08/2011

INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 8 - 2011

HACKEN MET EEN DEURKLINK

ACHTER DE WOLKEN SCHIJNT DE ZON (TE SCHIJNEN)

INFORMATIE-ASYMMETRIE IN DE BEVEILIGINGSMARKT

TO TRUST IS TO ASSUME

SMARTPHONE SECURITY

FOX-IT

... for a more secure society

Fighting cybercrime

Protecting secrets

Finding digital evidence

Ben jij de nieuwe foxer?

Fox-IT is het meest innovatieve IT Security bedrijf in Nederland en dé expert op het gebied van cybercrime, crypto en digitaal rechercheonderzoek. Met een enthousiast team van zo'n 100 betrokken en gedreven medewerkers vertalen wij de ambities van onze klanten in concrete oplossingen. Innovativiteit, vertrouwelijkheid, een excellente reputatie en de drive tot ontwikkeling zijn onze kernwaarden.

Actuele vacatures:

- Accountmanager CyberSecurity
- Software Developer Python
- Software Developer Forensics
- Security Expert Crypto
- Penetratietester
- Security Analyst Cybercrime

Meer weten? Kijk op www.werkenbijfox-it.nl of mail naar vacature@fox-it.com

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

VOORWOORD

CMM Level 1.
We noemen het gekscherend het domein van de cowboys.
Dit werkt door, zodanig dat 'cowboy' een negatieve bijklank heeft gekregen bij mij. Maar is dat terecht? Ook ik ben opgegroeid met de stripverhalen van mazzelende Luuk, die van alle markten thuis is en altijd victorieus uit iedere situatie wegkomt. Heel anders dan menige sheriff, barman, bankier, smid of machinist. Anders dan al deze figuren is Luuk altijd de generalist, niet de specialist. En altijd waakzaam. Het helpt als je sneller kunt schieten dan je schaduw, maar je moet ook voortdurend bewust zijn van wat er om je heen allemaal gebeurt. Luuk speelt de 'hero', andere personages krijgen vaak de rol 'zero' opgespeld. Zeroes en heroes - typisch voor het speelveld van CMM level 1…
Een ding wat die mazzelende Luuk ook kon was situaties snel analyseren en tóch uit de heup raak schieten. Dit is wat in de realiteit nu net niet kan worden gecombineerd…
Stel je de afronding van een project voor. De projectinrichting zat dik boven CMM level 1, dus bovenstaande parabel gaat hiervoor niet op. De opdrachtgever is ook tevreden, dus alles is rond, zou je denken. Maar zoals het altijd gaat als je oplevert, wordt er dan door buitenstaanders kritiek geleverd op wat je hebt gedaan. Dit is prima, iedereen mag van mij een mening hebben en die zelfs uiten, als we maar beschaafd blijven. Voor de onbeschofte reacties heb ik een ingebouwd filter (firewall?), dus die laat ik geheel buiten beschouwing. Dan houd je nog een hele serie reacties over die op mij overkomen alsof er uit de heup geschoten wordt - CMM level 1.
Ik kom tot de conclusie dat er 'security experts' zijn die graag de rol van onze cowboy hero, mazzelende Luuk, vervullen, maar niet verder komen dan een beperktere rol, zoals de barman of de smid. Als je naar een totaaloplossing kijkt en opmerkingen maakt over alleen de netwerkbeveiliging, het certificaatgebruik of de systeeminrichting, zonder dat je naar de som der delen kijkt, dan kun je lekker uit de heup schieten en vernietigende kritiek hebben. Je bent dan een specialist die een deel afschiet zonder het geheel gezien te hebben.
Dan denk ik terug aan de vele ontwerpbeslissingen die genomen zijn en discussies die daaraan vooraf gingen en kom weer tot de conclusie dat goede beveiliging gaat om het nemen van preventieve maatregelen, in combinatie met detectie en correctie. Bij de haast van het uit de heup schieten kijken de CMM level 1-specialisten van buiten alleen naar de tastbare preventieve maatregelen… want de rest kun je niet zomaar zien. "There is more than meets the eye…"
Moraal: kijk uit met kritiek uiten, durf vragen te stellen en te veronderstellen. Ga er eens van uit dat er wellicht het goede gedaan is en vraag je af wát dat dan is. En geef daarna pas kritiek, op basis van feiten. Dan kun je daarna tevreden als de held de zonsondergang tegemoet rijden…

INHOUDSOPGAVE

Ronald Prins, directeur Fox-IT

JE PRIVACY VERLIEZEN DOET PAS ECHT PIJN ALS JE HET VOELT

"Wie heeft het nog over Big Brother in deze tijd van Facebook en internet?" Dat vroeg de Korpschef van het KLPD, Ruud Bik, zich afgelopen jaar hardop af bij zijn nieuwjaarsspeech. Ondanks dat het open platformen zijn, zitten daar toch enorme privacyrisico's achter. Natuurlijk zetten we allemaal steeds meer foto's, filmpjes en zinnen van 140 tekens online, maar al die platformen lokken ook uit tot niet met het volledige publiek gedeelde privécommunicatie. En in de praktijk delen we veel meer persoonlijke informatie via deze platformen dan vroeger via telefoon of sms...

Privacy is een groot goed, misschien wel een van onze grootste. We zullen meer ons best moeten doen om haar te beschermen. We maken steeds meer gebruik van smartphones en tablets. Waar vroeger onze geheimen vluchtig waren, worden ze nu permanent. De technologische wereld kent geen 'social forgetfullness'. Een spannend verhaal over wat de buurman deed en met wie, wordt in de offline wereld 'vergeten' en zakt daardoor weg in de herinneringen van mensen. Het wordt misschien nog eens verteld tijdens de taart en koffie op een verjaardag, maar de details vervagen met de jaren. De onlinewereld kenmerkt zich door koppelbaarheid, kopieerbaarheid en een eeuwigdurend geheugen. Telefoongesprekken werden vroeger niet opgeslagen. En mocht iemand je willen tappen dan moest hij daar permanent technische voorzieningen voor treffen. We bellen minder, maar e-mailen, chatten, whatsappen en pingen des te meer. Omdat we dat ongeacht plaats en tijd kunnen, doen we het ook continu. Stap rond het spitsuur in de trein en je ziet niemand onder de 40 meer naar buiten kijken maar met zijn of haar telefoon spelen. En dat is niet alleen om te kijken of de trein vertraging heeft. Nee, afspraakjes worden gemaakt, de date van gisteravond wordt in detail besproken, en expliciete foto's gaan heen en weer. Omdat het in de praktijk zo handig werkt zijn we ook massaal verslaafd geraakt aan applicaties als Lattitude waardoor ook nog permanent onze locatie gedeeld wordt. Gingen deze gegevens alleen maar tijdelijk door de lucht. Helaas doen ze dat niet. Als ik op een nieuwe telefoon WhatsApp installeer, krijg ik zonder dat ik er iets voor hoef te doen vanzelf de communicatie met mijn vrienden en vriendinnen van de laatste drie maanden weer in beeld. Inclusief alle foto's en filmpjes die we elkaar hebben gestuurd in een jolige of geile bui. Blijkbaar worden mijn gegevens allemaal netjes bewaard op een server van WhatsApp en hoef ik niet meer te doen dan een sms'je te onderscheppen van iemand om ze allemaal binnen te krijgen. Ik durf ook rustig te stellen dat als anonymous ooit de WhatsApp-database weet te hacken dat dit een impact zal hebben in de orde van WikiLeaks. WikiLeaks zelf is natuurlijk ook een goed voorbeeld van hoe de nieuwe informatiemaatschappij ons kwetsbaar maakt. Nog maar een paar jaar geleden waren cables echt cables (telexen) en helemaal niet in enorme hoeveelheden beschikbaar. Zeker niet voor een soldaat eerste klasse die er vanuit Irak bij kon. Een diefstal tien jaar geleden had dozen vol papier opgeleverd die je niet zo gemakkelijk meeneemt als een dvd'tje in een LadyGaga-hoesje met daarop alle codetelegrammen van het ministerie van Buitenlandse Zaken van de laatste tien jaar.

> Realiseer je dat ooit iemand anders er ook toegang toe krijgt

'Archive instead of delete'

Eigenlijk zou je je bij elk e-mailtje, fototje of chatgesprek dat je voert moeten

realiseren dat ooit iemand anders er ook toegang toe krijgt. De permanentie van informatie zorgt ervoor dat we niet alleen nu een publiek hebben, maar ook in de toekomst. Sterker nog, dat toekomstige publiek is ook nog eens onzichtbaar omdat we op het moment van delen nog niet kunnen vermoeden wie de informatie allemaal onder ogen zal gaan krijgen. Ik heb het geprobeerd om spaarzamer om te gaan met het delen van informatie. Niet meer zomaar alles zeggen wat in me opkomt en stoppen met die impulsieve gesprekken met mijn vrienden en vriendinnen waarin we elkaar vertellen wat we allemaal meemaken. Maar dan ontdek je al snel dat de lol van die nieuwe apps voorbij is. En omdat storage zo goedkoop geworden is, willen de gratis e-mail-providers als Gmail en Live liever dat je nooit meer je e-mail weggooit: 'Archive instead of delete'. Kortom we communiceren meer, en het blijft nog allemaal keurig doorzoekbaar bewaard. Voor altijd!

Voor wie zijn we bang?

Wanneer *voel* je een privacyschending? Dat is uiteindelijk een belangrijke vraag. Zeker daar waar het gaat om het veranderen van het gedrag van mensen die te snel en te gemakkelijk alles delen zonder zich zorgen te maken over de juiste beveiliging. Het lekken van gegevens is bijna dagelijks aan de orde van de dag. De krant staat er vol mee. En toch lijkt het erop dat het gedrag van mensen nog steeds weinig verandert als het gaat om de veiligheid van hun eigen gegevens. Onze internetcommunicatie wordt al jarenlang grootschalig afgeluisterd. Rond 2001 werd duidelijk dat de Amerikanen, samen met het VK, Canada, Australië en Nieuw Zeeland miljarden investeren om gezamenlijk zoveel mogelijk communicatie af te luisteren. Dit is niet alleen gericht op buitenlandse terroristen maar na 9/11 werden ook Amerikaanse burgers en burgers uit bevriende landen grootschalig afgeluisterd. Toen dit uitkwam heeft het maar heel beperkt de internationale pers gehaald. Toch wordt het door veel burgerrechtenbewegingen als de grootste privacyinbreuk gezien. Een belangrijk element van staten die afluisteren, is dat ze dat zo geheim mogelijk doen. Ze zullen er dus ook alles aan doen om te voorkomen dat bekend wordt wat precies hun mogelijkheden zijn. Dit in combinatie met die geringe aandacht in de pers en in het maatschappelijke debat zorgt ervoor dat zo min mogelijk mensen geconfronteerd worden met deze privacyschending.

> Activisten met een goed doel, bewandelen een merkwaardig pad

Heel anders is dat bij traditionele cybercriminelen en de moderne hackersactivisten zoals Anonymous, Lulzsec en Anti-sec. Cybercriminelen verspreiden malware onder zoveel mogelijk internetgebruikers om grootschalig

privacygevoelige gegevens te verzamelen en uit te buiten. Denk dan aan bankgegevens, creditcardnummers maar ook wachtwoorden van Gmail-, Twitter- en Facebook-accounts. Dit doen ze zo goed dat we regelmatig in onderzoeken databases tegenkomen met daarin de gegevens van meer dan een miljoen mensen. De activisten onder de hackers hebben een goed doel, maar bewandelen een merkwaardig pad om dat doel te behalen.

Zij willen aantonen dat de beveiliging van het internet niet voldoende is en dat de gebruikers grote risico's lopen. Ze vinden dat de bedrijven die de gegevens opslaan van hun klanten niet voldoende hun best doen om de veiligheid daarvan te waarborgen. Ook de overheid laat steken vallen, vinden zij. Overheden dwingen bestaande privacywaarborgen niet voldoende af en gebruikers willen zo graag op Facebook communiceren met hun vrienden dat ze de eventuele risico's graag voor lief nemen. "Want hoe interessant ben ik nou voor hackers?", wordt vaak gedacht. Activisten vinden dat deze passieve houding gevaarlijk is en hebben daarom besloten de burgers de gevolgen van deze passiviteit te laten voelen. Ze hacken systemen van de politie en zetten gegevens van informanten online. Ze breken in op een datingsite en publiceren lijsten van tienduizenden mensen die op zoek zijn naar een relatie. En dat inclusief wachtwoorden zodat men goed beseft dat de buurman nu misschien ook even de liefdeshistorie aan het meelezen is.

Wat moet er gebeuren?

De activisten hebben gelijk. We zijn te naïef en veel gevoelige gegevens zijn nu niet goed beschermd. We zullen zeker niet stoppen met ons intensieve internetgebruik, dus de beveiliging moet worden verbeterd. Een aantal bedrijven zoals Google en Facebook biedt bijvoorbeeld als extra drempels two-factor authentication. Behalve een wachtwoord, heb je ook een code nodig die je via SMS ontvangt om toegang tot de site te krijgen. Ik gebruik het graag, maar merk dat mijn omgeving het te omslachtig vindt.

En zo werkt het vaker met preventieve beveiligingsmaatregelen. Hoe vaak zie ik niet dat bekende 'Windows update'-wereldbolletje staan rechtsonder op het scherm van een Windowsgebruiker, ten teken dat hij zijn computer moet updaten. "Ja, dat zou ik eigenlijk moeten doen." Vervolgens gebeurt er niets en is de computer een tijd lang niet afdoende beveiligd. Het interesseert veel mensen blijkbaar niet. Ze vinden dat ze niets te verbergen hebben, of denken dat het zo'n vaart niet zal lopen. Terwijl de realiteit van alledag steeds vaker uitwijst dat het zo'n vaart nu juist wel aan het lopen is. Misschien is dit het punt dat we ons als beveiligers of overheid wat paternalistisch moeten opstellen en die gebruikers moeten helpen.

> Ze vinden dat ze niets te verbergen hebben

Maar hoe doe je dat dan, als de gebruikers er zelf geen moeite in willen steken? Ik zie twee belangrijke acties. De een gericht tegen de cybercriminelen. Die hebben het nu te gemakkelijk en denken dat ze overal mee kunnen wegkomen. En net zoals in de straten waar graffiti onmiddellijk wordt verwijderd en minder fietsen worden gestolen, voorkomt bijvoorbeeld het opsporen van bekladders van websites ook dat cybercriminelen minder snel in de gelegenheid zullen raken om het online en daardoor ook het offline leven te ontwrichten. De grootste winst zit echter in het vroegtijdig kunnen detecteren van digitale aanvallen. Alleen al door het bestuderen van verkeersstromen op het internet blijken we in staat criminele activiteiten in een vroeg stadium te onderkennen. Natuurlijk brengt dat ook een privacy en grondrechtelijk risico met zich mee. Want wie gaan naar die verkeersstromen kijken? Waar moeten ze op letten? Hoe diep kijken ze eigenlijk in de internetpakketjes? En wie controleert dat diegenen die kijken naar de verkeersstromen dit doen volgens de regels? Het is nu tijd hier een discussie over te starten. Vanzelfsprekend moet het uitgangspunt van zo'n initiatief zijn dat de veiligheid van de gebruiker van het internet wordt verhoogd waarbij de privacy van diezelfde burgers als groot goed beschermd dient te worden. Daarom is het van belang in gesprek te gaan met digitale burgerrechtenbewegingen zoals Bits of Freedom. Die zien de overheid zelf als grootste risico. Maar ook bijvoorbeeld een College Bescherming Persoonsgegevens en de OPTA zouden betrokken moeten worden in de discussie. Wil de overheid echt effectief opereren in het voorkomen van cybercrime dan zal ze moeten aantonen dat zij zelf daarmee niet een nieuw risico introduceert, maar daadwerkelijk in staat is op het internet enige vorm van orde te handhaven. Gebeurt dat niet dan zal internet nog meer een vrijplaats worden voor alle vormen van criminaliteit die we nu in de fysieke wereld redelijk onder controle lijken te hebben.

COLUMN

DE TIEN STELLINGEN VAN INFORMATIE-BEVEILIGING & BURGERRECHTEN

Wij, het volk, regenten en onderdanen gelijkszins, dienen de volgende stellingen in het hart te dragen. Wij beloven deze stellingen gestand te doen ongeacht het zware weer waarin wij ons bevinden. Wij zweren dat wij niet meer alleen in het geweer zullen komen als het Lektober is of als DigiNotar omvalt. Wij, het volk, regenten en onderdanen gelijkszins, zweren trouw aan deze 10 stellingen.

1. Wij accepteren geen aflaat voor het schenden van Burgerrechten en de basisprincipes van de Informatiebeveiliging. Wij verschuilen ons niet langer achter drogredeneringen over kosten en baten, het nut voor het grotere goed en het oprekken van onze bevoegdheden omdat dit een goed doel zou dienen.

2. Wij beveiligen onze systemen volgens de laatste stand van de techniek. Denken aan de integriteit van onze gegevens, de vertrouwelijkheid en de beschikbaarheid. Altijd in samenspraak met de weging der essentiële belangen van de bevolking, de Burgerrechten.

3. Wij minimaliseren de benodigde gegevens, weten altijd voor welk doel wij deze verzamelen en beloven de gegevens te vernietigen als ze niet langer noodzakelijk zijn om onze doelen te verwezenlijken. Altijd in samenspraak met de weging der essentiële belangen van de bevolking, de Informatiebeveiliging.

4. Wij beloven ons met man en macht in te zetten voor het bevechten van Cybercrime en het oppakken van Cybercriminelen voor zover de wet ons dit toelaat. Wij zullen echter met schroom handelen in het oprekken van bestaande wettelijke bevoegdheden.

5. Wij zullen anonimiteit koesteren. Wij zullen privacy koesteren. Wij zullen vrijheid van meningsuiting koesteren. Wij zullen de vrijheid van de mens als hoogste goed beschouwen.

6. Wij beloven dat we niet meer stiekem zomaar van uw onbeveiligde wifi-verbinding gebruik zullen maken, maar dat we u in plaats daarvan zullen bijstaan in het opzetten van een beveiligde verbinding.

7. Wij beloven onze kennis te delen om tot een evenwichtige balans te komen tussen Informatiebeveiliging & Burgerrechten. Wij streven ernaar beide waarden met elkaar te verenigen.

8. Wij beloven dat we nimmer meer kond zullen doen van de volgende beweringen, en deze waar noodzakelijk te vuur en te zwaard zullen bevechten : "Ik heb niets te verbergen" evenals " In het kader van uw veiligheid zijn deze inbreuken op uw burgerrechten absoluut noodzakelijk".

9. Wij onderdanen beloven onze regenten bij te staan met de juiste informatie opdat zij goede beslissingen kunnen nemen. Wij regenten beloven de rechten van onze onderdanen te beschermen zowel op het gebied van Informatiebeveiliging als dat van de Burgerrechten.

10. Wij nemen altijd onze handdoek mee.

Wij het volk, regenten en onderdanen gelijkszins, beloven dat wij er gezamenlijk op zullen toezien dat deze stellingen, evenals de inhoud daarvan, zullen worden nageleefd. Wij voorzien in adequate handhaving, houden het scheiden van de machten in ere en beloven trouw te zullen zweren aan Informatiebeveiliging & Burgerrechten.

mr Rachel Marbus
@RachelMarbus op Twitter

HACKEN MET EEN DEURKLINK

Axel Eissens is al een aantal jaren werkzaam in het Identity & Access Management werkveld, voorheen bij Siemens IT Solutions wat is overgenomen door Atos. Axel is bereikbaar via axel.eissens@atos.net. Niels van Brecht is vier jaar werkzaam in het informatiebeveiligingswerkveld binnen de ING en is nu Security Manager bij ING Insurance. Niels is bereikbaar via niels.van.brecht@ingim.com.

Beiden zijn commissielid bij de PvIB Young Professionals commissie.

Stel je voor. Je staat eindelijk met je digitale gereedschapskist op een verdieping waar je eigenlijk niet mag komen. Dan blijkt dat alle kantoorruimtes met open deuren bezet zijn door mensen die jou niet kennen en dat alle andere kantoorruimtes geen deurkruk hebben. De Young Professionals commissie van PvIB organiseerde eerder dit jaar een 'Hacking event' in samenwerking met Deloitte Enterprise Risk Services. In deze sessie werden fysieke en logische penetratietesten besproken.

Tom Schuurmans van Deloitte presenteerde een case waarin de opdracht was de 'kroonjuwelen' van de opdrachtgever te vinden die zich op een informatiesysteem bevonden. De informatie vanuit het bedrijf en de beschikbare tijd voor deze opdracht waren beperkt. Deloitte werd slechts voorzien van een bezoekerspas met beperkte toegang en een zogenaamde 'get out of jail free card' mocht men hen gaan verdenken van een echte misdaad.

De penetratietester heeft als eerste een inventarisatie gedaan naar de fysieke omgeving en de mogelijkheden binnen het pand. Hierdoor kwam hij er snel achter dat de toegang beperkt was tot twee etages die druk bezet waren met externe medewerkers. Daar kon de penetratietester geen ruimte vinden met een aansluiting om rustig rond te gaan kijken op het netwerk.
Andere etages waren alleen bereikbaar voor geautoriseerde personen. In dit geval de vaste medewerkers, waarbij zowel de liftdeuren als de deuren in het

Hackers aan het werk.

trappenhuis geen toegang verleenden aan de tester. Het drukste moment van inloop gebruiken leek de beste strategie. Daardoor kon de tester letterlijk meeliften met andere medewerkers om zodoende op overige etages te komen. Toen hij zich eenmaal toegang had verschaft tot de beveiligde etages kwam er nog een ander probleem om de hoek kijken. De ruimtes die toegankelijk waren zaten vol met mensen en op alle andere deuren zat geen deurklink.

Na even rondkijken was het tijd om een stap terug te nemen met een kop koffie. Bij de koffiemachine hing een poster waarop aanpassingen werden aangekondigd aan het netwerk. Dat gaf informatie voor een goed achtergrondverhaal. Op deze manier raakte de tester aan de praat met een medewerker die hem vroeg wat hij hier kwam doen. De tester vertelde dat hij kwam om het netwerk sneller te maken. De medewerker sprong bijna een gat in de lucht en verwelkomde de tester met open armen. De tester maakte meteen gebruik van zijn prille vriendschap om zijn probleem aan te kaarten om een rustige ruimte te vinden. Daarbij vroeg hij naar het voor hem onverklaarbare ontbreken van deurklinken. Het bleek dat de deurklinken van de ongebruikte ruimtes waren verwijderd vanwege een ruimtegebrek en omdat de medewerkers op deze etage niet wilden dat kamers bezet werden door anderen.

Gelukkig begeleidde de medewerker de tester naar de beheerders van de deurklinken en er werd meteen gezocht naar een geschikte ruimte die voor de tester gereserveerd werd. De tester kon rustig aan de slag gaan. De netwerkaansluitingen bleken niet aangesloten of dusdanig beveiligd te zijn dat hij zijn laptop er niet op aan kon sluiten. De tester had echter wel de computer gezien die nog op het bureau stond en probeerde een USB-stick te gebruiken om data mee te kunnen nemen. Ook hier was een beveiliging op aangebracht, maar de tester had door eerdere ervaringen niet alleen zijn digitale gereedschapskist bij zich maar ook een schroevendraaier. Zodoende opende hij de computerkast en sloot zijn eigen opslagmedium aan. Vervolgens heeft de tester op het netwerk rondgekeken op zoek naar eventuele zwakheden in systemen en heeft daarbij ook het netwerkverkeer afgeluisterd. Op een later moment heeft de tester de opgeslagen data doorzocht op zoek naar nuttige gegevens. Zodoende werden de gegevens (username/password) van een database-

beheerder achterhaald. De gegevens gaven toegang tot de kroonjuwelen van het bedrijf, waarmee de tester zijn opdracht had voltooid.

In het tweede deel van de sessie werden de deelnemers aan het werk gezet en was het de bedoeling dat zij elkaars systemen gingen hacken. Deloitte heeft zelf een hacking game ontwikkeld waarbij alle teams dezelfde systemen, met daarop een webserver, een ftp-server en dezelfde beveiliging(sgaten), in beheer kregen. Het doel is daarbij om zoveel mogelijk punten te behalen. Punten haal je door de computers van de andere teams te hacken en punten verlies je wanneer je eigen computer gehackt wordt.
Een centrale server maakte continu contact met de webservers en ftp-servers om de informatie uit te lezen. Hierdoor was op elk moment zichtbaar welk team wel of niet gehackt werd.

De deelnemers hadden drie kwartier de tijd om zoveel mogelijk punten te scoren. Voor het startsignaal werden zij voorzien van beperkte informatie (ip-ranges en de administratieve logingegevens van de machines). De systemen die beheerd en gehackt moesten worden waren gevirtualiseerde Windows- en Linux-systemen.

Op deze computer draaide een aantal servers op verschillende platforms zoals FTP, HTTP, NetBios en VNC-server. Deze boden mogelijkheden om in te breken en het bestand van de tegenstander te wijzigen of te verwijderen. Door de kwetsbaarheden van het eigen systeem te onderzoeken, probeerden de deelnemers beveiligingsgaten te dichten en konden zij ook andere systemen hacken die het lek nog niet hadden gedicht.
De beste strategie tijdens het spel bleek om punten te verdienen door systemen te hacken in plaats van te voorkomen punten te verliezen door gehackt te worden.

De teams bestonden uit ervaren en onervaren hackers/beveiligers. Het bleek een pittige strijd te zijn tussen alle teams, waarbij sommige mensen het als lastig ervoeren, anderen het als gemakkelijk, en personen die het zichzelf moeilijker hadden gemaakt dan nodig was.
Toen de strijd gestaakt werd, werden de scores berekend en evalueerden de deelnemers wat er goed of fout ging. Dit gaf inzichten in de verschillende aanpakken van enerzijds beveiligen en anderzijds hacken. De winnaars werden beloond met een mooie prijs en ontvingen het boek 'Kingpin' dat het leven van een befaamde hacker beschrijft.

De sessie werd positief beoordeeld en men vond de combinatie van theorie en praktijk een leuke ervaring. Dat maakte het geheel leerzaam en interactief. Mocht je de komende tijd een penetratietest moeten uitvoeren, vergeet je deurklink niet!

ACHTER DE WOLKEN SCHIJNT DE ZON (TE SCHIJNEN)

Albert Brouwer RE is als business consultant werkzaam bij KPN Corporate Market BV en heeft dit artikel op persoonlijke titel geschreven.

De keuze van bedrijven en overheden voor het gaan naar de cloud wordt vaak op bedrijfseconomische gronden gemaakt. De flexibiliteit van geleverde capaciteit en functionaliteit gaat gepaard met betalen voor gebruik en dus niet betalen voor een investering die niet volledig wordt benut. Dat is aantrekkelijk. Die aantrekkelijkheid is zo groot dat issues met betrekking tot security en compliance onderbelicht dreigen te worden. We zien liever de zon achter de wolken. Hoe hiermee om te gaan? Weegt de energie die moet worden gestoken in de voorbereiding op de cloud op tegen de voordelen? Schijn de zon achter de wolken?

Cloud computing heeft o.a de volgende kenmerken:

- de toegang tot hardware, software en gegevens wordt tot stand gebracht via het internet;
- applicaties die in de cloud worden gebruikt staan niet op de computer en doorgaans niet op het bedrijfsnetwerk van de gebruiker;
- de gebruiker c.q. het bedrijf hoeft geen eigenaar te zijn van de gebruikte hard- en software;
- de cloud-leverancier is verantwoordelijk voor onderhoud en beheer van platformen, infrastructuur en geboden software;
- de gebruiker beschikt over een 'eigen', in omvang en mogelijkheden schaalbare, virtuele infrastructuur;
- de gebruiker betaalt opslag en gebruik van applicaties, platform en infrastructuur naar gelang het gebruik dat hij ervan maakt. Doorgaans gebeurt dat op basis van een vaste hoeveelheid voor een afgesproken maandelijks bedrag met de mogelijkheid tot overschrijding.

De grote aantrekkingskracht van cloud computing is het 'pay per use'-principe. Of het nu gaat om applicaties, platformen of infrastructuur, slechts voor de basis en voor het daadwerkelijke gebruik ervan wordt betaald. Eigen investeringen en beheerkosten behoren (bijna) tot het verleden. Gebruik is leidend, niet het bezit. Een grote zorg minder. Op inkoop- en onderhoudskosten wordt bespaard. Mogelijk ook op aantallen fte's en kennis. Kortom, niet al te veel zorgen meer, veel meer gemak en bovendien financieel aantrekkelijk.

Nuances

Een bedrijf dat de cloud ingaat doet afstand van het uitvoeren van een aantal taken dat tot voor kort in eigen beheer werd uitgevoerd. Bij elke vorm van uitbesteden van taken en activiteiten is dat het geval, maar iedere keer weer geldt het aloude adagium dat taken en activiteiten wel kunnen worden overgedragen, maar de verantwoordelijkheden niet. En bij die verantwoordelijkheden hoort dat verantwoording moet kunnen worden afgelegd over datgene waarover men verantwoordelijk is.

> De grote aantrekkingskracht van cloud computing is het 'pay per use'-principe

Bij elke vorm van delegatie moet een governance-model worden gezocht dat past in de gegeven situatie. Maar in elke vorm ligt de uiteindelijke verantwoordelijkheid daar waar de handtekening voor het uitbesteden, in dit geval de inkoop van de cloud, is gezet.
En daarmee ontstaat een governance issue. Wie is 'in control'? Waarover? En hoe is de keten van leveranties ingericht? Wie spelen daarin een rol? Wie is verantwoordelijk voor welke schakel in de keten? Hoe passen die schakels in elkaar? En is elke schakel wel even belangrijk?

Al deze vragen dienen doordacht en opgelost te zijn voordat de cloud in wordt gegaan. Het International Security Forum (ISF) waarschuwt voor de 'seven deadly sins of cloud computing' (Securing Cloud Computing: Addressing the seven deadly sins, January 2011). Een ervan gaat expliciet in op het niet vooraf goed doordacht hebben van de strategie en het oplossen van dit soort vragen. Het komt nog al eens voor dat de cloud al is betreden, maar de visie erop ontbreekt. Verwachtingen zouden hierdoor niet uit kunnen komen, want ook hier geldt: rubbish in is rubbish out.

Aan het betreden van de cloud gaat investering vooraf. Hoe beter men de eigen bedrijfsstrategie en onderliggende (administratieve) organisatie op orde heeft, hoe gemakkelijker en korter het voorbereidingstraject verloopt.
En hoe eerder de financiële en kwaliteitsvoordelen van de cloud kunnen worden binnengehaald.

Kwaliteit van dienstverlening

De kwaliteit van dienstverlening, dus ook die van ICT-dienstverlening, wordt afgemeten aan een aantal parameters, dat per dienst kan verschillen.

- Vertrouwelijkheid
- Integriteit
- Beschikbaarheid
- Effectiviteit
- Efficiency
- Controleerbaarheid

De eerste drie parameters samen worden ook wel 'informatiebeveiliging' of 'security' genoemd. De laatste drie parameters zijn meer het domein van IT-auditors, quality- en service-managers.

Een ding staat vast. De verantwoordelijke partij is gehouden aan het leveren van het gewenste, en soms verplichte, kwaliteitsniveau. Dat geldt ook als een deel van de leveringsketen is uitbesteed, geoutsourced, ge-offshored of 'gecloudsourced'.

In alle gevallen moet met toeleveranciers afspraken worden gemaakt, zodat kan worden geconstateerd dat de uiteindelijk gewenste kwaliteit ook daadwerkelijk wordt geleverd. Gaat het om levering in een keten, dan moeten alle leveranciers hetzelfde kwaliteitsniveau halen. De keten is immers zo sterk als de zwakste schakel.

In die gevallen waarin wet- en regelgeving of toezichthoudende organen een rol spelen, geldt dit des te meer. Wet- en regelgeving en toezichthouders eisen dat verantwoording wordt afgelegd. Zij eisen zelfs een zekere, voorgeschreven, kwaliteit van die verantwoording.

Met het, al dan niet voor een deel, tot stand brengen van dienstverlening uit de cloud, moet worden nagedacht over hoe de kwaliteit van dienstverlening kan worden geborgd en op welke manier daarover verantwoording moet worden afgelegd. En dat impliceert dat, alvorens de cloud in wordt gegaan, de kwaliteitskenmerken duidelijk moeten zijn zodat zij besproken en vastgelegd kunnen worden met de 'cloudleverancier(s)'. Want hoe dan ook, de eindverantwoordelijkheid voor product of dienst en degene die verantwoording moet afleggen, blijft dezelfde. Hoe het product of dienst ook tot stand is gekomen.

> Aan het betreden van de cloud gaat investering vooraf

Twee vragen zijn dus van belang:

1. Hoe ziet mijn leveringsketen eruit? Hierin zitten allerlei deelvragen die ook onder de paragraaf 'Nuances' zijn genoemd.
   a. Wie spelen daarin een rol?
   b. Wie is verantwoordelijk?
   c. Wie is aansprakelijk?
   d. Voor welke schakel in de keten?
   e. Hoe passen die schakels in elkaar (wie levert wat)?
   f. Welk belang vertegenwoordigen de schakels ten opzichte van elkaar?

2. Hoe en over welke parameters wordt verantwoording afgelegd? Aan wie? En met welke periodiciteit?

Zelfonderzoek

Voordat de cloud wordt betreden, is het dus voor alles nodig dat bedrijven zichzelf onderzoeken (selfassessment). In dat onderzoek moet een aantal vragen worden beantwoord.

- Wat is de kwaliteit die ik verlang?
- Wat is de kwaliteit die wet- en regelgeving van mij eisen?

- Wat verwachten mijn klanten?
- Hoe passen de te leveren cloud-diensten in mijn business model?
- Wat is de leveringsketen van mijn producten en diensten?

Pas als dat helder en goed communiceerbaar is, dan kunnen de cloud-diensten worden beoordeeld op de gewenste kenmerken en kan er worden gekozen tussen de meest profijtelijke aanbiedingen. Zonder eerst de eigen eisen helder te hebben, is verantwoord keuzes maken onmogelijk omdat een referentiekader ontbreekt. Dan zal goedkoop snel duurkoop blijken.
Nu zal al gauw de tegenwerping komen dat cloud-leveranciers vanzelfsprekend goede kwaliteit moeten leveren. Doen ze dat niet, dan zijn ze snel out-of-business. We weten uit de 'aardse' wereld dat dit argument voor vele andere diensten ook wordt gebruikt, maar dat men vaak bedrogen uitkomt. Het is de behoefte van de klant die uitmaakt of voldoende kwaliteit wordt geleverd. Diensten worden niet 'impliciet' geleverd. Ze moeten expliciet worden gemaakt en gevraagd. 'Ervan uitgaan dat…' leidt doorgaans niet tot succes. Gebruik gaan maken van de cloud betekent dus eerst nagaan 'wat wil ik eigenlijk?' Dat is op zich geen nieuws, want een bedrijf dat zijn ICT ordentelijk wilde outsourcen of offshoren werd met dezelfde vraag geconfronteerd. Pas als helder is wat wordt gevraagd, kan assurance worden gegeven op de geleverde prestaties van de cloud-leverancier.

'Ervan uitgaan dat….' leidt doorgaans niet tot succes

Het is juist dit zelfonderzoek op de kwaliteitskenmerken, dat ondernemingen doet aarzelen om de cloud in te gaan. De belangrijkste oorzaken van deze aarzeling zijn de gewenste mate van beveiliging (de eerste drie kwaliteitskenmerken) en de vraag of de cloud-leverancier dat wel kan waarmaken.
In het zelfonderzoek mag een risk assessment niet ontbreken. De uitkomsten van een goede risicoanalyse zijn medebepalend voor het type cloud-dienst dat kan worden afgenomen en welke zekerheden men daarbij wenst. Gebaseerd op het bestaansrecht van een onderneming, het type informatie en informatievoorziening, de wet- en regelgeving waaraan men onderhevig is, de mate waarin men bereid is om risico's te lopen enz. wordt bepaald welke eisen en garanties worden gesteld aan de cloud-leverancier en welk type cloud-dienstverlening (bijvoorbeeld de keuze tussen public, hybrid of private cloud) het meest aan de eisen voldoet.

Elke zichzelf respecterende cloud-leverancier heeft een beveiligingsbeleid. Vaak wordt dat beleid en de uitvoering daarvan door derde partijen beoordeeld/geaudit. SAS70/ISAE 3402-verklaringen, ISO-certificaten 27001 en 90001 zijn verkrijgbaar. Hier zit de devil in the details. De scope van de verklaringen en certificaten moeten goed worden nagekeken. Deze moet minimaal beslaan wat uit de risicoanalyse geacht wordt van belang te zijn. Wellicht gaan in de (nabije) toekomst twee concept-standaarden daarbij helpen.

- ISO/IEC 27014 Information technology – security techniques – Information security governance framework.
- ISO/IEC 27036 IT security – security techniques – Guidelines for security of outsourcing.

Hoewel deze niet specifiek voor cloud worden ontwikkeld, zijn er voldoende raakvlakken. In onderzoek is een studie naar de wenselijkheid om aparte standaarden over deze onderwerpen met betrekking tot cloud computing te krijgen. Het is niet te verwachten dat deze er snel zullen zijn.
ISF helpt in het eerder genoemde rapport over de seven deadly sins of cloud computing met hanteerbare 'common baseline arrangements'.

Hindernissen

Is het bij outsourcing (doorgaans in eigen cultuur) al een opgave om tot sluitende afspraken te komen? Bij offshoring is dat nog een tandje erger. Taalproblemen, cultuurverschillen en als gevolg daarvan andere taakopvattingen spelen daarin een belangrijke rol. De overeenkomst tussen deze twee uitbestedingsvarianten (offshoring en outsourcing) is wel dat de leverancier aanwijsbaar is en dat de fysieke locaties en daarmee de jurisdictie ook duidelijk is. Bovendien wordt de dienstverlening 'op maat' aangeboden.
Daar komen de verschillen met cloud computing om de hoek kijken. De leverancier is wel duidelijk. Daarvan worden de diensten afgenomen en daarmee wordt een contract gesloten en een financiële relatie aangegaan. De locatie, en daarmee de jurisdictie, is echter niet altijd duidelijk. De essentie is dat de dienst (of diensten) word(t) en afgenomen naar behoefte (omvang, tijd), en dat die word(t)en ingezet vanuit een locatie van de leverancier die niet vooraf duidelijk hoeft te zijn. En dan spreken we nog maar niet over varianten waarbij sprake is van meerdere leveranciers.
Het tijd-, plaats- en omvangonafhankelijk werken is voor de leverancier alleen maar aantrekkelijk als het via gedeeld gebruik kan worden opgezet. Dit tijd-, plaats- en omvangonafhankelijk werken speelt in governance- en assurancevraagstukken een grote rol bij het overgaan naar cloud computing.
Binnen alle kwaliteitskenmerken zijn drie belangrijke vragen aan de orde. Hoe is de verdeling in verantwoordelijkheden? Hoe veilig is de afgenomen cloud-dienst? En hoe bewijsbaar is het? Afgeleide vragen zijn:

- De controleerbaarheid. Hoe volledig en aantoonbaar is het spoor van handelen? Ongeacht de geografische locatie en de omvang van de cloud-dienstverlening moet kunnen worden vastgesteld welke handelingen hebben plaatsgevonden, wanneer, door wie en met welke autorisatie;
- Jurisdictie. De wetgeving in verschillende landen en continenten hebben verschillende invalshoeken.

De Europese privacywetgeving is strikter dan die van de Verenigde Staten van Amerika en weer anders dan die in Azië. Het bekende voorbeeld: de Patriot Act geeft de Amerikaanse overheid gelegenheid gegevens in te zien c.q. op te vragen die op haar grondgebied of bij een Amerikaans bedrijf zijn opgeslagen. Bedrijven die de cloud in gaan moeten zich hiervan bewust zijn. Cloud-aanbieders weten dat natuurlijk ook en bieden om die reden de mogelijkheid om te kunnen kiezen op welk grondgebied, en dus onder welke jurisdictie, de data wordt opgeslagen. Hierover is nog een levendige discussie tussen overheden gaande.

- Separatie. Omdat de aanbieders gedeelde infrastructuren aanbieden, is het van belang dat de verschillende afnemers (aantoonbaar) uit elkaar gehouden moeten worden. Niemand zal willen dat ongeautoriseerden aan hun data kunnen komen.
- Continuïteit. Er moeten goede afspraken worden gemaakt over de wijze waarop continuïteit van dienstverlening kan worden gegarandeerd. Van de cloud-leverancier moet worden verwacht dat deze de dienst ononderbroken kan aanbieden. Internet is daarin een component, maar ook de data en/of de applicaties. De leverancier moet zekerheid geven dat de continuïteit (ook na een disaster in of bij de datacentra waar de data opgeslagen lagen) gegarandeerd is binnen afgesproken service levels. Een complicerende factor is hierbij de samenstelling van de dienstverlening en de verschillende schijven waarover deze tot stand komt.

Meerdere leveranciers, maar bijvoorbeeld ook het internet, spelen een belangrijke rol. Belangrijk in dit verband zijn afspraken en garanties over de continuïteit van afgenomen diensten. Nagegaan moet worden wat de strategie van de aanbieden-de partij(en) is om de continuïteit te waarborgen.

- Toegang. 'Wie mag waaraan komen?', is met eigen personeel al een moeilijk te beheersen vraagstuk. Naarmate de keten langer en ingewikkelder wordt, wordt dit een issue dat nauwgezet moet worden bekeken. Simpelweg alle verbindingen versleutelen is een belangrijke zaak, maar op zichzelf onvoldoende. Een goed ingerichte identity management oplossing, autorisatie policy en uitvoering daarvan is onontkoombaar.

Retransitie

Stel, uw bedrijf zit in de cloud, maar wil van leverancier veranderen. Welke zekerheden worden gegeven over de wijze waarop de dienstverlening door de cloud-leverancier wordt 'teruggegeven'? Met name over uw data. Is bekend welke data van u is? Welke classificatie het heeft en hoe en of het na teruggave wordt gewist? Waar staan de back-ups? Waar bevinden zich eerdere versies? Hoe omkeerbaar verloopt het verwijderen?

Vragen die niet pas moeten worden bedacht en opgelost als partijen uit elkaar gaan. Deze vragen dienen voorafgaand aan een cloud-contract te worden besproken, opgelost en vastgelegd. Toeval moet worden uitgesloten.

Zongarantie is niet te geven

Schijnt de zon, of schijnt hij te schijnen?

Iedereen die de cloud betreedt verwacht dat achter de wolken de zon zal schijnen. Het wordt goedkoper, makkelijker en zonder zorgen. De verleiding is groot om de wolken maar even te negeren en zich te focussen op de zon. Toch is het even nodig om door het wolkendek heen te gaan om daarna volop te kunnen genieten.

Om dit te kunnen bereiken is goede voorbereiding absoluut noodzakelijk. Teleurstellingen zijn onvermijdelijk als de cloud onvoorbereid wordt betreden (en in hoeveel bedrijven is dat sluipend al niet gaande?). Een goede voorbereiding in combinatie met leveranciers die hun eigen verantwoordelijkheid nemen, is goede afspraken te maken over het avontuur dat wordt aangegaan. Zongarantie is niet te geven, maar met een goede voorbereiding op weg naar de eindbestemming is de kans erop zeer aanzienlijk.

Bij het voorbereiden kan natuurlijk ook gebruikgemaakt worden van de diensten van bedrijven die helpen bij het proces om de cloud te betreden.

INFORMATIE-ASYMMETRIE IN DE BEVEILIGINGSMARKT

Dr. S. (Saïd) El Aoufi is werkzaam als senior consultant bij MetaPoint BV en is lid van de redactieraad van dit magazine. Saïd is bereikbaar via said.el.aoufi@metapoint.nl.

Softwarekwetsbaarheid is een zwakke plek in software die een beveiligingsrisico vormt. Kwetsbaarheden zijn over het algemeen het gevolg van programmeerfouten. Het doel van beveiliging in software is het waarborgen van vertrouwelijkheid, integriteit en beschikbaarheid van gegevens. Net zoals bij auto's is beveiliging bij software een intern en technisch gegeven. Het betreft de programmacode van het softwareproduct en schuilt dus in zekere zin 'onder de motorkap'. Potentiële kopers hebben er geen zicht op. Er is hierdoor sprake van asymmetrische informatie op de markt. Dit artikel gaat in op de informatie-asymmetrie binnen de beveiligingsmarkt.

Organisaties zijn in grote mate afhankelijk van hun informatiesystemen die een vitale rol spelen in, en deel uitmaken van hun bedrijfsprocessen. Met de snelle groei van de afhankelijkheid van organisaties van hun informatiesystemen vereist informatiebeveiliging steeds meer de aandacht. Regelmatig is in de kranten te lezen dat er nieuwe kwetsbaarheden worden ontdekt. Beveiligingsincidenten bezorgen de samenleving steeds meer financiële schade. Denk hierbij aan de waarde van het bedrijf, de winst, de aandeelhouderswaarde of de reputatie. Oorzaak is de groeiende cybercrime.
Veel auteurs zijn het erover eens dat een aanzienlijk deel van de cybercrime wordt mogelijk gemaakt doordat softwareprogramma's programmeerfouten bevatten [Viega & McGraw, 2005]. Door deze fouten wordt het mogelijk voor hackers om de applicaties op een andere manier te gaan gebruiken dan oorspronkelijk werd bedoeld door de ontwikkelaars. Als er binnen de markt veel concurrentie is, zullen bedrijven de ontwikkelde producten zo snel mogelijk op de markt willen zetten. Bedrijven verkorten het ontwikkelingstraject door minder tijd te besteden aan het testen. Het gevolg hiervan kan zijn, dat er producten op de markt komen die nog veel fouten en beveiligingslekken bevatten.
Er is veel literatuur te vinden over de technische aspecten van softwarekwetsbaarheden, maar weinig vanuit een economisch perspectief. Recente onderzoeken [El Aoufi , 2011] maken duidelijk dat informatiebeveiliging niet alleen een technisch probleem is, maar ook een onderwerp dat vanuit een economische invalshoek dient te worden benaderd. Een studie over softwarekwetsbaarheden is die van Camp & Wolfram (2000). Zij behandelen in hun artikel de middelen voor het verbeteren van de beveiliging van softwareproducten. Arora et al. (2003) bestudeerden de investeringsbeslissingen van leveranciers omtrent de beveiliging van hun producten en het tijdstip van het uitbrengen van nieuwe patches van bekende kwetsbaarheden. Deze studie toonde aan dat kwaliteit van softwareproducten en de investering door de softwareontwikkelaar in patch-technologie strategisch substituten zijn. De aanwezigheid van patch-technologie zorgt ervoor dat leveranciers de markt eerder betreden met softwarebugs. De studie laat zien dat leveranciers er voor kiezen patches later uit te brengen dan verantwoord is.

> Producten bevatten nog veel fouten en beveiligingslekken

Kwetsbaarheden in softwareproducten
Omdat bedrijven winstmaximalisatie nastreven, zullen zij de neiging hebben om te kiezen voor de oplossing die het meeste oplevert, ongeacht de kwaliteit of de beveiliging van de desbetreffende oplossing. Zaken zoals features, ontwikkeltijd en gebrek aan informatie spelen hierbij een rol.

Functionaliteit versus beveiliging
Commerciële software bevat ontwerp- en implementatiebugs die gemakkelijk voorkomen kunnen worden. Hoewel productleveranciers veiliger software zouden willen produceren, is er hiervoor geen stimulans. Het langer ontwikkelen van 'veilige' software heeft namelijk ook gevolgen voor het aantal features (functionaliteiten) dat het eindproduct uiteindelijk zal bevatten. Een veilig softwareproduct zal dus steeds een minimum aan features bevatten. Er is sprake van een uitruil tussen functionaliteit en beveiliging. De onderstaande Production Possibility Frontier (PPF, productiemogelijkhedencurve) geeft de combinatie aan van functionaliteit en beveiliging, binnen de beschikbare middelen.

De veronderstelling is dat de beschikbare middelen zoals het beschikbare budget, vast staan. Als onder die condities software wordt ontwikkeld, zal er sprake zijn

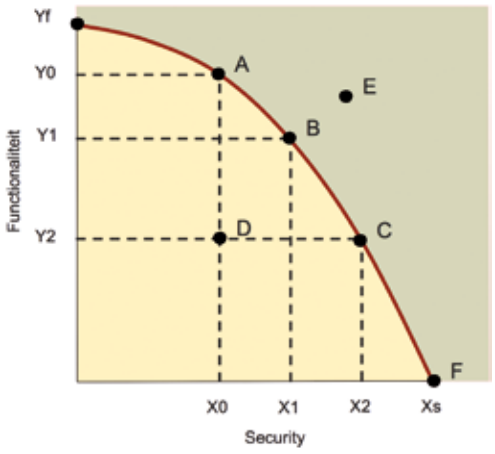


Fig. 1. PPF voor functionaliteit en beveiliging.

van een uitruil tussen beveiliging en functionaliteit. Deze uitruil houdt in dat, bij een vast budget, een keuze moet worden gemaakt tussen beveiliging en functionaliteit. Meer functionaliteit voor dezelfde prijs betekent minder beveiliging, terwijl een hogere mate van beveiliging alleen kan worden bereikt door de implementatie van minder functionaliteit. Zoals de nevenstaande figuur illustreert, zal om meer functionaliteit te produceren, de middelen moeten worden opgegeven die worden gebruikt voor het produceren van beveiliging (punt A). Als er meer beveiliging wordt toegevoegd in het informatiesysteem/applicatie (van X0 naar X1 of X2) (punt B en C) betekent het minder functionaliteit (van Y0 naar Y1 of Y2). De alternatieve kosten (opportunity costs of opofferingskosten) is wat er wordt opgegeven om iets anders te krijgen. De alternatieve kosten voor het produceren van een extra X0-X1-beveiliging is Y0-Y1 functionaliteit.

In de PPF zijn alle punten op de curve punten van maximale productieve efficiëntie (dat wil zeggen, dat er niet meer uitvoer kan worden behaald gegeven de input). Alle punten binnen de grens (zoals D) kunnen worden geproduceerd maar zijn productief inefficiënte. Alle punten buiten de curve (zoals E) kunnen niet worden geproduceerd met de beschikbare middelen.

Langere ontwikkeltijd

Veilige software produceren houdt in dat er rekening moet worden gehouden met het feit dat de tijd om veilige software te ontwikkelen veel hoger ligt dan de tijd die nodig is om software te ontwikkelen waarbij geen maximale aandacht wordt besteed aan het elimineren van kwetsbaarheden. Een goed beveiligingsontwerp kost tijd, en betekent waarschijnlijk ook gelimiteerde

Keuze softwareontwikkelaar om niet op voorhand in beveiliging te investeren

Voor de ontwikkeling van informatiesystemen wordt gebruikgemaakt van de Systems Development Life Cycle (SDLC). Dit is een model om op een gestandaardiseerde wijze de ontwikkeling van een informatiesysteem, dat voldoet aan de wensen van de organisatie, te volbrengen. Beveiliging dient in een vroeg stadium te worden meegenomen en in alles fasen van SDLC. Wanneer beveiliging niet in een vroeg stadium wordt meegenomen zal het oplossen van mogelijke bugs hogere kosten met zich meebrengen. Volgens een onderzoek van IBM blijkt dat:

- als fouten in de ontwerpfase worden gevonden, het oplossen van bugs X dollar bedraagt;
- als fouten in de implementatiefase worden gevonden, de kosten 6.5X zijn voor het oplossen van bugs;
- als fouten in de testfase worden gevonden, de kosten op 15X komen;
- als bugs in de productie gevonden worden dan komen de kosten op 100X.

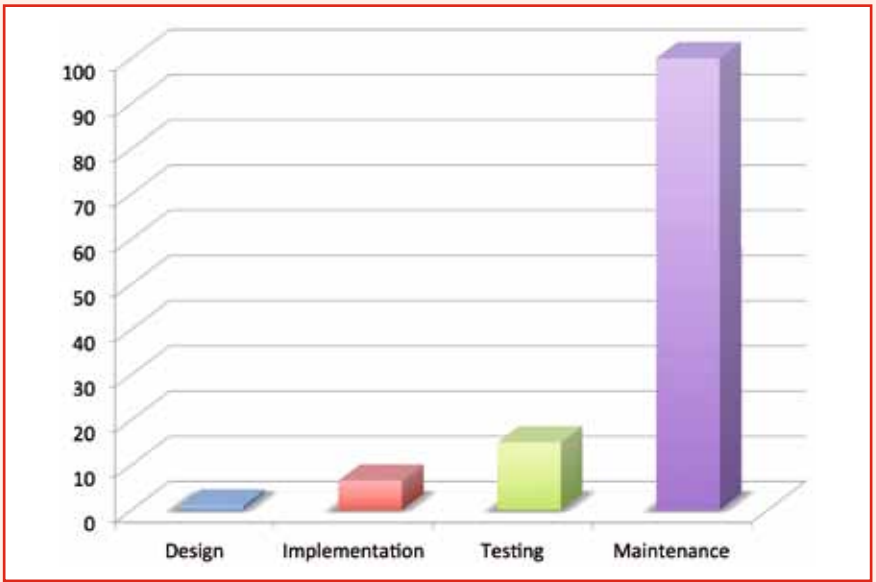


Fig. 2. Investeren in security in een vroeg stadium verlaagt de kosten voor het fixen van bugs (bron: [1]).

Om hogere kosten te voorkomen vanwege het oplossen van bugs dient beveiliging vanaf dag één mee ontworpen te worden. Alleen hierdoor wordt beveiliging een deel van het te ontwikkelen informatiesysteem. Denk hierbij aan het bouwen van een auto. Bijvoorbeeld, remmen en airbags worden mee ontworpen en niet achteraf ingebouwd. Als we daarom een vergelijking maken tussen de beveiliging van de auto's en de beveiliginginformatiesystemen is de eerste veel professioneler.

functionaliteit. Daarnaast kosten goede beveiligingstesten nog meer tijd. Investeren in beveiliging houdt voor de ontwikkelaar in dat het product later op de markt wordt gebracht tegen een hogere prijs. Zijn concurrent, die een zelfde product op de markt brengt maar minder belang hecht aan beveiliging, zal een lagere prijs kunnen vragen. Leveranciers geven daarom de voorkeur aan investeren in de zichtbare features in plaats van in beveiliging.

Voorbeeld: als leverancier A, software veilig en bug-vrij maakt, dan zullen de kosten hoger liggen en zal de tijd om het product te produceren langer zijn. Leverancier B laat dit in zijn voordeel werken door meer functionaliteit te bouwen en snel de markt te betreden.

Informatie-asymmetrie

In de economie houdt informatieasymmetrie zich bezig met de studie naar beslissingen van economische agenten in transacties, waarbij de ene partij over meer of over betere informatie beschikt dan de andere. Dit leidt tot een oneevenwichtigheid in macht in transacties. In 2001 werd de Nobelprijs voor de Economie toegekend aan George Akerlof, Michael Spence en Joseph E. Stiglitz voor hun analyses van markten met asymmetrische informatie[2].

Voorbeeld: verzekeringsmaatschappijen hebben te maken met asymmetrische informatie. De verzekerde is beter op de hoogte van de risico's dan de verzekeraar. De verzekerde is bijvoorbeeld beter op de hoogte van zijn/haar rijgedrag dan de verzekeraar. Als de verzekeringsmaatschappijen deze informatie tot hun beschikking zouden hebben, zou een goede chauffeur een lagere premie betalen dan een slechte chauffeur.

In 'The market for lemons (1970)' beschrijft Akerlof een productmarkt waarop de aanbieder meer weet over de kwaliteit van het product dan de koper. Akerlof illustreerde aan de hand van de tweedehands automarkt hoe de asymmetrische informatie ertoe kan leiden dat sommige markten ophouden te bestaan. 'Lemon' is de aanduiding voor een tweedehandsauto van minderwaardige kwaliteit.

Te late beveiliging leidt tot hogere kosten voor het oplossen van bugs

Volgens Akerlof gaat de kwaliteit van aangeboden auto's op een 'lemon'-markt constant achteruit, omdat de koper 'maar' een gemiddelde marktprijs wil betalen. Omdat de koper de goede en de slechte producten niet kan onderscheiden, zal er een gewogen prijs worden geboden. Het resultaat is dat de aanbieders van de betere auto's de markt zullen verlaten en de aanbieders van 'lemons' de markt zullen overspoelen.
De karakteristieken van de 'lemon'-markt doen zich ook voor op de beveiligingsmarkt. Omdat de koper niet in staat is verschil te maken tussen een veilig en een onveilig product, zal de prijs richting de onveilige producten gaan. De meer veilige producten zullen de markt verliezen, want de softwareontwikkelaar zal omwille van de 'lemon-markt' ervoor kiezen om niet op voorhand in beveiliging te investeren, maar pas na afloop van het ontwikkelproces. Hierdoor heeft de softwareontwikkelaar zekerheid dat zijn product winst zal opleveren en is hij bereid in beveiliging te investeren. Dit doet de ontwikkelaar door het regelmatig uitbrengen van upgrades, die hem van een verdere bron van inkomsten verzekeren. Voor de gebruiker is dit nadelig, omdat hij enerzijds met een onveilig product zit en wordt blootgesteld aan mogelijke beveiligingsrisico's en hij betaalt achteraf alsnog voor beveiliging wat al bij aanschaf inbegrepen had moeten zijn.

'Bug.'

Tot slot

De beveiliging van software is een onzichtbaar gegeven. De klant kan het verschil niet beoordelen tussen goede en slechte softwareproducten. Er is geen stimulans voor de ontwikkelaars om te investeren in de beveiliging van softwareproducten. Zowel aan de vraagzijde van de markt als aan de aanbodzijde worden oplossingen aangedragen voor het probleem van asymmetrische informatie. Aanbieders nemen vaak het initiatief tot het bieden van garanties ('niet goed, geld terug') en service na verkoop om daarmee de kwaliteit van hun product te signeren. Het opbouwen van een goede reputatie is daarbij van het grootste belang. De vraagzijde van de markt biedt eveneens oplossingen. De consument kan investeren in het zoeken naar informatie over de kwaliteit van de goederen of kan de prijs van het goed gebruiken als een kwaliteitsindicator. Ook kan de consument informatie kopen, bijvoorbeeld lid worden van CERT enz.

Referenties

[1] *Implementing Software Inspections, IBM Systems Sciences Institute*

[2] *The Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel 2001: Information for the Public: http://www.nobelprize.org/nobel_prizes/economics/laureates/2001/*

Literatuur

Akerlof, G.A., 2005, The market for 'lemons': Quality Uncertainty and the Market Mechanism, Explorations in pragmatic economics, New York: Oxford University Press, p. 27-38.

Arora, A., J. P. Caulkins, & R. Telang, Provision of Software Quality in the Presence of Patching Technology, Working paper, Carnegie Mellon University, 2003.

Camp, L. J., & C. Wolfram, Pricing security. In Proceedings of the CERT Information Survivability Workshop, Boston: CERT, 2000, p. 31–39.

El Aoufi, S., Information Security Economics, The Stationery Office UK, ISBN 9780117068728, 2011.

Viega, J., & McGraw, G., Building Secure Software. How to Avoid Security Problems the Right Way, New York , Addison-Wesley Professional Computing, 2001, p. 528.

TO TRUST IS TO ASSUME

HET VERTROUWEN, DE PRIMAIRE KWETSBAARHEID

Maurice Gittens CISA werkt 20 jaar als zelfstandig consultant met informatiemodelleren, informatieverwerking, informatiearchitecturen en informatiebeveiliging. Zijn passie is de structuur en beheersing van taal, informatie en betekenis. Hij is te bereiken via maurice@gittens.nl

De veronderstelling dat het vertrouwen, ook in de context van risicomanagement, een noodzaak is lijkt wijd verspreid. Deze opvatting ligt mijns inziens ten grondslag aan fundamentele misvattingen in opzet, bestaan en werking van risicomanagementsystemen. Als concreet voorbeeld beschouwen we onder meer PKI (Public Key Infrastructure). Een verbetering van PKI zal schetsmatig worden ontworpen door eenvoudig het concept van een trusted third party te elimineren.

Laten we om te beginnen ingaan op de essenties van het vertrouwen. Wat is vertrouwen nou eigenlijk? In dit artikel luidt de definitie van het vertrouwen: *'Een eenheid van het vertrouwen is datgene dat ontstaat als een onbewezen hypothese wordt verondersteld geldig te zijn. Niet het formuleren van een hypothese leidt tot het vertrouwen, nee, juist het toevoegen van de veronderstelling van geldigheid aan een onbewezen hypothese leidt tot het ontstaan van een eenheid van het vertrouwen.'* Deze eenheid noemen wij in dit artikel een vertrouwensrelatie.

To trust is to assume!

Uit deze definitie volgt onder meer:

- vertrouwen is veronderstellen;
- het verschil tussen het vertrouwen en het weten is het bewijs;
- als je in een bepaald verband over het kennen (of het weten) beschikt kan er in het betreffende verband het vertrouwen niet bestaan.

Uit deze definitie van het vertrouwen volgt ook een definitie van kennis. Deze luidt: *'Een eenheid van kennis ontstaat in alle situaties waar een hypothese wordt bewezen geldig te zijn.'* Uit het voorgaande is vast te stellen dat iedere vertrouwensrelatie in essentie een kwetsbaarheid is.

To trust is to be vulnerable!

Laten we, nu we toch op dreef zijn, definiëren wat we onder het beveiligen verstaan. Dit doen we langs twee sporen: 'feel good security' en 'effective security'.

1. Feel Good Security

Een definitie van risicomanagement waar het beveiligen wat mij betreft onder valt komt in de praktijk vaak neer op: *'het geheel aan maatregelen die we inzetten om veronderstelde kwetsbaarheden te adresseren.'* Uit deze definitie volgt vrij direct dat er in de praktijk veel placebo's als beveiligingsmaatregel worden ingezet.

> In de praktijk worden placebo's als beveiligingsmaatregel ingezet

Deze maatregelen leveren schijnveiligheid en voldoen doorgaans prima om de emotionele of bedrijfspolitieke waan van de dag gerust te stellen. Herkenbaar?

2. Effective Security

Een definitie van risicomanagement die mijns inziens de voorkeur geniet is juist gefundeerd op hypothesen die bewezen zijn. Risicomanagement is het geheel aan maatregelen die we inzetten om bewezen kwetsbaarheden passend te adresseren. Bij deze insteek worden vertrouwensrelaties (dus aannames) in beveiligingssystemen systematisch opgespoord en geëlimineerd. Kwetsbaarheden die overblijven zijn systemische kwetsbaarheden die ook zonder het bestaan van betreffende vertrouwensrelaties gelden. Onder het passend adresseren van deze systemische kwetsbaarheden verstaan we het behandelen van het risico (risk

treatment) zonder de inzet van het vertrouwen.

Voorbeelden van systemische kwetsbaarheden zijn:
- wat vliegt kan neerstorten;
- wat vaart kan zinken;
- wat geheim is kan openbaar worden;
- integriteit kan gecompromitteerd worden.

Voor systemische kwetsbaarheden geldt ten principale dat corresponderende gebeurtenissen kunnen optreden. Op basis van het bovenstaande definiëren we het concept van Effective Security als: *'Het geheel aan maatregelen die we inzetten om bewezen systemische kwetsbaarheden passend te adresseren.'*

Strong PKI: een toepassing van Effective Security

Het bovenstaande kan overkomen als een academische en/of filosofische uiteenzetting zonder praktische waarde. Dus de vraag: "Waartoe zou het in de praktijk kunnen leiden?" lijkt me legitiem. Op deze vraag gaan we in door op basis van bovenstaande denkwijze evidente verbeteringen voor PKI-certificaten af te leiden.

Zoals de lezer zal weten worden PKI-certificaten ondertekend door een Trusted Third Party (TTP, de Certificate Authority CA). We stellen in dit artikel in essentie dat de CA in zijn huidige vorm ongewenst is, juist omdat deze in bestaande PKI-systemen *trusted* zijn. Zie de conclusie van het artikel in IB 7 'PKI, geen mysterie en zeker geen magie' van Shaun.

Dit vertrouwen is onnodig en kan eenvoudig worden geëlimineerd door een certificaat door meerdere, het liefst onafhankelijke, CA-partijen te laten ondertekenen. Een certificaat voor bijvoorbeeld pvib.nl zou in dit geval niet door één trusted third party worden ondertekend maar in plaats daarvan door een aantal onafhankelijke third parties (let op het weglaten van het woord 'trusted').
Je zou het kunnen zien als een paspoort waar telkens een stempel door een andere CA op kan worden geplaatst.
Deze door meerdere CA's getekende certificaten wil ik *Strong Certificates* dopen.

Resilience

Het fijne van Strong Certificates is dat het compromitteren van één van de CA's die een certificaat hebben ondertekend niet hoeft te leiden tot de ongeldigheid van een certificaat. Per slot van rekening zijn er meerdere partijen die authenticiteit van de informatie in het certificaat onderschrijven.

Spoor aannames in beveiligingssystemen op en elimineer ze

De overheid en andere afnemers van DigiNotar-certificaten hadden in het geval dat er Strong Certificates werden gebruikt geen enkele disruptie van de dienstverlening hoeven ervaren en dat om de doodeenvoudige reden dat, in opzet, er geen single point of failure meer zou bestaan.
Het feit dat Strong Certificates het compromitteren van een CA zonder disruptie kunnen weerstaan maakt dat het vertrouwen in een CA ook niet nodig is. De kracht van het PKI-systeem wordt nog meer verbeterd wanneer de CA's ook voor hun eigen certificaten gebruikmaken van Strong Certificates. PKI op basis van Strong Certificates dopen we bij deze: Strong PKI!
Bonuspunten zijn te verkrijgen als we Strong PKI ontwerpen terwijl het niet kwetsbaar is voor het compromitteren van de gebruikte cryptografische algoritmiek. Al is het maar door certificaten te signeren met wezenlijk verschillende algoritmen.

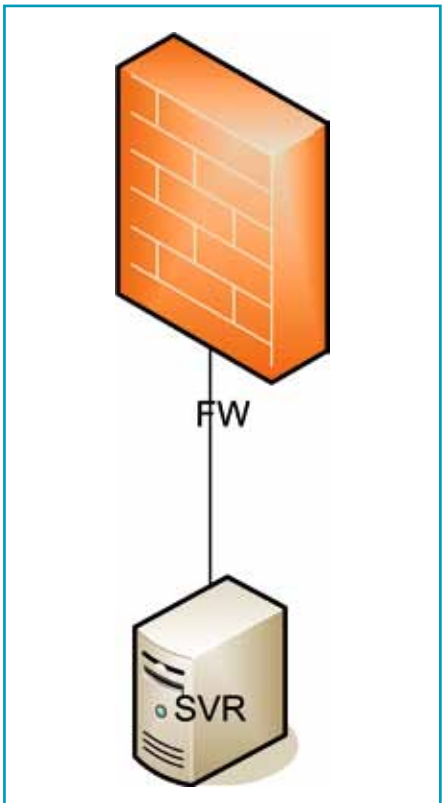
The bloody details

Ik wil de lezer de cryptografische details besparen die nodig zijn om deze Strong Certificates te realiseren. Met een knipoog stel ik: 'U kunt er op vertrouwen dat dit geen *rocket science* is'.
Een andere kwestie is de vraag wat het minimum aantal ondertekenaars is dat nodig is om een certificaat zijn geldigheid te laten behouden? Het antwoord op deze en andere gerelateerde vragen is wellicht een thema voor een andere artikel.
De PKI kwetsbaarheden en de mitigerende maatregelen die in dit artikel genoemd zijn, zijn ongetwijfeld al bij velen bekend. In het samenstel van belangen die spelen blijft de vraag of een variant van Strong PKI een commerciele realiteit zal blijken, open staan.
Tot zover het voorbeeld over PKI.

Een tweede voorbeeld: Effective Security en Netwerkarchitecturen

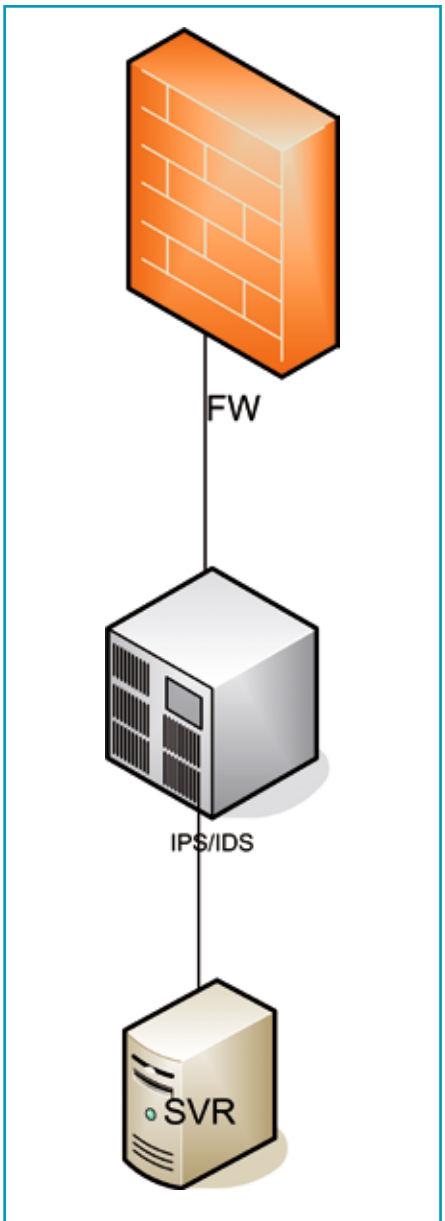
De toepasbaarheid van dit gedachtegoed op netwerkbeveiliging wordt aan de hand van het volgende zeer vereenvoudigde voorbeeld geïllustreerd.

In dit voorbeeld wordt de firewall FW ingezet om de server SRV te beschermen. We spreken af dat de firewall slechts HTTP-verkeer toelaat. De server SRV wordt zo geconfigureerd dat uitsluitend http-connecties worden geaccepteerd. Waarom is deze maatregel op de server nodig? Omdat het statistisch gezien een feit is dat over de levensduur van de server, de firewall ooit niet effectief zal blijken. We vertrouwen de firewall dus niet.



Firewall zonder IPS/IDS.

Dit voorbeeld kunnen we verder uitwerken. We erkennen het feit dat HTTP de informatie op de server blootstelt aan veel risico's. Dit risico adresseren wij door de inzet van IPS/IDS-technologie terwijl we de software stack op de server onderwerpen aan periodieke penetration testing en vulnerability scanning en bij in productiename en wijzigingen aan secure code review.



Firewall met IPS/IDS.

De laatste controle die we inzetten is event monitoring en state monitoring op alle componenten. Dit is een detectieve control die zal kunnen detecteren of andere controls ineffectief zijn. Het uitgangspunt bij het kiezen van de in dit voorbeeld ingezette controls is dat er niet 100% effective controls bestaan.

We gaan dus niet van het vertrouwen uit. In plaats daarvan ontwerpen we controls die, als samenstel, sterker zijn dan de som der delen. Het effect van deze controls is dus synergetisch.

Over kwantificeerbaarheid

Een belangrijk aspect van de definitie van het vertrouwen dat in dit artikel is gepresenteerd wil ik u niet onthouden.

To trust is to be vulnerable!

Dit wil zeggen dat een vertrouwensrelatie een kwetsbaarheid is. Omdat kwetsbaarheden in een beveiligingsarchitectuur te enumereren zijn, kunnen we de beveiligingsarchitecturen onderling vergelijken door de aantallen kwetsbaarheden tussen architecturen te vergelijken. Hoe minder vertrouwensrelaties, hoe minder kwetsbaar vanuit dit perspectief. De exploitatie van de kwantificeerbaarheid van kwetsbaarheden leidt tot een alternatieve definitie van het begrip risico en is mogelijk een onderwerp van een ander artikel.

Een vertrouwensrelatie is een kwetsbaarheid

Meer over het vertrouwen

Natuurlijk is er veel meer over het vertrouwen te zeggen. We denken hierbij bijvoorbeeld aan:

- het vertrouwen als asset;
- de stakeholders in vertrouwensrelaties;
- leverage en het vertrouwen;
- deze en andere aspecten van het vertrouwen vallen buiten de scope van dit artikel.

Resumerend

Dit artikel stelt dat het vertrouwen in de context van het risicomanagement de primaire kwetsbaarheid is. Deze opvatting volgt uit de realisatie dat het vertrouwen, zoals het in dit artikel is gedefinieerd, tot misconcepties in *opzet, bestaan en werking* van risicobeheersingsregimes leidt. Architecten die met het ontwerp van risicobeheersingssystemen belast zijn worden aangemoedigd om bewust om te gaan met het vertrouwen en dit zoveel mogelijk te vermijden.

Anders gezegd: Is niet *Effective Security* boven *Feel Good Security* te verkiezen?

SMARTPHONE SECURITY

Drs. ing. D.H. Hut, Security specialist bij TNO en E.G. Broenink M.Sc., Security specialist bij TNO

Volgens de IDC Worldwide Quarterly Mobile Phone Tracker groeit de wereldwijde smartphonemarkt naar verwachting 49,2% in 2011. Geen wonder want deze apparaten met hun krachtige processors en snelle videochipsets worden door leveranciers in een hoog tempo geüpgraded. Gecombineerd met een multi-touch besturingssysteem en een breed palet aan telecommunicatiemogelijkheden voor zowel korte als lange afstand zijn smartphones de 'one-stop-shop' aan het worden voor al uw mobiele computing- en communicatiewensen. Zowel thuis, onderweg, als op het werk. Het enorme aanbod aan apps biedt veel flexibiliteit en keuze voor een relatief lage prijs vergeleken met de traditionele software- en games-markt. De populariteit van smartphones is dan ook terug te zien in de verkoopcijfers van een aantal grote leveranciers.

Dat toch niet alles koek en ei is, blijkt uit de vele nieuwsberichten op security georiënteerde websites en in magazines. Moet u zich als gebruiker zorgen maken over de beveiliging van uw smartphone? En dan bedoelen we dit in de brede zin. Niet alleen de informatie die u erop zet of die u ermee consumeert of produceert maar bijvoorbeeld ook de informatie die ontstaat uit de sensoren of het gebruik van bepaalde applicaties of specifieke functies.
In dit artikel wordt aan de hand van enkele voorbeelden toegelicht met welke beveiligingsproblemen gebruikers van smartphones te maken kunnen krijgen. Ook worden enkele zowel bestaande als nieuwe security-ideeën beschreven die als tegenmaatregel kunnen worden ingezet om de smartphone veiliger te maken. Daarbij moet wel worden opgemerkt dat sommige maatregelen wellicht wat te ver gaan voor de gemiddelde smartphone-gebruiker.

Achtergrond

Waar een telefoon vroeger uitgeleverd werd met een beperkt aantal simpele basisfuncties, bieden smartphones veel functionaliteit. Mede daardoor zijn ze vergelijkbaar geworden met personal computers. Beide zijn opgebouwd volgens een relatief open 'verticale stack' van hardware en software (fig. 1) en op beide platformen is veel software beschikbaar van externe partijen.

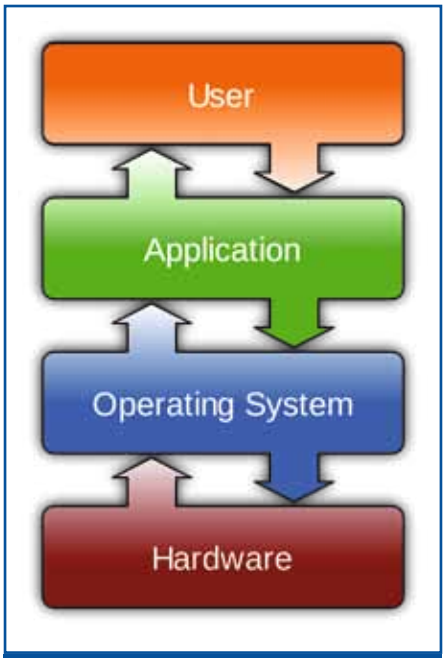


Fig. 1. Verticale stack.

Verticale stack

In elke laag van de stack kunnen, afhankelijk van het type smartphone, verschillende leveranciers actief zijn. Voor het besturingssysteem gebruiken fabrikanten soms hun eigen implementatie en soms een versie van een derde partij, eventueel aangevuld met een user-interface schil.

Vele apps

Gebruikers kunnen allerlei apps op hun smartphone installeren. Soms gaat dat via een online 'app'-winkel zoals Google's Android Market, Apple's iPhone App Store of Amazon Appstore. Soms kunnen gebruikers apps buiten zo'n winkel om installeren. De markt van apps is relatief open, in de zin dat externe partijen apps kunnen ontwikkelen en deze kunnen aanbieden in de verschillende app-winkels.

Veel data

Mede doordat smartphones zijn uitgerust met sensoren die waardevolle informatie kunnen opleveren, is de hoeveelheid gebruikersinformatie op een smartphone sterk gestegen. Ook kunnen smartphones gebruikt worden als mobiele storage devices, vergelijkbaar met bijvoorbeeld een usb-stick, voor het opslaan van foto's, filmpjes, muziek, e-mail, elektronische boeken enz.

Deze aspecten kunnen beveiligingsrisico's introduceren. De flexibiliteit rondom het kunnen installeren van apps is prettig voor de gebruiker maar schept ook verplichtingen. Een gebruiker moet aan de hand van de door een app aangevraagde permissies kunnen inschatten wat de consequenties zijn van het installeren van een app. De grote hoeveelheid gebruikersdata op de smartphone inclusief sensorinformatie zoals locatie zorgt ervoor dat een gebruiker een steeds grotere 'aanvals-

> Moet u zich zorgen maken over de beveiliging van uw smartphone?

oppervlakte' krijgt waarvan misbruik gemaakt kan worden. De verschillende aanbieders van de app-winkels ten slotte hanteren verschillende niveaus van kwaliteitscontrole waardoor kwaadaardige apps al dan niet doorgang vinden via een app-winkel naar de gebruiker.

Beveiligingsrisico's

Gebruikers van smartphones kunnen worden geconfronteerd met beveiligingsproblemen in allerlei categorieën. We schetsen kort enkele voorbeelden en verwijzen per categorie naar gevallen uit de praktijk op basis van artikelen in de media.

Toegang tot microfoon, camera of locatie

Door het ongemerkt aanzetten of op een andere manier misbruiken van de microfoon [1] of camera [2] is het mogelijk dat een aanvaller telefoongesprekken of omgevingsgeluid kan afluisteren of foto's in handen krijgt. Ook is het mogelijk dat locatiegegevens worden doorgestuurd naar derden doordat de GPS-sensor wordt uitgelezen [3].

Flexibiliteit installeren apps prettig, maar schept ook verplichtingen

Ongewenst bellen of sms'en

Een spelletje dat rondgaat voor smartphones, blijkt in werkelijkheid kwaadaardige software te zijn dat gebruikers met hoge kosten opzadelt door te bellen naar dure nummers [4].

Afluisteren inloggegevens, wachtwoorden en transactiecodes

De uit de pc-wereld bekende kwaadaardige software 'Zeus' heeft de overstap naar smartphones gemaakt en steelt toetsaanslagen en inloggegevens [5]. De malware SpyEye heeft een mobiele variant en onderschept sms'jes met tan-codes en stuurt die naar een externe server [6].

Een smartphone kan op verschillende manieren geïnfecteerd raken met kwaadaardige software. Bijvoorbeeld door het installeren van een kwaadaardige app. Soms worden bekende apps gekopieerd en opnieuw in een app store gezet maar pas nadat ze zijn voorzien van kwaadaardige functies. Soms is het openen van een link in een sms of e-mail of het surfen naar een kwaadaardige website al genoeg. Ook kan in de firmware zelf al ongewenste functionaliteit zitten [7, 8].

Voor wat betreft de security-prestaties van de verschillende mobiele platformen beschikken wij niet over onafhankelijke data om een goed vergelijk te kunnen maken. Symantec, een grote aanbieder van security software, heeft in een whitepaper [9] de verschillende sterke en zwakke punten van zowel iOS als Android vergeleken. De conclusie is dat mobiele devices productiviteit verhogen maar ook nieuwe risico's introduceren. Volgens een rapport [10] van McAfee (peildatum 2-2011), een andere grote aanbieder van security software, is kwaadaardige software voor Android OS sterk in opkomst en is Android OS nu het meest aangevallen platform. Lookout, een bedrijf dat zich richt op het leveren van smartphone security software, noemt in haar Mobile Threat Report 2011 [11] dat de hoeveelheid met 'malware' geïnfecteerde Android apps gestegen is van 80 apps in januari 2011 tot meer dan 400 apps in juni 2011.

Conclusie: mobiele devices verhogen productiviteit en introduceren nieuwe risico's

Maatregelen

Voor het preventief voorkomen of ten minste voor het kunnen detecteren van de beschreven beveiligingsproblemen is de gebruiker vooral afhankelijk van systeemupdates van de leverancier en de kwaliteitscontrole van de app winkels. Virusscanners zoals we die kennen uit de pc-wereld zijn langzaam in opkomst voor smartphones maar het is nog maar de vraag wat dit type product voor gevolgen heeft

voor de performance van de smartphone en de accuduur. Er zijn echter ook andere beveiligingsmaatregelen denkbaar die minder belastend zijn voor de smartphone zelf maar meer inspanning vereisen van de gebruiker.

Runtime permissiemodel

Sommige smartphones vragen de gebruiker tijdens de installatie van een app akkoord te gaan met bepaalde permissies die een app nodig zegt te hebben. Veel apps vragen echter teveel rechten en bovendien geven veel gebruikers gewoon toestemming voor alles wat een app vraagt. Een mogelijke verbetering zou zijn om niet bij installatie om permissies te vragen, maar een 'runtime' permissiemodel te gebruiken waarbij de gebruiker meer dynamisch kan toestaan of een app bijvoorbeeld bij de adressenlijst of bij de GPS mag komen. Bij deze oplossing bestaat wel het gevaar dat gebruikers continu om input worden gevraagd.

Lockdown

In het geval van diefstal kan het wenselijk zijn om de smartphone te kunnen locken of wissen op afstand. Er zijn apps verkrijgbaar die deze functionaliteit bieden zoals MobileIron, soms in combinatie met een website of soms met een enterprise server binnen een bedrijfsomgeving.

> Veel gebruikers geven toestemming voor alles wat een app vraagt

Custom firmware

Personal computers kunnen allerlei variaties aan besturingssystemen draaien en sommige daarvan hebben een expliciete focus op beveiliging. Ook voor Android smartphones ontstaan speciale varianten van dit besturingssysteem met specifieke security en/of privacy features die niet in de oorspronkelijke versie zitten.

Conclusie

De vele referenties over kwaadaardige software voor smartphones zijn een indicatie dat gebruikers geconfronteerd kunnen worden met beveiligingsproblemen. Het Android OS platform laat een sterke stijging zien in de hoeveelheid malware. Er worden echter ook, net als bij personal computers, beveiligingsmaatregelen ontwikkeld. Het is de vraag hoe deze markt zich gaat ontwikkelen. Volgt de smartphone-markt haar grotere broer, de personal computer-markt, in de ontwikkeling van virusscanners en firewalls of zullen andere type maatregelen tegen kwaadaardige software noodzakelijk gaan worden?

Referenties

1. New apps hijack the microphone in your cell phone to listen in on your life, 19 april 2011, http://info-wars.org/2011/04/19/new-apps-hijack-the-microphone-in-your-cell-phone-to-listen-in-on-your-life/

2. Mobile Malware Threats Grow! Now They can Steal Photos From Your Phone, August 22, 2011, http://slashnext.com/2011/08/mobile-malware-threats-grow-now-they-can-steal-photos-from-your-phone/

3. Mobile Apps Invading Your Privacy, 5 april, 2011, www.veracode.com/blog/2011/04/mobile-apps-invading-your-privacy/

4. Trojan jaagt mobiele bellers op torenhoge kosten, 9 april 2010, www.security.nl/artikel/33007/1/Trojan_jaagt_mobiele_bellers_op_torenhoge_kosten.html

5. Don't bank on your phone – it could be hacked by Zeus, 22 July 2011, www.guardian.co.uk/money/2011/jul/22/smartphones-hacked-zeus-malware

6. Android-malware steelt sms'jes van je bank, 15 september 2011, www.zdnet.be/news/131236/android-malware-steelt-sms-jes-van-je-bank/

7. Apple sued over iPhone location tracking, 25 april 2011, www.theregister.co.uk/2011/04/25/apple_sued_for_location_tracking

8. Google faces $50 million lawsuit over Android location tracking, 1 mei 2011, http://arstechnica.com/tech-policy/news/2011/04/google-faces-50-million-lawsuit-over-android-location-tracking.ars

9. The Current State of Mobile Device Security, Symantec, 28 Jun 2011, www.symantec.com/connect/blogs/new-symantec-research-current-state-mobile-device-security

10. McAfee Threats Report: Second Quarter 2011, McAfee Labs, www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2011.pdf

11. 2011 Mobile Threat Report, Lookout Mobile Security, August 2011, www.mylookout.com/mobile-threat-report

SCHRIJF U NU IN ALS VIP VAN INFORMATIEBEVEILIGING
EN UW DAG IS GEHEEL GRATIS!

8e editie

IT & Information Security

Voorkom reputatieschade

Donderdag 2 februari 2012
Congrescentrum 1931, 's-Hertogenbosch

Waarom mag u dit congres niet missen:

- 300 aanwezige vakgenoten
- Uitgebreide netwerkmogelijkheden
- Inspirerende visie verhalen en praktijkvoorbeelden
- Beursvloer met 20 aanbieders en specialisten
- Dagvoorzitter ing. John Hermans, Partner, KPMG IT Advisory

VIP Vermeld de VIP-code 8789/07 bij uw inschrijving. Alleen dan is uw dag geheel gratis met lunch en parkeerkaart. Uitsluitend eindgebruikers kunnen zich als VIP aanmelden.

security.heliview.nl

DENIAL OF SERVICE AANVALLEN (2)

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.

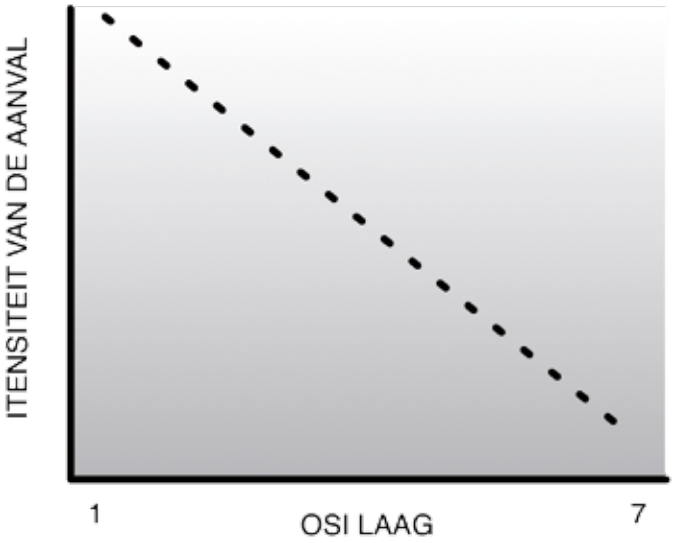
U hebt een op het internet ontsloten platform. En alle standaard beveiligings- en performancemaatregelen zijn getroffen. Toch blijft er een risico op aanvallen die uw dienstverlening lam kunnen leggen, zogenaamde (Distributed) Denial Of Service Attacks. In een vorig artikel ging ik in op aanvallen die redelijk eenvoudig zijn af te slaan. In dit artikel belicht ik graag een paar attacks die lastiger zijn af te weren. Ik zal hierbij niet elke aanval specifiek belichten, maar ingaan op de methodieken die worden gebruikt.

Op vrijwel elke I(C)T-opleiding wordt het Open Systems Interconnection, ofwel het OSI-model uitvoerig uitgelegd. Helaas beperkt de uitleg zich vaak tot de individuele lagen en blijft de correlatie tussen de lagen vaak onderbelicht. Kwaadwillenden zoeken juist vaak in deze afhankelijkheden naar mogelijkheden om problemen te veroorzaken.
Even kort het OSI-model. Dit model beschrijft welke lagen er noodzakelijk zijn om (van bekabeling tot aan de gebruikerstoepassing) informatie te versturen over een netwerk. Het voert te ver om individueel alle lagen te gaan benoemen, maar om vast te stellen hoe veilig een omgeving is en hoe een omgeving mogelijk tegen aanvallen te beschermen is, is gedegen kennis van de onderlinge interactie van het OSI-model essentieel. Met een aanval is elke laag afzonderlijk uit te schakelen, maar belangrijker is dat een aanval verstrekkende gevolgen kan hebben omdat de diverse lagen als een keten zijn gekoppeld.

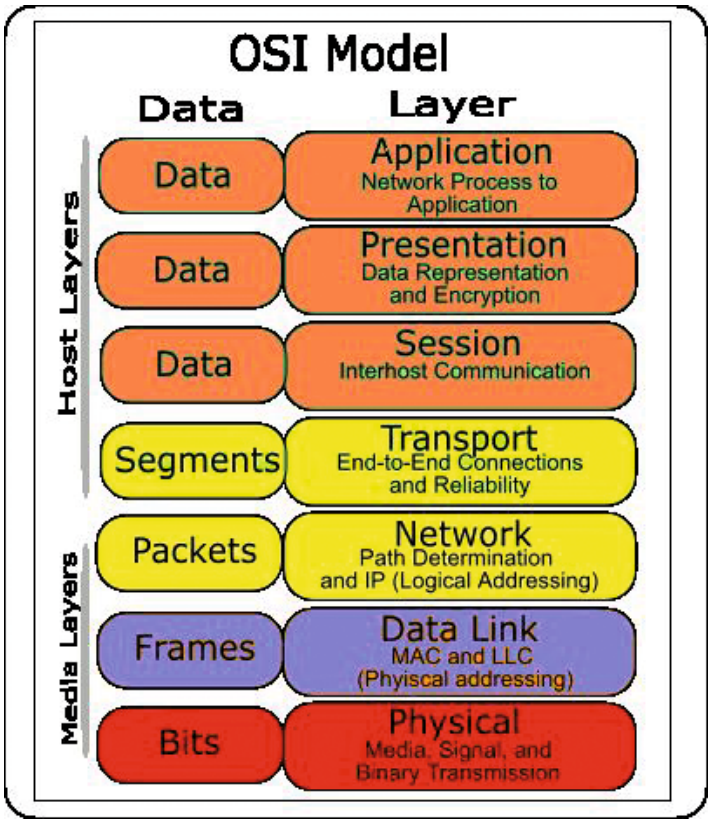
De meeste en meest lastige aanvallen vinden plaats op de lagere niveaus zoals de netwerk- of transportlaag. Interessant, in ieder geval vanuit technisch oogpunt, is dat deze aanvallen voor de aanvaller meestal relatief eenvoudig te initiëren zijn, maar voor het doelwit erg lastig zijn om tegen te houden. De complexiteit zit hem veelal in het volume. Het onderstaande diagram illustreert dit.

Helemaal onder in het OSI-model bestaan er diverse 'control'-protocollen. Deze protocollen hebben voornamelijk als doel om het internetverkeer in juiste banen te leiden of om bijvoorbeeld in diagnostische informatie te kunnen voorzien over bepaalde infrastructuren. Omdat deze berichten bedoeld zijn om het verkeer in de juiste banen te leiden, zijn ze ook heel interessant voor een aanvaller om te manipuleren en zo het verkeer te verstoren. Tegenwoordig zijn vrijwel alle apparaten die die controleprotocollen ondersteunen beveiligd tegen manipulatie van dergelijke berichten. Deze beveiliging vormt echter meteen het grootste probleem. Want wanneer er op heel grote schaal gemanipuleerde pakketjes worden verstuurd, is het ontvangende apparaat alleen nog maar bezig met het doorgronden van de kwaliteit en

Aanvallen op netwerk- of transportlaag meest complex



Aanvallen van dit niveau zijn vaak gebaseerd op zwakheden in de lagere protocollen.



Gegevenssoorten binnen het OSI-model.

de toepasbaarheid van de pakketjes. Het gevolg is dat het apparaat geen resources meer overhoudt om verder verkeer netjes af te werken.

Iets hoger in het OSI-model zit het TCP-protocol. Dit protocol wordt onder andere voor het transport van http (websites) en smtp (mail) gebruikt. Het TCP-protocol is 'connection based', hetgeen wil zeggen dat er een logische verbinding wordt gelegd tussen twee onderdelen. Dit betekent dat er allerlei extra informatie wordt gecommuniceerd over het maken van de verbinding, de manier waarop pakketten heen en weer worden verzonden en over hoe en wanneer de verbindingen worden beëindigd. Daarnaast is het TCP-protocol 'stateful', wat inhoudt dat er tijdens de verbinding allerlei relevante informatie wordt uitgewisseld over de kwaliteit ervan. Dit maakt TCP een zeer betrouwbare vorm van communiceren. Helaas introduceert deze handelswijze ook problemen. Veel DDoS-aanvallen zijn er namelijk juist op gericht om al deze 'extra' informatie te verstoren om zo een bepaalde dienst plat te leggen. Aanvallen als SYN, RST/FIN, ACK of SYN-ACK floods sturen malafide pakketjes bij het initiëren, communiceren of beëindigen van een TCP-verbinding. Een SYN flood stuurt bijvoorbeeld heel grote hoeveelheden verzoeken naar een server om een sessie aan te gaan. De server reserveert na het ontvangen van een SYN-verzoek resources die vervolgens nooit worden gebruikt. Een overvloed aan reserveringen kan ertoe leiden dat er voor nieuwe legitieme verbindingen geen ruimte meer is. Een lastig probleem. Vaak wordt er relatief weinig netwerkverkeer gegenereerd maar zijn de gevolgen dat een omgeving compleet wordt uitgeschakeld. Ook het identificeren van de aanvaller is moeilijk tot onmogelijk. Aanvallers gebruiken vaak gespoofte afzender IP-adressen. In dat geval is de afzender-header op het pakketje vervangen door een random IP-nummer, dus niet het werkelijke adres van de aanvaller.

Gaan we nog hogerop in het OSI-model dan worden vaak de zwakheden in applicatieprotocollen misbruikt. Een van de meest gebruikte protocollen van het moment is HTTP, met als 'veilige' en versleutelde tegenhanger HTTPS. Beide protocollen worden gebruikt voor het weergeven van websites en het doen van online transacties. Zoals al werd aangeven, maakt HTTP(s) ook gebruik van TCP, waardoor die diensten dus gevoelig zijn voor de zwakheden van het transmission control protocol. Daar bovenop introduceren ze nog extra zwakheden. HTTP biedt bijvoorbeeld de mogelijkheid tot het 'open houden' van een verbinding. In plaats van dat een gebruiker voor elk verzoek een nieuwe verbinding met de server maakt, wordt zoveel mogelijk een bestaande verbinding gebruikt. In principe is dit een mooie methode om sites sneller te maken, want het maken van een verbinding kost nou eenmaal tijd. Maar deze methode leidt ook tot een enorm DDoS-risico. De aanvaller kan tijdens een aanval namelijk grote hoeveelheden HTTP 1.1 sessies aanvragen. De server moet al deze verbindingen beschikbaar houden, want hij 'weet' dat er mogelijk meerdere verzoeken volgen over die verbindingen. Al snel raakt de server door zijn resources heen en is hij niet meer bereikbaar. Dit soort aanvallen worden ook wel met de term 'VERB session' aangeduid. Ook deze aanval is relatief eenvoudig in te zetten. Er is weinig bandbreedte

DNS-risico's vaak onvoldoende belicht

nodig, terwijl ook de terugkerende bandbreedte laag blijft. Er worden immers geen pagina's teruggestuurd.

Een protocol waarvan vrijwel alle internetdiensten afhankelijk zijn, is het DNS-protocol. Dit vormt in de keten van beschikbaarheid voor een webplatform dan ook een essentiële en zeer kritische schakel. Een schakel die over het algemeen volledig over het hoofd wordt gezien. DDoS-bescherming krijgt gezien de toename in het aantal aanvallen steeds meer aandacht. Bedrijven kopen verschillende soorten apparatuur die ze zouden moeten beschermen tegen een veelvoud van aanvallen. Vaak staat dergelijke apparatuur specifiek voor de webapplicatieomgeving. Men vergeet echter de afhankelijkheid van DNS. Immers, wat gebeurt er als de eindgebruiker niet langer uw domeinnaam kan vertalen naar het werkelijke adres van de server? Of wat als een DNS-server door extreme loads vergiftigd (poisoned) wordt, waardoor een servernaam niet langer naar uw infrastructuur verwijst maar naar de servers van een aanvaller? Voordat een platform enigszins als veilig mag worden beschouwd, moeten al deze componenten worden bekeken en beveiligd.

In mijn vorige artikel noemde ik per soort aanval een methode van bescherming. Met deze complexere aanvallen ligt het helaas iets minder eenvoudig. Aanvallen zoals de hiervoor genoemde VERB session attacks zijn nog wel op te lossen door het kiezen van de juiste webserversoftware en een nauwkeurig opgezette configuratie. Maar bij hoge volumes wordt het altijd ingewikkelder. Vaak zijn dan de enige oplossingen specifieke apparaten die goed zijn in twee dingen. Ten eerste moeten ze hoge volumes verkeer kunnen 'doorvoeren'. Daarnaast moeten ze in staat zijn dit verkeer real-time te analyseren en op basis van een breed scala aan algoritmen kunnen beslissen om bepaalde delen in het vervolg te gaan blokkeren.

DOS aanvallen relatief eenvoudig uit te voeren

Dergelijke apparaten vragen om veel expertise. De configuratie is complex en tijdens een aanval zal er nog het nodige moeten worden bijgesteld.

Uit wat we eerder schreven, blijkt wel dat (D)DoS aanvallen relatief eenvoudig zijn. Het is dus bijzonder dat er naar verhouding weinig (D)DoS-aanvallen plaatsvinden. Dit soort attacks zal in de toekomst echter gaan toenemen en voor vele partijen tot verstoring leiden van een steeds belangrijker deel van de bedrijfsvoering. Een substantieel deel van (D)DoS-preventie is te realiseren door een aantal basisstappen te doorlopen. Het OSI-model is hierbij voor de analyse altijd een goede leidraad, omdat het prima weergeeft welke onderdelen er zijn en welke afhankelijkheden ze hebben met elkaar. Als blijkt dat een omgeving zeer belangrijk is en dat het niet beschikbaar zijn ervan veel geld of zelfs mensenlevens kost, dan doet de betrokkene er goed aan om een partij in te schakelen met voldoende kennis om dergelijke risico's tot een minimum te beperken.

ACHTER HET NIEUWS - VOORUITBLIK 2012

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.

Deze keer in Achter het nieuws een vooruitblik op het nieuws van volgend jaar. Redacteuren gaan in op trends die zij het komende jaar zien doorzetten: opkomende kwetsbaarheden, beveiligingstrends of ICT-trends met beveiligingsgevolgen.

Lex Borger:
Jarenlang was Cloud Computing dé trend, maar een te vaag begrip. De opvolger is Big Data. Ook hier de nodige vaagheid, maar wat wel duidelijk is, is dat met meer data de mogelijkheden tot aggregatie van informatie groeien. Al zal hier een slimmere rekenkracht nodig zijn omdat het volume groeit. Vooral analysemogelijkheden van Big Data zullen groeien, met het bijbehorend misbruik van die mogelijkheden. Andere huidige trends: BYOD (Bring Your Own Device), mobile computing en het nieuwe werken gaan helemaal in elkaar op. ICT wordt een commodity. De eerste grote bedrijven zullen ICT de deur uit doen. Beveiliging wordt dan formeel en contractueel geregeld. Is dat beter of slechter? Initieel zie ik het eerder somber in omdat we met zijn allen nog moeten leren hoe dit in de praktijk moet. En dat in een tijd dat kosten nog steeds onder druk staan. Een ander aspect vind ik moeilijk te peilen: Aan de ene kant wordt er aanhoudend bespaard in de ICT-sector, aan de andere kant worden er tekorten aan opgeleid personeel voorspeld. Die twee aspecten zullen elkaar waarschijnlijk opheffen. Eén ding staat voor mij vast: we hebben nog zat goed opgeleide beveiligingsexperts nodig.

Maarten Hartsuijker:
Wat hebben Sony, Cheaptickets, DigiNotar, SIM, RSA, Lockheed Martin en de nucleaire reactor in Bushehr met elkaar gemeen? Voor informatiebeveiligers is deze vraag natuurlijk een open deur. 2011 werd gekenmerkt door de ene high-profile hack na de andere waardoor overheden en bedrijven dit jaar pijnlijk met de neus op de beveiligingsfeiten werden gedrukt.
Als ik in mijn glazen bol kijk, dan vermoed ik dat dit hack-geweld nog even aanhoudt. 2012 zou een jaar moeten zijn waarin bedrijven orde op zaken stellen. We zullen actiever moeten zijn in het beschermen van kernsystemen en informatie die klanten ons toevertrouwen. Dit betekent veiliger ontwerpen en bouwen en achteraf goed testen. De strijd om de tablets en smartphones onder botnet-herders zou in 2012 wel eens in alle hevigheid los kunnen barsten. Deze desktopvervangers worden steeds intensiever gebruikt. Beveiligingsbarrières worden geslecht om de gebruikersvriendelijkheid van deze alleskunners te behouden en dat maakt ze natuurlijk een lekker hapje voor een cybercrimineel. In alle eerlijkheid: wie kan er nou in de toekomst kijken? Het enige dat ik weet is dat ik als vakidioot uitkijk naar alles wat ons in 2012 weer brengt.

Aart Jochem:
Wat brengt 2012 op het gebied van informatiebeveiliging? In ieder geval een nieuw nationaal cyber security centrum, dat op 1 januari van start gaat. Dit centrum is gericht op het verhogen van de weerbaarheid tegen allerlei cyberbedreigingen. Dat gebeurt samen met publieke en private organisaties, waarbij informatie en expertise bij elkaar worden gebracht, the best of both worlds. Maar ik denk ook dat we zwaarder weer krijgen als beveiligers. Er zullen nog een aantal organisaties worden geconfronteerd met ernstige hacks. We hebben afgelopen jaar een paar keer gezien hoe de staat van de beveiliging van informatie in werkelijkheid is, zoals RSA, de DigiNotar-case en Lektober. Ook hebben hackers laten zien dat met een beetje aandacht en doorzettingsvermogen ze tot achter in een corporate netwerk kunnen doordringen. CIO's: watch your back! Als laatste verwachting voor 2012 denk ik dat het PvIB met het nieuwe bestuur en de nieuwe bestuursvorm en aanpak wat meer zichtbaar gaat worden buiten de beroepsgroep. En dat is niets te vroeg, gezien mijn tweede verwachting!

André Koot:
Ik wens u een voorspoedig 2012. Naast hacken, cracken, en lekken, staat ons meer te wachten. Ten eerste, nieuwe oplossingen voor onder andere Trust in de Cloud. Na het DigiNotar-debacle is de security-gemeenschap op zoek naar nieuwe, veiligere oplossingen voor het vertrouwen van digitale identiteiten, services en websites. En vooral ook om die op een eenvoudige en transparante manier in gebruik te kunnen nemen. Ik verwacht daar positieve resultaten van. Naast deze technische en architecturale verbeteringen denk ik dat er betere 'governance'-oplossingen zullen ontstaan. Daarin zal duidelijk worden wat de ANSI- en ETSI-standaarden inhouden, hoe providers daarmee om moeten gaan en wat wij daar per saldo aan hebben. Binnenkort zal wel duidelijk worden wat de waarde is van Trust. In dat kader verwacht ik ook een nauwere samenwerking tussen security professionals, auditors en toezichthouders. Ten tweede: ik verwacht een toename van het gebruik van Open Standaarden. Flash wordt niet lang meer ondersteund, en ook Silverlight lijkt zijn langste tijd te hebben gehad. Allebei als gevolg van de overstap op HTML5. De impact is nog nauwelijks in te schatten, maar minder gesloten oplossingen betekent enerzijds minder kopzorgen (wat fietst er over onze lijntjes), anderzijds levert dat nieuwe hoofdpijn op: zijn onze fietspaden nog wel deugdelijk? 2012 wordt een mooi jaar!

IIR ICT in samenwerking met webwereld

Leden van het PvIB krijgen € 400,- korting op de deelname prijs

Vermeld uw PvIB nummer + de naam van uw organisatie

Masterclass Informatiebeveiliging

Voorkom datalekken en reputatieschade

Verscherp uw beveiligingsbeleid aan de hand van praktijkkennis van Nederlands beste IT Security goeroes

Dr. Ir. Paul Overbeek RE, Partner OIS Information Risk & Security Management

Voorkom menselijk falen en creëer maximaal informatie veiligheidsbewustzijn.
Praktijkcasussen: Dilemma's Social Media en regievoering bij uitbesteding

Mr. Ir. Arnoud Engelfriet, ICT Jurist

Houd u aan de regels: Pas de wet computercriminaliteit, de Wet bescherming persoonsgegevens en privacy toe in de praktijk.
Praktijkcase: Computercriminaliteit of digitaal protest?

Tom Sanders, Hoofdredacteur Webwereld

Hoor alle achtergronden van spraakmakende lekken en trek hieruit de lessen.
Discussieleider tijdens praktijkcasussen.

Brenno de Winter, IT Beveiliging Journalist

Hands-on Hacken en Lekken met Brenno
Praktijkcasussen: OV-Chipkaart, Diginotar, Lektober, Gemeente Lekken, Het lekken van informatie bij online Sociale netwerken.

Data: 30 en 31 januari 2012
Locatie: Olympisch Stadion Amsterdam

www.iir.nl/informatie-beveiliging

VERTROUWEN IS GOED…

We hebben een nieuw kanaal om te communiceren met onze auteurs. Een besloten LinkedIn-groep. We stelden hier de volgende vraag:

Stalin wist het al: "Vertrouwen is goed, controleren is beter." Maar hoe controleer je dat vertrouwen? En hoe vertrouw je de controleur? Ergens blijft er een stuk vertrouwen over en een stuk controle liggen. Of niet? Is het systeem waterdicht te krijgen?

De volgende reacties ontvingen we:

Marco Koelmans:
Als je vertrouwen gaat controleren is het geen vertrouwen meer (zie je tweede zin). Aan de basis van controle staat altijd een wantrouwen. Een wantrouwen dat er iets fout gaat (bewust of onbewust). Ergens zul je echter een basis moeten leggen voor het vertrouwen. Je kunt de controleur van de controleur van de controleur controleren maar wie controleert deze dan weer? Er zal een balans moeten zijn tussen controle en de kosten daarvan en de consequenties (materieel en immaterieel) van een doorbreking van het geautoriseerde proces. De risicoafweging waarom je controle doet is daarin essentieel. Een risico nemen is niet erg zolang je het bewust doet en na afweging van de mogelijke consequenties. Dat geldt voor alle security-maatregelen en ook voor controles. Daarnaast is het heel moeilijk om alles te controleren. Hoe controleer je bijvoorbeeld misbruik van bevoegdheden door middel van samenspanning in een vier-ogen-principe-proces?

Ed Bronner:
Vertrouwen tussen mensen is iets wat je opbouwt door langdurig blijk te geven van voldoende compliant en open en eerlijk functioneren.
In het geval van waardetransacties, of omgang met zeer vertrouwelijke gegevens sluipen er soms secundaire behoeftes bij de mens in. Ook bij het uitvoeren van bewerkingen of operaties die bijzonder specialistisch of herhalend handmatig ingrijpen vragen, wordt de hulp ingeroepen van geautomatiseerde systemen en een sluitend controlesysteem eromheen. Als hulp en tegelijk voorzien van preventie, detectie en correctie met logging en monitoring. Invoerbeperking op systemen helpt de mens te beschermen tegen zichzelf.
Een raamwerk van bevoegdheidsbeperkingen (rollen) en meerpersoonsautorisaties dwingen de mens verder in kaders. Daarbij is risicomanagement en audit als een soort tweede en derde lijncontrole, veelal als lastig beschouwd, niet altijd in staat de business acceptatie te krijgen om betrouwbaarheid te borgen.
Betrouwbaar handelen van de mens vraagt geen bijzondere attitude, maar wel voortdurend aandacht. En er zijn vele emotionele, fysieke en andersoortige verstoringen die de aandacht afleiden van het primaire doel van betrouwbare informatieverwerking. Daarbij een scala aan veranderende omstandigheden en verleidingen die medewerkers vandaag 100% en morgen 99% of minder betrouwbaar maken. Dan ontstaat de kans dat men met 'slippend' gedrag en vaak in kleine stapjes, zolang onbemerkt of ongecorrigeerd, verder afdwaalt.
Hoe lastig is het om op de snelweg voldoende afstand te houden, de gepaste snelheid, respect en vriendelijk gedrag voor medeweggebruikers, vertrouwende op de technische staat van de auto, veilig van A naar B te komen? Bij de combinatie van technische, organisatorische en procedurele maatregelen is het in de meeste gevallen de mens die een aanrijding veroorzaakt. Files worden dan ook niet veroorzaakt door zoveel mogelijk auto's dicht op elkaar te laten rijden (spookfiles en trombose) maar door voldoende afstand in te bouwen om vloeiende doorstroming te kunnen waarborgen (mijn stokpaardje).
Leidinggevenden die oog houden voor de geestelijke en fysieke welgesteldheid van hun medewerkers kunnen tijdig hulp bieden of naar optimalisatie van de omstandigheden zoeken. Vertrouwen geven is vertrouwen krijgen. Voldoende voorbeelden en vergelijkingen te bedenken.

Elisabeth de Leeuw:
In het geval dat partijen elkaar vertrouwen en een gedeeld belang of business case hebben bij de controle wordt controle door gecontroleerde ervaren als wederzijdse steun. De controleur wordt op zijn of haar beurt gesteund door gecontroleerde en in de loop der tijd wordt het controlebouwwerk verbeterd.
Maar dat geldt niet altijd. In het geval partijen elkaar niet vertrouwen dan wel geen gedeeld belang of business case hebben wordt controle door gecontroleerde ervaren als inbreuk op eigen belang en business. De controleur wordt ontweken, gedesinformeerd en anderszins tegengewerkt. In de loop der tijd wordt het hele controlebouwwerk ondermijnd. Ofwel, zonder common ground geen werkelijk vertrouwen, zonder vertrouwen geen werkelijke controle.

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

IN MEMORIAM

Op 5 oktober (daags na de introductie van de iPhone 4S) overleed Steve Jobs na een lang ziekbed. Steve Jobs, de vroegere oprichter en bedenker van Apple en de CEO van Apple tot 2011.
Ik schrijf deze column omdat Apple toch een bijzonder onderdeel van mijn leven heeft uitgemaakt. In 1984 kocht ik mijn eerste Apple Macintosh. Een bijzonder uitziend kastje met diskettedrive. Het eerste systeem dat commercieel werd aangeboden met een muis en een grafische interface. Een geweldig apparaat.
En ondanks het feit dat mijn kinderen nog niet allemaal geboren waren werd deze machine uiteindelijk veel door hen gebruikt. Ze speelden hun spelletje, tekenden hun tekening en vermaakten zich uitstekend op een computer die eenvoudig zelf door hen kon worden bediend.
Toen was het computeren nog ongecompliceerd. Geen internet, geen social media, zo nu en dan een bulletin board waarop je met je modempje inlogde en daar software of content wist te downloaden.

Inmiddels zijn we bijna 30 jaar verder en is het leven sterk veranderd. Nu heb ik allerlei apparaten met het Applelogo in huis en daar kan ik dagelijks van genieten. Mijn kinderen hebben hun eigen kinderen die bij mij thuis op de iPad mogen spelen. Apple maakt nog steeds intuïtieve apparatuur want zowel mijn kleinzoon van vier als mijn moeder, die ruim 20 keer ouder is, weten de apparatuur te bedienen. In plaats van het 35 pagina's tellende document dat mijn werkgever had laten maken, en die ik moest doorlopen om mijn eerste schreden op internet te zetten, kun je met de iPad in een zeer beperkt aantal stappen je eerste www-adres opzoeken. Ondanks het feit dat de apparatuur zeer veel complexer is geworden, is de gebruikersvriendelijkheid alleen maar toegenomen. De apparatuur staat op mijn bureau in de kamer en wordt door iedereen gebruikt. Een technisch hoogwaardig apparaat is gewoon een gebruikersapparaat geworden. Het is niet meer belangrijk hoeveel intern geheugen in het ding zit. Transfersnelheden van de Ipad? Geen idee. Processorsnelheid? Snel genoeg. Deze vragen hoefde je tien jaar geleden niet te stellen want het antwoord begreep je alleen als je wiskunde had gestudeerd. Gelukkig is dit volstrekt oninteressante informatie geworden.

Niet alle veranderingen zijn positief te noemen. Mijn kinderen kregen op de eerste Macintosh niets mee over beveiliging, privacy (bestond het woord toen al?), diefstal van gegevens, fishing, digitaal pesten en noem maar op. Antivirus was helemaal niet nodig want niemand kon de malware op je machine zetten. Inmiddels is dit op vele manieren mogelijk en de security updates van Microsoft komen dan ook dagelijks binnen. Privacy is lastig te garanderen als je zelf de risico's niet kunt inschatten. De meest intieme zaken kom je tegen op de verschillende Facebook- en Hyves-pagina's waarvan je je afvraagt of degene die het erop heeft gezet zich bewust is van het feit dat alle 'vrienden' deze berichten kunnen lezen. Daarmee is aangetoond dat het begrip 'vriend' een heel andere betekenis heeft gekregen. Tegenwoordig is het niet opzienbarend als je meer dan 500 vrienden hebt.

Er worden zaken aan de mailbox toevertrouwd waarvan de schrijver geen idee heeft dat als die informatie in verkeerde handen valt, je daar heel veel last van kunt krijgen. In mijn lange carrière in de automatisering is informatiebeveiliging slechts sinds een aantal jaren een issue. In vroegere tijden had je geluk als de managers in de ICT, of de managers van de business enigszins gevoel hadden bij informatiebeveiliging. Het werd in geen geval afgedwongen. Gelukkig is dat beeld wel enigszins veranderd. Ik ben zelf nu fulltime aan het werk in de informatiebeveiliging en heb daar mijn handen vol aan. Om mij heen worden bedrijven gehackt en wordt relevante informatie gekopieerd (gestolen wordt het bijna nooit). RSA, DigiNotar en Sony zijn de bekendste voorbeelden van dit jaar. De terughoudendheid om hier openlijk over te communiceren is begrijpelijk maar tegelijkertijd zeer sterk af te keuren. Ik weet niet of er momenteel instanties zijn gekraakt waarvan wij nu nog geen weet hebben maar ik durf wel aan te geven dat dit het geval is.
Kortgeleden hadden we thuis weer een mijlpaal bedacht die we konden gebruiken om een feestje te vieren en het onderwerp kwam op Steve Jobs. Ik heb de Macintosh uit 1984 van zolder gehaald, de diskettes van het stof ontdaan en op tafel gezet. Mijn kinderen zaten onmiddellijk gedrieën achter de Mac te genieten van al die herinneringen. Ik stond erbij en keek ernaar waarbij ook bij mij allerlei herinneringen boven kwamen.

Groetjes, Berry

Discover the best thing since the introduction of FTP!

BEFINE cryptshare®

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

CRYPSYS Data Security is de expert op het gebied van security oplossingen en distributeur van Cryptshare. Neem contact op via sales@crypsys.nl of via 0183 62 44 44 voor een gratis evaluatie.

CRYPSYS data security