Aanvallen van binnenuit (deel 2)

In het vorige nummer van CBM hebben Righard J. Zwienenberg en Eddy Willems geschreven over social engineering en de gevaren van het gebruik van sociale netwerken. Nu komen andere risico's aan bod, zoals onafgebakende bedrijfsnetwerken. Zwienenberg en Willems geven bovendien een top-9 van de gevaren van cloud computing.

TEKST: RIGHARD ZWIENENBERG
EN EDDY WILLEMS

Netwerken van tegenwoordig zijn niet duidelijk afgebakend. Het is niet zo eenvoudig om te bepalen waar een (bedrijfs)netwerk eindigt. Heel wat mensen kunnen gewoon vanuit huis werken via een beveiligde VPN-verbinding. Maar dat is niet altijd het geval. Sommige bedrijven stellen delen van hun netwerk open voor de buitenwereld. Gebruikers loggen op openbare plaatsen in op het e-mailsysteem van hun bedrijf om hun e-mails te lezen. Het spreekt voor zich dat malware om wachtwoorden te stelen en andere spyware gemakkelijk kunnen worden gebruikt om de echte aanmeldings- en wachtwoordgegevens te achterhalen, waardoor hackers zonder problemen toegang krijgen tot interne bedrijfsgegevens.

Mobiele toestellen

Andere problemen zijn meer en meer afkomstig van mobiele toestellen waarop het opvragen van e-mails heel normaal is geworden, en die zelfs kunnen worden gebruikt om in te loggen op een terminal server. Als u dit toestel op een openbaar netwerk gebruikt, kan de hacker die een cappuccino zit te drinken in de bar waar u uw e-mails leest, gemakkelijk uw aanmeldingsgegevens achterhalen.

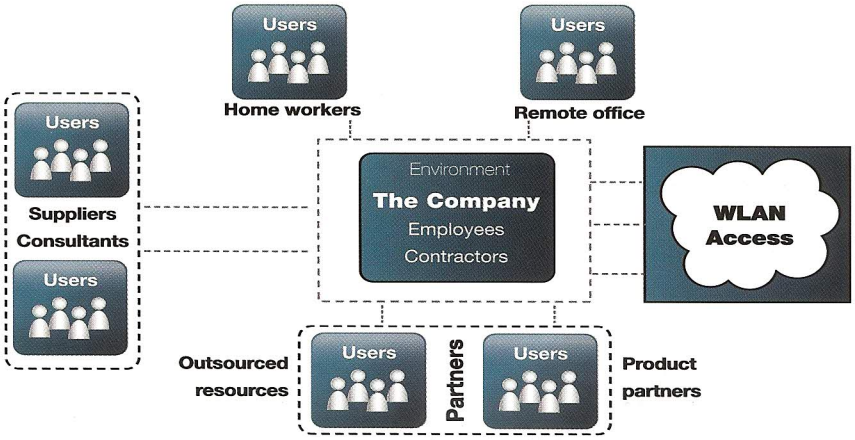
De meesten onder ons hebben thuis een goede beveiliging maar heel wat mensen houden geen rekening met de mogelijke problemen op openbare plaatsen. Omdat de netwerken tegenwoordig niet duidelijk zijn afgebakend, wordt het steeds moeilijker om te bepalen wat zich precies binnen en buiten het bedrijfsnetwerk bevindt. Voor normale gebruikers wordt het zelfs steeds moeilijker om zich te beschermen en de echte risico's achter elk gedeelte van het netwerk te detecteren. Dit probleem zal de komende jaren ongetwijfeld alleen maar groter en problematischer worden.

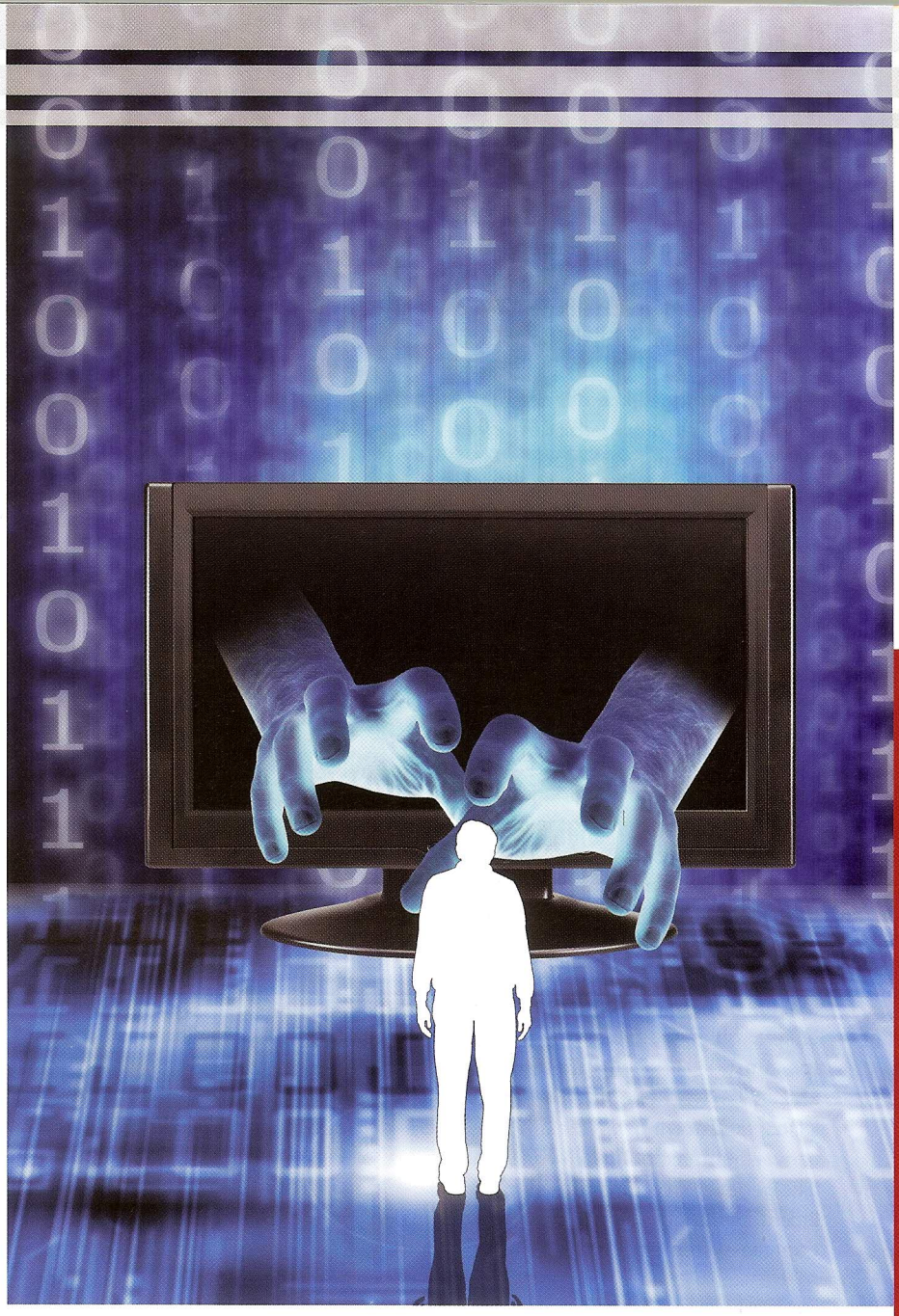
Protocollen

De netwerksegmenten, zowel intern als extern, zijn zo nauw met elkaar verbonden dat elke soort infectie zich over het hele netwerk zal verspreiden. Elke Trojan die het netwerk op open shares scant, zal deze vinden. Door de jaren heen verspreidt de meeste malware die het intranet van bedrijven aanvalt zich via drie bekende protocollen: CIFS, SMB en RPC.

Zelfs als u aan alle aspecten van de beveiliging hebt gedacht, zoals de opleiding van gebruikers, patchbeheer, herstel van hardware en anti-malware

De Belg **Eddy Willems** is Security Evangelist bij G Data Software AG. Hij is al sinds 1989 actief op het gebied van IT-beveiliging. Tijdens die periode heeft hij gewerkt voor invloedrijke organisaties, zoals EICAR, waarvan hij medeoprichter en directeur pers en informatie is, verschillende CERT-instellingen, internationale politiediensten, de organisatie achter de WildList en commerciële ondernemingen zoals NOXS en Kaspersky Lab Benelux. Als Security Evangelist bij G Data vormt hij de link tussen de technische complexiteit van IT-beveiliging en de gebruiker.





beheer, zullen met nieuwe soorten hardware en onbekende risico's ook nieuwe infecties ontstaan op uw intranet via deze of andere veelgebruikte protocollen zoals HTTP, FTP, SMTP, TFTP, POP3 en IRC. De beste manier om deze potentiële infecties te voorkomen, is een transparante realtime malwarescanner voor netwerken. Of beter nog, een In-Line Network Content Scanner. Dit apparaat werkt onzichtbaar (ongeordende modus), heeft kennis van de verschillende protocollen en kan dus alle verkeer met deze protocollen scannen. Om de overhead tot een minimum te beperken, kan dit geen proxy oplossing zijn. Deze zou namelijk al het verkeer vast houden totdat het laatste pakketje binnen is alvorens de data te kunnen scannen en doorsturen.
Door dit apparaat op strategische plaatsen in te zetten, wordt het risico tot een minimum beperkt, omdat infecties eerder kunnen worden gedetecteerd. Deze kunnen worden beperkt tot een kleiner netwerksegment. Ze kunnen zelfs netwerken met oude besturingssystemen beveiligen die nog vatbaar zijn voor aanvallen omdat ze (sommige van) de protocollen niet begrijpen en er geen anti-malwaresoftware verkrijgbaar voor is.
Ook moderne omgevingen zonder beveiliging zijn met deze apparaten te beveiligen. De laatste tijd zijn aanvallen op SCADA-omgevingen in het nieuws geweest. Of het nu gaat om een gerichte aanval of een toevallige bijwerking van de malware die binnen een SCADA-omgeving actief is of wordt, de gevolgen kunnen desastreus zijn. Kleppen die niet meer dicht of open gaan of robots die niet meer accuraat werken; er zijn talloze problemen te bedenken.

De laatste gerichte aanvallen zijn nog niet zo schadelijk geweest, maar het feit dat er meer SCADA-omgevingen getroffen worden, geeft aan dat de malware-schrijvers ook deze vector voor aanvallen hebben gevonden.

Cloudgevaren

Cloud computing biedt een aantal beveiligingsvoordelen.

- De voordelen van schalen en snelle en slimme schaalbaarheid van resources
- Standaardinterfaces voor beheerde beveiligingsdiensten
- Controle en verzamelen van bewijs
- Meer tijdige, doeltreffende en efficiënte updates en standaardinstellingen

Het is overbodig om al het materiaal dat is geschreven over de economische, technische, architecturale en ecologische voordelen van cloud computing te herhalen. Maar er zijn ook gevaren. Volgens recente berichten uit de 'echte wereld' moet een onderzoek van de beveiligingsproblemen verbonden aan cloud computing worden afgewogen tegen een overzicht van de specifieke beveiligingsvoordelen ervan. Cloud computing heeft een aanzienlijk potentieel om de beveiliging en het herstelvermogen te verbeteren, maar er moet extra aandacht worden besteed aan verschillende toekomstige dreigingen. We geven een top-9 van de belangrijkste problemen.

9 Identiteitsbeheer

U kunt nooit zeker zijn wie wie is. Aanvallers kunnen uw identiteit misbruiken. De cloud weet niet wie u (fysiek) bent. Als aanvallers toegang krijgen tot

uw netwerk, kunnen ze communiceren met de cloud. Omdat de cloud denkt dat ze nog steeds communiceert met een vertrouwde bron (uw netwerk), kan informatie worden onderschept of kan verkeerde informatie in de cloud worden ingevoerd.
Een andere mogelijkheid is een man-in-the-middle-aanval, waarbij de aanvaller zich tussen het netwerk (slachtoffer) en de cloud bevindt.

8 Misbruik van diensten

Providers geven hun klanten de illusie dat ze over onbeperkte verwerkings-, netwerk- en opslagcapaciteiten beschikken, vaak gekoppeld aan een eenvoudige registratieprocedure waarbij iedereen met een geldige creditcard zich kan registreren en onmiddellijk de clouddiensten kan beginnen te gebruiken. Sommige providers bieden zelfs gratis proefperiodes aan. Door misbruik te maken van de relatieve anonimiteit achter deze registratie- en gebruiksmodellen, kunnen criminelen hun activiteiten soms zonder een enkel probleem uitvoeren. Huidige en toekomstige aandachtspunten zijn het kraken van wachtwoorden en sleutels, DDoS, de lancering van dynamische aanvalspunten, het hosten van schadelijke gegevens, commando- en controlecentra voor botnets en het kraken van Captcha-systemen.

7 Het kapen van accounts/diensten

Als de cloud-account of -dienst op de een of andere manier wordt gestolen, kan deze worden misbruikt voor allerlei misdrijven, afhankelijk van de oorspronkelijke dienst van de cloud. Wanneer dit gebeurt, kan dat heel vervelende gevolgen hebben voor zowel de gebruiker als het getroffen bedrijf. Uiteindelijk wordt de eigenaar van de account beschuldigd. Een klassiek voorbeeld hiervan is het beruchte Twittergate.

6 Financiële DDoS

Er zijn verschillende mogelijke scenario's waarin de resources van een cloudklant op een kwaadaardige manier door andere partijen kunnen worden gebruikt met financiële gevolgen.
-Identiteitsdiefstal: een aanvaller gebruikt een account en de resources van de klant in zijn eigen voordeel of om de klant economische schade te berokkenen.
-De cloudgebruiker heeft geen effectieve beperkingen ingesteld op het gebruik van betaalde resources en ervaart een onverwachte belasting van deze resources door kwaadwillige acties.
-Een aanvaller gebruikt een openbaar kanaal om de gemeten resources van de klant op te maken, bijvoorbeeld wanneer de klant per HTTP-aanvraag betaalt. Een DDoS-aanval kan dit effect hebben.
Een financiële DDoS vernietigt economische middelen; in het slechtste geval gaat de klant failliet of heeft dit ernstige economische gevolgen.

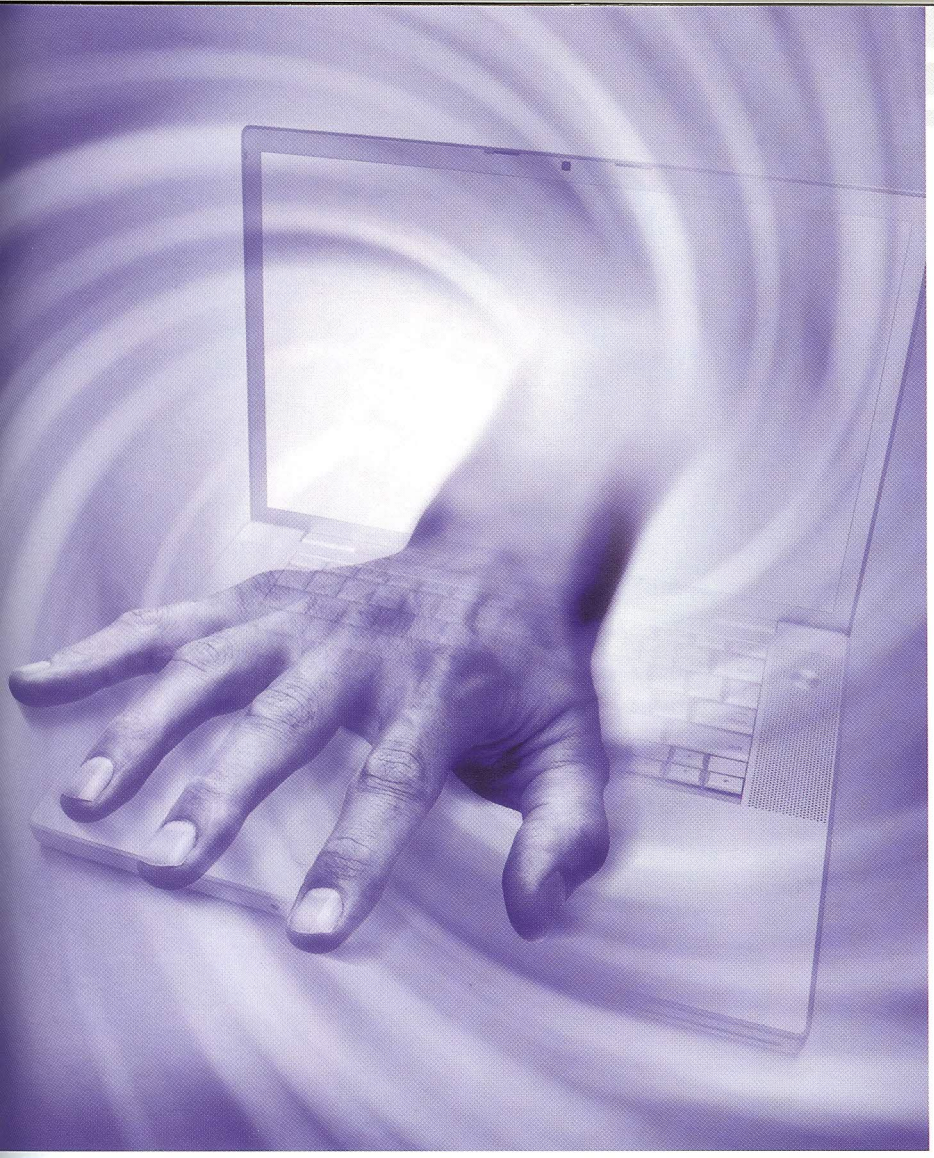
5 Gegevensverlies/ gegevenslekken

Stel u voor dat een document met geheime informatie in de cloud wordt opgeslagen of gescand. Wie bevindt zich achter de cloud? Wordt het document automatisch doorgestuurd naar 'iemand' of 'iets' anders? Als het in de cloud wordt gescand en verkeerd wordt geïdentificeerd (false positive), wordt het dan in de cloud in quarantaine geplaatst?

4 Onbekend risicoprofiel

Een van de positieve aspecten van cloud computing is dat er minder hard- en software moet worden aangekocht en er minder onderhoud nodig is, waardoor bedrijven zich meer kunnen concentreren op hun kernactiviteiten. Dit heeft aanzienlijke financiële en operationele voordelen, die zorgvuldig moeten worden afgewogen tegen de beveiligingsgevaren. Versies van software, updates van codes, beveiligingspraktijken, kwetsbaarheidsprofielen, inbraakpogingen en beveiligingsstructuur zijn allemaal factoren die een belangrijke rol spelen in de beveiligingstoestand van uw bedrijf. Informatie over wie uw infrastructuur deelt kan relevant zijn, net als logboekbestanden van inbraakpogingen in het netwerk, omleidingspogingen en -successen en andere logboekbestanden. Beveiliging door onbekendheid kan dan wel eenvoudig zijn, maar ook resulteren in blootstelling aan onbekende risico's. Het kan ook een impact hebben op de diepgaande analyse van uiterst gecontroleerde en gereguleerde werkgebieden. Bij het gebruik van een clouddienst kunnen de functies en functionaliteit goed worden weergegeven. Maar hoe zit dat met de details of naleving van interne beveiligingsprocedures, configuratiebeveiliging en toepassing van patches? Hoe worden uw data en bijbehorende logboekbestanden opgeslagen en wie heeft toegang hiertoe? Welke informatie zal de verkoper bekendmaken in geval van een beveiligingsincident? Dergelijke vragen worden vaak niet duidelijk beantwoord of worden over het hoofd gezien, waardoor klanten een onbekend risicoprofiel hebben. Een duidelijk voorbeeld van dit probleem is de gegevensdiefstal bij Heartland. De betalingsverwerkingssystemen van Heartland maakten gebruik van bekende kwetsbare software en werden geïnfecteerd, maar Heartland was, vol-

Righard J. Zwienenberg is de Chief Research Officer van Norman. Hij begon zich in 1988 bezig te houden met computervirussen, nadat hij de eerste virusproblemen ontdekte op een systeem aan de Technische Universiteit van Delft. Zwienenberg bestudeert sindsdien het gedrag van virussen en ontwikkelt oplossingen en detectiemethoden. Na een overname sloot hij zich in 1998 aan bij het ontwikkelingsteam van Norman, waar hij aan de engine van Norman Virus Control werkt en Norman vertegenwoordigt in verschillende samenwerkingsorganen. In 2005 kreeg Zwienenberg de functie van Chief Research Officer.



gens een artikel op pcworld.com "enkel bereid het absolute minimum te doen en te voldoen aan de staatswetgeving in plaats van extra inspanningen te leveren om elke klant op de hoogte te brengen van het feit dat hun gegevens gestolen werden."

3 Verborgen logboekbestanden/ inbraakpogingen

Een rechtstreekse aanval op een bedrijfsnetwerk wordt geregistreerd en is zichtbaar in de logboekbestanden van de gateways. Maar wat in geval van een aanval op de cloud? Een aanvaller kan alle berichten naar zichzelf doorsturen; er wordt niets geregistreerd in de logboekbestanden van de gateways van het bedrijf.

2 Misbruik door insiders

De kwaadwillige activiteiten van een insider kunnen mogelijk een impact hebben op de vertrouwelijkheid, integriteit en beschikbaarheid van allerlei soorten data, IP, allerlei diensten en daardoor onrechtstreeks op de reputatie van het bedrijf, het vertrouwen van de klanten en de ervaringen van de werknemers. Dit is vooral belangrijk in het geval van cloud computing, omdat voor cloudarchitecturen vaak bepaalde rollen nodig zijn die enorm risicovol zijn. Voorbeelden van dergelijke rollen zijn systeembeheerders en controleurs en providers van beheerde beveiligingsdiensten die zich bezighouden met inbraakdetectierapporten en reageren op incidenten. Naarmate een cloud meer wordt gebruikt, worden de werknemers van cloudproviders steeds vaker het doelwit van cybercriminelen. Misbruik door insiders bij cloudbedrijven brengt meer risico's met zich mee in vergelijking met normale bedrijven, omdat de impact zelf veel groter kan zijn en op meer bedrijven in plaats van een bepaald bedrijf gericht kan zijn. De kwetsbaarheden zijn duidelijk en lopen uiteen van onduidelijke rollen, kwetsbaarheden van het systeem of besturingssysteem, onvoldoende fysieke beveiligingsprocedures tot toepassingsproblemen of zelfs slecht patchbeheer. Om de zaken nog ingewikkelder te maken, is er vaak weinig of geen zichtbaarheid in de normen voor indienstneming en praktijken voor cloudwerknemers. Het is duidelijk dat de toegangsrechten een crimineel toegang kunnen geven tot vertrouwelijke gegevens of volledige controle kunnen geven over de clouddiensten zonder dat deze het risico loopt gedetecteerd te worden. Het is ook duidelijk dat heel wat van dit soort problemen vaak niet openbaar worden gemaakt, omdat ze te grote financiële gevolgen kunnen hebben voor de provider van de clouddienst.

1 Gecentraliseerd misbruik van/ vertrouwen in AAA

Authenticatie, autorisatie en accounting (AAA) is een voorwaarde voor een framework om de toegang tot computerbronnen op een intelligente manier te controleren, beleid af te dwingen, gebruik te controleren en informatie die vereist is voor de facturering te verschaffen. Deze gecombineerde processen zijn belangrijk voor doeltreffend netwerkbeheer en effectieve netwerkbeveiliging. Als de AAA niet kan worden gegarandeerd, bijvoorbeeld als een account wordt gekaapt, dan gebeurt dit voor rekening van de houder en dan is hij of zij verantwoordelijk.

Kortom: hoe goed u uw netwerk ook tegen aanvallen van binnenuit probeert te beschermen, er zijn nog heel wat mogelijkheden waarop deze aanvallen toch kunnen gebeuren. Van onbekende externe partijen of diensten met onbekende risicoprofielen tot wangedrag van werknemers en social engineering. Het kan resulteren in aanvallen op uw netwerk. Aanvallen van binnenuit.

Heeft u als lezer van CBM een vraag over security, of wilt u graag de mening van Eddy Willems en Righard J. Zwienenberg over een bepaald onderwerp in het blad zien? Stuur uw vraag of onderwerp door naar de eindredactie van CBM (j.van.leeuwen@kantoornet.nl). De mails worden vervolgens aan Eddy en Righard voorgelegd.