iB
INFORMATIEBEVEILIGING
jaargang 14 - 2014
#6

HACKEN

Phishing: slinkse manieren om binnen te dringen

Klik, klik, klik het geluid van een gezonde werkvloer

Veel voorkomende networkrisico's

De Security Survival Pyramid

HTTPS over Open Wi-Fi blijft kwetsbaar

29 - 30 OKT 2014 JAARBEURS UTRECHT

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

REGISTREER NU VOOR GRATIS TOEGANG TOT ALLE DRIE DE VAKBEURZEN VIA:

WWW.INFOSECURITY.NL | WWW.STORAGE-EXPO.NL | WWW.THETOOLINGEVENT.NL

KEYNOTES | SEMINARS | CASE STUDIES | RUIM 175 EXPOSANTEN

Mede mogelijk gemaakt door:

cisco intel

Intel, the Intel logo, Xeon, and Xeon Inside are trademarks or registered trademarks of Intel Corporation in the U.S. and/or other countries.

Reed Exhibitions marqit

Jaarbeurs

DE BERLIJNSE MUUR

Ik ben onlangs weer in Berlijn geweest. Hierbij hoort ook een bezoek aan de restanten van de muur. Anders dan de muur rond Jericho was deze muur bestemd om mensen binnen te houden en informatie buiten te houden. Dat eerste lukte het Oost-Duitse regime prima, door zowel de kans als de impact van ontdekking bij ontsnapping hoog te houden. Informatie buiten houden ging moeilijker, door een veel lagere kans op ontdekking. Verboden goederen uit het westen waren ruim aanwezig en werden als waardevol gezien.
Uiteindelijk is de val van de muur van binnen uit gegaan. De Oost-Duitsers wilden de afscheiding niet, toen de macht van het Oostblok afnam, heeft de lokale bevolking de muur onderuit gehaald. Het westen heeft hier geen rol in gehad. De Oost-Duitse politiek kon daarna eigenlijk niets anders doen dan aanzetten tot hereniging met West-Duitsland.
Hierna volgt een periode van veel veranderingen. Ik bezocht Berlijn voor het eerst tien jaar na de val. Berlijn is op dat moment een bouwput, zoekend naar een nieuwe identiteit, de stad heeft een grote leegstand. Nu, vijfentwintig jaar na de val van de muur, is die nieuwe identiteit gevonden. De stad bruist van creatieve energie en geen enkel stadsdeel kent nog leegstandsproblemen. Er valt me iets anders op als ik de twee bezoeken vergelijk: Vijftien jaar geleden was op straat sprake van een duidelijk aanwezige beveiliging. Nu is daar weinig van te zien, de stad voelt open en vrij. Toch zijn de vele belangrijke objecten zeer duidelijk en zwaar beveiligd, maar met minimaal militair vertoon.
Hier wil ik een vergelijking bij trekken, een parallel met het internet, BYOD en het gebruik van cloud services. Ook hierbij zie je dat gebruikers getrokken worden naar gebruiksgemak, ondanks alle verboden vanuit de werkgever. Gebruikers vinden, ondanks tegenwerking, toch gebruiksmogelijkheden - vaak tegen het uitdrukkelijk beleid van de werkgever in. Maak u geen illusies: de muur is al gevallen. We zitten wat BYOD en cloud betreft nu in de bouwput van 15 jaar geleden in Berlijn, zoekend naar nieuwe mogelijkheden, uitlaatkleppen voor de nieuwe energie die onderhuids al aan het bruisen is. Dit proces is niet te stoppen. Beveiliging moet dus heel anders. We moeten zorgen dat in de sfeer van openheid alles in de basis veilig is, in feite dus algemene regels voor beveiligingshygiëne naleven. Tevens horen we de hoogrisico objecten te identificeren en deze met de nodige maatregelen extra te beveiligen.
Beveiliging vergelijken met de Berlijnse muur is in mijn ogen passender dan de vergelijking met de muur van de stad Jericho. Misschien is het tijd voor een paar Berlijnse beveiligingsprincipes...

Lex Borger, hoofdredacteur

In dit nummer

PHISHING: SLINKSE MANIEREN OM EEN ORGANISATIE BINNEN TE DRINGEN

De term 'phishing' is tegenwoordig bij veel mensen bekend. Vrijwel iedereen heeft intussen wel eens phishing mail ontvangen, waarin op de een of andere manier werd gevraagd om bancaire gegevens. Dergelijke bancaire phishing mails bevatten over het algemeen een tekst die de gebruiker aanzet tot een actie. Bijvoorbeeld: "Uw account is tijdelijk uitgeschakeld, klik hier om deze weer te activeren." Het doel van de aanvaller is om de inloggegevens van de gebruikers, al dan niet inclusief een TAN-, response- of toegangscode, te achterhalen. Met deze informatie proberen criminelen dan toegang te krijgen tot uw bankrekening om vervolgens een overboeking te doen naar hun eigen rekening of naar een andere rekening waar zij toegang toe hebben.

Maar phishing beperkt zich niet alleen tot de bancaire wereld. Deze aanvalstechniek wordt veelvuldig toegepast voor de 'reguliere' verspreiding van malware. Hierbij ontvangt een gebruiker een bestand dat een virus of trojan of het installatiemechanisme voor een virus of trojan bevat of de e-mail bevat een link naar een kwaadaardige website waar de gebruiker vervolgens besmet wordt. De tekst van de e-mail is zo opgesteld dat het de gebruiker probeert te verleiden tot een actie. Dat kan op allerlei manieren:

1. Door een noodzaak te creëren - voorbeeld: in een e-mail wordt aangegeven dat de gebruiker binnen een bepaalde tijd actie moet ondernemen, bijvoorbeeld om te voorkomen dat een dienst wordt opgeschort of een bedrag in rekening wordt gebracht.
2. Door nieuwsgierigheid te wekken - voorbeeld: de gebruiker krijgt via een e-mail informatie aangeboden, zoals een Excel-bestand met het salarisoverzicht van een bepaalde afdeling of de loonstrook van de CEO. De gebruiker wordt daarmee verleid om het bestand te openen. Als hij dit doet verschijnt er een melding dat het bestand corrupt is. Op de achtergrond heeft de malware die in het bestand verstopt zat zijn werk al gedaan. Waardoor de aanvaller bijvoorbeeld toegang heeft gekregen tot het systeem van de gebruiker. Vaak durft die gebruiker zelf geen melding te maken van het incident, omdat hij/zij immers willens en wetens vertrouwelijke informatie heeft willen bekijken.
3. Door gebruik te maken van een bekende afzender - voorbeeld: in een e-mail van het hoofd ICT wordt een migratie van de webmail omgeving aangekondigd. De gebruiker moet, om de migratie af te ronden, via een link in de e-mail eenmalig inloggen. Deze link stuurt de gebruiker echter alleen door naar de foutmeldingspagina van de originele webmailsite en de gemiddelde gebruiker zal denken dat hij/zij een fout wachtwoord heeft ingevoerd. Vervolgens voert de gebruiker nogmaals de inloggegevens in, die door de aanvaller ongemerkt worden onderschept.

Een bekend voorbeeld van een phishing e-mail is er een die afkomstig lijkt te zijn van DHL Express. De e-mail betreft de verzending van een pakket en alle links in het bericht verwijzen ook daadwerkelijk naar de DHL-website. De bijlage bevat echter PDF bestand dat gebruikmaakt van een kwetsbaarheid in Adobe Reader om de malware te downloaden, te installeren en uit te voeren. Dit risico is echter niet beperkt tot alleen PDF's of Adobe, vele applicaties bevatten dergelijke kwetsbaarheden.

Phishing aanvallen op bedrijven

Hoewel we phishing vooral kennen van acties gericht op consumenten, wordt deze aanvalsmethode ook regelmatig gebruikt om 'binnen te komen' bij bedrijven. Zakelijke gebruikers zijn vaak minder alert bij het openen van e-mails en het downloaden van bijlagen, zeker wanneer deze e-mails afkomstig lijken te zijn van een medewerker binnen de eigen organisatie of van een vertrouwde partner of klant. Het idee is toch: "Ik moet die informatie openen, wie weet is het belangrijk!". Deze gedachtegang is natuurlijk begrijpelijk, maar het maakt de zakelijke gebruiker wel kwetsbaar voor een aanval. Een voorbeeld van een zakelijke phishing e-mail is de hierboven genoemde e-mail over een migratie van de webmail omgeving. De tekst kan er bijvoorbeeld als volgt uit zien: "Wij stappen vanaf vandaag over op e-mail in de cloud. Om de migratie van uw mailbox af te ronden dient u eenmalig in te loggen".

Wanneer een e-mail er verdacht uitziet, kan de gebruiker deze het beste laten beoordelen door iemand die hier meer ervaring in heeft, zoals een systeembeheerder. Zakelijke phishing mails kunnen bijvoorbeeld de volgende vorm hebben:

- Een verzoek om éénmalig in te loggen op een bestaande webapplicatie, verzonden door een collega;
- Een support/ICT medewerker die telefonisch of via e-mail om inloggegevens vraagt;
- Een collega met een hogere functie binnen de organisatie vraagt om een bepaalde handeling uit te voeren of om een website te bezoeken;
- Een e-mail met bestanden waarvan de gebruiker kan vermoeden dat deze niet voor hem of haar bedoeld zijn. Na het openen blijkt het bestand corrupt;
- Er wordt geen aanleiding of uitleg gegeven, er komt alleen het verzoek om in te loggen. De schijnbare afzender is dan vaak het hoofd van de ICT-afdeling of zelfs een verzonnen persoon.

De ervaring leert dat er binnen elke organisatie meerdere personen zijn die direct voldoen aan dit soort verzoeken. Door een website te bezoeken, gebruikersnamen en wachtwoorden in te vullen of bestanden te openen. Op deze wijze verkrijgt een aanvaller toegang tot het bedrijfsnetwerk. Werknemers achten

Rik van Duijn is consultant bij Dearbytes. Hi is per e-mail bereikaar via Rik.VanDuijn@dearbytes.nl

zich binnen een bedrijfsomgeving vaak ten onrechte veilig, waardoor dit een relatief eenvoudige weg is om een organisatie aan te vallen.
Een gerichte phishing actie tegen een bedrijf kan grote impact hebben. Neem bijvoorbeeld een aanvaller die toegang krijgt tot de mailbox van een medewerker. Vaak wordt onderschat wat een schat aan informatie zo'n mailbox bevat. Dat loopt uiteen van wachtwoorden tot bedrijfskritische informatie. Het kan voor een bedrijf zeer schadelijk zijn als dit soort gevoelige informatie bij een concurrent of een klant terecht komt. Maar het kan ook nog hele andere gevolgen hebben. Het e-mail wachtwoord kan bijvoorbeeld ook gebruikt worden om op afstand toegang te krijgen tot het bedrijfsnetwerk (bijvoorbeeld om thuis te kunnen werken, of tot het wifi-netwerk. Daarmee heeft een aanvaller dus toegang tot veel meer informatie en bedrijfsmiddelen dan alleen een mailbox.

Het bewustzijn vergroten

Gezien de grote hoeveelheid gevoelige informatie waarover een medewerker beschikt en de groeiende inzet van phishing door criminelen is het voor organisaties belangrijk dat zij het bewustzijn hierover bij medewerkers vergroten. Want de resultaten van recente zakelijke phishing acties zijn alarmerend. Zo heeft de Rijksuniversiteit Groningen onlangs het eigen personeel getest door alle 6.000 medewerkers een phishing e-mail te sturen [1]. 3.000 mensen lazen deze e-mail, maar liefst 2.800(!) medewerkers klikten op de link in de e-mail en niet minder dan 1.000 medewerkers voerden gevoelige informatie in op de pagina. Vergeet daarbij niet dat het klikken op een link al voldoende kan zijn om malware of een backdoor op het systeem te installeren.
Ook de beruchte diefstal van meer dan 40 miljoen credit- en debitcard nummers bij de Amerikaanse retailer Target eind vorig jaar, lijkt gestart te zijn via een phishing aanval [2]. Die aanval was gericht op één van de leveranciers van Target die verantwoordelijk was voor de luchtzuiveringsinstallaties van het bedrijf. Via faciliteiten voor billing- en projectmanagement kregen aanvallers toegang tot de Target-infrastructuur. Zo zijn ze er uiteindelijk in geslaagd om malware op de kassasystemen te installeren, waarmee vervolgens de credit- en debitcardnummers zijn verzameld.

Iedere organisatie is een potentieel doelwit

Phishing is dus wel degelijk een beveiligingsaspect waar organisaties zich bewust van moeten zijn. Een van de uitdagingen hierbij is echter dat organisaties vaak niet het idee hebben dat zij zelf een risico lopen. Want waarom zou een aanvaller nu juist hun bedrijf op de korrel nemen? Dat is een verkeerd uitgangspunt. Hoewel er misschien geen directe aanleiding bestaat om in een organisatie te infiltreren, is de organisatie wel degelijk een potentieel doelwit.
Een andere factor die bepaalt of het de moeite waard is om een aanval op te zetten op een specifieke organisatie, is de afweging hoe moeilijk het is om de gewenste informatie te bemachtigen. Er kan bijvoorbeeld redelijkerwijs van uit gegaan worden dat data van een HR-afdeling relatief eenvoudig toegankelijk is door middel van een phishing aanval. Met de identiteitsgegevens die daar te halen zijn kunnen criminelen bijvoorbeeld een lening aanvragen of een telefoonabonnement afsluiten.
En er zijn nog andere manieren om misbruik te maken van gestolen identiteitsgegevens. Zo werd er bij een kennis van mij enige tijd geleden via een wifi-hack scans van paspoorten gestolen van zijn harde schijf. Deze hack bleef onopgemerkt en werd pas ontdekt nadat de slachtoffers een onbekend pakket ontvingen. Dit pakket bevatte 10 iPhone toestellen, inclusief bijbehorende abonnementen. Niet lang na ontvangst werden ze gebeld door de fraudeur, die liet weten dat er per ongeluk een pakketje was bezorgd en "dat ze deze wel even kwamen ophalen…".
Andere bedrijven beschikken over systemen die logistieke processen aansturen. Door hierop in te breken kunnen criminelen informatie aanpassen voor bijvoorbeeld smokkelpraktijken, zoals in havens. Het is zelfs mogelijk om vrachtwagens met waardevolle goederen te traceren en deze vervolgens op een stille parkeerplaats leeg te roven.
Veel bedrijven voeren overboekingen uit op basis van een geautomatiseerd proces. Hoewel banken deze opdrachten monitoren op ongeregeldheden, is er geen garantie dat alle verdachte transacties door de bank gedetecteerd worden. Kleine transacties van bedragen die niet te veel afwijken van voorgaande transacties hebben een goede kans van slagen.
Uit al deze voorbeelden blijkt dat vrijwel iedere organisatie beschikt over informatie die waardevol is voor criminelen. En dat maakt iedere organisatie in principe een interessant doelwit.

Een phishing aanval voorkomen

Een gerichte phishing actie is bijzonder moeilijk te voorkomen, omdat er dan verschillende tegenmaatregelen tegelijkertijd actief moeten zijn. Een e-mail gateway moet controleren of een e-mail echt afkomstig is van de opgegeven afzender en/of de bijlagen geen virussen bevatten. Niet alleen .exe bestanden kunnen virussen bevatten, maar bijvoorbeeld ook Microsoft Office-documenten, in de vorm van een macro-virus. En via een macro is het mogelijk om een schadelijk VB script uit te voeren.
De medewerkers moeten kritisch kijken of het een legitieme e-mail is en of er geen acties gevraagd worden waaraan zij niet zouden moeten voldoen. Mocht een medewerker toch ergens op geklikt hebben, dan zal hij/zij direct contact moeten opnemen met de IT-afdeling om aan te geven wat er gebeurd is. Daar moet vervolgens bepaald worden of het gaat om phishing en als dat inderdaad het geval is, aangeven worden hoe verder te gaan. Moeten bijvoorbeeld alle werknemers op

de hoogte worden gesteld? Moeten de wachtwoorden misschien worden gewijzigd?
De ervaring leert echter dat er toch regelmatig zaken fout gaan. Zelfs wanneer de detectie goed verloopt en de gebruiker keurig contact opneemt met systeembeheer. Het is bijvoorbeeld voorgekomen dat een systeembeheerder iedereen waarschuwde voor een aanval, maar vergat om het wachtwoord van het slachtoffer te wijzigen. Ook dan is er het voorbeeld van een systeembeheerder die aan iedereen per e-mail een waarschuwing stuurde, met daarin het originele phishing mailtje toegevoegd. Het gevolg was dat gebruikers uit nieuwsgierigheid toch op een linkje klikten en gegevens invulden, met alle gevolgen van dien.
Het is voor alle organisaties dan ook zaak om goed na te denken over hoe om te gaan met een toekomstige aanval. Iedere medewerker, van eindgebruiker tot systeembeheerder, moet weten hoe hij/zij moet handelen. Door gebruikers op te leiden en te informeren over de risico's kan een groot deel van die risico's worden afgevangen. Een manier om dit bewustzijn te vergroten, is door eens als test een phishing 'aanval' uit te voeren op de organisatie, zoals in het hierboven beschreven voorbeeld van de Rijksuniversiteit Groningen. Een dergelijke proef heeft vaak een grote impact op het bewustzijn van medewerkers en zij onthouden de lessen die ze daaruit leren. Daarnaast is het belangrijk om bij een incident altijd direct contact op te nemen met de security organisatie en/of de IT-afdeling. Zij zullen op hun beurt een plan klaar moeten hebben over hoe om te gaan met een dergelijke aanval. Welke acties moeten worden ondernomen, of welke juist niet? Wie moeten er vanuit de organisatie betrokken worden? Zijn er wachtwoorden buit gemaakt? Hebben de aanvallers toegang tot onze systemen? Wat kunnen we doen om de boel 'dicht te timmeren'?

Nuttige adviezen voor individuele gebruikers/werknemers:

1. Vertrouw de afzender van een e-mail bericht niet klakkeloos: een e-mail adres kan vervalst worden ('gespoofed') en de mail kan in werkelijkheid door iemand anders verstuurd zijn.
2. Controleer of de naam van de afzender overeenkomt met het e-mailadres.
3. Controleer hyperlinks door er met de muis boven te 'hangen' (dus niet er op klikken!) en ga na of deze naar een te verwachten website/pagina verwijzen.
4. Controleer e-mail bijlagen, ook als het 'vertrouwde' bestandstypen betreft. Niet alleen .exe bestanden kunnen malware bevatten!.
5. Neem bij twijfel altijd contact op met de afdeling systeembeheer, deze beschikt over de nodige expertise.
6. Ga de volgende zaken na: Heb ik om deze informatie gevraagd? Komt dit overeen met het gedrag binnen onze organisatie? Lijkt het te mooi om waar te zijn? Moet ik ergens mijn meest vertrouwelijke gegevens invullen (PIN codes / wachtwoorden)?
7. Wees alert op slordig taalgebruik in het betreffende bericht, dit kan duiden op een phishing- poging.
8. Wordt u in het bericht gevraagd om persoonsgegevens, wachtwoorden, creditcardgegevens of andere gevoelige data ergens in te voeren of terug te mailen? Wees dan extra alert.
9. In veel phishing aanvallen wordt een noodzaak gecreëerd om snel te reageren: "Uw account wordt gesloten als u niet snel reageert", "De boete dient nu betaald te worden anders krijgt u een BKR-aantekening!" etc. Denk na of dit wel klopt en laat u niet verleiden tot overhaaste acties.

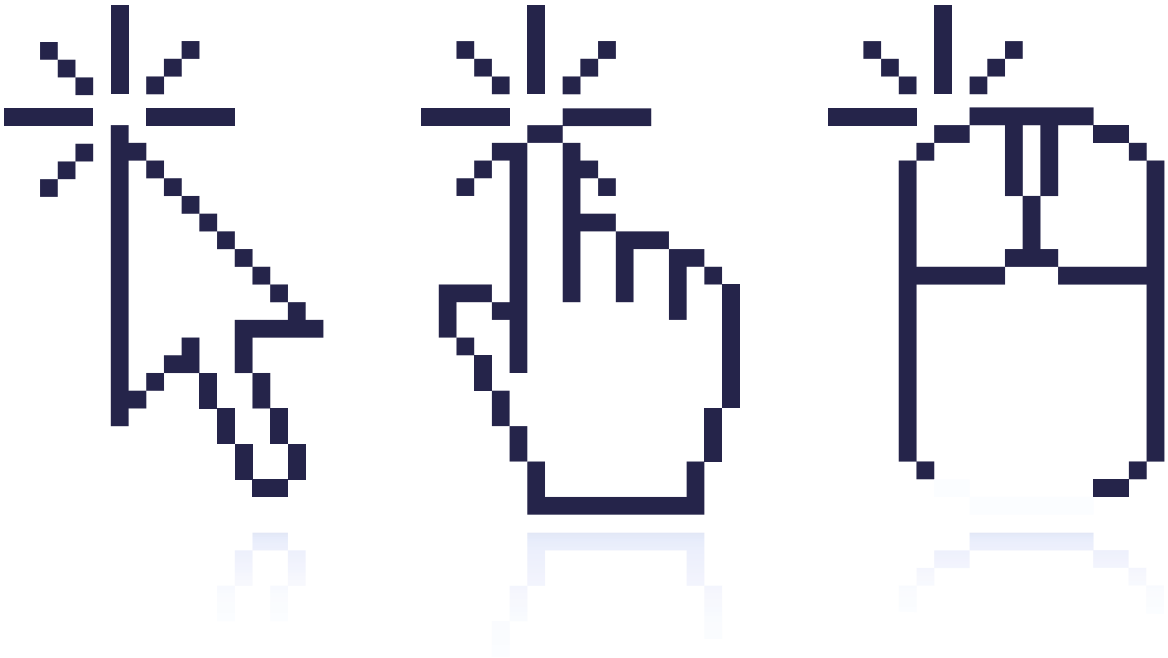
Adviezen voor een security organisatie/IT-afdeling

1. Maak de organisatie bewust van de risico's van phishing` via een bewustwordingscampagne. Maak daarbij gebruik van een gesimuleerde phishing aanval op medewerkers.
2. Beschrijf in een actieplan hoe er gehandeld moet worden bij een (phishing) aanval.
3. Ga na of de DNS-records van uw organisatie SPF (Sender Policy Framework) bevatten. Via SPF-records is het mogelijk om te controleren of een e-mail daadwerkelijk afkomstig is van de geclaimde afzenderorganisatie. Controleert de e-mail gateway deze SPF-records? Een valide mailrecord is weliswaar nog geen garantie dat de betreffende e-mail geen phishing mail is, maar laat in ieder geval zien of de e-mail afkomstig is van een mailserver die geautoriseerd is om voor dat domein e-mail te verzenden.
4. Wordt er gemonitord op vreemde connecties van gebruikers naar het internet? Wanneer een gebruiker geïnfecteerd is kan het zijn dat er verbindingen naar buiten worden opgezet om kwaadaardige software of commando's op te halen of om informatie te verzenden.
5. Is het antivirus systeem up-to-date? Hiermee kan een groot aantal bekende malware-varianten worden geblokkeerd. Zeer nieuwe malware of malware die speciaal is ontwikkeld voor een aanval op een specifieke organisatie zal hierdoor echter niet worden herkend.

Bovenstaande inzichten en tips helpen om de beveiliging van de organisatie aan te scherpen en de risico's op een phishing aanval te vermijden. Het allerbelangrijkste: blijf alert!

Links

[1] http://www.rug.nl/science-and-society/centre-for-information-technology/organisation/pictogram/2009-2/phishing.pdf
[2] http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores



KLIK, KLIK, KLIK HET GELUID VAN EEN GEZONDE WERKVLOER

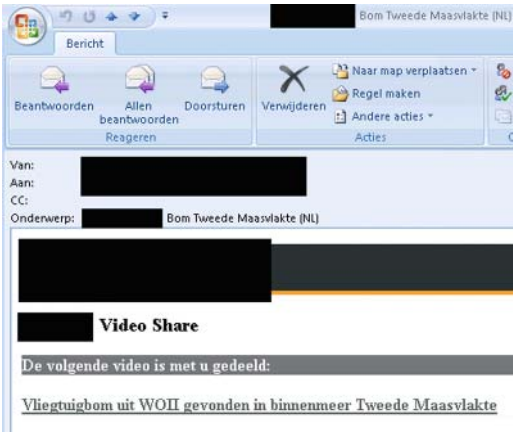
Gebruikers zijn een populair doelwit voor phishing en andere vormen van digitale social engineering aanvallen. Een veel gehoord devies naar aanleiding van deze dreigingen is om vooral niet meer op linkjes te klikken. Maar een gebruiker of medewerker die nooit op linkjes klikt is ook een medewerker die het web nooit meer normaal kan gebruiken, wat zich makkelijk laat vertalen naar een medewerker die zijn werkzaamheden niet goed kan uitvoeren. De eerstvolgende vraag is dan vaak: hoe zorg je er dan wel voor dat dit soort aanvallen succesvol kunnen worden aangepakt? Kan een blik in de keuken van ethische hackers daarbij helpen? Of verschilt de werkwijze van ethische hackers en niet-ethische hackers daarvoor teveel?

Succesfactoren

De kans op succes bij een social engineering aanval wordt in doorslaggevende mate bepaald door het scenario dat opgesteld wordt. Hoe specifieker het scenario aansluit bij de betrokken organisatie, hoe groter de kans op succes. Vaak kan de kans op een succesvolle aanval vele malen worden verhoogd door het scenario vast te stellen op basis van een kort open bronnen onderzoek. Staat het gebouw van de betrokken organisatie bijvoorbeeld al een tijd in de steigers? Zou je dan via een organogram op de website kunnen achterhalen wie daarvoor verantwoordelijk is? Hoeveel medewerkers zou je uit zijn of haar naam kunnen verleiden om een bestand te openen waarin ze denken de locatie van hun nieuwe werkplek te kunnen vinden?

Naast het scenario is de gebruikte techniek van belang. Gaat de hacker voor een aanval met gebruik van 0-days of richt hij zich volledig op de medewerking van de persoon om beveiligingsmaatregelen te omzeilen. In beide gevallen zijn er genoeg technische valkuilen waardoor de aanval al dan niet per ongeluk faalt. Slaagt de aanval wel, dan is de volgende vraag of bij besmetting van één persoon de hacker direct toegang heeft tot gevoelige informatie. Misschien moet de

hacker eerst meer rechten bemachtigen binnen het nu geïnfecteerde netwerk.
De laatste elementen die van belang zijn, zijn de omvang van de groep medewerkers en het niveau van hun beveiligingsbewustzijn. Het product van deze twee elementen bepaalt in belangrijke mate of de social engineering aanval een succes wordt of niet. Medewerkers die eerder zijn aangevallen of recent een security awareness training hebben doorlopen zijn een lastig doelwit. Maar als met een aantrekkelijk scenario de groep medewerkers groot genoeg is, dan weten een paar medewerkers altijd wel de nodige technische hordes te nemen.



Uitdagingen voor de ethische hacker

Het uitvoeren van een digitaal social engineering onderzoek kan om diverse redenen plaatsvinden en de onderzoeken bestaan dan ook in alle soorten en maten. Als het onderdeel is van een onderzoek om de weerbaarheid tegen spionage te testen, dan kiezen we er vaak voor om druppelsgewijs een zo klein mogelijke groep medewerkers aan te vallen met technische middelen die geen achterdocht wekken. Gaat het juist om het in kaart brengen van het beveiligingsbewustzijn van medewerkers? Dan past het beter om een grote en representatieve groep aan te vallen op een manier waar een getrainde medewerker niet in zou moeten trappen. Eén element hebben alle onderzoeken echter gemeen: je probeert inzichtelijk te maken hoe groot de kans is dat medewerkers kunnen worden verleid om beveiligingsmaatregelen te omzeilen of doorbreken.
Het uitvoeren van zo'n onderzoek brengt uiteenlopende uitdagingen met zich mee. Voor de ethische hackers gelden daarbij nog meer uitdagingen dan voor niet-ethische hackers. Kwaadwillende hackers worden niet gehinderd door dezelfde ethische overwegingen of hetzelfde plichtsbesef. We willen nu eerst enkele van de uitdagingen toelichten die specifiek van toepassing zijn op ethische hackers.

De menselijke factor testen

Het uitvoeren van digitale social engineering opdrachten houdt meer in dan hopen dat medewerkers op je linkjes klikken. Enerzijds is het de uitdaging om ervoor te zorgen dat de gebruikte techniek aansluit bij de kwetsbaarheid van de betrokken organisatie, zodat de aanval niet stukloopt op de beveiligingsmaatregelen die daarbinnen van toepassing zijn. Anderzijds moet de aanval zo worden opgezet dat op enig moment de medewerker een handeling moet verrichten die een beveiligingsmaatregel omzeilt, zoals het negeren van beveiligingswaarschuwingen of het openen van een uitvoerbaar bestand. Als er bij een test gebruik wordt gemaakt van macro's binnen Microsoft Office, dan krijgt de medewerker bij het openen van het document meestal een waarschuwing te zien.
Het daadwerkelijk inschakelen van de macro is duidelijk een menselijke handeling waarbij een beveiligingswaarschuwing wordt genegeerd en daarmee een beveiligingsmaatregel wordt omzeild. Tijdens een aanval kan het voor komen dat macro's standaard al worden toegestaan. In dat geval wordt de medewerker praktisch buiten spel gezet en wordt eenvoudigweg de code uitgevoerd. Hoewel dit mooie resultaten oplevert als je kijkt naar het aantal succesvolle 'infecties' uit een aanval, geeft het een sterk vertekend beeld over het beveiligingsbewustzijn van de medewerkers.

Ethische dilemma's

De lat ligt voor ethische hackers vaak hoger dan voor de gemiddelde aanvaller, aangezien je niet altijd van dezelfde middelen gebruik mag maken. Ter illustratie kan het leven van een ethische hacker lastig worden gemaakt door het beperken van uitvoerbare code tot bekende of gesigneerde executables. Minder ethische hackers kunnen dan nog terugvallen op code signing certificaten die ze eerder op andere plaatsen hebben

Daniël Niggebrugge
Na 8 jaar pentesten bij Fox-IT heeft Daniël een neus om snel kwetsbaarheden in de beveiliging te vinden en klanten te voorzien van praktische adviezen.

buitgemaakt. Je kunt daarbij denken aan de wijze waarop Oracle in recente versies Java verder heeft dichtgetimmerd. Voorheen kregen gebruikers een pop-up met een beveiligingswaarschuwing waarbij zij op 'Run' konden klikken.

In de meest recente versies mogen alleen nog Java-applets worden uitgevoerd die door erkende partijen zijn ondertekend. Dit is tegelijk een voorbeeld waarin patchmanagement een rol kan spelen in het beschermen tegen social engineering aanvallen.

Geen kwetsbaarheden introduceren

Een digitale social engineering aanval die in opdracht van een klant wordt uitgevoerd, mag natuurlijk geen kwetsbaarheden introduceren die door anderen misbruikt kunnen worden. Dit aspect is vooral van toepassing op de zogenaamde 'payload' die wordt uitgevoerd bij een succesvolle aanval. Deze payload kan variëren van een eenvoudige 'ping' naar de ethische hacker tot het installeren van een volledige backdoor die de hacker de mogelijkheden biedt om verdere aanvallen uit te voeren op het netwerk. Het is belangrijk dat de payload alleen aan de ethische hacker toegang biedt tot het systeem en de informatie daarop. Een eenvoudige 'bind shell' zou een slecht voorbeeld zijn, omdat ook andere hackers op het netwerk dan toegang kunnen krijgen tot het gecompromitteerde systeem van de medewerker.
Niet onbelangrijk is ook de manier waarop verzamelde gegevens geëxtraheerd worden (indien dat bij de opdracht past). Wie weet kijkt er al een kwaadwillende hacker mee naar het netwerkverkeer van het doelwit. Het zou meer dan vervelend zijn als bij een ethical hack vertrouwelijke interne gegevens in de schoot van een kwaadwillende hacker geworpen worden. Door op een correcte wijze versleuteling toe te passen kan dit voorkomen worden. Deze uitdaging is voor een kwaadwillende hacker in veel gevallen helemaal niet relevant, die zoekt gewoon de makkelijkste en snelste weg naar buiten voor de bemachtigde data.

Uitdagingen voor alle hackers

Naast de paar extra uitdagingen die ethische hackers moeten aangaan, zijn er ook veel overeenkomsten die voor beide typen hackers gelden. In organisaties van enige omvang zijn vaak diverse beveiligingsmaatregelen van toepassing om de organisatie weerbaar te maken tegen een breed spectrum van mogelijke aanvallen. Maar welke maatregelen vormen nou echt een uitdaging voor een hacker die een digitale social engineering uit probeert te voeren en welke maatregelen helpen de organisatie om een dergelijke aanval vroegtijdig te detecteren?

Gescheiden van het internet

Wellicht de grootste uitdaging tijdens het uitvoeren van een digitale social engineering opdracht is de mogelijkheid dat het doelwit zijn internetactiviteiten heeft gescheiden van zijn reguliere werkzaamheden. Hierbij wordt het directe verkeer van

Paul Pols
Paul voegt gegeven zijn achtergrond als meester in de rechten, toegepast ethicus en hacker een boeiende mix toe aan de pentesten van Fox-IT.


Van: verbouwing <verbouwing[redacted]
Aan: [redacted]
CC:
Onderwerp: Update Verbouwing
Verzonden: [redacted]

Beste collega,

In het kader van de derde fase van de verbouwing zullen er nog enkele verhuizingen moeten plaatsvinden. In dit document staat een interactief overzicht van deze verhuizing per afdeling.

Met vriendelijke groet,

Werkgroep verbouwing

medewerkers naar het internet geblokkeerd. De invoering van zo'n maatregel kan afhankelijk van de werkzaamheden van de medewerkers problematisch zijn. Meerdere technische oplossingen zijn mogelijk, zoals:

- Het gebruik van fysiek gescheiden systemen;
- Het gebruik van virtueel gescheiden systemen;
- Het gebruik van een remote desktop oplossing voor de internetactiviteiten.

Deze oplossingen hebben allemaal hun eigen uitdagingen voor de hacker, maar verschillen ook sterk in gebruiksgemak voor de medewerkers van de organisatie. Een van de meer gebruiksvriendelijke oplossingen die wij in de praktijk tegen zijn gekomen gebruikt een remote desktop oplossing voor internettoegang. Voor de medewerker werd daarbij transparant zijn browser in een externe sessie gestart.

Voor de meeste oplossingen geldt dat gangbare aanvallen vervolgens niet meer werken. Het infecteren vanuit de browser geeft slechts toegang tot de internetactiviteiten van de medewerker. Hoewel dit best interessant kan zijn, blijft de informatie op het interne netwerk buiten het (directe) bereik van de hacker. Daarentegen ontbreekt het een hacker bij een infectie in het interne netwerk (bijvoorbeeld via een bijlage bij een e-mail) aan een (directe) weg terug naar de hacker. In de meeste gevallen zijn per situatie wel aanvallen te bedenken om de beperkingen te omzeilen, bijvoorbeeld door op zoek te gaan naar de mogelijke koppelingen en/of kwetsbaarheden die ten behoeve van gebruiksgemak zijn geïntroduceerd. De lat wordt daarmee echter aanzienlijk hoger gelegd voor (potentiële) hackers, zeker als de inrichting van deze infrastructuur extern niet vooraf kenbaar is.

Antivirus en contentfiltering proxies

De discussie over de effectiviteit van antivirussoftware en de mogelijkheden om deze te omzeilen zullen we in dit artikel niet voeren. De praktijk wijst uit dat zowel ethische hackers als niet-ethische hackers geregeld (al dan niet bewust) steken laten vallen in het onzichtbaar blijven voor de verdediging. Ook bij social engineering opdrachten zijn er geregeld momenten dat een vorm van antivirussoftware of contentfiltering een aanval opmerkt. Hoewel ook ethische hackers regelmatig zelf software schrijven om detectie door antivirussoftware te voorkomen, worden toch soms bepaalde eigenschappen als verdacht geclassificeerd. Vooral de wijze waarop de payload moet worden afgeleverd kan op verschillende manieren een vlaggetje doen rijzen. Voorbeelden uit onze praktijk zijn:

- Een contentfiltering proxy die Java-applets inspecteert en bepaalde Java-functies eenvoudigweg blokkeert;
- Antivirussoftware die bepaalde scriptcode herkent als een generieke 'download and execute' methode.

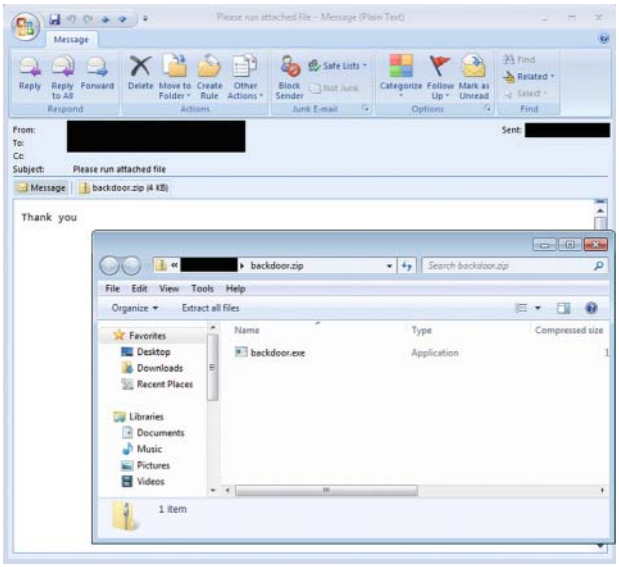
Vaak zijn dergelijke blokkades met minimale inspanning alsnog te omzeilen. In enkele gevallen is de detectie van de aanval dan echter al mogelijk geweest voor het doelwit. Uiteraard kan het uitvoeren van een uitgebreider vooronderzoek helpen om de aanval een grotere kans van slagen te geven. Informatie uit open bronnen, maar ook informatie uit headers van browsers en e-mailberichten kunnen de beveiligingsmaatregelen vooraf vrijgeven. Daarmee kan de aanval beter voorbereid en afgestemd worden op het doelwit.

Onvertrouwde uitvoerbare bestanden niet toestaan

Als een Windows-systeem wordt ingericht voor medewerkers is het natuurlijk aan te raden om daarbij gebruikersaccounts te hanteren met beperkte rechten. Maar als er eenmaal code kan worden uitgevoerd op het systeem, dan is escalatie naar hogere rechten vaak eenvoudig en bovendien voor een hacker meestal helemaal niet meer nodig. Malware kan prima leven in userland en medewerkers hebben over het algemeen toegang tot de meest interessante gegevens.

Francisco Dominguez

Francisco is senior pentester bij Fox-IT. Met zijn technische creativiteit brengt hij al 6 jaar de meest uiteenlopende pentesten tot een succesvol einde.



Medewerkers die alleen zijn aangeleerd om niet op linkjes te klikken zijn een makkelijk doelwit

Een betere verdedigingslinie is daarom om te voorkomen dat medewerkers onvertrouwde code kunnen uitvoeren. Soms is dat een softwarespecifieke maatregel, zoals het voorkomen dat macro's door de medewerker ingeschakeld kunnen worden en het whitelisten van alleen specifieke Java-applets. Deze maatregelen houden direct bepaalde aanvalsvectoren tegen.

Onder Windows kan in bredere zin gebruik gemaakt worden van Security Restriction Policies of Applocker in recentere nieuwere versies. Belangrijk hierbij is dat de configuratie van de technische middelen goed wordt afgestemd op de omgeving waarin het gebruikt wordt. Het komt nog regelmatig voor dat voorbeeldconfiguraties gebruikt worden die weinig tot geen toegevoegde waarde hebben.

Meer dan preventie

Na jarenlang sterk in preventieve maatregelen geïnvesteerd te hebben, komen steeds meer organisaties tot de conclusie dat deze maatregelen zelden het gewenste risiconiveau realiseren. Veeleer moet gezocht worden naar de balans tussen preventieve en detectieve maatregelen. Deze maatregelen moeten bovendien aangevuld worden met procedures om krachtig te kunnen reageren in het geval een (poging tot) digitale inbraak gedetecteerd wordt.

Veel van de preventieve maatregelen produceren, zelfs als deze omzeild worden, nuttige output om detectie en response te voeden. Denk daarbij aan logs van antivirussoftware, firewalls en proxies. Daarnaast bestaan er natuurlijk maatregelen die zich volledig op detectie richten, zoals host en network IDS-systemen. Deze maatregelen genereren veel informatie waar adequaat op gereageerd moet worden. In het ideale geval is een organisatie in staat om de verschillende informatiebronnen met elkaar te correleren. Een vaak voorkomende oplossing is dan het inzetten van een security information & event manager (SIEM). Uiteraard bieden dergelijke oplossingen geen magische totaaloplossing voor dit complexe probleem, maar kan het bijdragen aan de balans van de verschillende aspecten van informatiebeveiliging.

Bewust klikken

Medewerkers die alleen zijn aangeleerd om niet op linkjes te klikken zijn een makkelijk doelwit, als zij zich van andere beveiligingsrisico's in hun dagelijkse werkzaamheden niet of nauwelijks bewust zijn. Het devies dat medewerkers vooral niet op linkjes moeten klikken geeft hen een vals gevoel van veiligheid en kan er zelfs toe leiden dat andere waarschuwingen in de wind geslagen worden. Medewerkers bewust maken van beveiligingsrisico's is dan ook niet iets dat zich in een slogan laat vangen, maar is een kwestie van het aanleren van aan bepaalde attitude ten opzichte van risicovolle handelingen.

De manier waarop wordt gekeken naar de rol van medewerkers in het afslaan van digitale social engineering aanvallen is over het algemeen veelzeggend over het beveiligingsniveau van een organisatie. Worden medewerkers gezien als de bron van mogelijke infecties en daarbij aangemerkt als de enige verdediging tegen digitale dreigingen van buitenaf? Dan heeft de organisatie waarschijnlijk niet de juiste beveiligingsmaatregelen getroffen of deze niet goed op elkaar afgestemd. Wordt het beveiligingsbewustzijn van medewerkers gezien als de voelsprieten van een meer omvattend pakket aan beveiligingsmaatregelen? Misschien ben je dan als organisatie op de juiste weg om hackers tijdig te detecteren of zelfs buiten de deur te houden.

PARC@ING: IK WEET WAAR JE JE BIPS PARKEERT POESJE!

Ik had hier kunnen schrijven over de onbegrijpelijke uitspraak van het Hof in Den Bosch. Kunnen fulmineren over het feit dat het grondrecht op privacy geofferd wordt voor Big Brother. Dat de staat nu lekker mag grasduinen in het parkeergedrag van alle burgers. Want wie niets te verbergen heeft… Dat ga ik niet doen. Ik ga het hier hebben over katten.

Iedereen weet natuurlijk dat katten de heersers van de virtuele wereld zijn (net zoals bekend is dat muizen over de offline wereld heersen). Het is dan ook niet verassend dat uit recent Brits onderzoek blijkt dat selfies maar magertjes afsteken tegenover catfies. Elke dag worden 3,8 miljoen kattenfoto's gedeeld en slechts 1,4 miljoen selfies. Vijftien procent van de katteneigenaars plaatst foto's online van hun zo geliefde huisdier. Dit laatste feit bracht Professor Owen Mundy ertoe de website www.iknowwhereyourcatlives.com in het leven te roepen. Iknowwhereyourcatlives maakt gebruik van de metadata in foto's van katten om zo de locatie van de betreffende kat weer te geven met OpenStreetMap.

"With an estimated 7.8 meters accuracy, if you took a photo of your cat in your home you might find it near that location on the map, or you might not. Every cat we visualize could be accessed just as easily by searching popular photo sharing websites. So, no, we do not know where your cat lives, nor do we care. We set out on this adventure with a mission in mind: to point out the ease of access to data and photos on the web. We sought to showcase how readily available social media users' information and snapshots are to the general public."

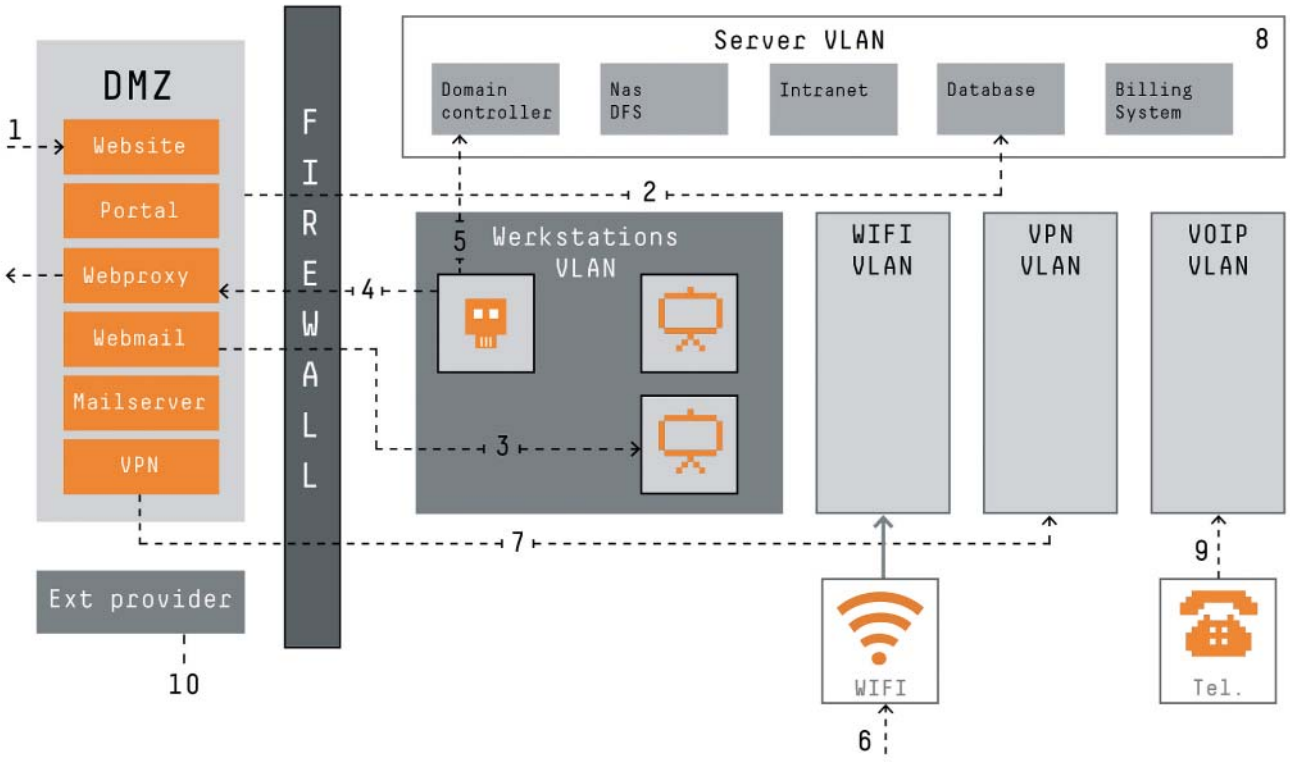
Even afgezien van de privacy-impact, legt het project ook bloot dat GPS (alsook die afgeleide metadata dus) niet een 100% zekerheid geeft over de locatie waar iemand zich bevindt. Ofwel, zoals de Amerikaanse overheid zelf stelt op www.GPS.gov. "The actual accuracy users attain depends on factors outside the government's control, including atmospheric effects, sky blockage, and receiver quality."

Toch nog even over dat parkeren. Deze massale privacyschending door de Nederlandse overheid wekt ook meer privacybewustheid op bij parkeerboeren. Servicehuis Parkeren (SHPV) heeft de bewaartermijn van de bij haar opgeslagen parkeerdata namelijk teruggebracht tot 13 weken. Heeft de Belastingdienst er niets meer aan. Dat vele parkeerboeren maar mogen volgen. Als de Staat dan toch zo graag door wil blijven gaan met het schenden van de privacy van haar burgers, is het aan ons om het haar onmogelijk te maken. En zo strooien de muizen zand in de raderen van Big Kitteh Brother.

Toch nog even over die katten. En die GPS. Kunnen we dat parkeren niet massaal GPS-based maken en als de Belastingdienst dan komt kloppen samen een proefproces starten over de betrouwbaarheid van GPS? Iedereen die wel eens Facebook gebruikt weet dat je met enige regelmaat volgens je telefoon op bizarre locaties bent omdat dit volgens GPS zo is. (Nee Facebook, ik woon echt niet in Duindorp, zelfs niet op 7,8 meter ervandaan). Oh ja, en dan betalen we natuurlijk ook allemaal met Bitcoins en maken we gebruik van Anonymous Identity Providers.

So long, and thanks for all the fish!

Mr. Rachel Marbus,
@rachelmarbus op Twitter



10 VEEL VOORKOMENDE NETWERKRISICO'S EN PRO-ACTIEVE MAATREGELEN

Vrijwel elke organisatie beschikt over een bedrijfsnetwerk. De praktijk leert dat de security van deze netwerken in vele gevallen suboptimaal is. In dit artikel beschrijven we tien veel voorkomende, risicovolle situaties. Voor elke situatie geven we aan hoe een 'breach' gedetecteerd kan worden. Bijgaande illustratie geeft een bedrijfsnetwerk weer met de algemene systemen die in de meeste bedrijfsomgevingen aanwezig zijn. De cijfers in deze illustratie corresponderen met de volgende tien situaties die gevaar kunnen opleveren.

1. Webserver bevat een kwetsbaarheid

Een service of webapplicatie bevat een kwetsbaarheid waarmee een aanvaller toegang verkrijgt tot een server in de Demilitarized Zone (DMZ). Een DMZ is in de regel zo ingericht dat uitsluitend systemen die er onderdeel van uitmaken, vanaf het internet te benaderen zijn. Verbindingen vanaf het internet naar de overige systemen worden in principe afgesloten. Als er toch verbindingen vanuit de DMZ naar het interne netwerk nodig zijn, zouden die zeer beperkt moeten zijn. Als een aanvaller er in slaagt op een webserver binnen de DMZ te komen, kunnen de andere systemen binnen de DMZ worden onderzocht en kan gevoelige informatie worden aangetroffen. Mogelijk kunnen ook verbindingen naar het interne netwerk worden gelegd.

Impact: de aanvaller heeft toegang tot de DMZ vanuit waar het mogelijk is de resterende servers in de DMZ aan te vallen.

Tips:

1. Ga na welke diensten worden aangeboden op het internet door de DMZ-systemen. Kijk daarbij kritisch naar deze diensten. Zijn ze noodzakelijk?
2. Beperk het verkeer tussen onderlinge DMZ-systemen zoveel mogelijk. Ook deze systemen kunnen kwetsbaarheden bevatten die vanaf andere DMZ-systemen uit te buiten zijn.
3. Gebruik geen Active Directory-accounts in een DMZ. Ook als het onmogelijk is om vanuit de DMZ een verbinding te maken met het interne netwerk. Andere kanalen zoals wifi, webmail of de verbinding voor thuiswerken bieden mogelijk wél toegang.
4. Ga na welke verbindingen vanuit de DMZ naar het interne netwerk mogelijk zijn en kijk kritisch naar de noodzaak van deze verbindingen.

2. Webserver uit DMZ maakt verbinding naar het interne netwerk

Een webapplicatie vanuit de DMZ maakt gebruik van een databaseserver uit het server VLAN (virtueel LAN). Zojuist hebben we aangegeven dat een dergelijke situatie onwenselijk is. Toch komt deze situatie regelmatig voor. Een portal applicatie heeft bijvoorbeeld een verbinding met een databaseserver in het server VLAN. Wanneer derden in staat zijn vanaf de server in de DMZ query's uit te voeren op de databaseserver in het server VLAN is het mogelijk toegang te verkrijgen tot de server. Vanaf dat moment is het voor een aanvaller eenvoudig om vervolgens een backdoor op de databaseserver te installeren om zo toegang te verkrijgen tot het server VLAN.

Impact: aanvallers hebben toegang tot het server VLAN vanaf een van de DMZ-servers.

Tips:

1. Monitor al het verkeer vanuit de DMZ naar het interne netwerk. Bepaal aan de hand van de koppelingen van de DMZ naar het interne netwerk op welk type verkeer gemonitord moet worden.
2. Beperk de toegang vanaf het server VLAN en het internet, laat alleen strikt noodzakelijke verbindingen toe.
3. Ga na welke verbindingen mogelijk zijn vanuit de DMZ naar het interne netwerk, beperk deze zoveel mogelijk.

3. Werknemer ontvangt phishing e-mail

Een werknemer ontvangt een e-mail die kennelijk bedoeld was voor de directeur. De bijlage van deze e-mail is echter een PowerPointpresentatie met daarin reorganisatieplannen. De nieuwsgierig geworden werknemer opent de presentatie, maar ziet een lege pagina met de melding: "Om de presentatie weer te geven dienen macro's ingeschakeld te worden". De werknemer schakelt de macro's in en er komt een melding dat het bestand corrupt is. Ondertussen is op de achtergrond een backdoor gedownload en uitgevoerd.

Impact: De aanvaller heeft directe toegang tot het interne netwerk via het systeem van de medewerker.

Tips:

1. Maak personeel bewust van de risico's van phishing aanvallen en leer werknemers een phishing aanval te herkennen.
2. Gebruik antivirus om malware te herkennen, zolang de aanvallers standaard backdoors gebruiken kunnen deze gedetecteerd worden.
3. Monitor het netwerkverkeer van werkstations naar internet, met name op langdurige of repeterende sessies.

4. Geïnfecteerd werkstation

Het werkstation van een werknemer is geïnfecteerd met malware. Deze malware maakt contact met een command-en-controlserver om commando's op te halen. De aanvaller geeft via deze weg bijvoorbeeld opdracht om het volledige netwerk te scannen en na te gaan welke diensten beschikbaar zijn. De aanvaller heeft toegang tot gedeelde mappen en de bestanden van de werknemer zelf. Door gedeelde bestanden

Rik van Duijn is consultant bij Dearbytes. Hi is per e-mail bereikaar via Rik.VanDuijn@dearbytes.nl

te infecteren kan de aanval zich uitbreiden. Verder is het mogelijk om te zoeken naar wachtwoorden in de gedeelde bestanden. Het komt voor dat organisaties wachtwoorden gebruiken in de opstartscripts of wachtwoorden opslaan in v werknemers beschikbare documenten en die worden dan gevonden.

Impact: toegang tot het interne netwerk en bestanden van de organisatie. De aanvallers hebben vanaf nu de mogelijkheid zich te verspreiden door het netwerk om zo de grip te vergroten.

Tips:

1. Monitor netwerkverkeer van werkstations naar het internet op verdacht verkeer.
2. Breng een duidelijke segmentering aan tussen werkstation en VLANs om de functies te scheiden. Aan de hand van de functie kan bepaald verkeer toegelaten worden, of als verdacht aangemerkt worden.
3. Monitor verkeer van werkstations naar serversystemen. Een werknemer heeft waarschijnlijk geen reden om verbinding te maken met de management interface van een server.
4. Controleer waartoe een werknemer toegang heeft. Ga vervolgens na of dit noodzakelijk is en of niet teveel informatie beschikbaar is.

5. Gebruiker wordt toegevoegd aan Windows-groep

Een aanvaller heeft een gebruiker toegevoegd aan een groep met hogere rechten of een groep die toegang biedt tot gevoelige informatie. Denk bijvoorbeeld aan domeinbeheerders of een Windows-groep die toegang biedt tot de Gemeentelijke Basis Administratie (GBA) database.

Impact: In vele gevallen verkrijgt de aanvaller hogere rechten zonder dat de beheerorganisatie hier enige weet van heeft. Een nieuw aangemaakte domeinbeheerder zal mogelijk snel opvallen, maar andere groepen worden wellicht minder vaak gecontroleerd en dan valt een verandering niet zo snel op.

Tips:

1. Breng de groepen die toegang verschaffen tot hogere rechten of gevoelige informatie in kaart.
2. Stuur automatisch een e-mail naar systeembeheer en/of de security-organisatie zodra een nieuwe gebruiker wordt toegevoegd.

6. Derden verkrijgen toegang tot het draadloze netwerk voor werknemers

Via phishing of een directe aanval op het wifi-netwerk, verkrijgen aanvallers toegang tot het medewerkers-wifi. Via het medewerkers-wifi zijn de diensten toegankelijk die een medewerker in staat stellen zijn werk te doen. Deze diensten kunnen kwetsbaarheden bevatten die een aanvaller kan benutten om het bedrijfsnetwerk aan te vallen. Dergelijke diensten kunnen inherent kwetsbaar zijn, doordat bijvoorbeeld elke gebruiker toegang heeft tot gevoelige informatie.

Impact: Aanvallers hebben beperkte toegang tot het netwerk en mogelijk gevoelige informatie.

Tips:

1. Gebruik 802.1x om toegang tot het wifi-netwerk te reguleren. Laat gebruikers met de loginnaam en het wachtwoord van hun Active Directory account authentiseren.
2. Geef gebruikers niet meer rechten dan noodzakelijk.
3. Beperk de toegang via wifi tot het interne netwerk. Biedt bij voorkeur alleen een 'internet only' wifi aan om de waarde van toegang voor derden te beperken.

7. VPN-verbinding van de leverancier

Een VPN-verbinding met een leverancier wordt gebruikt om bepaalde functionaliteit te ontsluiten. Een dergelijke verbinding kan beperkt zijn tot de systemen die nodig zijn voor de leverancier. Het komt echt ook voor dat zo'n VPN-verbinding een verkapte thuiswerkimplementatie is. Dit houdt in dat de leverancier onbeperkt toegang heeft tot het interne netwerk van de organisatie, als ware het een medewerker. Recent heeft één van de grootste creditcarddiefstallen plaatsgevonden via zo'n VPN-verbinding voor een leverancier.

Impact: Toegang geven aan een leverancier kan resulteren in onbeperkte toegang tot het interne netwerk van de organisatie.

De aandacht voor de beveiliging van organisaties gaat vooral naar de externe omgeving en onvoldoende monitoring van gebeurtenissen op het interne netwerk is de voornaamste reden dat incidenten te laat worden ontdekt

Tips:

1. Inventariseer de toegangsmogelijkheden vanaf de verschillende VPN-verbindingen.
2. Beperk de verbindingen tot strikt noodzakelijke servers en poorten om misbruik te voorkomen.
3. Gebruik two-factor authenticatie om toegang tot VPN of wifi te reguleren.
4. Onderzoek de beschikbaar gestelde systemen op kwetsbaarheden om mogelijkheden van aanvallers te beperken.

8. Interne server geeft malware-melding

Een interne server geeft een melding van malware. Het gaat in dit geval om een detectie van het type: 'hacktool'. Het is weliswaar mogelijk dat malware geautomatiseerd een tool inzet om een actie uit te voeren, maar de kans is groter dat het gaat om een aanvaller die direct toegang heeft tot een systeem. Stel: de detectie betreft de tool 'MimiKatz', deze tool kan wachtwoorden uit het geheugen achterhalen. Dit betekent dat de aanvaller vanaf dit moment deze wachtwoorden kan gebruiken.

Impact: een aanvaller heeft vanaf dit punt directe toegang tot het systeem en voert verschillende tools uit.

Tips:

1. Antivirussoftware kan een signaal afgeven, in het bijzonder op servers is dit een sterke, maar geen waterdichte indicatie van een aanval.
2. Evalueer malwaredetecties zorgvuldig, mogelijk hebben derden direct toegang tot een systeem.

9. VoIP-VLAN wordt gerouteerd

Het netwerk maakt gebruik van Network Access Control (NAC), maar dit wordt niet op het VoIP-VLAN toegepast. Door een netwerkkabel van een VoIP-telefoon te gebruiken kan de aanvaller dan toegang krijgen tot het interne netwerk. Vlans impliceren vaak dat er een scheiding is tussen de verschillende gebruikte subnets, maar vaak worden deze VLANs alsnog gerouteerd. Dit betekent dat vanaf het VoIP-VLAN toch het volledige netwerk te benaderen is. Interne netwerken kennen vele kwetsbaarheden en 'stepping stones' naar hogere rechten, waar de aanvaller vervolgens gebruik van kan maken.

Impact: De aanvaller heeft nu toegang tot het volledige interne netwerk. Vanaf daar is het mogelijk de resterende systemen aan te vallen.

Tips:

1. Pas NAC op alle VLANs toe.
2. Routeer niet klakkeloos tussen elke VLAN, identificeer welk verkeer nodig is naar welke machines en beperk de resterende mogelijkheden.
3. Ga na of de VLANs niet te algemeen zijn opgezet. Hoe specifieker deze VLANs zijn ingericht, hoe beter de mogelijkheden te beperken zijn. Dit brengt echter wel een grotere administratieve last met zich mee.
4. Monitor verkeer uit VLANs op onverwacht verkeer. Een remote desktop-sessie vanuit het VoIP-VLAN is een voorbeeld van onverwacht verkeer.

10. Webapplicatie bij externe partij gehost

Een webapplicatie is ondergebracht bij een externe partij. Zodra de applicatie of externe partij gecompromitteerd wordt is dit vervelend, maar op het eerste gezicht niet desastreus. Het komt voor dat de gebruikte wachtwoorden die bij zo'n externe partij worden buitgemaakt overeen blijken te komen met de intern gebruikte wachtwoorden van een van de beheerders van deze extern gehoste applicatie. Verder kunnen de extern gehoste webapplicaties informatie bevatten over de organisatie.

Impact: aanvaller heeft toegang tot informatie over de interne organisatie en kan mogelijk wachtwoorden verkrijgen om toegang te krijgen tot webmail, thuiswerkfaciliteiten, het werknemers-wifi-netwerk en managementinterfaces van systemen.

Tips:

1. Gebruik wachtwoorden eenmalig.
2. Beperk de beschikbaarheid van gevoelige informatie op extern gehoste systemen. Voor interne systemen is het zaak na te gaan wie precies toegang heeft tot deze systemen.

Op het eerste gezicht lijken bovenstaande tips eenvoudig, vanzelfsprekend en mogelijk zijn ze al opgenomen in een procedure. Toch komen al deze situaties in de praktijk regelmatig voor. De kunst voor een aanvaller is hierbij steeds voorbij de eerste horde te komen. Eenmaal binnen blijkt vaak dat vanaf dat punt (bijna) alle systemen door de aanvaller onbeperkt te benaderen zijn. De aandacht voor de beveiliging van organisaties gaat vooral naar de externe omgeving en onvoldoende monitoring van gebeurtenissen op het interne netwerk is de voornaamste reden dat incidenten te laat worden ontdekt.

WOENSDAG 8 OKTOBER 2014 SECURITY-CONGRES

Thema: Behoorlijk Beveiligd

Locatie:
Postillion Hotel
Utrecht Bunnik
Kosterijland 8
NL-3981 AJ Bunnik

www.postillionhotels.com

PE 5

Hét congres zonder files, georganiseerd door ISACA, NOREA en PvIB

Al ingeschreven op het succesvol terugkerend congres? Mis het niet en schrijf u nu in!

Wederom is getracht een mooi en afwisselend programma samen te stellen. Wat kunt u verwachten:

Dagvoorzitter: André Beerten, GHZ

Keynote speakers:
> Jaya Baloo, KPN
> Michel Huffaker, iSIGHT partners

Topics parallelle sessies:
> Privacy
Uw sprekers zijn:
- Simon Hania, TomTom
- Rachel Marbus, NS

> Risk Based Security
Uw sprekers zijn:
- Ronald van der Knaap, PWC en Gert Maneschijn, RDW
- Marcel Baveco, DNB

> Application Security
Uw sprekers zijn:
- Fred Hendriks en Tim Hemel, iComply
- Ad Kint en Marcel Koers, UWV en Rober van der Veer, SIG

Onderdeel van het programma is de uitreiking van de Joop Bautz Information Security Award.

Het volledige programma vindt u op **www.security-congres.nl**.

Dit congres wordt mede mogelijk gemaakt door:

ONSIGHT
IT Security Experts

TSTC
ICT en Security Trainingen

FOX IT
FOR A MORE SECURE SOCIETY

Wij ontmoeten u graag op 8 oktober 2014!

Meer informatie:
www.security-congres.nl

Organisatie:

ISACA
In dienst van IT Governance-specialisten
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

PvIB
Platform voor InformatieBeveiliging

HTTPS OVER OPEN WI-FI BLIJFT KWETSBAAR

Het is al langer bekend dat open Wi-Fi netwerken niet veilig zijn op het moment dat gegevens onversleuteld worden verzonden. Het open karakter van deze netwerken maakt het onderscheppen en manipuleren van data door aanvallers erg eenvoudig. Echter, veel internetgebruikers veronderstellen dat het gebruik van een versleutelde HTTPS-verbinding op een open Wi-Fi netwerk toch nog voldoende bescherming biedt tegen deze aanvallers. En dat is helaas niet waar…

Ir. Dennis Baaten is information security officer bij de ANWB en bereikbaar via dbaaten@anwb.nl

Computerapparatuur (laptops, tablets, telefoons) met een ingeschakelde Wi-Fi verbinding zoekt continu naar draadloze netwerken in de buurt. Vaak zijn deze apparaten ingesteld om automatisch verbinding te maken met bekende netwerken. Als er meerdere bekende netwerken in de buurt zijn, zal het apparaat het netwerk met het sterkste signaal selecteren. Heb je bijvoorbeeld vorige week verbinding gemaakt met het open Wi-Fi netwerk restaurant-wifi, dan zal je laptop ook op andere locaties naar dit netwerk zoeken om vervolgens automatisch te verbinden.

Een aanvaller kan dit mechanisme misbruiken voor het uitvoeren van een zogenaamde man-in-the-middle (MITM) aanval. Met behulp van speciale apparatuur (bijvoorbeeld de WiFi Pineapple t.w.v. $99) kan een aanvaller zich namelijk voordoen als een willekeurig Wi-Fi netwerk. De aanvaller vangt de zoeksignalen op van apparaten die zoeken naar bekende Wi-Fi netwerken. Wanneer het een zoeksignaal naar een open netwerk betreft, zal de aanvaller zich voordoen als het desbetreffende netwerk.

Het apparaat van het slachtoffer zal verbinding maken en denkt verbonden te zijn met het netwerk van het restaurant, terwijl er in werkelijkheid verbinding is gemaakt met het vervalste Wi-Fi netwerk van de aanvaller. Vanaf dat moment heeft de aanvaller de controle over de Wi-Fi verbinding tussen je laptop en het internet; de aanvaller is nu de man-in-the-middle.

Maar de aanvaller is nog niet klaar; alleen het onversleutelde (HTTP) verkeer is nu zichtbaar terwijl gevoelige gegevens vaak met behulp van versleutelde SSL-verbindingen (HTTPS) worden verstuurd. Het kraken van de sleutel van een SSL-verbinding is voor menig aanvaller onbegonnen werk, maar met behulp van speciale software (zoals SSL-strip) kan de aanvaller de browser van het slachtoffer forceren tot het gebruiken van een onversleutelde HTTP verbinding. Het gebruik van SSL tussen de aanvaller en het slachtoffer wordt daarmee omzeild, maar de verbinding tussen de aanvaller en de bestemming op internet blijft wel versleuteld met SSL. En dan is de aanvaller in staat om gevoelige gegevens te onderscheppen of te manipuleren alvorens deze hun beoogde bestemming op internet bereiken. Denk hierbij bijvoorbeeld aan het aanpassen van internetbankierentransacties of het onderscheppen van wachtwoorden.

Om het risico op misbruik te verlagen hebben veel website eigenaren maatregelen genomen of overwegen ze deze te nemen. Een populaire maatregel is het toepassen van de zogenaamde HSTS header die bij het bezoeken van een website door de server wordt mee gezonden naar de browser van de bezoeker. HSTS staat voor HTTP Strict Transport Security en zorgt ervoor dat browsers die dit ondersteunen gedurende de gespecificeerde periode (bijvoorbeeld een half jaar oftewel 15768000 seconden) uitsluitend een beveiligde verbinding opzetten met deze website. De browser zal dan geen onversleutelde HTTP-verbinding meer accepteren voor deze website.

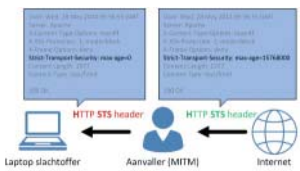
Op het moment van schrijven wordt het gebruik van deze header echter niet ondersteund door alle browsers. Zo heeft bijvoorbeeld nog geen enkele versie van Microsoft's browser Internet Explorer ondersteuning voor HSTS, waardoor deze browser zich ondanks het gebruik van een HSTS-header nog steeds laat forceren tot het gebruiken van een onversleutelde HTTP-verbinding.

Toch vormt HSTS bij de browsers die het wél ondersteunen geen waterdichte maatregel. Deze maatregel werkt namelijk pas wanneer het slachtoffer de desbetreffende website eerst via een ongecompromitteerde internetverbinding heeft bezocht; pas ná het verwerken van de HSTS-header weigert de browser

Maak geen verbinding met open Wi-Fi netwerken, maar gebruik altijd een Wi-Fi netwerk dat minimaal is beveiligd met WPA

onversleutelde verbindingen met de website. Hierdoor lukt het de aanvaller in een aantal specifieke gevallen nog steeds om, ondanks de aanwezigheid van een HSTS-header de browser van een slachtoffer te forceren tot het gebruiken van een onversleutelde HTTp-verbinding:

1. Bij een eerste bezoek aan een website zal de browser nog niet weten dat de desbetreffende website alleen over HTTPS benadert dient te worden. Als de aanvaller de browser dan forceert tot het gebruiken van HTTP, en vervolgens ook nog in staat is om de HSTS-header te verwijderen of te veranderen naar nul (0) voordat deze bij de browser aankomt, dan kan de aanvaller zijn MITM blijven handhaven.



2. De browser slaat de HSTS waarde op in de browsergeschiedenis. Wanneer de browsergeschiedenis wordt gewist of wanneer de browser wordt gestart in de privé of incognito modus, dan zal de browser bij de eerstvolgende keer starten niet weten dat de desbetreffende website uitsluitend via HTTPS dient te worden benaderd. Voor de browser is de situatie dan namelijk gelijk aan het hierboven beschreven "eerste bezoek".

3. Na het verlopen van de HSTS-waarde (bijvoorbeeld na een half jaar) zal de browser bij de eerstvolgende keer opstarten ook weer in een situatie zitten die gelijk is aan het "eerste bezoek".

Kortom, als het nemen van maatregelen beperkt blijft tot het gebruik van een HSTS-header in combinatie met een browser die dit ondersteunt, is misbruik door een aanvaller tijdens het gebruiken van een open Wi-Fi netwerk niet uit te sluiten. Het risico is wel flink afgenomen, maar is niet nihil. Om het risico nog verder te verlagen kunnen aanvullende maatregelen worden genomen:

a. Verwijder alle Wi-Fi netwerken eenmalig uit je apparaat en begin opnieuw. Wen jezelf aan om vanaf dat moment alleen nog maar beveiligde netwerken op te slaan, zodat je apparaat niet meer automatisch zal proberen te verbinden naar open Wi-Fi netwerken.

b. Stel je apparaat bij voorkeur zo in, zodat deze niet automatisch verbinding maakt met bekende Wi-Fi netwerken. Smartphone gebruikers kunnen eventueel gebruik maken van apps (zoals bijvoorbeeld Wi-Fi Matic) die je Wi-Fi verbinding automatisch in- of uitschakelt afhankelijk van je locatie.

c. Maak geen verbinding met open Wi-Fi netwerken, maar gebruik altijd een Wi-Fi netwerk dat minimaal is beveiligd met WPA. De beveiligingsprotocollen WPA en WPA2 kennen namelijk een zogenaamde four-way handshake waarmee er op basis van het wachtwoord en de SSID een unieke sessie-sleutel per Wi-Fi gebruiker wordt gegenereerd. Dit is momenteel voor een aanvaller erg moeilijk te misbruiken, ook wanneer het wachtwoord bij de aanvaller bekend is. In het laatste geval is misbruik alleen mogelijk wanneer een aanvaller bewust een vervalst access point opzet met hetzelfde SSID en wachtwoord.

Wanneer een of meerdere van deze aanvullende maatregelen worden ingezet in combinatie met HSTS en een browser die hier ondersteuning voor biedt, dan wordt het aanvallers knap lastig gemaakt om een man-in-the-middle aanval op een open Wi-Fi netwerk uit te voeren. Voorlopig is het risico dan in de meeste gevallen acceptabel, totdat aanvallers weer nieuwe trucs uit de hoge hoed toveren.

EEN BIJZONDERE CONFERENTIE OVER EEN BEKEND THEMA

Begin april vond in Amsterdam de tweedaagse conferentie Secure Cloud plaats. Deze bijeenkomst, georganiseerd door CSA [1], Enisa [2] en Fraunhofer [3] besteedde aandacht aan tal van aspecten die uiteindelijk ervoor moeten zorgen dat wij allemaal meer gebruik van cloud gaan maken, allemaal op basis van een veilig aanbod. Cloud en veiligheid zijn inmiddels al zo lang onlosmakelijk met elkaar verbonden begrippen en thema van menig congres dat de vraag rijst of deze conferentie nog wel nodig was.

Om antwoord te geven op die vraag kan worden verwezen naar het programma [4]. Dit maakte op voorhand duidelijk dat de sprekers verschillende disciplines vertegenwoordigden en daarmee ook uiteenlopende invullingen zouden geven aan het begrip secure cloud. De diversiteit was ook zichtbaar bij de ruim 150 aanwezigen, dit was duidelijk geen conferentie uitsluitend bedoeld voor één beroepsgroep. Doordat de groep zo gemêleerd was, werd tijdens de presentaties en discussies veelvuldig teruggegrepen op nadrukkelijk niet-cloud gerelateerde issues en voorvallen. Dit was geen zwakte bod, het hielp juist de probleemstelling vanuit meerdere invalshoeken te bekijken. Deze wisseling van perspectief zal het voor non-insiders overigens lastig gemaakt hebben delen van het programma te volgen. In tegenstelling tot andere bijeenkomsten was hier het hebben van parate kennis van afkortingen minder een pre dan het signaleren van een gewijzigde invalshoek. Het was verder een bijeenkomst waar het tempo hoog lag. Sprekers en zaal reageerden zeer snel op elkaar en dat gaf de conferentie al vanaf de start een opvallende dynamiek. Het is daarom ook minder eenvoudig puntsgewijs weer te geven wie waar over sprak.

Rashid Niamat is journalist en werkzaam bij ISPam.
Rashid is te bereiken via rashid@niamatmediagroup.nl

De bondige keynotes van onder andere Neelie Kroes over de doelstellingen van de EC op het vlak van uitgebreidere cloud adoptie, omdat het een banenmotor is en Richard Clarke over de werkwijze van de NSA en de veranderingen die deze organisatie moet doorvoeren, staken in dat opzicht schril af tegen de rest van het programma. Kroes gaf aan dat meer cloud in de EU tot 400.000 nieuwe bedrijven kan leiden en het EU BNP met 1000 miljard kan vergroten. Clarke deed zijn uiterste best de balans te beschrijven tussen de noodzaak tot incidenteel zeer vergaande surveillance en de nog grotere noodzaak te voorkomen dat er wordt doorgeschoten naar een 24/7 surveillance staat. Verder was dit een conferentie waar in

het plenaire gedeelte nadrukkelijk geen ruimte was voor salespitches en marketing activiteiten. De sprekers en de zaal hielden zich daar voorbeeldig aan en het gevolg was dat de aandacht niet onnodig werd afgeleid. Nadeel kan zijn geweest dat bij bepaalde thema's aan de beoogde gebruiker van secure cloud diensten – namelijk de klant – te weinig aandacht is besteed. De rest van het programma was, zoals al aangegeven, minder simpel samen te vatten. Wat wel mogelijk kan is het aantal termen of begrippen dat deze twee dagen steeds terugkwam te beschouwen als een rode draad, dat levert een lijst op met de volgende zeven begrippen:

1. **Taal**
2. **Telco's**
3. **Snowden en NSA**
4. **EU**
5. **Standaarden, welke Standaarden?**
6. **Juridische issues en cloud techniek**
7. **Security in de cloud - de praktijk**

Taal

Het klinkt als een open deur, maar zeker bij een thema als secure cloud is het nodig dat partijen opletten dezelfde taal te spreken. Hiermee wordt niet bedoeld taal , bijvoorbeeld Engels, als de voertaal tijdens een debat, maar taal als essentieel instrument bij het streven naar duidelijkheid en transparantie. Gedurende deze conferentie werd diverse keren duidelijk dat

Dit was duidelijk geen conferentie uitsluitend bedoeld voor een beroepsgroep

een woord of begrip door sprekers en zaal verschillend werd gebruikt of soms echt niet door allen werd begrepen. Om met dat laatste te beginnen, door meerdere sprekers werd gewezen op de noodzaak van een eigen Europese of nationale cloud omgeving. Landen als Frankrijk en Griekenland gaan hier vrij ver in, omdat wetgeving verhindert dat bepaalde data (denk aan archieven) buiten de nationale landsgrenzen wordt opgeslagen. De Amerikaanse sprekers zijn uiteraard niet gecharmeerd van een dergelijk ontwikkeling en pleitten voor open grenzen en internationalisering van de cloud. Het begrip dat daarbij werd gehanteerd is "balkanisering van de cloud". Het is zonder meer een beladen term en achteraf bleek dat echt niet iedereen in de zaal begreep wat er mee bedoeld werd.

Een ander voorbeeld van taalgebruik in relatie tot cloud werd genoteerd bij de presentatie van Evangelos Floros van GrNET, de IaaS oplossing voor de academische sector toepassing [5]. Een van de randvoorwaarden die daarvoor gold was dat die cloud secure en sustainable moest zijn. In Nederland associëren we het begrip subliminale vooral met groen of duurzaam. In Griekenland heeft het uitsluitend te maken met het rond krijgen van de businesscase. Peleus Uhley van Adobe, gaf in zijn presentatie een praktijk voorbeeld van onjuiste taal- en beeldgebruik. Hij merkte op dat we heel vaak cloud afbeelden als een wolk en daarin de servers aan de frontend en de backend als twee losse serverkasten. Dat beeld is herkenbaar en laat zich makkelijk uitleggen, maar het is inmiddels te vaak onjuist. Tegenwoordig zijn backend en frontend steeds vaker geen separate fysieke machines meer maar elk weer onderdeel van een virtuele omgeving. Dat legt moeilijker uit, gaf de spreker direct toe, het kan verwarring geven door 3 wolken in een afbeelding te stoppen. Maar het is wel nodig want anders leggen we de zaak niet goed uit en ontstaat onvermijdelijk spraakverwarring op enig moment.

Telco's

De eerste panelsessie waren gewijd aan de rol die telco's nu en op termijn spelen op het vlak van secure cloud. Telco's zijn allemaal gewend te denken in grote aantallen en perfect in

Telco's kunnen complexe billingstraten runnen, daarom zijn zij cloud leverancier geworden

staat complexe billingstraten te runnen. Dat laatste werd door enkele sprekers uit die sector aangegeven als een belangrijke zo niet de belangrijkste reden waarom ook zij allemaal cloud leverancier gaan worden. Opvallend was verder dat in deze groep de link werd gelegd tussen het begrip critical infrastructure, de core business telefonie en datatransport en secure cloud. Tegelijkertijd werd duidelijk dat telco's hier een positie claimen omwille van new-business maar nog niet helemaal klaar zijn met de invulling van de case. Gaat de focus uit naar enterprise cloud, MKB cloud diensten of juist voor de grote aantallen, de SoHo en consumenten markt. Cloud is voor elk van deze segmenten een ander aanbod (achter de schermen hoeft dat trouwens niet) en elk segment vraagt ook weer een aparte benadering. Gaan telco's dit allemaal zelf uitvoeren of worden ze in toenemende mate reseller van white-label cloudoplossingen die elders worden ingekocht. Voorbeeld van dat laatste is een cloud oplossing dat Belgacom haar klanten biedt. Dit is een dienst van F-Secure dat relabelled is. Ander voorbeeld is de wijze waarop Britse telco's en internetproviders mail leveren, dat is voor bijna alle grote spelers een van de bekende Amerikaanse SaaS oplossingen. De wijze waarop telco's die inkoopslag combineren met focus op security zal nog wel vaker aan de orde komen. Ook voor partijen die niet de consumentenmarkt (B2C) als speerpunt hebben of zich positioneren als leverancier van telco's vormt dit al een ontwikkeling die de moeite van het volgen waard is.

Snowden en NSA

Onvermijdelijk waren deze twee begrippen en zeer prominent aanwezig tijdens de conferentie. Waar Richard Clarke zijn best deed de vernieuwde NSA te beschrijven was dit bij alle andere sprekers keer op keer aanleiding voor kritische noten. Duidelijk was dat de onrust die de Snowden affaire heeft veroorzaakt, nog lang niet voorbij is. Amerikaanse aanbieders maar ook Britse sprekers worstelden hier mee en in elke zaal was er wel iemand die daar lastige vragen over wist te stellen. De impact in de dagelijkse praktijk werd door meerdere sprekers geïllustreerd. Aernout Reymer van BT gaf aan dat de affaire direct leidde tot een ander type vragen van klanten. Het is niet meer 'are you safe?', maar 'show me you're safe!' De spreker van Verizon, Lee Miller, ging hierin mee en wees erop dat aantonen waar data staat relatief eenvoudig is. Door de onrust

van de laatste maanden verlangen klanten nu ook vooral dat wordt aangetoond dat data ergens niet staat. Dat is in een fysieke omgeving al lastig, maar hoe toon je dat aan in de context van cloud. Beide sprekers sloegen hiermee een brug naar een permanent terugkomend onderwerp tijdens de conferentie: audits. Audits om vertrouwen te verkrijgen of om het afkalvende vertrouwen te herstellen. De spreker van Google, Peter Dickman, plaatste een terechte opmerking toen het begrip "right to audit", dat sinds de Snowden onthullingen schijnbaar nog vaker wordt gebezigd, werd besproken. 5 miljoen klanten en het "right to audit"? Dat is het grootst mogelijke security risico dat je je maar kunt voorstellen. Die relativering kwam komisch over, maar had een uiterst serieuze ondertoon. Een pasklare oplossing voor bedrijven met veel klanten die steeds vaker met audits eisen was op deze conferentie niet beschikbaar.
Desondanks zal iedere bezoeker aan deze conferentie in antwoord op de vraag wat rond het onderwerp Snowden en NSA de meeste indruk heeft gemaakt een antwoord geven dat geen betrekking heeft op bovenstaande. Zoals ook elders is beschreven hebben twee aspecten van de keynote van Richard Clarke veel indruk gemaakt. De eerste was de – wellicht cynisch bedoelde – opmerking dat iedereen die zich zorgde maakte om het aftappen van zijn cloud of data door de NSA gewoon zijn spullen op Amerikaanse bodem moet zetten. Daar heeft de NSA namelijk veel minder bevoegdheden en mogelijkheden. In het buitenland daarentegen, dat hoefde de zaal amper te worden uitgelegd. Haaks op die opmerking stond zijn slotwoord: het was de oprechte bezorgdheid dat we veel te weinig doen om 'the police surveillance state' tegen te houden.

EU

De keynote van Neelie Kroes is al aan het begin genoemd, maar ook gedurende de gewone sessies was de EU een van de centrale thema's. EU werd gehanteerd als motief voor een lokalisering van cloud, als een factor die uitwisseling van data in het algemeen bepaalt en natuurlijk als handelsblok dat gewoon kwaliteitseisen kan stellen.
Een interessante opmerking hierover werd gemaakt door Udo Helmbrecht, de executive director van Enisa. Hij wees op het EU verplichte logo voor veilig speelgoed. Waarom, vroeg hij zich hardop af, hebben we EU breed nog geen label systeem dat zowel SME's als burgers helpt de kwaliteit van het cloud aanbod te bepalen. Elders werd verwezen naar de energie labels, zou dat niet een manier zijn om specificaties van cloud zoals veiligheid eenduidiger weer te geven. De vertegenwoordigster van de Zweedse Piratenpartij, Amelia Andersdotter, had een variatie op het thema EU labels. Prijzen voor consumenten in de EU moeten altijd inclusief BTW zijn. Kunnen we van cloudaanbieders ook niet eisen dat bepaalde privacy en security componenten altijd verplicht inclusief zijn?
De EU bezorgdheid over labels was nadrukkelijk aanwezig. Op de vraag waar die zorg vandaan komt zijn meerdere antwoorden mogelijk. De EU-sceptici vrezen dat dit de voorbode is voor een zoveelste EU-loket en toename van de administratieve lasten voor ondernemers. Anderen, in ieder geval Kroes en de medewerkers van EU instellingen, zullen wijzen op de achterblijvende vraag in de EU naar clouddiensten. Met in het achterhoofd de rapporten die wijzen op een maximale bijdrage aan de EU economie tot 2020 in de vorm van 400.000 nieuwe SME bedrijven en 4.000.000 nieuwe banen is het begrijpelijk dat die laatste groep vooral op zoek is naar manieren cloud te stimuleren. Wat geen van de partijen hardop zei is dat alle argwaan en twijfel die er bestaat rond de veiligheid en betrouwbaarheid van IT nu wordt gefocust op cloud. Cloud als zondebok of bliksemafleider? De EU medewerkers en natuurlijk alle aanbieders van deze en gene zijde van de grote plas hebben daar duidelijk geen behoefte aan. Cloud als multifunctionele toolbox om de stagnatie dan wel recessie te bestrijden: daar heeft men duidelijk wel behoefte aan.

Standaarden – welke standaarden?

Voor een buitenstaander is het vreemd te horen dat cloud geen echte standaarden kent. IaaS, SaaS, PaaS, die termen lijken te verwijzen naar in beton gegoten industriestandaarden, maar zijn het niet. Na twee dagen was tevens duidelijk dat begrippen als veiligheid en beschikbaarheid door partijen verschillend worden geïnterpreteerd. Daar is niets mis mee, zolang de beoogde gebruiker van de diensten in kwestie dit maar vooraf op een eenduidige en heldere wijze is medegedeeld. Op dat punt trok menig spreker de volle aandacht van de zaal. Professionals en insiders weten het al lang, maar ISO certificering is slechts een point in time. Bedrijven als SAP kunnen hier weinig mee. Dit soort partijen voorspelden dan ook dat continuous auditing de oplossing zal zijn. Maar vooralsnog is het vooral een pittige uitdaging om zoiets intern van de grond te krijgen en extern verkocht en geaccepteerd te krijgen. De methodiek die CSA heeft ontwikkeld (STAR) kwam uiteraard ook uitgebreid ter sprake. Wie meer wil weten van de discussies over ISO tijdens de conferentie: Bart Veldhuis heeft daarover een goed verslag gemaakt dat op computable.nl [6] te lezen is.

Juridische issues en cloud techniek

Dat tijdens een bijeenkomst over cloud ook de juridische valkuilen ter sprake komen is onvermijdelijk. De secure cloud conferentie was in zoverre een uitzondering op die regel, dat het aantal besproken valkuilen meeviel. De vaak gehoorde opmerking dat legal en techniek niet te synchroniseren zijn is deels terecht, maar Danielle Catteddu van CSA gaf aan dat we vooral moeten onthouden dat binnen bestaande contracten en wetgeving cloud niet meer is dan de variatie op een thema.

Dat cloud techniek aanleiding geeft voor nieuwe contractbepalingen werd eveneens duidelijk. Wellicht inhakend op de opmerking van Lee Miller, die opmerkte dat het voor cloud aanbieders lastig is aan te tonen dat data ergens niet staat, vestigde Catteddu de aandacht van de zaal op het verschijnsel cloud termination. Voor meer dan alleen security experts en informatie beveiligers is dit een onderwerp waar in bestaande en nieuwe contracten echt aandacht moet worden besteed. Catteddu noemde als andere dealbreakers: het ontbreken van goede contracten tussen de verschillende processors van data en de situatie waarin twee partijen als data controllers worden aangemerkt. Als laatste stelde hij nog de vraag: wat moet je doen als tijdens een contractperiode een van de partijen in de waardeketen (los van het gegeven of het een producent of bewerker is) wordt overgenomen? Het antwoord op de vraag kon hij zelf niet geven, wel de tip dat op dit punt de bestaande contracten nog eens goed moeten worden doorlopen.

Security in de cloud - de praktijk

Dat tijdens secure cloud heel vaak het begrip security werd gehanteerd zal niemand verwonderen. Het begon al bij de keynote van Kroes die de zaal om de oren sloeg met cijfers over data breaches en datalekken en de vraag stelde "why are we so vulnerable?" Het was weinig opmerkelijk dat zowel sprekers uit de profit sector zich terughoudend opstelden bij het geven van voorbeelden ter illustratie van veiligheid. Wat zonder twijfel het meest werd genoemd was encryptie. Of het nu gaat om encryptie van data, opslag of transport, iedereen leek van mening te zijn dat dit een eerste en zeer belangrijke stap is cloudgebruik op een hoger acceptatie- en veiligheidsniveau te brengen. Over de vormen van encryptie en het gebruiksgemak liepen de meningen sterk uiteen, dit kan deels komen omdat nogal wat partijen hier een eigen commercieel belang hebben.
Het beschrijven van risico's – die nadrukkelijk niet uitsluitend cloud only waren – ging de meesten makkelijker af. Voor de hand liggende constateringen als re-use van wachtwoorden passeerden de revue. Meerdere sprekers legden ook de link tussen het onderschatten van de waarde van data en de kans slachtoffer te worden van een security- of data breach. Brian Honan van Iriscert [7] had in het kader van monitoring van risico's de nodige tips. Een viel op omdat deze echt 100% cloud gerelateerd was. Medewerkers die tijdelijk iets in de cloud stallen en daarbij bestaande bedrijfspolicies omzeilen zijn een te traceren risico. Zorg dat de boekhouding bij de controle van betalingen met de bedrijfskredietkaart of de maandelijkse declaraties van medewerkers extra oplet bij posten die verwijzen naar cloudaanbieders. Dat veronderstelt samenwerking tussen boekhouding en IB'ers of de IT-security staff, iets dat in zijn optiek wel vaker voor verbetering vatbaar is.

Oordeel over Secure Cloud

Aan de hand van zeven verschillende begrippen is een beeld geschetst van de complexiteit die onlosmakelijk verbonden is met het gebruik van clouddiensten. Waar de meeste events voor een beperkte invalshoek kiezen, heeft Secure Cloud nadrukkelijk voor een brede kijk op de materie gekozen. Dat maakte de tweedaagse bijeenkomst soms lastig te volgen, maar het bood zowel plenair als in de marge van de bijeenkomst heel wat ruimte de samenhang tussen de verschillende factoren te analyseren. Zoals te verwachten viel: voor geen van de genoemde problemen was na de twee dagen een kant en klaar antwoord beschikbaar.
Misschien is dat ook het best mogelijke resultaat. Iedereen die hoopte direct toepasbare oplossingen gepresenteerd te krijgen keerde wat dat betreft met lege handen naar huis. Hij of zij heeft wel geleerd dat het inzien van de samenhang tussen de verschillende factoren meer dan eens nodig is om te begrijpen waarom cloud – as we know it – in de perceptie van vooral gebruikers niet veilig genoeg kan zijn. De balans vinden tussen emotie en ratio, tussen verwachtingen en realiteit, weten dat het geen of-of keuzes betreft, dit alles veronderstelt inzicht in de factoren die inhoud geven aan het begrip cloud. Wat dat betreft is de opzet van deze conferentie zonder meer geslaagd.

Links

[1] https://cloudsecurityalliance.org/

[2] https://www.enisa.europa.eu/?

[3] https://www.fokus.fraunhofer.de

[4] https://cloudsecurityalliance.org/events/securecloud2014/#_agenda

[5] https://www.grnet.gr/

[6] http://www.computable.nl/artikel/opinie/cloud_computing/5049473/2333364/iso-27001-is-geen-garantie-voor-veilige-cloud.html

[7] http://www.iriss.ie

SMART SECURED

It is always the goal of this column to keep up with the times and the changes that follow, applying SABSA thinking to new situations and evolving new Business Attributes. In this issue we shall examine a recent concept that is about to be launched into reality – the Internet of Things (IoT). These 'things' are of course 'smart things' that the home of the future will embrace. Here is a short list of examples: smart home security and fire protections systems; smart domestic appliances, smart heating, lighting and energy management systems, smart technology integrated into cars, and, just to show the extensiveness of this concept, smart children's toys.

The technology architecture to realise this concept is fairly straightforward. Each 'smart thing' will have an embedded processing and memory chip, a power source (battery or mains) and a communications interface (probably wireless). Each home will have a local server to communicate internally with the 'smart things' and a communications hub connected to the server and to the Internet. Users will then have apps on their smart mobile devices that allow them to control their 'smart things' remotely. Each smart mobile device becomes a remote control for almost everything on the house or car (and probably the boat too if you own one). There are essentially two modes of operation – 'home' and 'away'. Maybe one day there will be robots to take stuff out of the smart fridge and put in into the smart oven, but not in the first wave. However, the smart fridge will probably soon be able to influence the online food shopping to re-stock items that are running low.

As with all new digital technology applications there needs to be a business driven approach to risk and security. The application of these technologies in this context brings with it a whole new range of operational risks – opportunities to improve the quality of life at home, but also a number of threats to the stability and comfort of that newly controlled, highly integrated, hi-tech lifestyle.

One commentator talks of the 'malicious teddy bear' as an attack vector, bought perhaps at a market stall, the provenance of the internal software untrusted, manufactured in a foreign country, and potentially containing malware that could be used to steal family bank account details, private health records and other sensitive private information. Another attack scenario might not be aimed at the family, but at the critical national infrastructure. Malware that could increase domestic demand for electricity in every smart home at exactly the same moment would threaten the stability of the national energy grid and perhaps cause power outages. There are many such attack scenarios that need some modelling tools to explore fully the potential risks.

Huge opportunities exist for industry and commerce too, with many new business applications of the IoT being developed in the future. Take for instance the ability to link incubators protecting premature babies to powerful analytics engines to monitor baby health in real time and recognise patterns that suggest a baby may be in distress. There will be many other patient monitoring possibilities too, which will transform health care efficiency. Security will be needed to protect the lives of people at risk.

There has been talk of the need for a new security standard to protect these new smart applications from a wide variety of threats, but as usual the talk is being led from the technology viewpoint, taking only a technical view. There are also commentators warning of too much focus on safety and security being a block to innovation. This is an area where SABSA can bring a lot of value to the table. It is essential that the threat scenarios be properly modelled so that the potential attack vectors and motivations can be identified. It is also essential that the true risk/reward balance be achieved through innovative risk management models. Only then will the industry be able to develop appropriate technology controls and enablers that fit with the actual risk profile of this smart landscape.

The Attributer

Verantwoorde onthullingen #9

TE GOEDKOOP VOOR SECURITY?

@1sand0s vindt geen gehoor bij de Youfone helpdesk

Ga ik naar een bijeenkomst waar ook hackers zijn, dan gooi ik er meestal even een tweet uit: "Nog tweeps aanwezig?" Zo kom ik aan cases voor deze column. 28 april was er weer zo'n bijeenkomst: #hackdetoekomst @De_Zwijger. Diverse bekenden reageren op mijn tweet. Zo ook @1sand0s, die ik die avond zie in de bar van Pakhuis de Zwijger. Hij heeft een zwart T-shirt aan met de tekst "I hacked my ISP and all I got was this lousy shirt." Dus ik roep: "He, heb jij een ethische hack op je naam?" Inderdaad. Hij kon bij zijn telecomprovider Youfone vrij eenvoudig accounts overnemen en heeft dit gemeld. Niet dat hij van hun dit T-shirt kreeg. Dat is van het NCSC, zoals te zien is aan het logo op zijn mouw.

Chris van 't Hof
De voorgaande case studies zijn te vinden op www.cvth.nl/vo

@1sand0s is volgens zijn Twitter profiel "researcher and teacher on the arts moving of 1s and 0s (preferably securely and privately) — RCX". Het blijkt te gaan om Jeroen van der Ham van de UvA. Hij studeerde en promoveerde daar en was er vier jaar Post Doc. Nu is hij onderzoeker en docent System and Network Engineering en begeleidt ongeveer 35 studenten in hun onderzoek. Die doen natuurlijk veel verantwoorde onthullingen, dus heeft hij met twee collega's nu een ethische commissie opgericht die de onderzoeken toetst. Ze kijken al bij de opzet van het onderzoek hoe de studenten omgaan met gevoelige persoonsgegevens en of hun onthulling verantwoord is. Elk onderzoek wordt voorzien van een risicoclassificatie, voor adequate begeleiding. Dat gaat over het algemeen goed.

Deze onthulling niet. Die kwam ook niet uit de opleiding, maar uit zijn persoonlijke omgeving. Zijn vriendin heeft namelijk een mobiel abonnement bij Youfone. Als ze oktober vorig jaar op haar persoonlijke pagina wil inloggen lukt dat niet. Ze probeert een nieuw wachtwoord aan te vragen, maar de site herkent haar e-mail adres niet. Of Jeroen er even naar wil kijken, het is immers zijn werk. Maar het lukt hem ook niet het wachtwoord aan te passen. Vreemd. Zelf heeft hij ook een Youfone abonnement, dus hij probeert of hij bij zijn eigen account wel een nieuw wachtwoord kan instellen. Dat lukt wel.

Tot zijn verbazing ziet hij dat hij zijn e-mail niet hoeft te verifiëren en er een wachtwoord wordt gegenereerd dat bestaat uit zijn postcode en huisnummer. Als je dus het e-mail adres en postcode

Geen zin, geen tijd, geen prioriteit? Of zijn sommigen gewoon te goedkoop voor security?

van een andere Youfone gebruiker hebt, kun je dus zo een account overnemen. Vervolgens kun je het abonnement aanpassen, het rekeningnummer zien, hoeveel er gebeld is en ook met wie en wanneer… Hij graaft wat dieper in de browser en ziet dat de communicatie niet versleuteld is en de interactie plaatsvindt met een sessie cookie. Dat betekent dat je er tussen kan gaan zitten en wachtwoorden af kan vangen. Dit is wel een hele reeks standaard security fouten.

Hij stuurt daarom meteen een mailtje naar de Youfone klantenservice. Vanaf zijn werkadres, want dan weten ze meteen dat ze hier te maken hebben met iemand die er verstand van heeft. Geen reactie. Dan maar openbaar. @1sand0s tweet aan @youfone: "Ik heb via contactformulier een bericht gestuurd, maar nog geen reactie. Het is best ernstig en zou z.s.m. antwoord willen zien!". Dan volgt wel een reactie: "Beste Jeroen, je krijgt binnen maximaal 5 werkdagen een reactie op je ticket. Stuur je 06 nummer in een pb, dan kijken wij alvast wat er aan de hand is." In de discussie die volgt via de DM, stelt de helpdeskmedewerker dat het lek niet echt een probleem is. Jeroen vraagt of hij het aan de media kan melden. Hij doet maar…

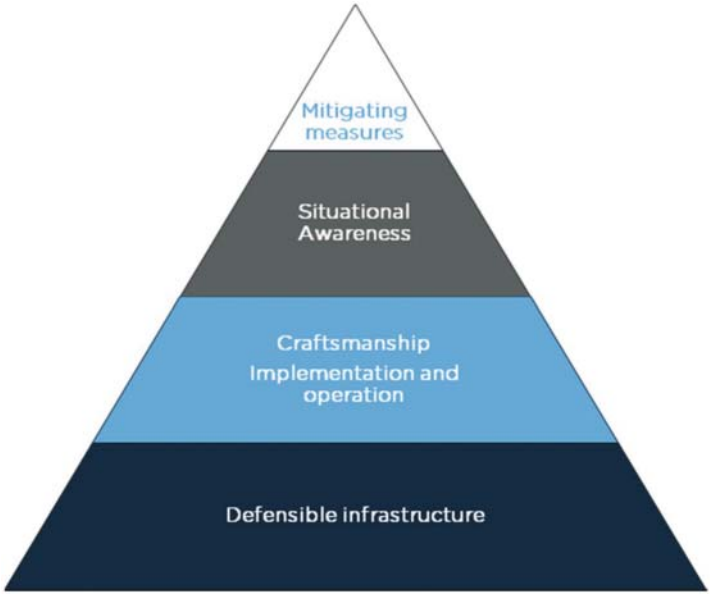
Dan maar naar het NCSC. Het is inmiddels vrijdagavond. Jeroen weet dat hun response team ook in het weekend werkt, maar dan alleen op de meest urgente meldingen reageert. Maandag krijgt hij een reactie. Het centrum ziet dit niet als haar primaire verantwoordelijkheid, maar omdat er ook burgers getroffen kunnen worden willen ze wel helpen. Een medewerker meldt dat Jeroen het beste contact kan opnemen met de directiesecretaresse en geeft hem haar e-mail adres. De secretaresse reageert op de mail dat ze ernaar zullen kijken. Als hij woensdag nog geen reactie heeft, mailt hij nogmaals…

Ondertussen benadert Jeroen de bouwer van de site, maar die reageert geïrriteerd: "Je moet ons niet lastig vallen, dit is iets wat Youfone zelf moet oplossen". Hij benadert ook verschillende journalisten die wel eens onthullingen hebben gedaan, maar die tonen geen interesse. Jeroen: "Zo'n melding is blijkbaar niet sexy meer". Dan maar weer wachten. Anderhalve week later heeft hij nog steeds geen reactie van Youfone. Hij blijft via de mail aandringen om een belafspraak met de directeur. Die belt na een paar dagen zowaar zelf terug. Hij vraagt: "Hoe erg is dit nou? Hoe zou je dit kunnen uitbuiten?" De directeur luistert geïnteresseerd wat iemand met dit lek zou kunnen en belooft dat de site gefixed wordt.

Dat gebeurt inderdaad. Jeroen moet het vernemen via de Youfone nieuwsbrief, waarin staat dat de site vernieuwd is, zonder vermelding van het incident of Jeroens melding. Als hij de site checkt blijkt er nog steeds geen e-mail verificatie te zijn. Er wordt gelukkig nu wel een random wachtwoord gegenereerd en niet een postcode. Ook de encryptie en de sessie cookie is aangepast. Vreemd is wel dat het certificaat dat erachter hangt dateert van 22 juli 2013, drie maanden voor zijn melding. Ze hadden dus al een oplossing klaar liggen, maar om de een of andere reden niet ingevoerd.

Jeroen vond het al met al erg frustrerend. Hij is er drie weken mee bezig geweest, zonder enige reactie van hun kant. "Er moet begrip zijn voor persoon die de melding doet, want die doet dat vrijwillig, zonder belang. Je zou snel afspraken moeten maken met de melder over vrijwaring van vervolg en hem op de hoogte houden van de voortgang" Hij stuurt Youfone tot slot nog een mailtje waarin hij schrijft blij te zijn dat het nu is opgelost en krijgt een kort bedankje. Dan stuurt @1sand0s 7 november zijn laatste tweet over de zaak: "Na een responsible disclosure procedure (met dank aan @ncsc_nl) heeft @youfone nu een veiligere klantenportal."

Responsible Disclosure beleid zou volgens de andere telco's die ik tegenkom in mijn onderzoek sector-breed zijn ingevoerd. Bij deze blijkbaar niet. Op www.youfone.nl (een site die ongevraagd cookies plaatst) staan vooral "superrrrr goedkope aanbiedingen", maar nog steeds geen e-mailadres waar je veiligheidsproblemen kunt melden, laat staan een richtlijn. Geen zin, geen tijd, geen prioriteit? Of zijn sommigen gewoon te goedkoop voor security?



Security Survival Pyramid – CC BY Frank Breedijk

DE SECURITY SURVIVAL PYRAMID

Een model om de effectiviteit van controls in te schatten

Bij het beveiligen van complexe systemen is het stellen van de juiste prioriteiten essentieel, zeker als er sprake is van beperkt budget. De Security Survival Pyramid van Joshua Corman van de Carnegie Mellon University is daarbij een uitstekende leidraad. Hoe een model dat werd bedacht om een zombie apocalyps het hoofd te bieden kan helpen bij het beslissen over beveiligingsmaatregelen.

Frank Breedijk is Security Officer bij Schuberg Philis, een organisatie die zich richt op de outsourcing van complexe bedrijfskritische applicatie infrastructuren met hoge beschikbaarheidseisen. In het verleden was hij manager van het EMEA Security Operations Center voor managed security services van Unisys en werkte hij als security officer voor Interxion. Tevens is hij de auteur van het open source security security programma Seccubus.
Hij is bereikbaar op fbreedijk@schubergphilis.com

Corman legde zijn Security Survival Pyramid voor het eerst uit aan de hand van de bekende zombiefilms. Een effectieve verdediging tegen een massale aanval van de ondoden volgt dezelfde regels als een effectieve securityomgeving volgens Corman. Corman liet zich voor zijn model duidelijk inspireren door de piramide van Maslow en Sun Tzu's 'The Art of War.'

Missing Cycles - CC-BY Camil Tulcan

In het kort komt de gedachte achter Corman's piramide hier op neer: wie zich wil verdedigen tegen een tegenstander moet zich concentreren op de meest effectieve verdedigingsmethode: de methode die met de laagste kosten en de minste inspanning het meeste doet om de tegenstander te pareren.

Het fundament is de basis van het model: een zwakke eerste laag tast de effectiviteit van de bovenliggende lagen aan. Elke laag bouwt immers voort op de vorige. Het model van Corman beoogt inzicht te geven in de eigen securityomgeving, niet de verschillende securitymaatregelen definitief te categoriseren: tussen de lagen van de piramide is overlap mogelijk.

Verdedigbare infrastructuur

Aan de basis van de piramide staat het innemen van een positie die langdurig, effectief en met zo min mogelijk middelen kan worden verdedigd, de zogenaamde defensible infrastructure. Het klassieke voorbeeld hiervan is het afschermen van de infrastructuur van het internet door middel van een firewall. Dit is lange tijd ook het enige middel geweest dat door de informatiebeveiliger werd ingezet, maar tegenwoordig is alleen een firewall niet langer voldoende. De moderne tegenstander heeft immers een enorme slagvaardigheid.

Een verdedigbare positie, hoe stevig ingericht ook, is niet genoeg. De volgende laag in de piramide benoemt het vakmanschap van de verdedigers, door Corman operational excellence genoemd. In de praktijk blijkt dit vakmanschap bijvoorbeeld uit hoe de firewall is ingericht, maar toont het zich ook in hoe systemen worden gepatcht door systeembeheer. Dit vakmanschap gaat bovendien verder dan de deskundigheid van security experts alleen: de gehele organisatie, inclusief alle medewerkers, moet streven naar optimale beveiliging, bijvoorbeeld om phishing-aanvallen te voorkomen.

Situatiekennis

Defensible infrastructure en operational excellence zijn het fundament onder de volgende beschermingslaag: situational awareness. Voor een effectieve beveiliging is kennis van de actuele situatie onmisbaar, zowel van het eigen systeem als de wereld daarbuiten. Weten dat het systeem afwijkend reageert kan al de eerste stap van de verdediging zijn. Een SIEM-systeem kan daarbij helpen.
Daarnaast is het van belang om inzicht te hebben in de kracht van de tegenstander, door security gerelateerd nieuws te volgen en threat intelligence diensten te gebruiken.

Specifieke maatregelen

De top van de piramide wordt gevormd door mitigating measures: maatregelen die er op zijn gericht één specifieke bedreiging te mitigeren. Door de beperkte toepasbaarheid van deze maatregelen leveren zij beveiligingstechnisch weinig op. Hierbij gaat het bijvoorbeeld om een software escrow agreement, maar ook om het dichtlijmen van usb-poorten om een virus dat via usb wordt verspreid te weren. Mitigating measures kunnen zeker effectief zijn, maar het is verstandig ze alleen in te zetten als de situatie dat dicteert.

Toch zijn het juist deze zeer specifieke maatregelen die in de security industrie buitensporig veel aandacht krijgen. Een experiment van Corman, waarbij hij de onderwerpen van de voordrachten tijdens een RSA-conferentie heeft geprojecteerd op de piramide, laat zien dat de securityindustrie voornamelijk praat over mitigerende maatregelen en onvoldoende over het creëren van een solide basis, bestaande uit een verdedigbare infrastructuur en vakmanschap. Een praktijkvoorbeeld als de DigiNotar-hack laat zien wat de gevolgen kunnen zijn van het ontbreken van een goede basis.

Helemaal serieus was Corman waarschijnlijk niet, toen hij zijn model presenteerde aan de hand van een zombie apocalyps. Maar zij die zich moeten verdedigen tegen de ondoden doen er goed aan het model van Corman te bestuderen. Hetzelfde geldt voor security experts: in beide gevallen is de tegenstander immers zeer vasthoudend.

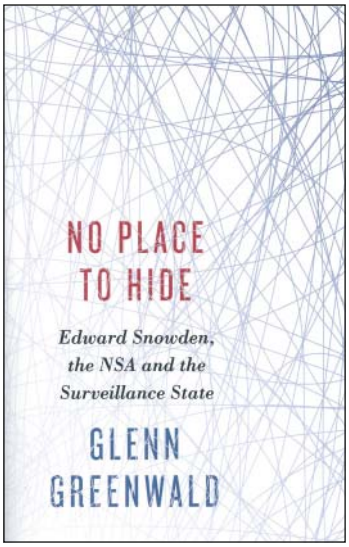
Links:

Artikel op ITWeb:
http://www.itweb.co.za/index.php?option=com_content&view=article&id=68638

Slides van Corman presentatie:
http://www.security-innovation.org/pdfs/Corman%20Presentation.pptx

Artikel van Trusted Software Alliance:
http://www.trustedsoftwarealliance.com/2013/06/13/software-survival-guide-pyramid/

NO PLACE TO HIDE



Productdetails
Titel: No place to hide
Auteur: Glenn Greenwald
Taal: Engels
ISBN-10: 162779073X
ISBN-13: 978-1627790734

Glenn Greenwald is wereldwijd bekend geworden als de journalist, die de eerste NSA documenten publiceerde, die door Edward Snowden aan hem waren doorgespeeld. Ook is hij een bekend tegenstander van massa surveillance door de overheid. Hij heeft hierover al eerder boeken gepubliceerd en is een bekend blogger over dit thema. In dit boek beschrijft Greenwald hoe het contact met Snowden tot stand is gekomen en hoe hij bijna deze primeur had gemist. De titel van het boek komt uit een statement van Senator Frank Church, voorzitter van de senaatscommissie, die al in 1975 onderzoek deed naar de "intelligence" activiteiten van de Amerikaanse overheid. In de eerste drie hoofdstukken beschrijft Greenwald hoe het contact met Snowden via anonieme e-mails tot stand kwam. Omdat Greenwald in eerste instantie geen versleuteling voor zijn e-mail gebruikte duurde het enkele maanden voordat hij uiteindelijk via een kennis in Hong Kong in contact werd gebracht met Snowden. In het boek wordt uitvoerig stil gestaan bij de persoon Edward Snowden, zijn achtergrond en zijn beweegredenen om uiteindelijk zoveel geclassificeerde informatie naar buiten te brengen. In de beschrijving komt hij over als een "mens met een missie", namelijk het aan de kaak stellen van de verregaande aantasting van Amerikaanse staatsburgers door de NSA en haar partners. Verbazingwekkend is ook om te vernemen hoeveel van die partners commerciële (grote) bedrijven zijn, die ook in Europa actief zijn. Verder wordt duidelijk dat 9/11 door de Amerikaanse overheid, en met name de NSA, is aangegrepen om dit soort "surveillance" op te zetten, en later zelfs (via FISA en Patriot Act) een formele basis te geven. Het leidende motto van de toenmalige directeur van de NSA generaal Keith Alexander, was "collect it all", dat zegt genoeg. Greenwald beschrijft hoeveel invloed de Amerikaanse overheid achter de schermen heeft op de pers in de USA, wat voor hem reden was om de eerste publicaties in "The Guardian" te laten verschijnen, een van oorsprong Britse krant. Als je leest hoeveel moeite hij heeft moeten doen om dit gepubliceerd te krijgen, begin je jezelf af te vragen wat er nog meer in de beerput zit waarover de pers niet wil schrijven. In de laatste twee hoofdstukken gaat Greenwald in op het gevaar van een "surveillance state" à la 1984, waarbij het opvalt dat hij vooral de gevaren voor de Amerikaanse staatsburgers voorop stelt. De rest van de wereld komt er een beetje bekaaid van af. De Amerikaanse overheid gebruikt vooral het argument van terrorismebestrijding om deze activiteiten goed te praten, maar Greenwald geeft aan dat de kans dat een Amerikaan door de bliksem wordt getroffen vele malen groter is dan dat hij of zij door een terroristische daad om het leven komt. Wat verder opvalt is dat de Amerikaanse oppositie tegen dit soort massa spionage activiteiten is, maar als ze aan de macht komen, praten ze het ineens goed (denk aan de wisseling van Bush naar Obama).

Conclusie: *als u op zoek bent naar een compleet overzicht van alle documenten, die door Edward Snowden publiek gemaakt zijn, moet u op internet zoeken. Als u interesse heeft in waarom Snowden dit gedaan heeft en hoe de publicaties uiteindelijk tot stand gekomen zijn, dan is dit precies het boek voor u.*

Lex Dunn. Lex is werkzaam bij Capgemini en redacteur van dit blad. Hij is bereikbaar via lex.dunn@capgemini.com


Lex Dunn


André Koot

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

Internet of Things

Het komt er niet al aan, maar het is er al… Misschien weten jullie het niet, maar ooit had XS4ALL een mooie 1 april grap, een Senseo koffiezetter die je op internet kon aansluiten (de kopie van de aankondiging is hier nog te vinden: http://www.wie-niet.nl/overig/senseo/copy/).

Maar het downloaden van koffie vanaf het internet is tegenwoordig niet het grootste risico, wel dat al die apparaten enorme hoeveelheden openbare en vertrouwelijke informatie over het net heen en weer versturen. In een recent onderzoek (http://fortifyprotect.com/HP_IoT_Research_Study.pdf) bleek dat op dit moment 70% van de connected devices geen idee heeft van beveiliging. Wat vinden onze redacteuren hiervan? Is een smart koelkast of een smart bloeddrukmeter een risico?

Lex Dunn

Internet of Things, Internet of Everything, alles aan elkaar geknoopt, alles praat met alles, klinkt goed, maar wat gaat dat ons als securisten aan uitdagingen opleveren? Heel veel, vrees ik. We hebben hier duidelijk te maken met een "technology push", die zonder al te veel aandacht te schenken aan beveiliging over ons uitgestort wordt. Er zijn al legio voorbeelden genoemd van waar het mis kan gaan: koelkasten op afstand uitschakelen (kom je terug van vakantie, is alles bedorven en je hele huis stinkt), lantaarnpalen willekeurig aan- en uitschakelen, ramen of schuifdak van je elektrische bolide worden door je prettige collega's open gezet tijdens een stevige Hollandse regenbui en ga zo maar door. Voorlopig zie ik slechts één beveiligingsmechanisme voor dit soort zaken en dat is "security by obscurity": er zijn straks zoveel dingen gekoppeld, dat je door de bomen het bos niet meer ziet. Maar moeten we daarop vertrouwen? Nee, wij moeten als consumenten en zakelijke gebruikers van de leveranciers eisen dat zij hun producten van "voldoende" beveiliging voorzien. Wat mij betreft is dat dus minimaal versleuteld verkeer, toegangsbeveiliging middels gebruikersnaam/wachtwoord (liever nog twee-factor authenticatie), logging en rapportage (bv het kunnen versturen van logs naar jouw mailbox om inbraakpogingen te signaleren), mogelijkheid om de software te updaten (als er kwetsbaarheden bekend worden wil je toch dat de leverancier daar wat aan doet) en wellicht een soort beveiligingsclassificatie (analoog aan het Politiekeurmerk voor sloten), maar vooral goede voorlichting voor de gebruikers. En ja, dat zal geld kosten, maar met dit soort maatregelen kan een gebruiker zelf kiezen of 'ie voor goedkoop en niet beveiligd gaat, of toch liever wat meer geld uitgeeft om goede beveiliging te krijgen. En apparaten, die potentieel dodelijk kunnen zijn voor hun gebruiker, zouden minimaal vijf sterren moeten hebben (pacemakers, insulinepompjes). Tot slot zouden de gebruikers zich af moeten vragen of het wel nodig/wenselijk is dat hun apparaat aan het net wordt gekoppeld: er zijn bijvoorbeeld nu al wasmachines die je via internet van nieuwe wasprogramma's kunt voorzien. Daarvoor hoeft het apparaat zelf helemaal niet permanent aan internet te hangen, je kunt ook een update via een USB-stick uitvoeren. Voor de SF liefhebbers onder ons: lees "Accelerando" van Charles Stross eens, dan heb je een idee waar dit allemaal toe kan/gaat leiden ;-).

André Koot

Als ik denk aan het Internet of Things, dan moet ik, hoe gek het ook klinkt, altijd denken aan mijn koelkast die automatisch mijn bier bestelt als 'ie merkt dat de voorraad op is. Handig en zo heb je ook altijd grip op de vervaldatum van de producten in de koeling. Oude potjes BBQ saus zijn met IoT geen zorg meer. Maar het oplossen van dat probleem leidt meteen tot een nieuw probleem. Het betekent dat mijn koelkast mij gaat kennen, weet wat mijn gedrag is en dat dan vermoedelijk ook doorspeelt aan de leverancier van de potjes saus of aan de leverancier van de koelkast. Op zich ben ik daar niet meteen bang voor. Dan weet meneer Liebherr dat ik ga barbequen, nou en? Dat is nou niet heel spannend, wat spannender is, dat is dat misschien ook anderen dat te horen krijgen, als ze het al niet ruiken. Nee, er is een ander probleem: Als mijn koelkast op internet zit, dan zit internet op mijn koelkast. En daar mogen we ons wel zorgen gaan maken. Hoe is gewaarborgd dat alleen ik, als gebruiker, invloed heb op wat mijn koelkast doorseint. Niet. Heel simpel. En hoe we dat weten? Nou, als zelfs in professionele omgevingen die waarborg niet bestaat, hoe zal dat dan in consumentenomgevingen zijn geregeld? We weten vast nog wel dat enige tijd geleden de sluis in de gemeente Veere via het internet te bedienen was met gebruikersnaam Veere en wachtwoord Veere. Als de sluis op internet zit, dan zit internet op de sluis. Ik geloof dus meteen dat IoT betekent dat de producenten heel snel ICS en Scada moeten bestuderen voordat ze besluiten dat ik een nieuw kratje bier moet hebben. Gelukkig hoef ik daar niet bang voor te zijn, want wij bewaren de voorraad bier niet in de koelkast, maar in de kelder en daar heb ik geen bereik.

COLOFON

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

PvIB
Platform voor InformatieBeveiliging

REDACTIE
Lex Borger (hoofdredacteur, werkzaam bij i-to-i)
e-mail: hr@pvib.nl
Motivation Office Support bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

REDACTIERAAD
Tom Bakker (Digidentity BV)
Kas Clark (NCSC)
Lex Dunn (Capgemini)
Ronald van Erven (Timeos Pensioendiensten)
Maarten Hartsuijker (Classity)
André Koot (Strict)
Rachel Marbus (NS, IT Advisory)
Bart van Staveren (UWV)
Martijn Veken (SNS REAAL)

ADVERTENTIE ACQUISITIE
e-mail: adverteren@pvib.nl;
of neem contact op met MOS
(Motivation Office Support)
T (033) 247 34 00
ibmagazine@pvib.nl

VORMGEVING EN DRUK
VdR druk & print, Nijkerk
www.vdr.nl

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

ABONNEMENTEN 2014
De abonnementsprijs in 2014 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

TO HACK OR NOT TO HACK

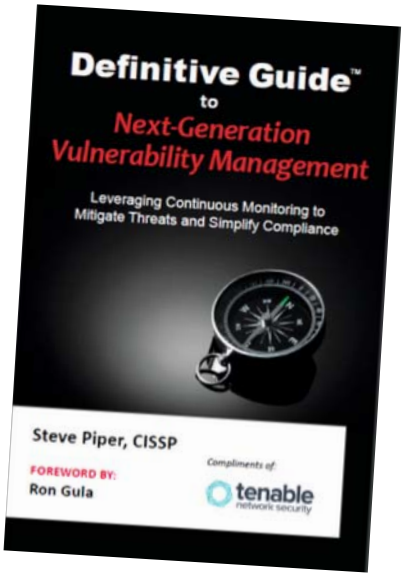
Behalve dat er verschrikkelijke dingen in Rusland gebeuren die groot menselijk leed tot gevolg hebben zijn ook veel russen actief als hacker. Een klein bericht in het NRC van augustus laat zien dat er maar liefst 1,2 miljard gebruikersnamen en wachtwoorden in hun bezit zijn, verzameld vanaf zo'n half miljoen websites. Combineer dat met de wetenschap dat de meeste internetgebruikers slechts één wachtwoord hebben dan kun je je voorstellen dat dit wel een hele vervelende zaak is voor de eigenaren van de gehackte gegevens.
Zouden mijn inloggegevens van DigiD er ook bij zitten? Bij de audit van 2013 door DigiD bleek dat 5% van de gebruikers van DiGiD een zeer hoog risico liepen via de site die ze gebruikten. Ik weet niet of mijn gemeente erbij zit, maar heb voor de zekerheid mijn password maar even gewijzigd. Een bijkomend probleem is dat je eigenlijk nooit weet of er gegevens van je website zijn gekopieerd als er onvoldoende maatregelen zijn getroffen, maatregelen kosten geld en dat hebben sommige bedrijven er niet voor over. Veel bedrijven nemen onvoldoende maatregelen, maar verplichten je wel jouw gegevens achter te laten. Hoe vaak laat u uw fiets zonder slot achter in de binnenstad? Hoe vaak laat je je portemonnee op het terras liggen en gaat u binnen even naar het toilet? Twee kleine voorbeelden, maar het grote verschil met het datalekken is dat u ervoor gekozen hebt om uw fiets en portemonnee kwijt te raken. Terug naar het onderwerp, op dit moment is het mogelijk dat er grote boetes uitgedeeld gaan worden bij datalekken, maar hoe weten zij dat het mijn data is die gelekt is? Stel dat ze mijn e-mailadres tegenkomen, hoe weten ze dan van welke site die gekopieerd is? Hoe weet de eigenaar van de site dat de data zijn gekopieerd als je daar niet de goede middelen ter beschikking hebt?
Internet is eind vorige eeuw in de lucht gekomen om simpele berichten onderling uit te wisselen. Om elkaar goedemorgen of -middag te wensen, afhankelijk van de tijd dat je elkaar groet. Internet is niet bedoeld voor bankzaken, webshops, bestandsuitwisseling, back-up medium en al dat soort zaken. We gebruiken het daar wel voor omdat het zo makkelijk is en omdat ik nu met een aantal toetsaanslagen kan zien waar de door mij gewenste TV het goedkoopst kan worden besteld of welke autoverzekering bij mij het beste past. Mijn bank is nu een website, mijn verzekeraar is een website. Ik heb ook niet zoveel keus, nog sterker, alle bankgebouwen en verzekeringskantoren zijn weg, her en der nog een kantoor met beleidsmedewerkers en techneuten. Mijn mail en mijn internetgebruik vind ik gewoon terug in de advertenties die ik op diverse websites tegenkom. Zelfs het type schoen waar ik gisteren naar gekeken heb, zag ik ineens tussen de advertenties. Ik weet het niet of mijn inloggegevens bij de 1,2 miljard gegevens zitten. Ik weet niet of die op dit moment worden gebruikt. Ik weet niet of ze nu mijn creditcard aan het plunderen zijn. Is er een weg terug? Nee, er is geen weg terug. Internet zal meer en meer misbruikt worden om apparaatskosten terug te dringen en handel te genereren. Kunt u nog terug? Nee, u leest de berichten en krabt zich eenmaal op het achterhoofd en gaat verder met de dingen die u die dag gepland had. Ik ga dat nu ook doen. Ik had vandaag op de planning om alle voor mij nog bekende sites een wachtwoord wissel te doen en dan maar hopen dat ze aan het eind van de dag niet weer worden gehackt.

Berry

How can you protect what you don't know?

1. Identify Vulnerabilities
2. Reduce Risk
3. Ensure Compliance

Dowload the eBook to learn more on www.crypsys.nl



or request a hardcopy via www.crypsys.nl

Als value-add distributeur heeft CRYPSYS de afgelopen jaren veel organisaties geadviseerd. Met 25 jaar ervaring zit security in ons DNA.

Secure computing is onze "way of life"
Met zorg selecteren wij onze partners om de juiste oplossing te kunnen bieden voor iedere omgeving. Hierbij kijken wij niet alleen naar de functionaliteit, maar zeker ook naar innovativiteit, continuïteit en betrouwbaarheid. Dankzij deze ervaring beschikt CRYPSYS over alle expertise op het gebied van security om succesvol samen te werken met haar resellers. Met als resultaat een tevreden eindklant.

CRYPSYS oplossingen zijn fexibel

CRYPSYS 25