelden op het hoogste rollenniveau worden geïmplementeerd en dat er vervolgens door middel van een stapeling van steeds specifiekere rollen autorisaties aan worden toegevoegd. Dat kan problemen gaan veroorzaken in geval van rolwijzigingen waarbij ongemerkt conflicterende autorisaties worden uitgedeeld (die niet samen mogen voorkomen in verband

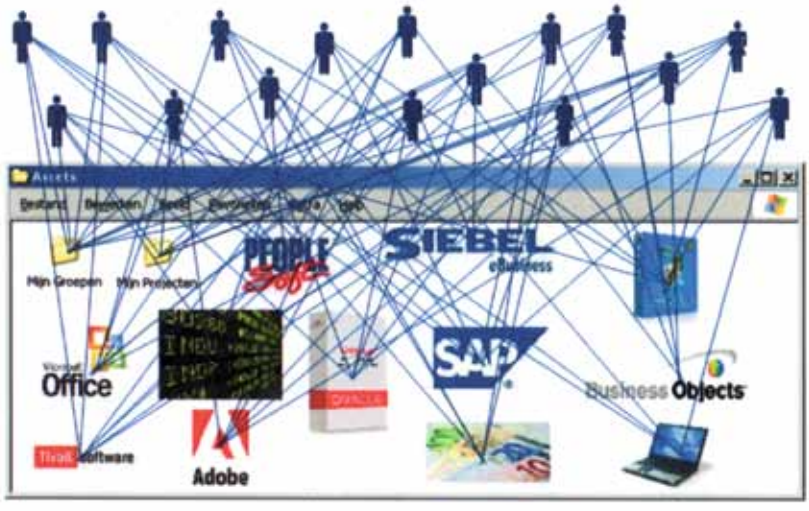


Fig. 1. Persoonlijke autorisaties versus RBAC.

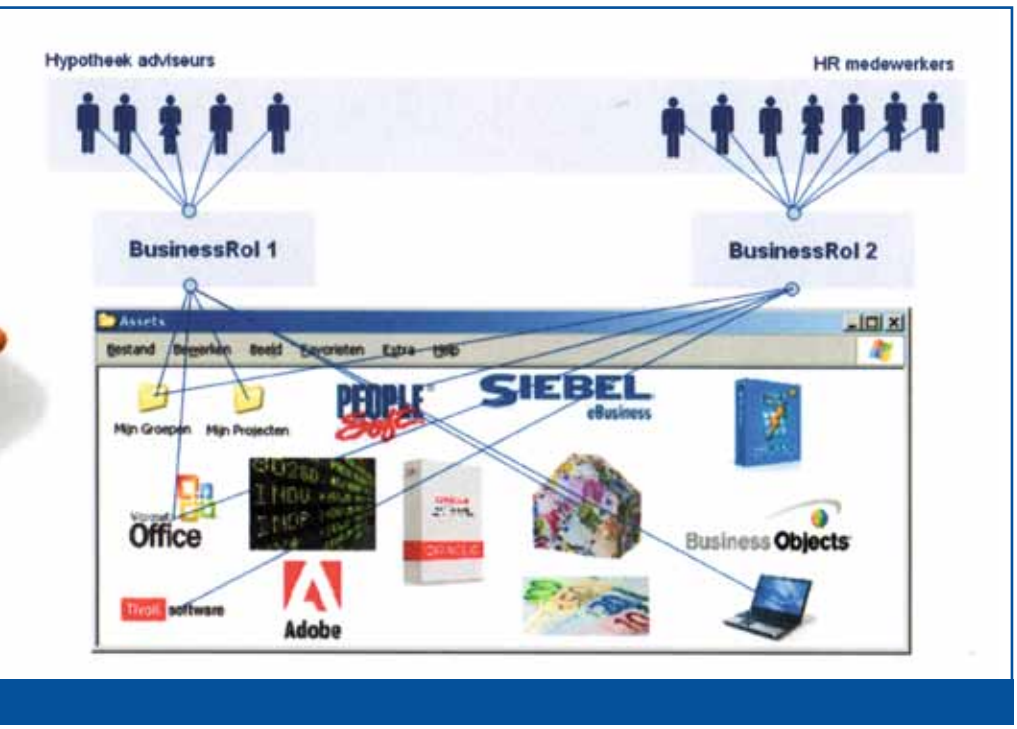
met functiescheidingen). Het kan best zijn dat je in een rol op hoog niveau een autorisatie hebt die niet verenigbaar is met een autorisatie in een rol op een lager niveau. Dat is makkelijker te constateren en te controleren met platte modellen. Daarom waren we er snel achter dat het in een snel veranderende organisatie wellicht handiger zou zijn om platte, procesgerichte rollen te definiëren waarbij een gebruiker in principe maar een rol heeft. Het totaal aantal rollen wordt daardoor gelijk minder, want iedere extra laag rollen houdt direct een toename van het aantal te onderhouden rollen in. Wij maken in een enkel geval wel gebruik van additionele rollen maar dat beperken we echt tot het minimum. Deze platte rollen zijn veel stabieler en hoeven niet zo vaak gewijzigd te worden. Een organisatie verandert vaak sneller als diens business processen. Binnen de ING zullen altijd hypotheken en leningen verstrekt worden. De stappen in die processen veranderen niet veel. Dat merkten we bijvoorbeeld bij effecten. De rollen voor dat proces zijn vijf jaar onveranderd gebleven. We hebben ook even gewerkt met een combinatie van het platte model en het hiërarchische model. Dat was echter geen succes. Al snel bleek dat deze aanpak leidde tot een gebrek aan transparantie in het proces omdat het niet uit te leggen was waarom in het ene geval alleen een platte rol aangevraagd kon worden en in een ander geval er gebruikgemaakt kon worden van gestapelde rollen.

> Het is handiger om platte, procesgerichte rollen te definiëren

Aanpak

Als aanpak wilden we niet alleen de implementatie doen van RBAC, maar ook tegelijkertijd een schoning doen in de rechten op de systemen. Er is genoeg tooling te vinden die kijkt naar de bestaande situatie van autorisatiegroepen en dan de autorisaties daarvan bundelt in rollen. Je kan dan vrij snel RBAC implementeren door middel van role mining, maar dan krijg je een vervuilde RBAC-implementatie. Dat wilden we niet. We zijn er wel achter gekomen dat, als je een goede en geschoonde implementatie van RBAC wilt, je een lange adem moet hebben. In 2005 begonnen we echt met de implementatie van RBAC en we besloten om twee sporen hierbij te volgen: top-down en bottom-up. Met de top-down benadering brachten we de processen in kaart en keken we welke functiescheidingen we aan moesten brengen. We vroegen de business: "Wat zijn je processen, wie voeren die processen uit en wat is hun rol daarin?" Bij de bottom-up benadering keken we naar de applicaties en welke rechten de medewerkers hadden. De werknemers waarvoor de business had aangegeven dat zij een bepaalde rol vervulden werden gebundeld en in eerste instantie werden hun rechten bij elkaar gezet en met elkaar vergeleken. We gingen ervan uit dat als een autorisatie maar belegd was bij 20% van de medewerkers die een rol hadden in een proces, en de overige 80% van de medewerkers met diezelfde rol binnen hetzelfde proces hadden deze autorisaties niet, dat ze dan overbodig waren. De overige medewerkers die dezelfde werkzaamheden uitvoerden klaagden immers niet? Deze rechten werden ingetrokken. Natuurlijk ga je dan wel eens de fout in maar we voerden deze wijzigingen zo door dat ze op zeer korte termijn weer rechtgetrokken konden worden. Je moet je voorstellen dat we weinig autorisatiematrices hadden en dat er ook maar weinig systeemeigenaren bekend waren. En dat binnen een bedrijf met 40.000 werknemers. Daarnaast vroegen we de business om 'model'-gebruikers. Dat waren gebruikers met een goede beoordeling en die weinig van functie waren veranderd waardoor overerving van rechten een gevaar zou zijn. Op basis daarvan konden we ons ook een beeld vormen van veel overbodige autorisaties en, nog belangrijker, van de autorisaties die wel voor een rol van belang waren. Al met al hebben we zo al zeer veel individuele rechten kunnen intrekken, zonder negatieve gevolgen voor de business.

> We besloten om twee sporen te volgen: top-down en bottom-up



We hadden centraal binnen het project een team zitten die zich bezighiel-

den met het in de gaten houden en administreren van rollen, normeringen en tabellen. Bij de security administrators zat een toegewijd team die met de rechten ging schuiven en die oude groepen weggooide en nieuwe schone rollen ging definiëren. Bij de business hadden we lokale projecten, die gingen aan de gang met onze bevindingen over eventuele overbodige en benodigde autorisaties. De beoordeling of onze bevindingen terecht waren en wat er mee gedaan moest worden maakten zij. Daarbij kregen we ook meer en meer inzicht in de koppeling tussen techniek en applicatie waardoor het ook steeds makkelijker voor de business werd om een gedegen beoordeling te maken. We kenden toen we begonnen maar 8% van de systeemeigenaren. Gedurende de RBAC-implementatie is dat percentage sterk omhoog gegaan omdat we deze systeemeigenaren nodig hadden voor de beoordeling van de autorisaties. Nu kennen we bijna alle systeemeigenaren. We werden vervolgens in 2006 onderbroken door de komst van SOx. Daar moesten onze mensen ondersteuning verlenen. Pas in 2007 zijn we vervolgens full swing door gegaan met de invoering van RBAC.

RBAC-gerelateerde Terminologie

Compliance - Begrip waarmee wordt aangeduid dat een organisatie werkt in overeenstemming met vigerende wet- en regelgeving.

Entitlement - Het bepalen of iemand het recht heeft om bepaalde autorisaties te hebben op basis van zijn functie en vigerende wet- en regelgeving.

Provisioning - Het proces van het verstrekken van faciliteiten en permissies aan een persoon.

Role Mining - Het identificeren van sets van rechten die samen voorkomen, ze definiëren als rollen, en het zoeken van gebruikers die deze rechten hebben, zodat deze rechten kunnen worden toegewezen aan rollen.

Beheer

We hebben bij de implementatie het beheer zoveel mogelijk naar de technische laag gebracht om de rollen zo stabiel mogelijk te houden.

Beheer op de TI-laag

Ik bedoel daarmee dat de rollen op entitlement niveau, bij de ING binnen IBM Tivoli Identity Manager (ITIM), beschrijven wat iemand kan en mag. Het beheer vindt echter plaats op de Technische Infrastructuur (TI)-laag. Daar worden de rolgroepen beheerd waarbij de autorisaties en de personen aan elkaar worden gekoppeld. De rollen in de entitlement-laag hebben dezelfde naam als de bijbehorende rolgroepen op de TI-laag. Zolang een organisatie nieuwe producten maakt of koopt weet je dat er ook wijzigingen in de autorisaties plaats zullen moeten vinden. Een autorisatiewijziging leidt meestal niet tot een wijziging van de rol op de entitlement-laag, maar in de wereld daaronder (de TI-laag). Maar die moet je toch wijzigen in verband met nieuwe of verschuivende autorisaties. Daar zal je altijd beheer op nodig hebben.

We werken niet meer met individuele autorisaties. Er wordt ook dagelijks gecontroleerd op de aanwezigheid van individuele autorisaties en deze worden vervolgens verwijderd. We zijn nu ook bezig met automatische

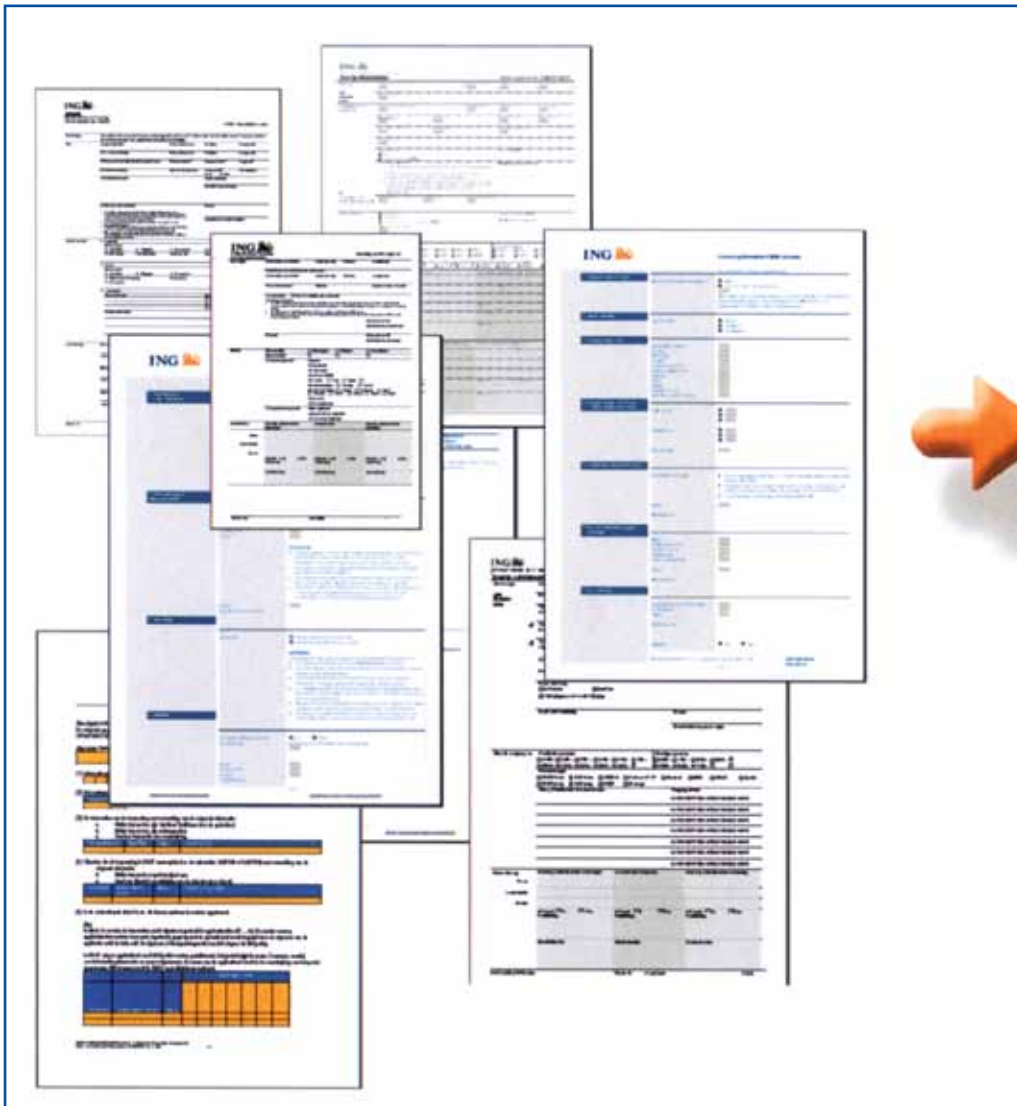


Fig. 2. Papieren aanvraag versus digitaal (ITIM).

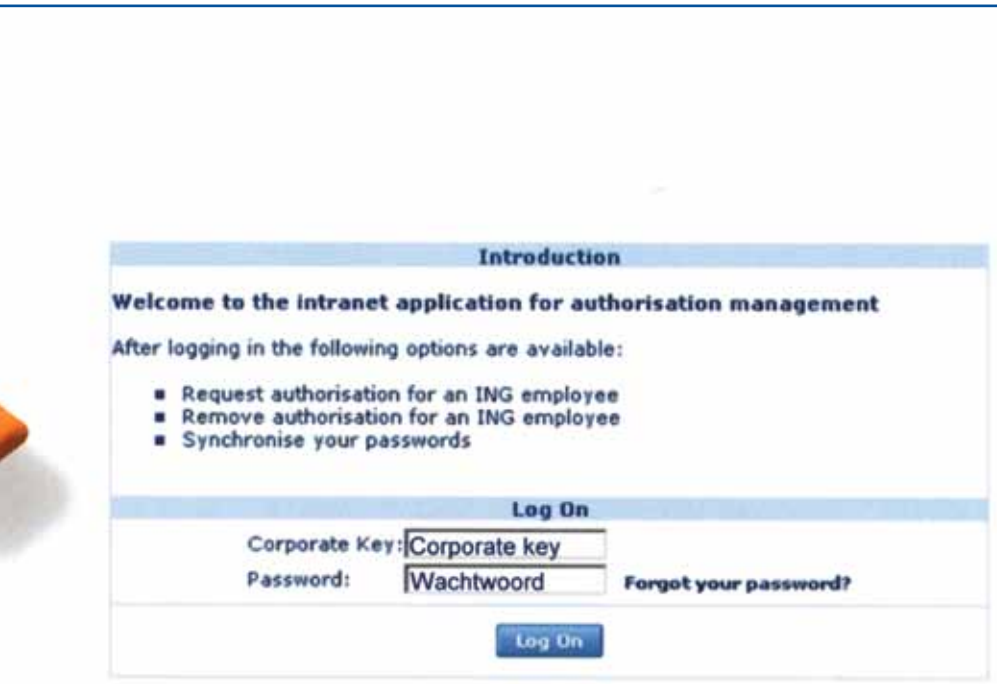
provisioning. Dan worden ze zelfs automatisch ingetrokken. We hebben wel eens een rol die wijzigt. Die TI-laag had je altijd al, de entitlement-laag is nieuw. Dat is dus extra werk. Maar die maakt wel ineens een hoop inzichtelijk voor wat betreft de autorisaties die behoren bij een rol, en die maken in een klap compliance een stuk gemakkelijker. De business kan eenvoudiger en in, voor hun begrijpelijke taal, aanvragen doen en beoordelen. We kunnen rapporteren over IST- en SOLL-situaties. We weten ook te allen tijde wie welke aanvragen heeft gedaan en wie ze mag accorderen. Rechten worden niet meer uitgegeven aan personen maar aan rollen waardoor de uitgifte een stuk sneller wordt. Die tijd wordt verkort van enkele weken in het verleden tot enkele minuten als straks de automatische provisioning is geregeld.

> We hebben zo veel individuele rechten kunnen intrekken

Governance

We hebben binnen de governance-teams security administrators zitten die zich alleen met userid's bezig mogen houden. Zij koppelen gebruikers aan groepen maar doen niets met de autorisaties op de groepen. Ze kunnen niets aan rechten wijzigen. Andere teams van security administrators houden zich weer bezig juist met de rechten op die groepen.

> Vooraf kenden we maar 8% van de systeemeigenaren, nu bijna allemaal



Verder hebben we het Role Control Centre. Die gaat over het rollenmodel en het kiezen van de juiste rollen. Bij de business hebben we roleigenaren die verantwoordelijk zijn voor de functiescheiding over de applicaties heen. De systeemeigenaren zijn uiteindelijk eindverantwoordelijk voor de inhoud van de rollen omdat zij uiteindelijk de toestemming moeten geven om de autorisaties aan de rollen te hangen. Dit hele proces wordt via een gestructureerd aanvraagproces ondersteund. Nu door middel van een .NET-applicatie en in de nabije toekomst door een mooie webinterface waarin aanvragen kunnen worden gedaan. Daarna gaat de aanvraag volautomatisch naar de systeemeigenaren en pas na hun akkoord wordt hij naar de Security Administrators gestuurd om het aan te brengen. Die systeemeigenaar krijgt alleen nog maar een aanvraag als een rol toestemming vraagt om van zijn functionaliteit gebruik te maken en niet meer bij allerlei afzonderlijke gebruikers. Bij de rol zit een gedegen functionele omschrijving waardoor de systeemeigenaar kan begrijpen waarom die rol de autorisatie nodig heeft en daardoor kan hij volmondig ja of nee zeggen tegen de aanvraag.

In de nieuwe tooling die eraan zit te komen wordt bij aanvragen ook gelijk gecontroleerd of er conflicterende rechten worden aangevraagd die vervolgens op die grond geweigerd gaan worden. Nu vindt er achteraf een handmatige controle plaats maar straks gaat dat dus automatisch en vooraf gebeuren. Er wordt elke nacht een volledige dump van alle autorisaties op alle platformen gemaakt. Deze wordt straks ook aan de database van het Role Control Centre gekoppeld waarin de SOLL-matrices staan, waardoor we straks vol automatisch verschillen kunnen rapporteren aan roleigenaren en systeemeigenaren. Als dit wordt gerealiseerd hebben we de laatste

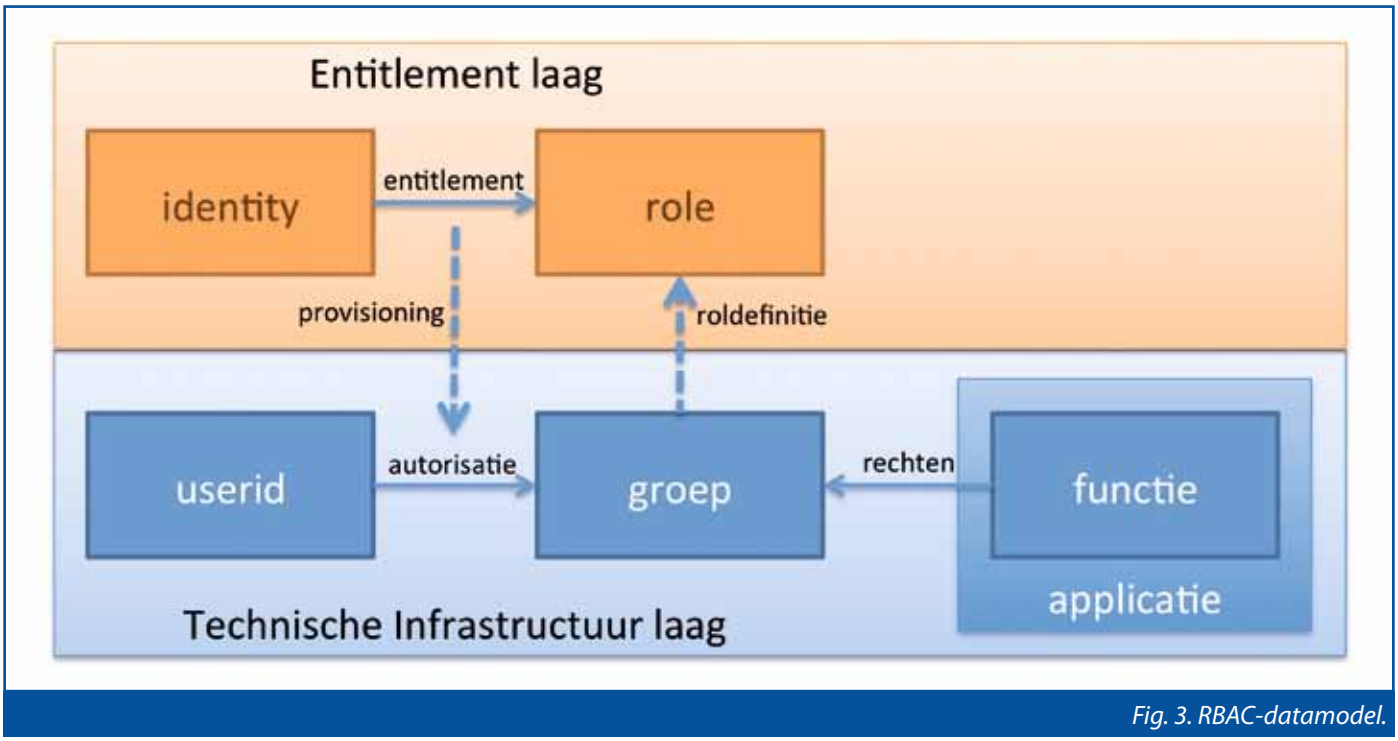


Fig. 3. RBAC-datamodel.

verificaties ook geautomatiseerd. Dat is wat ook Forrester heeft aangegeven.

Uiteindelijk heeft het ook tot resultaten geleid die de uitgangspunten die ik in het begin aangaf hebben geholpen. De DNB heeft tijdens hun laatste onderzoek aangegeven dat ze wel zien dat er nu veel mensen bezig zijn met User Access Management maar dat het wel heel strak is geregeld bij de ING.

Next Steps

We gaan nu meer automatiseren omdat dat leidt tot kostenbesparing in de administratie en het vergaren van het compliancybewijs. Daarnaast gaan we de 'niet persoonlijke accounts' (NPA's) en System en Batch-accounts ook onder RBAC brengen. Daarmee kunnen we ook dataflows in kaart brengen en de systeemeigenaren in de gelegenheid stellen om te zien wat er met hun data in de keten gebeurd en wie er allemaal via welke interfaces en applicaties bij die data kunnen. De samenhang over applicaties heen wordt daarmee inzichtelijk.

Er komt een nieuwe tool om vanuit de techniek te helpen om SOLL-matrices te maken. Die kijkt naar bestaande combinaties van rechten en voedt daarmee de eigenaren die vervolgens kunnen beoordelen welke combinaties terecht zijn voor een bepaalde business-rol. Daarmee kunnen we ook nieuwe afdelingen en organisatieonderdelen snel onder RBAC brengen. Rapportages worden op de doelgroepen afgestemd. De lijnmanager krijgt bijvoorbeeld een overzicht van zijn medewerkers en de rollen waaraan zij gekoppeld zijn. De roleigenaren krijgen overzichten van hun rollen en de mensen die er aanhangen. De systeemeigenaar krijgt een overzicht van zijn systemen en welke rollen daarbij kunnen. Zo krijgt iedereen de informatie die zij kunnen controleren en die relevant is, en, niet onbelangrijk, die voor hem begrijpbaar is. De actoren kunnen door middel van knoppen gaan reageren (op onderdelen OK of Not OK drukken) en vervolgens wordt er automatisch (in geval van een Not OK) een workflow opgestart waarin de stakeholders worden geïnformeerd. Die krijgen dan de tijd om te reageren. Blijft de beoordeling op Not OK staan dan gaat de workflow verder en wordt er actie genomen. Allemaal automatisch.

Laat de business de voordelen zien

De HR-systemen worden gekoppeld aan onze RBAC-administratie in die zin dat de uitvoerenden in het RBAC-proces worden gevolgd. Als een roleigenaar van kostenplaatscode wisselt dan is hij misschien ook geen roleigenaar meer. Dat komt er straks in een rapportage uit waarna wij de roleigenaar de vraag kunnen stellen of hij de roleigenaar nog wel is. Tussen ITIM en de HR-administratie was altijd al een koppeling.
We gaan de tussenlaag waarin de vertaling tussen functionaliteit en techniek plaatsvindt verder in beeld brengen, samen met de business.
Als die volledig in beeld is kan de business geheel de zaken in eigen hand gaan houden. Ze begrijpen namelijk de functionele aanvraagtermen die in de aanvraagmenu's komen te staan. Bij de workflow vindt dan de vertaling plaats van de functionaliteit van bijvoorbeeld 'opvoeren hypotheek' naar autorisaties op bepaalde technische componenten. Hierdoor kan iedereen, zowel de business als de IT-organisatie begrijpen waar men mee bezig is. Uiteindelijk is het de bedoeling dat de verantwoordelijkheden, en daarmee ook de acties, zoveel mogelijk bij de business komen te liggen zodat zij direct in control zijn over hun eigen systemen. Daarbij wordt de techniek verzorgd door de TI-laag en het Role Control Centre buigt zich over de vraag of alles wel voldoet aan de regels rondom de rollen die zijn afgesproken en op begeleiding en consultancy naar de business toe.

Do's en Don'ts

Wat ik in ieder geval aan andere organisaties aanbeveel is; ben je een kleine organisatie die weinig organiseert? Ga dan gerust naar het hiërarchische model. Maar ga nooit per platform beginnen omdat je op het ene platform een andere structuur kunt hebben dan op het andere platform. Kijk naar het proces en dan zul je zien dat er voor een proces op het ene platform 50 rollen nodig zijn maar op een ander platform heb je er misschien wel 75 nodig omdat daar een veel fijnmaziger scheiding wordt doorgevoerd.
Als je voor een rollenmodel kiest, blijf er dan ook bij. We hebben geleerd bij een implementatie dat door vermenging van modellen het niet meer te begrijpen is voor de business. Wat moeten ze nou aanvragen als je de ene keer gestapelde rollen moet aanvragen waar dat op een ander moment niet is toegestaan? En hoe vervat je dat in een automatisch provisioning-model?
Leg je beheer niet op een hoog niveau als je veel verschillen hebt in complexiteit in functies en platformen. Als je de boeken erop nakijkt zeggen ze allemaal dat dat handig is maar dat levert extra onderhoud op omdat je extra lagen creëert die allemaal onderhouden moeten worden.
Durf pragmatisch te zijn en beslissingen te nemen. Die schoning: gewoon doorvoeren en die autorisatie: gewoon intrekken. Doe dat wel beheerst met een snelle fallback-mogelijkheid.
Laat de business zien dat ze terug gaan van 25 verschillende formulieren naar 1 formulier. Informeer ze over de kortere doorlooptijden. Laat ze hun voordelen zien, dat verhoogt de acceptatiegraad. Je doet het voor hen en niet voor de IT-organisatie. Op een gegeven moment is onze ervaring dat ze er dan zelfs lol in krijgen om de zaken in de hand te houden en de controles goed uit te voeren. Ze snappen namelijk waar ze mee bezig zijn.

Links:

RBAC Wikipedia: nl.wikipedia.org/wiki/Role-based_access_control

Sarbanes Oxley: nl.wikipedia.org/wiki/Sarbanes-Oxley

DENIAL OF SERVICE AANVALLEN – DEEL 1

Eelco van Beek is CEO van Jitscale, een IT-beheerorganisatie die gespecialiseerd is in het ontwerpen, inrichten, beheren en optimaliseren van zeer uiteenlopende bedrijfskritische IT-platformen. Jitscale bedient klanten in binnen- en buitenland, zoals Achmea, Sanoma Media, Albelli, Allianz, Amber Alert en Unigarant.

Als je mag afgaan op de berichtgeving in de media, is er de afgelopen tijd een ware hausse geweest van hackpogingen, DDoS-aanvallen, en andere activiteiten van kwaadwillenden. Voorbeelden te over. Zo heeft het PlayStation-netwerk wereldwijd zeer zwaar onder vuur gelegen, is de site van Nintendo gehackt, werden de certificaten van DigiNotar waardeloos door toedoen van hackers, is de module waarmee de Rabobank het internetbankieren beheert lamgelegd door een DDoS-attack, en zijn ook Stichting Brein, Radio Nederland Wereldomroep en Rijksoverheid.nl ten prooi gevallen aan Dos-aanvallen. De invloed van en aandacht voor groepen als LulzSec en Anonymous, die zich vaak bedienen van DDoS-tools, worden alsmaar groter.

Reden voor Informatiebeveiliging om in een serie artikelen diverse methodes en oplossingen achter (D)DoS- en andere aanvallen de revue te laten passeren. Eelco van Beek, CEO Jitscale, leidt ons door het hele scala, gaande van de meest eenvoudige situaties, oorzaken en oplossingen tot de zeer complexe en vaak georganiseerde gevallen.

Eenvoudige (D)Dos-aanvallen

'Een internetdienst, meestal een website, wordt op een bepaalde manier gemanipuleerd met als gevolg dat die dienst niet langer of verkeerd functioneert'. Een heel klinische definitie voor een steeds relevanter en belangrijker probleem. Het is overigens niet zo dat er tegenwoordig meer mogelijkheden zijn voor dergelijke aanvallen, de effecten zijn alleen 'interessanter'. Het internet wordt immers steeds meer gebruikt voor kritische processen en diensten, waardoor het voor bepaalde partijen weer aantrekkelijk wordt om die diensten te saboteren.

Een DoS-aanval hoeft lang niet altijd gedistribueerd te zijn of te maken hebben met hoge volumes. Bij veel succesvolle aanvallen wordt vaak vooraf een webapplicatie geanalyseerd op eventuele bottlenecks. Dit zijn bijvoorbeeld onderdelen in een webapplicatie die bij het verwerken van een verzoek een vertraging hebben. De zwakste schakel, oftewel het slechtst presterende onderdeel in zo'n keten van componenten, bepaalt de gevoeligheid voor een aanval. Denk bijvoorbeeld aan een transactie waarbij een backend-omgeving wordt geraadpleegd. Een analyse van zo'n transactie is vrij eenvoudig te maken. Er bestaan diverse tools, zoals Nagios, VMWare Hyperic, WebPerf en Gomez, die inzicht kunnen geven in de laadtijd en andere KPI's van de diverse componenten op een site. Door vervolgens een redelijk volume aan verzoeken te genereren op zo'n specifieke component ontstaat er vaak vanzelf een Denial of Service-situatie. Bijvoorbeeld doordat de connectie-pool op een server volloopt omdat de server wacht op antwoord van een achterliggende machine, of omdat er meer onderdelen afhankelijk zijn van dezelfde backend-omgeving en met hun (snelle) verzoeken in een wachtrij worden geplaatst.

> Meest effectieve DOS valt bottleneck aan

Een andere methode waarbij er weinig inspanning nodig is om een DoS te initiëren, is een aanval die gericht is op een webomgeving waarop grote en niet geoptimaliseerde componenten worden gebruikt. Denk hierbij aan video's, grote afbeeldingen of grote javascript-bestanden. Door een dergelijk object veel op te vragen – en dit kan in veel gevallen al vanaf een simpele DSL-verbinding met een laptopje, want de vraag is vele malen kleiner dan het antwoord – slibt de verbinding van de server dicht. Daardoor is de server niet in staat om nog aan nieuwe verzoeken te voldoen, en voilà: een DoS is gerealiseerd.

Soms is het zelfs niet eens noodzakelijk om een volledige http-sessie te initiëren. Moderne webservers ondersteunen keepalive-sessies. Deze sessies maken het mogelijk om meerdere http-verzoeken over dezelfde verbinding uit te voeren. Indien een webserver hier goed op ingericht is (dit is bijvoorbeeld regelmatig het geval bij Apache-installaties) is een DoS eenvoudig te realiseren door heel veel van die keepalive-sessies aan te maken. Opnieuw vergt dat weinig energie aan de client-kant maar kunnen de gevolgen desastreus zijn.

> Asynchroniteit in transacties belangrijke beschermingsmaatregel

Het klinkt allemaal vrij eenvoudig. En dat is het ook. Dat geldt overigens ook voor de oplossing. Toch is het zo dat dit soort situaties in de praktijk, juist ook bij de heel grote omgevingen, continu aan de orde is. Op de prioriteitenlijst staat immers functionaliteit nog vaak bovenaan. Pas veel later, meestal zelfs achteraf als de problemen reeds zijn ontstaan, wordt er gekeken naar performance en security. Om dit te kunnen herstellen zijn de kosten vaak aanzienlijk. Niet omdat de oplossing zelf duur is, maar met name door het feit dat er vooraf geen rekening is gehouden met het probleem.

Voorkomen is beter dan genezen

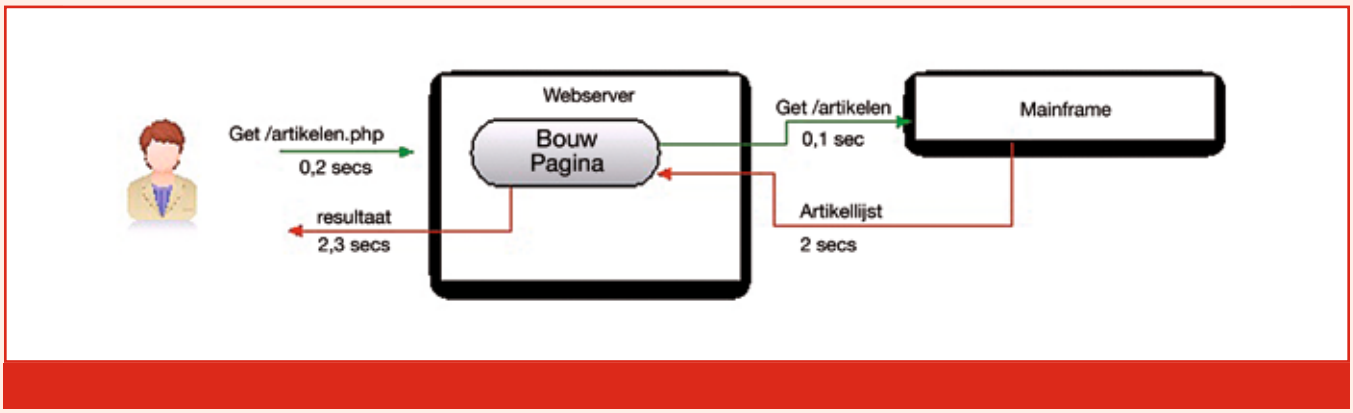
De oplossingen zijn dus vaak eenvoudig, met name omdat de oorzaak van het probleem inzichtelijk is. Eenvoudig, maar daarmee helaas niet altijd goedkoop, vooral als er achteraf gerepareerd moet worden. In dat geval is vaak behoorlijk wat inspanning vereist, bijvoorbeeld om software te herschrijven, of zelfs om de infrastructuur volledig op de schop te gooien.

> Zwakste schakel bepaalt uw kwetsbaarheid

Met name in de situatie waarbij er sprake is van bottlenecks in de omgeving ligt de oplossing vrijwel altijd in de architectuur ervan. In die architectuur ligt namelijk niet alleen de manier vast waarop de netwerkinfrastructuur is ingericht, maar ook de wijze waarop de applicaties communiceren. En het gaat zelfs tot op applicatie-inhoudelijk niveau. Zowel wat de applicaties precies communiceren als welke afhankelijkheden er bestaan zijn beide van groot belang.

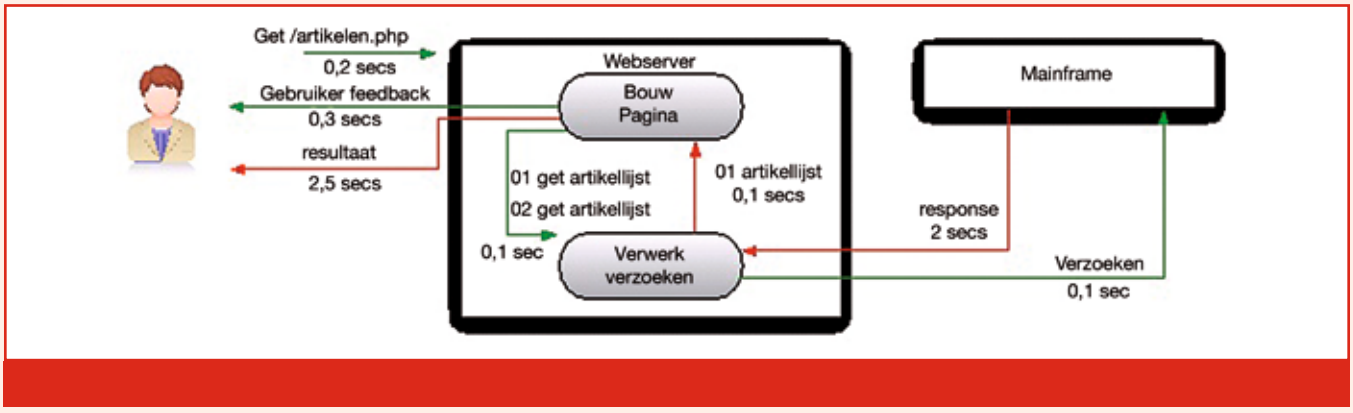
Om minder vatbaar voor (D)DoS-aanvallen te zijn is het verstandig om zoveel mogelijk asynchroniteit in het platform te verwerken. Dit houdt in dat de diverse componenten, dus applicatieservers met de diverse applicaties, databases, enzovoort, niet afhankelijk zijn van de response van een andere applicatie voor de uiteindelijke response naar de eindgebruiker.

Een simpel voorbeeld. *Synchrone communicatie* gaat als volgt:



Er komt een verzoek binnen op de webserver. Dit verzoek wordt doorgestuurd naar de applicatieserver. De applicatieserver heeft informatie nodig van een andere applicatieserver, bijvoorbeeld op een mainframe. Deze informatie wordt opgevraagd. Zolang hier nog geen reactie op geweest is blijft de hele keten wachten, tot aan de eindgebruiker toe.

Asynchrone communicatie is als volgt schematisch weer te geven:



In het geval van asynchrone communicatie stuurt de applicatieserver in een apart proces meerdere verzoeken over eenzelfde verbinding. In het voorbeeld (kader) wordt dat gedaan door de verzoeken te nummeren. Wanneer de achterliggende applicatie op bijvoorbeeld een mainframe een antwoord heeft op een bepaald verzoek, zal deze reageren met het nummer van de vraag met daaraan gekoppeld het antwoord. Door deze methode ontstaat er geen 'uitputting' op de applicatieserver. Vervolgens houdt de applicatieserver een lijstje bij van welke verzoeken er zijn gedaan. Ondertussen kan het originele webserver-proces de gebruiker op de hoogte houden door geregeld informatie terug te sturen over de voortgang. Hierdoor is de keten niet langer afhankelijk van de langzamere applicatie op het mainframe.

Oplossingen

Websites die zich tegen (d)dos-aanvallen willen beschermen, maar nog geen gebruikmaken van asynchrone transacties, doen er verstandig aan dit alsnog in de site te integreren. Het is een vrij specialistisch, tijdrovend en ingrijpend proces om de complete architectuur op de schop te gooien, dat moge duidelijk zijn. Vaak is het nodig zowel de applicatie als de infrastructuur aan te passen.

De oplossingen voor de aanvalsmethode waarbij grote componenten zoals video's en afbeeldingen worden 'misbruikt', zijn daarentegen eenvoudig, en zijn in principe zelfs door een hobbyist door te voeren. Zo kunnen grote plaatjes bijvoorbeeld worden verkleind, gewoon door een goede compressie toe te passen. In plaats van videomateriaal te laten 'downloaden', is het aanbieden van een stream vaak een betere oplossing. Bij een videostream kan de aanbieder de bitrate, oftewel afspeelsnelheid, bepalen. In feite hoeft het bestand niet met een hogere snelheid dan die bitrate naar de eindgebruiker te worden gestuurd. Dit komt de piekbelasting van het netwerk, en dus de gevoeligheid voor een Denial of Service, ten goede. Verder bestaan er veel javascript-optimizers die de bestanden kleiner en efficiënter kunnen maken en biedt CSS-optimalisatie de mogelijkheid om de vormgeving van webpagina's los te koppelen van hun feitelijke inhoud en deze centraal vast te leggen.

> Simpele DSL-verbinding vaak voldoende voor succesvolle aanval

> Comprimeer content voor beperking bandbreedte-gebruik

Een andere oplossing is het verplaatsen van statische objecten, zoals video- en beeldmateriaal maar ook javascript en CSS-pagina's, naar zogenaamde caching-servers of edge-servers. Deze servers zijn geoptimaliseerd om snel statische content bij de eindgebruiker af te leveren. In het geval van edge servers is het zelfs zo dat de servers netwerktechnisch zo dicht mogelijk bij de eindgebruikers zijn geplaatst om een zo laag mogelijke vertraging en een zo hoog mogelijke doorvoersnelheid te behalen.

Tot slot

Veel DoS-aanvallen zijn kinderlijk eenvoudig. Maar via een aantal eenvoudige maatregelen kunt u ervoor zorgen dat uw site hier vele malen minder kwetsbaar is dan de gemiddelde website. Indit artikel gaven we u al enkele eenvoudige tips en trucs voor. Deze oplossingen dienen overigens niet alleen ter bescherming tegen DoS-aanvallen. Alle tips dragen ook in algemene zin bij aan de optimalisatie van uw website. Dit komt naast de reductie van de vatbaarheid voor DoS-aanvallen ook de gebruikersbeleving ten goede.

In deel 2 zullen we de meer geavanceerde aanvallen belichten.

BOEKBESPREKING

DE MACHT VAN MICHAEL BELLINGER

Lex Borger is een principal consultant bij Domus Technica en hoofdredacteur van dit magazine. Hij is te bereiken via lex.borger@domustechnica.com

Boekreview van twee boeken van Charles den Tex, uitgegeven bij De Geus:
***Cel*, 2008, ISBN 9789044511086, 378 pagina's;**
***Wachtwoord*, 2010, ISBN 9789044514308, 347 pagina's.**

Ik ben geen literatuurkenner. Wijn is geen probleem voor mij, maar literatuur herken ik niet. Ik hang de filosofie aan dat ik weet wat lekker weg leest als ik het lees, net zoals ik weet welk wijntje lekker smaakt. Bij de wijnhobby is het gegroeid tot meet, bij lezen niet echt. Waarschijnlijk lees ik te veel professioneel… aan literatuur kom ik gewoon niet toe.
Het was dan ook de professionele kant wat me aantrok om eens een boek van Charles den Tex te gaan lezen. In de krant zag ik dat hij schreef over onderwerpen die ook terugkomen bij informatiebeveiliging. Dus ik zorgde dat ik twee boeken in huis kreeg: *Cel* en *Wachtwoord*. Heel traditioneel Nederlands, gekocht van boekenbonnen die ik op mijn verjaardag gekregen had. Toch heeft het bijna een jaar geduurd voordat ik het eerste boek werkelijk oppakte eraan te beginnen. Pas toen ik op vakantie ging creëerde ik de gelegenheid om *Cel* te gaan lezen.
En toen ik het boek eenmaal geopend had gebeurde er iets wat ik niet voor mogelijk had gehouden. Ik kon me er niet meer uit losrukken. Het moest af. Het boek wat ik rustig tussendoor had willen lezen tijdens mijn hele vakantie had ik uit op dag twee.
Vervolgens ging het naar vrienden waar ik verbleef. Nederlanders in het buitenland zijn losgeraakt van het moederland. Een origineel Nederlands boek moet het dan opnemen tegen Amerikaanse bestsellers. Binnen een week nadat we terug waren in Nederland kreeg ik enthousiaste reacties. Dus binnenkort gaat ook *Wachtwoord,* die ik inmiddels ook gelezen heb, verhuizen naar Californië.
Ik houd van spannende boeken, maar moet me er meestal worstelend in vast lezen. De eerste 50 pagina's zijn moeilijk. Daarna zit ik in het verhaal en kan ik er prima doorheen komen, in gepaste doses.

> Het boek wat ik rustig tussendoor had willen lezen had ik uit op dag twee

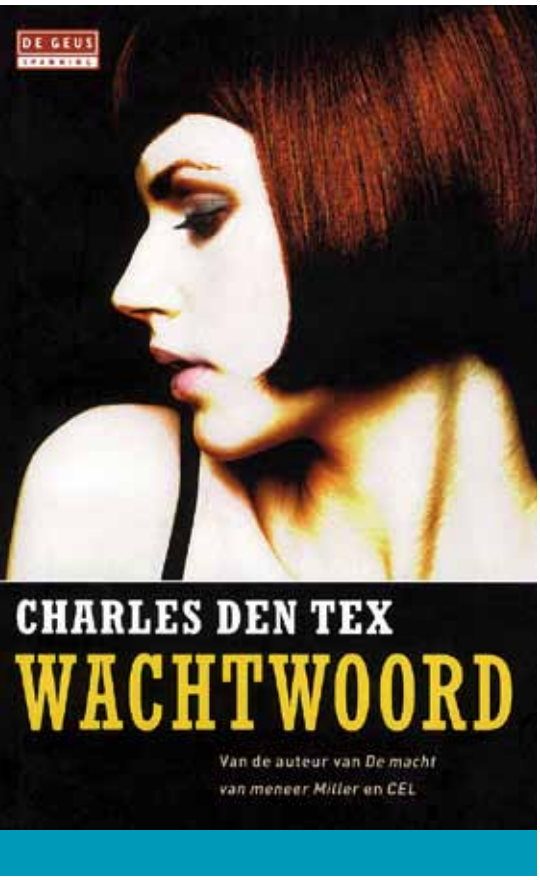
Het vorige boek waarbij dat niet nodig was, was de Da Vinci Code van Dan Brown. Bij *Cel* had ik dus een vergelijkbare reactie.
Het grappige was, dat ik achteraf bemerkte dat, terwijl ik het boek aan het lezen was in Nederland, de opnames werden gemaakt voor de verfilming ervan. Zes afleveringen voor tv. Dus volgend jaar, wanneer deze serie op de buis komt (nou ja, het scherm), ga ik waarschijnlijk weer iets doen wat ik niet veel doe, tv kijken. En natuurlijk moet ik nu ook *De Macht van Meneer Miller* lezen, het eerste deel uit de trilogie.

Charles den Tex is een schrijver die in mijn ogen nog wel wat gaat losmaken in Nederland en daarbuiten. Want zijn boeken worden vertaald. Ook in het Duits, want daar houden ze wel van een spannend boek. Daarnaast is zijn stijl heel realistisch. Dat heb ik nodig. Alles wordt visueel beschreven en wat controleerbaar is, is ook te controleren. Verder weet hij een spanning op te bouwen waarbij, als je daarmee niet bekend bent, je tijdens het lezen denkt: "Moet dat er nu bijgehaald worden?" en "Waarom besteed je daar nu zoveel tijd aan?" Maar uiteindelijk zijn het delen van de puzzel die hij tijdens het verhaal voor je in elkaar legt. Het leuke is dat het verhaal niet helemaal voorspelbaar is. Als de paar laatste puzzelstukjes op zijn plaats worden gelegd dan gaan ineens de lampen branden en besef je je waarom alles met alles te maken heeft.

Ik heb kennissen in het Westland. Amsterdam is tegenwoordig mijn eigen achtertuin. *Cel* speelt zich vooral af op deze twee locaties, met wat Haags tussendoor, uit mijn geboortestad.
En het grappige is dat je het helemaal

Charles den Tex

kunt volgen. Zelfs wanneer locaties net even niet bij de juiste naam worden genoemd is het helemaal te plaatsen. Deze boeken spelen zich af in het Nederland van vandaag.
Je krijgt gewoon de neiging om achtervolgingen door Monster en Poeldijk na te willen rijden. Of het huis te willen vinden in Iepenburg waar Michael op de loer heeft gelegen.



In *Wachtwoord* neemt Charles je ook mee naar Odessa. Daar ben ik dan nooit geweest, maar door de ervaring die ik heb met de realiteit van het Nederlandse landschap twijfel ik er niet aan dat ik in Odessa ook zo de weg zou kunnen vinden waar het verhaal zich afgespeelt. Het overheidslandschap wat Charles schetst is herkenbaar en ook a-politiek. Het is duidelijk het Nederland van na Pim Fortuyn, met alle parlementaire onderzoeken en informatielekken, maar zonder enig herkenbare politicus.

Daar waar de locaties in zijn verhalen realiteit zijn, kun je de personages die Charles creëert hooguit realistisch noemen. De hoofdpersoon in de trilogie is Michael Bellinger. Hij is een goed gekozen personage door Charles. Als consultant is hij van veel markten thuis en kan hij geloofwaardig overal over de vloer komen, maar hij heeft ook zijn menselijke beperkingen. Hij is geen IT-specialist, wel een IT-gebruiker. Dat maakt dat het personage zich uitstekend leent om IT en de bijbehorende cyberproblematiek vanuit het gebruikersperspectief uit te leggen. Ook vergeef je Michael hierdoor de soms naïeve manier waarop hij zaken benadert.

> Je krijgt de neiging om de achtervolgingen na te willen rijden

Michael is omringd met andere personages die helpen de aspecten uit te diepen die uitdieping nodig hebben. Omdat hij zijn kantoor in Amsterdam deelt met een softwarebedrijf kunnen de medewerkers van dat bedrijf helpen om specialistische IT-zaken uit te diepen. Maar ook personages uit de overheid of advocatuur sleept hij vrolijk mee in het verhaal. In *Cel* introduceert hij Guusje van Donnee, en zij mag ook in *Wachtwoord* terugkeren. Haar initialen maken dat je denkt: "Pas op!" En dat is niet voor niets.
In *Wachtwoord* is er aardig wat IT-ondersteuning nodig, hiervoor introduceert Charles Sterre. Het is handig dat ze ook een aantrekkelijke vrouw is, daardoor kan ze ook voor wat seksuele spanning zorgen.

Cel gaat over identiteitsfraude binnen overheid en bedrijven, *Wachtwoord* behandelt meer de persoonlijke identiteiten die we hebben of onszelf aanmeten. Beide boeken pakken voor de spanning een stevige verbintenis met traditionele criminaliteit. De afbeelding van de cybereffecten is in mijn ogen reëel, maar vanuit het perspectief van de gebruiker. Als beveiligingsspecialist vind je al snel dat hij met een te grove penseel wat belangrijke details wegstrijkt, maar het doet het verhaal geen geweld aan. Ik heb eerder geschreven hoe ik dat wel vond bij Dan Browns 'Digital Fortress'.

Het is duidelijk dat Charles comfortabeler wordt met cybercrime in de tijd tussen het schrijven van *Cel* en *Wachtwoord*. Daar waar hij in *Cel* nog pornosites en Second Life nodig heeft om zijn verhaal te vertellen, gaat het in *Wachtwoord* directer over hacken van computers en afluisteren van communicatie.

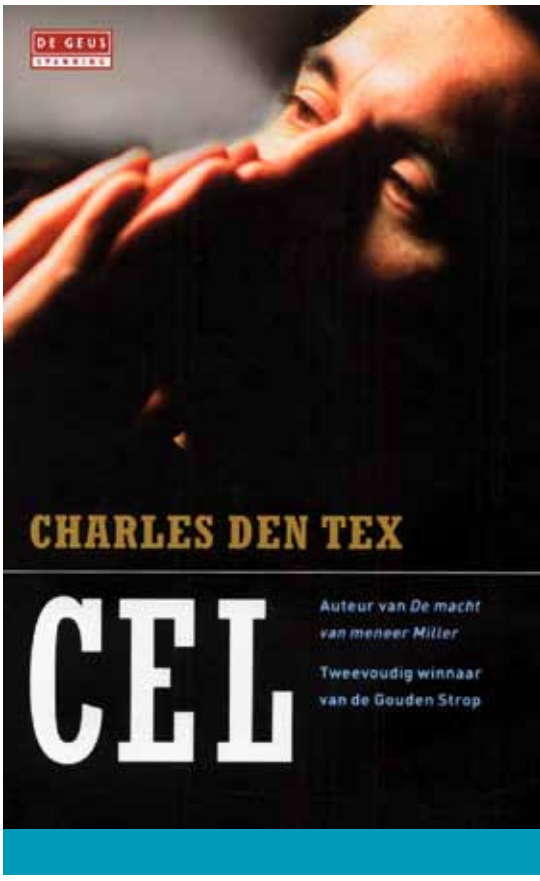
Cel en *Wachtwoord* zijn leuke boeken om te lezen zowel als computergebruiker als beveiliger. Charles pleit niet voor grote hervormingen in de automatisering, maar stelt wel een aantal problemen aan de kaak die voortkomen uit de manier waarop we in de hedendaagse maatschappij omgaan met automatisering.

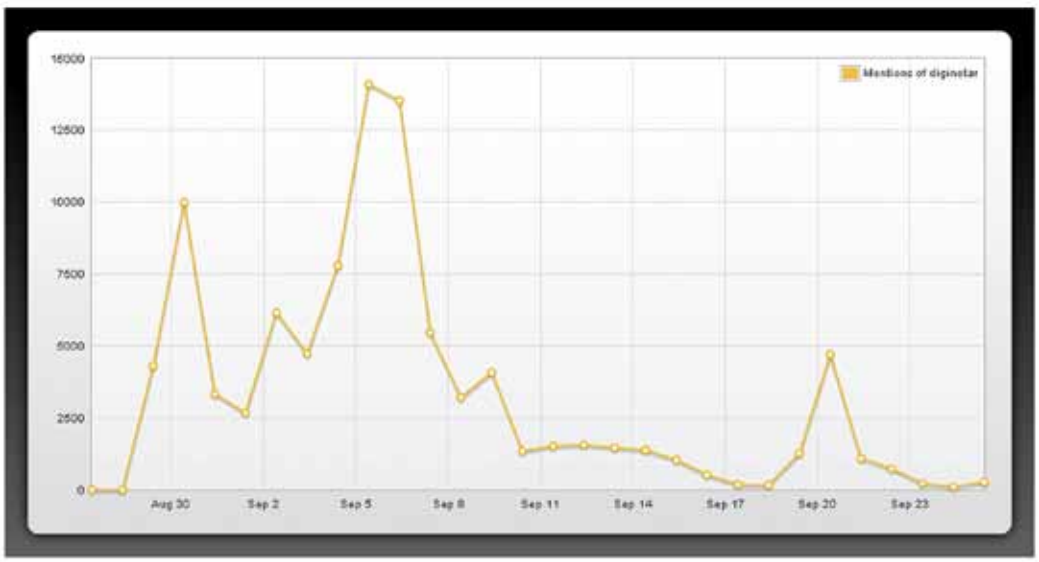
Links:

Website Charles den Tex:
http://www.charlesdentex.com/

Auteurspagina bij De Geus:
http://auteurs.degeus.nl/tex/

Review in Crimelink: http://www.crimelink.nl/blog/charles-den-tex-virtuele-bandieten-en-geldezels





HET DIGINOTAR-DRAMA

We hebben getracht de uitzonderlijke casus rondom de DigiNotar-hack voor u te vatten in een aantal relevante en belangrijke tweets.
Zoals u ziet in de tweetstatistiek begon alles op 28 augustus 2011. Er hoorde een support-vraag aan Google bij. Deze vraag is op deze pagina bovenaan te lezen: http://bit.ly/qJkh1E

ichsunx Sun Ich
Just hacked the Pentagon
12 jul

hkashfi Hamid Kashfi
#Google MiTM attack by #Iran #government, again? bit.ly/
can anybody confirm or provide pcap & traceroute? please
28 aug

st0rmz Andrew Storms
bye bye DigiNotar
29 aug

loerror Jacob Appelbaum
Dear everyone in #Iran and the rest of the world: REMOVE #DigiNotar from your browser trust root. THIS IS NOT OPTIONAL! REMOVE IT NOW!
30 aug

mikkohypponen Mikko Hypponen
Microsoft has removed the DigiNotar root certificate from the Microsoft Certificate Trust List. bit.ly/rpKU46 Bye bye.
30 aug

sanitybit Daniel Kluckmann
Putting in an order with DigiNotar for *.mil - I hope I'm not too late to the party
30 aug

csoghoian Christopher Soghoian
We are all in debt to Google's @scarybeasts & @agl__ whose code detected DigiNotar HTTPS cert. Chrome leads on security. Shame about privacy
31 aug

mikeot Mathijs R. Koot
(I don't know whether it's reasonable to suggest #DigiNotar problems could extend to #PKIoverheid, let's await @fox-it's report on this)
31 aug

andreasudo Andreas Udo de Haes
En @bronno knalt weer: DigiNotar deed geen aangifte na hack...bit.ly/pHHLIG
2 sep

cryptoron Ronald Prins
#DigiNotar breach report will be sent to the Dutch Parliament this monday and made public.
4 sep

TrendLabs TrendLabs
New post: Diginotar: Iranians - The Real Target
blog.trendmicro.com/?p=36667
5 sep

globalsign GlobalSign
We are aware of the Comodo hacker BLOG that claims access to a number of major CAs including #GlobalSign. W... (cont)
deck.ly/~9GvPD
5 sep

WellPond Chris Wysopal
Comodo Hacker Claims Credit for DigiNotar Attack. Claims he owns 4 other CAs bit.ly/r52DZ9
5 sep

VASCODataNews VASCO Data Security
VASCO Announces Bankruptcy Filing by DigiNotar B.V.
bit.ly/p4OvSM
20 sep

De eerste, kinderlijke tweet in het overzicht was van ComodoHacker zelf (ich sun). Brongrafiek: http://topsy.com, zoekfrase Diginotar

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.

Iedere beveiliger weet inmiddels wel dat DigiNotar gehackt is en dat er zich een wereldwijd drama heeft afgespeeld waarbij Nederland, DigiNotar, Comodo en soms ook Vasco door de mangel zijn gehaald. Een prangende vraag is wat was in dit drama de rol van deze en andere partijen en in de certificaatdienstverlening in het algemeen? Dit is een wereld die vaart op het verkopen van vertrouwen. DigiNotar was een gerespecteerde partij in deze wereld. Maar is er nu een grens van vertrouwen overschreden? Is vertrouwen wel te koop? Waarom is er niet eerder alarm geslagen? Was dit te voorkomen en hoe? Of was dit alles onontkoombaar? Met andere woorden; als het DigiNotar niet was geweest, zou dan misschien een ander partij slachtoffer zijn geworden? De hacker die de verantwoordelijkheid voor de verschillende hacks opeist, hint hier in ieder geval wel naar. Onze redacteuren laten hun licht schijnen over dit nieuws.

Rachel Marbus:
Vertrouwen zou moeten worden behandeld als een schaars goed. Het is een niet vanzelfsprekende aanwinst. Als het eenmaal verkregen is, dan moet het worden gekoesterd. Hetgeen zoveel inhoudt dat we daarbij continu alert moeten blijven. Het stellen van kritische vragen en het telkens herijken van de huidige situatie zijn daarbij een must. En dat is niet een zaak van slechts een partij. Het is een zaak die de hele informatiebeveiligingsgemeenschap aan het hart dient te gaan. Samen moeten we daarom nadenken over datgene wat er is gebeurd en wat de gevolgen zijn van de ontstane vertrouwensbreuk.
Dat begint met het herstellen van het systeem en ervoor zorg dragen dat niet alleen de onderste steen boven komt, maar ook dat communicatie weer in vertrouwelijkheid wordt hersteld. Daarnaast moeten we tezamen de koppen bij elkaar steken om te zien hoe we kunnen nadenken over en werken aan een beter systeem. Het herstellen van vertrouwen en het werken aan een betere veiligheid is een taak van velen.
"To state the facts frankly is not to despair the future nor indict the past. The prudent heir takes careful inventory of his legacies and gives a faithful accounting to those whom he owes an obligation of trust."
John F. Kennedy

Aart Jochem:
Het DigiNotar-debacle heeft ons een aardig kijkje achter de schermen van PKI gegeven. Wereldwijd vertrouwen massa's mensen op een techniek en de betrouwbaarheid van zo'n 650 bedrijven die certificaten uitgeven. Als er een certificaat van zo'n bedrijf wordt gebruikt, vertrouwen we er onze financiële zaken aan toe, onze privacy en in sommige totalitaire staten ook vrijheid en veiligheid. En is dat terecht? Het PKI-sprookje is nu wel doorgeprikt. Of het nu over een overheidssysteem gaat of dat het een gewone commerciële dienst is waarvan bedrijven gebruik kunnen maken. Er wordt door allerlei organisaties verdiend aan het verstrekken van digitale certificaten. De CSP zelf, natuurlijk, maar ook de auditor, het ICT-beveiligingsbedrijf en de toezichthouder. De DigiNotar-crisis laat zien dat het zonder teveel kwaliteitsbesef kan. De achtergronden van de Comodo- en StartCom-hacks kennen we niet, maar de kans dat er tussen de 650 CSP's nog enkele rotte appels zitten is reëel. Voor veel toepassingen lijkt een self-signed-certificaat net zo betrouwbaar. Een ander aspect is dat andere organisaties, niet zijnde trusted third parties maar browserfabrikanten, het vertrouwen in een CA kan intrekken. Omdat ze vinden dat dat moet.
Kortom; wat een raar systeem van vertrouwen. Het probleem is dat er nog geen goed alternatief is. Dus kopen we onze certificaten bij bedrijven die nog niet slecht in het nieuws zijn geweest. Reputatie vervangt dus vertrouwen. Het goede nieuws is dat de crypto van PKI niet gekraakt is. Gelukkig hebben we de crypto nog!

Ronald van Erven:
Afgaande van wat ik uit de publieke nieuwsbronnen heb kunnen lezen viel al snel het blinde vertrouwen op in certificate autorities (CA's), zogenaamde vertrouwensdiensten. Dit komt deels doordat bij de aanvraag van certificaten je het hemd van het lijf wordt gevraagd door de CA. De CA controleert alles van jou, dus al snel hebben mensen het gevoel van 'dat zit wel goed'. Daar overheen komen rapportages van auditors. Wat blijkt nu in het geval van Diginotar? Qua beheer en technische implementaties zit het niet goed terwijl het bedrijf wel door ging met het aanbieden van vertrouwensdiensten. Het is nu makkelijk om te wijzen naar de beheerders of op tv te roepen: "Ik heb het jullie gezegd". Het probleem ligt aan de 'tone-at-the-top' en dat het leveren van vertrouwensdiensten een van de moneymakers van afgelopen jaren op internet is geweest. De vele

jaren dat mensen in dergelijke diensten hun vertrouwen hebben gegeven is binnen een paar weken weg. De stelling 'vertrouwen komt te voet en gaat te paard' geldt hier echt. Zeker nu bekend is dat bij meerdere CA-leveranciers een en ander fout zit.
Maar zegt dit ook niet iets over het vakgebied van de auditors, de zogenaamde derde verdedigingslinie? Kijken auditors niet teveel naar de administratieve (AO) wereld omdat deze makkelijker te begrijpen en bij te houden is? De technologische ontwikkelingen gaan immers snel. Moeten zij niet meer diepgaande technische audits houden en zeker bij deze diensten continu een vinger aan pols houden? Is de AO-wereld wel representatief genoeg voor de werkelijke (technische) wereld? Hoeveel vertrouwen moet je nog hebben in rapportages van auditors? En natuurlijk, dit alles kost geld. En hier komt de 'the-tone-at-the-top' om de hoek kijken. Je levert een vertrouwensdienst wel of niet, maar nooit half. En het geven van vertrouwen moet anders gaan worden getoetst.

Gerrit Post:
Recentelijk was op tv een kort item te zien over het EK voetbal dat in 2012 in Polen en Oekraïne wordt georganiseerd. Heeft u ook zo gelachen over het aanbestedingstraject van die snelweg? Een Chinese firma was de laagste inschrijver maar bleek na de gunning geen idee te hebben hoe je zoiets moest aanpakken. Nu moeten er extra kosten worden gemaakt om nog iets van een weg te kunnen aanleggen. Iets dergelijks kan zich hebben afgespeeld rond de aanbesteding van uitgave en beheer van de certificaten rond DigiD. Nou is dat op zich nog niet erg maar wat mij stoort is het zwartepieten dat de overheid direct in gang zet met als doel de eigen straat schoon te vegen. Voor van alles en nog wat in dit land moet je vergunningen hebben en is er een controleapparaat. Voor iets cruciaals als onze digitale snelweg is er totaal, helemaal, niets. De overheid, die ons verplicht om DigiD te gebruiken, is degene die verantwoordelijk is voor de beveiliging van die digitale infrastructuur en niemand anders. Die overheid heeft gefaald in het toezicht dat zij moest organiseren, in de controle die zij op DigiD moest uitvoeren. Dat zij de beveiliging en misschien ook de controle wenst uit te besteden is prima, maar zij is en blijft verantwoordelijk. Misschien dat iemand in het parlement die vragen nog eens kan stellen en ook kan vragen in hoeverre de overheid nou geleerd heeft uit deze zeperd? De overheid, en aanverwante takken van sport, loopt momenteel voorop in het eisen van ISO27000-certificaten van aanbieders, een goede zaak. Maar ze kan zich daar niet achter verschuilen.

André Koot:
Met alles wat er fout is gegaan, zou ik ook een paar interessante zaken willen belichten die we niet over het hoofd moeten zien. In de eerste plaats leidde de kraak tot een volkomen uitval van alle digitale overheidsdiensten. C2G (DigiD), B2G (BAPI) en G2G allemaal plat. Ik kan me geen aanvalsscenario voor de geest halen waarbij door een gecentraliseerde aanval zo'n effect werd bereikt. Een CDoS-aanval, dat bestond nog niet. Voer voor beoefenaren en onderzoekers van cyberwar en cybercriminaliteit. Maar wat ook niet onbenoemd mag worden is dat alle overheidsdiensten op het internet plat lagen. Landelijke overheid, maar ook lokale overheidsdiensten waren niet beschikbaar. Minister Donner riep zelfs op om maar een pen te hanteren (niet doen! dat zou tot een papieren DDoS leiden...). Maar uit deze casus blijkt dat de overheid wel degelijk doet aan beveiliging. Plaatsen van een SSL-certificaat is niet meer spannend, maar de overheid heeft dat dus mooi wel voor elkaar!
Laatste aspect, en dat mis ik eigenlijk in alle analyses... wat gebeurt er met alle documenten, contracten enz. die met DigiNotar-certificaten zijn ondertekend? Technische gevolgen? Juridische gevolgen? Lijkt me een onderzoekje waard.

Maarten Hartsuijker:
Vertrouwen is natuurlijk niet te koop. Maar als je een Trusted Third Party bent, dan hoor je er natuurlijk wel alles aan te doen om het vertrouwen dat in je wordt gesteld waar te maken. Dit kun je als een uitdaging zien, maar je kunt er als commerciële aanbieder natuurlijk ook voor kiezen om zo min mogelijk te doen zodat je telkens met de hakken over de sloot je TPM haalt. Dit betekent niet dat de TPM niets waard is. De auditerende partijen, zoals PWC bij DigiNotar, dienen zich vanzelfsprekend aan de geldende normenkaders te houden. Deze normen staan vast. Maar de diepgang waarmee wordt gecontroleerd is erg afhankelijk van het visiterende auditteam. Niet elke auditor is een PKI-expert. Het eerste dat vaak sneuvelt is het diepgaand controleren van de techniek. Daarnaast concurreren grote auditkantoren met elkaar. Dit leidt tot een lagere prijs, wat meestal direct of indirect tot uitdrukking komt in de diepgang van de audit. Maar de concurrentie is ook een prikkel om extra voorzichtig te zijn met het uitbrengen van een negatieve TPM. Je ziet je klant een jaar later immers graag terugkeren.
Deze gang van zaken is niet DigiNotar- of *ETSI* TS 101 456- (de PKI-certificering) specifiek. Ook IT-bedrijven die de moeite nemen om zich ISO 27001 te certificeren doen dit veelal op basis van een commerciële afweging.
Als je als bedrijf erg afhankelijk bent van de diensten van derden, dan bieden de certificeringen van die bedrijven een mooi uitgangspunt. Maar wil je meer zekerheid, dan kan een aantal eigen steekproeven geen kwaad. Ook hier geldt het adagium: 'vertrouwen is goed, controle is beter'.

GESLAAGD SECURITY CONGRES VAN PvIB, NOREA & ISACA

Opening congres.

Edo Roos Lindgreen.

Andre Smulders.

Foto: Tom Bakker

André Koot.

Rachel Marbus.

Grote belangstelling.

Foto: Tom Bakker

Onderonsje van Rachel en Edo.

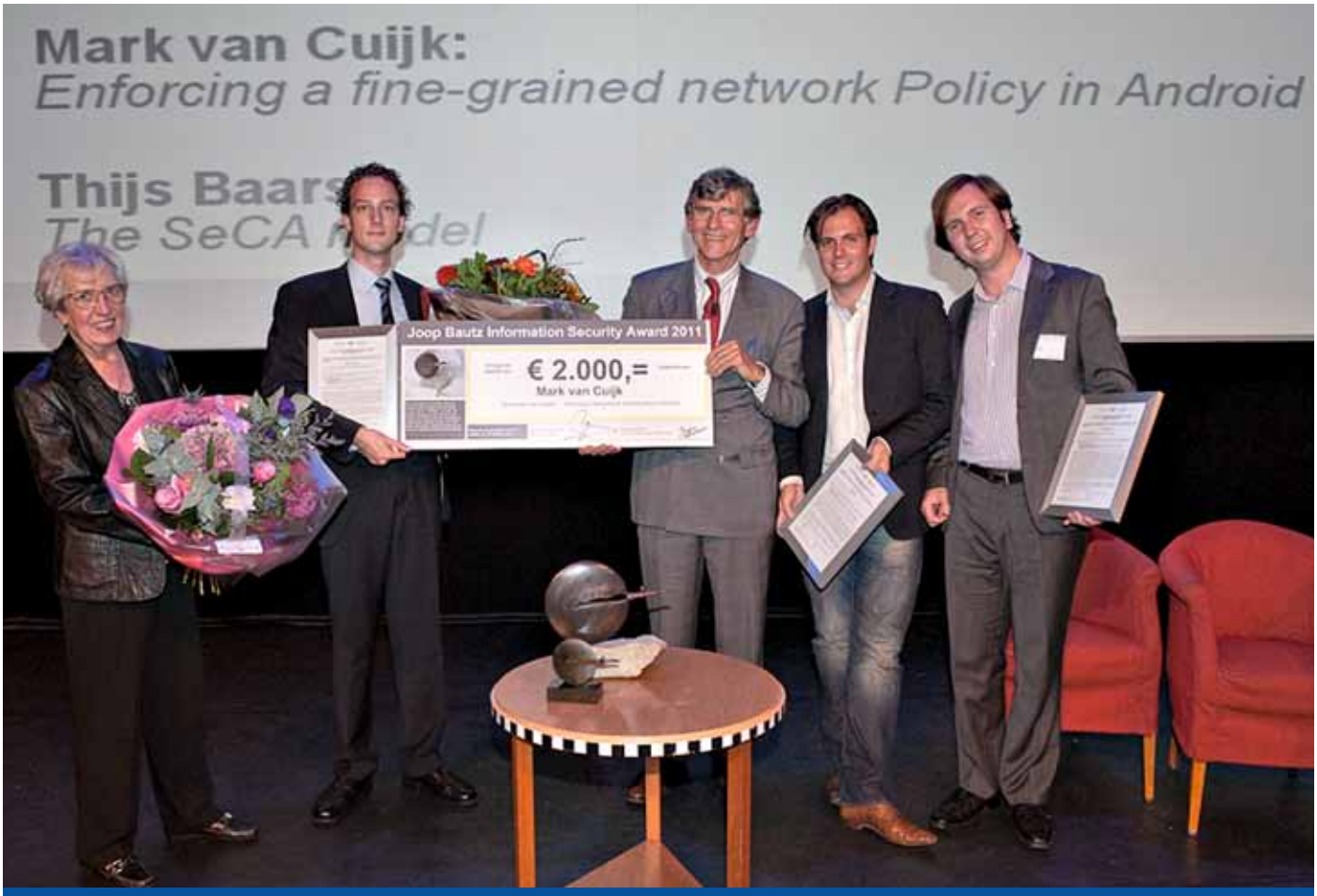
Foto: Tom Bakker

JOOP BAUTZ INFORMATION SECURITY AWARD

12 oktober 2011: Mark van Cuijk wint de JBISA 2011
Op 12 oktober 2011 heeft Mark van Cuijk tijdens het Security-Congres de prestigieuze Joop Bautz Information Security Award (JBISA) 2011 in ontvangst mogen nemen.
Mark heeft de JBISA gewonnen met zijn scriptie getiteld: *Enforcing a fine-grained network Policy in Android.*

Links:
Winnende scriptie:
www.jbisa.nl/download/?id=17674013
Juryrapport:
www.jbisa.nldownload/?id=17674357

Mark van Cuijck (R), winnaar JBISA 2011.



Genomineerden JBISA 2011.

COLOFON

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

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

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

Advertentieacquisitie
e-mail: adverteren@pvib.nl

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

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

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

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

ISSN 1569-1063

‘GELUKKIG IS ER NIETS GEBEURD...’

Ik ben de laatste jaren somberder en somberder geworden over mijn veiligheid. Niet op straat, want in de omgeving waarin ik woon kunnen bewoners op een losse en ongedwongen wijze met elkaar omgaan en doen dat ook. Ik heb het geluk in een omgeving te wonen waar bomen, vijvers, koeien, paarden en vogels niet verdrongen zijn door flats, parkeerterreinen en andere ruimtevreters. Nee, daar zul je mij dan ook niet over horen. Ik ben bijzonder gelukkig in en met mijn omgeving. Mijn veiligheid op internet, dát baart mij zorgen. In voorgaande columns heb ik gesproken over RSA, Sony en andere opzienbarende inbraken in grote en veilig geachte systemen. De inkt was nog niet droog van die columns toen mij het volgende onthutsende bericht bereikte: Mijn DigiD was niet meer veilig! Je kunt veel vinden van DigiD (fervente tegenstanders vinden het namelijk zeer slecht dat DigiD altijd weet welke ambtelijke instellingen door jou zijn bezocht en vinden dit een inbreuk op de privacy) maar ik ben er over het algemeen wel heel tevreden over. Ik vind het een veilige toegangsmethodiek waarbij je je eigen wachtwoord en user-id net zo moeilijk kunt maken als je zelf zou willen. En als je daarnaast nog een sms-authenticatie aanzet dan zou het allemaal wel veilig kunnen zijn. Met de nadruk op zou want als een onderliggend certificaat wordt gestolen en misbruikt dan weet je dat het mogelijk is in te breken in een systematiek die veilig lijkt. Het leverende bedrijf speelt de onschuld en geeft ons aan dat er allemaal niets aan de hand is. Minister Donner komt op vrijdag na middernacht op televisie en geeft ons aan dat we net als hij meer brieven moeten schrijven en belangrijke zaken niet op internet moeten uitvoeren. Meneer Donner lijkt de weg kwijt te zijn en heeft volgens mij geen idee waar hij over spreekt. Gelukkig is het laat en kijkt er bijna geen mens naar zijn persconferentie. Jammer genoeg hebben de grote kranten wel een verslaggever uit hun nachtrust weten te halen en die tekenen alles in de ochtendkranten op. Gelukkig worden we nog steeds gerustgesteld door het bedrijf die de certificaten uitgeeft, er is niets gebeurd en ze zullen met een gerust hart de resultaten van het onderzoek van Fox-IT afwachten. Inmiddels kennen we die en weten we ook dat het uitgestraalde optimisme blijkbaar gespeeld is. Certificaten werden op zijn zachtst gezegd knullig beheerd op machines waar geen antivirus of andere beschermende middelen op geïnstalleerd stonden en die bovendien niet waren gepatcht. Wachtwoorden waren wel heel simpel en er was toegang tot de certificatenomgeving zonder beschermende tussenlagen. Het bedrijf is geselecteerd door de Nederlandse overheid en soms denk je dan dat het wel goed zit. Blijkbaar heeft de Nederlandse overheid geen controlerende activiteiten die ervoor zorgen dat het niet alleen goed zit bij het begin maar ook na een bepaalde tijd. Misschien dat minister Donner het bedrijf heeft geselecteerd maar dat zal toch wel niet.

Erger vind ik de glasharde ontkenning dat er iets aan de hand is terwijl de hackers boodschappen achterlieten op de systemen van de certificaat leverende partij. Niemand zag het of misschien zagen ze het wel maar was het lastig om dit naar buiten te brengen. Ik weet het niet maar de gevolgen zijn duidelijk geworden. Gemeenten die hun werk niet konden doen, autodealers die hun nieuwe auto’s niet konden uitleveren omdat ze gewoon niet op naam gezet konden worden. Directeuren van bedrijven die DigiD gebruiken maken het leven van de beveiligingsmensen in zijn bedrijf zuur omdat hij een oplossing wil voor zijn probleem. Dezelfde directeur die in een sneer laat blijken dat hij wel wat meer had verwacht van zijn duur betaalde beveiligingsmensen die nog proberen uit te leggen dat zij er echt niets aan kunnen doen en dat het probleem door DigiD is geïmporteerd. Inmiddels is alles weer wat rustiger geworden. Certificaten zijn allemaal vervangen, een aantal medewerkers van het bewuste bedrijf zoekt een andere baan en er wordt nog steeds geroepen dat het moederbedrijf echt helemaal niets te maken heeft met de certificatenuitgever.

Tja, en wat kan ik als internet gebruiker ermee? Lessons learned? Ja, ik heb weer geleerd dat mijn user-id en wachtwoord net zo moeilijk kunnen zijn zoals ze nu zijn maar dat dit eigenlijk niets helpt. Dat er in de donkere hoeken van internet, hackers op jacht zijn om gaten in de beveiliging te zoeken en op sommige plekken hoef je dan niet eens zo lang te zoeken. Peinzend schuif ik mijn toetsenbord aan de kant en vraag aan mijn vrouw of we nog briefpapier hebben. Ze kijkt mij aan met een blik die veel verbazing verraadt. Misschien heeft minister Donner toch wel gelijk.

Groetjes, Berry

SOPHOS

SECURITY SO COMPLETE YOU FEEL INVINCIBLE

WORRY LESS. ACCOMPLISH MORE. WWW.SOPHOS.COM

CRYPSYS Data Security is de expert op het gebied van security oplossingen en distributeur van Sophos. Neem contact met ons op via sales@crypsys.nl of via 018 362 44 44 voor een gratis evaluatie versie! Voor meer informatie kunt u ook terecht op onze website: **www.crypsys.n**

CRYPSYS data security