Security door de ogen van een specialist

Na een geslaagde Masterclass in Houten rees de vraag of wij voor CBM elke editie twee pagina's kunnen vullen met betrekking tot actuele security problematiek. Na enig overleg leek het ons het beste om dit vooral te doen naar aanleiding van vragen die de lezers van CBM hebben. Stuur uw security-gerelateerde vragen dus gerust in. Vooralsnog zullen we, bij gebrek aan vragen voor de eerste keer, enige onderwerpen uit de Masterclass wat verder uitwerken.

Privacy is een afweerrecht dat de persoonlijke levenssfeer beschermt. Het recht op privacy wordt ook wel omschreven als het recht om met rust te worden gelaten. Privacy is een ruim begrip: het gaat onder meer om de bescherming van persoonsgegevens, de bescherming van het eigen lichaam en van de eigen woning, de bescherming van familie- en gezinsleven, en het recht vertrouwelijk te communiceren via, brief, telefoon, e-mail en dergelijke. Privacy betekent dat men dingen kan doen zonder dat de buitenwereld daar inbreuk op maakt of zelfs weet van heeft. Maar zouden we ons beter niet de vraag stellen wat blijft hiervan over de laatste jaren.
Een voorbeeld dat we soms gebruiken tijdens lezingen over de problemen in verband met de combinatie van privacy en sociale netwerken is het verhaal van Bono's (zanger U2 red.) foto's op Facebook. Ongeveer 2 jaar geleden was de bekende U2 ster op vakantie in St Tropez. Daar ontmoette hij zijn goede vriend Simon Carmody, een voormalig lid van de minder bekende Ierse band Golden Horde. Deze nodigde hem uit voor een gezellig verjaardagsfeestje waar onze superster belandde in de armen van twee 19-jarige studentes, Andrea Feick en Hannah Emerson. Deze lieten zich tezamen met Bono fotograferen. Leuk was het natuurlijk niet voor de vrouw van Bono die een dag later de compromitterende foto's zag opduiken op Facebook. Ja, wie wil er nu niet gezien worden met Bono.

Sociale netwerken

"Online privacy is niet langer de sociale norm naarmate gebruikers van sociale netwerken het gewoon worden om informatie op het internet uit te wisselen", vertelde Mark Zuckerman, oprichter van Facebook, een tijdje geleden. In december vorig jaar zei Google-CEO Eric Schmidt in een interview met de Amerikaanse zakenzender CNBC iets gelijkwaardigs: "Als je iets hebt waarvan je niet wilt dat iemand het weet, dan moet je dat misschien om te beginnen niet doen." Schmidt gaf in het interview ook expliciet toe dat Google wel degelijk af en toe informatie uitwisselt met de Amerikaanse autoriteiten. "De Amerikaanse Patriot Act geldt voor iedereen en het is dus mogelijk dat alle informatie aan de autoriteiten wordt gegeven", aldus Schmidt. De uitspraken van Zuckerman en Schmidt roepen herinneringen op aan een beroemde opmerking die Sun-CEO Scott McNealy al in 1999 maakte tegenover een groep analisten en journalisten: "Jullie hebben sowieso nul komma nul privacy. Get over it." Dat onze privacy in een online en altijd verbonden wereld steeds verder onder druk staat, is ondertussen een dooddoener. Trouwens, is het ooit anders geweest? Meer en meer loop ik gewone burgers tegen het lijf die de mening zijn toegedaan dat privacy overbodig is voor wie niets te verbergen heeft. Want ook in het dagelijkse leven wordt de gemiddelde West-Europeaan zeven keer per dag gefilmd door de één of andere camera. Denk maar eens hoeveel wegcamera's en bewakingscamera's je per dag passeert. Waarom zouden we onze online privacy dan ook niet vrijwillig mogen opgeven via Facebook, Hyves, Netlog, Youtube, Twitter en andere sociale netwerksites? Allemaal online diensten die ons immers ook heel wat plezier en voordelen opleveren, is het niet? Niet toevallig zijn het bijna allemaal Amerikaanse bedrijven die erachter zitten. Alles is daar voor geld te koop, met inbegrip van je privacy. Er is veel geld mee gemoeid. Amerikaanse bedrijven verdienen soms massa's geld met de persoonlijke gegevens die ze veelal ongemerkt verzamelen. Want wie leest nu de kleine lettertjes in de meestal pagina's lange gebruikersvoorwaarden van al die sites? In Europa zijn de privacyregels voorlopig gelukkig strenger. Maar ze staan onder druk: de grootste bedreiging komt wellicht uit de online hoek. Het lijkt er bijna op alsof sociale netwerksites met opzet zijn uitgevonden om binnen te dringen in de privaatsfeer van burgers. Burgers die er vaak geen idee van hebben hoeveel informatie over zichzelf ze eigenlijk vrijgeven. En hoe lang die informatie hen kan achtervolgen, bijvoorbeeld bij potentiële werkgevers of toekomstige partners. Probeer Facebook maar eens zo te configureren dat je privacy volledig is beschermd. Dit is niet evident, alhoewel een zeer recente update dit wel beter aanpakt. Maar toch, veel mensen springen inderdaad

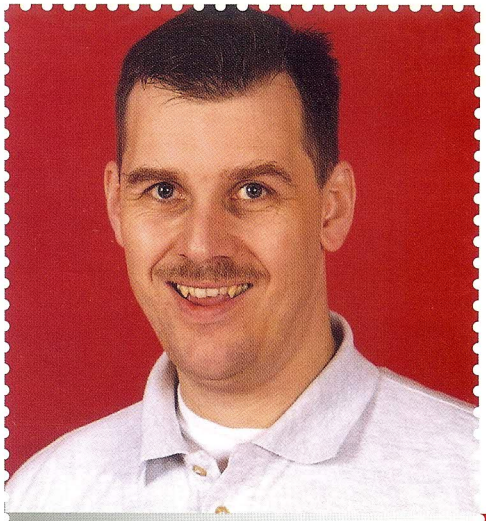
heel licht om met deze zaken. Misschien is het wel zo dat net door het online gebeuren we afstevenen op een zware wijziging van onze privacy regels of worden we er allemaal veel losser door. Misschien is het net dat wat op de loer ligt. Voor velen lijkt het evident en geen probleem dat iedereen weet dat ze veel tijd vertoeven op Farmville of Maffiawars. Wel, mij geeft het net dat ietsjes meer informatie waarmee ik hun kan beoordelen op een heel andere manier en net deze manier kan ook gebruikt of misbruikt worden door de cybercriminelen.
Dus mij lijkt het net of onze privacy aan het evolueren is. Het lijkt dat velen onder ons alleszins helemaal niet meer inzitten over wat men allemaal aan het uitspoken is of ben ik alleen met deze mening?
Wat denken julle als lezer hierover? Misschien hebben jullie helemaal andere ervaringen?

Malware

'Exploits & Vulnerbalities' zijn helaas niet meer weg te denken uit deze tijd. Waar malware voorheen via bestandsuitwisseling en later via e-mail verspreid werden, zijn de malware schrijvers overgestapt op het gebruiken van gaten in het besturingssysteem en applicaties. CodeRed, Sasser en Nimda zijn voorbeelden waarbij goed gebruik werd gemaakt van bufferoverflows in netwerk-pakketten voor verschillende protocollen. Het leuke van de mensh is dat deze zich aanpast aan de omstandigheden en dus werden er over de jaren heen allerlei gaten gedicht door middel van beveiligingssoftware. Vandaar dat we nog maar sporadisch virussen zien die zich verspreiden door andere bestanden te infecteren, of zichzelf versturen via e-mail. Wat we wel zien is een enorme toename van malware die zich op een of andere manier verbergt in 'databestanden' van applicaties, zoals onder andere in bestanden van Microsoft Office of Acrobat Reader.
In eerste instantie was het misbruiken van de macro-functionaliteit van Microsoft Office natuurlijk een gigantisch probleem. Ik weet nog goed dat we toen met gemak 1000 nieuwe virussen per maand hadden (een fractie van de 40.000+ stuks unieke malware van tegenwoordig). Later werd er overgestapt om vooral bufferoverflows te gebruiken om uitvoerbare codes, die verborgen zitten in niet gebruikte delen van het Office bestand, uit te voeren. Na een lange tijd zijn de meeste gaten wel gedicht en ook sinds Microsoft overstapte van het OLE2 naar het OpenOffice XML (OOXML) formaat, zien we nog wel malware die zich verstopt in Office bestanden, maar hoofdzakelijk OLE2 bestanden. Ondanks dat OOXML de standaard is voor Office 2007 (en straks 2010), is er altijd nog een compatibiliteitsmode waardoor een eventuele bufferoverflow aanval via OLE2 mogelijk blijft.

Nieuw slachtoffer

De malware schrijvers zijn overgestapt op hun volgende slachtoffer: het PDF-formaat van Acrobat. De laatste twee jaar is er een schrikbarende toename van PDF-bestanden met een zogenaamde Trojan aan boord waarbij misbruik wordt gemaakt van de gaten in de implementatie van het PDF-formaat. De laatste aanval is van vrij recent waarbij het de "/launch"



Righard J. Zwienenberg is in 1988 begonnen met virusbestrijding toen hij tegen zijn eerste virus problemen aanliep op de Technische Universiteit Delft. Zijn interesse was gewekt. Zwienenberg bestudeert sindsdien het gedrag van virussen en maakt hier oplossingen voor. In eerste instantie begon hij als onafhankelijk consulent, om in 1991 CSE Ltd mede op te richten. Binnen CSE was hij de Research and Development Manager.

In oktober 1995 verliet Zwienenberg CSE. Een maand later begon hij op de Research and Development afdeling van ESaSS BV, ontwikkelaar van ThunderBYTE. In 1998 werd ESaSS gekocht door Norman Data Defense Systems en Zwienenberg stapte over naar het Norman Development team waar hij zich ging bezig houden met de scanner-engine van Norman Virus Control en om Norman te vertegenwoordigen in verschillende samenwerkingsverbanden. In 2005 werd Zwienenberg Chief Research Officer bij Norman. Momenteel houdt hij zich bezig met gedragsanalyse van malware en In-The-Cloud problemen.

Tevens vertegenwoordigt hij Norman in verschillende international initiatieven tegen cybercrime en botnets. Nadat AMTSO was gevormd werd Zwienenberg daar gekozen als president. Hij vervult verschillende rollen in de industrie. Zwienenberg is sinds 1992 lid van CARO. Hij is een frequente spreker op conferenties, waaronder Virus Bulletin, EICAR, AVAR, RSA, InfoSec, en seminars.

De Belgische Eddy Willems is al twee decennia actief op het gebied van IT security. In die tijd heeft hij gewerkt voor invloedrijke instituten, zoals EICAR, waarvan hij mede-oprichter en directeur pers en informatie is, verschillende CERT-instellingen en de organisatie achter de Wildlist, als ook bij commerciële ondernemingen, zoals NOXS en Kaspersky Labs Benelux.

Bij GData vormt Eddy Willems als Security Evangelist de link tussen de technische complexiteit van IT security en de gebruiker. Hij is verantwoordelijk voor een heldere communicatie van het G Data SecurityLab naar de security community, pers, distributeurs, resellers en eindgebruikers.

functionaliteit wordt misbruikt. Nu hoor ik de sceptici al denken: "Neem dan gewoon de Foxit PDF Reader, kleiner, sneller en geen gevaar." Helaas, de Foxit PDF Reader ontkomt ook niet aan dit soort problemen. Ook de Foxit PDF Reader ondersteunt deze functionaliteit en heeft dit keer, in tegenstelling tot Adobe, nog geen patch uitgebracht voor dit probleem. Wat mij eigenlijk verbaast is waarom iedereen zoveel "active content" in een bestand wil stoppen. Ooit was PDF gewoon een formaat waarbij je een document mooi kan typesetten. Nu willen we er JavaScript en andere uitvoerbare onderdelen bijzetten. Waarom?
Je ziet trouwens in het laatste geval dat de aanval ook gepaard gaat met een staaltje van social engineering. Social engineering geeft maar weer eens aan dat de zwakste schakel van beveiliging toch altijd weer de mens is. Ik weet nog goed dat een ex-collega voor zichzelf begon, wat op zich een nobel streven is. Maar toen ik een e-mail van hem kreeg dat er een geheim bericht voor mij klaar stond, was ik natuurlijk 'nieuwsgierig'. Niet zozeer wat hij mij verstuurd had, want dat hij dit niet had gedaan was gelijk duidelijk, maar wat er achter zit.

De website waar de link naar toe verwijst, vraagt mij om in te loggen met mijn MSN gegevens. In de kleine lettertjes die je moet accepteren, staat dat ik gelijk toestemming geef om een soortgelijk bericht naar al mijn contactpersonen te versturen. Als je de gegevens goed invult (waarbij de websitebeheerder natuurlijk direct je MSN-gegevens heeft), kom je vervolgens op een scherm waar je nog even je mobiele nummer mag invoeren zodat je direct gewaarschuwd kan worden als er berichten van kennissen klaar staan. Ook hier staat in de kleine lettertjes duidelijk dat dit om een (nogal dure) berichtenservice gaat; zo'n service waar je niet meer vanaf komt.

De gebruikers van deze website vallen bijna allemaal voor het feit dat het bericht afkomstig is van een bekende en "dan zal het wel goed zijn". Iets waar genoeg andere mensen, de cybercriminelen, dankbaar gebruik van maken. Het domein wat hier gebruikt werd, was precies een week voor gebruik geregistreerd. Alle contactinformatie van de eigenaar is vals, op zijn e-mail adres na. Het Hotmail-adres is nog steeds actief en waarschijnlijk de persoon achter dit adres ook. Ik kan zo een verscheidenheid aan social engineering aanvallen geven waarbij een ieder zegt "daar trap ik niet in" en toch gebeurt het aan de lopende band. Educatie, eventueel aangevuld met een policy, is hier het toverwoord.

Misschien hebben jullie ook andere vragen in verband met internet en veiligheid. Dat is dan ook de reden waarom ik jullie de vraag stel om ons te bestoken met jullie vragen of problemen. Laat het ons weten! Hier kunnen we dan elke maand een selectie uitmaken en deze kunnen we beantwoorden als security-expertteam voor dit magazine. Tot een volgende keer. Stuur uw vraag naar redactie@computerweb.nl.

Groeten,
Eddy Willems en Righard Zwienenberg