
Bescherming van uw netwerk tegen e-maildreigingen

Het belang van degelijke servergebaseerde e-mailbeveiliging

In dit white paper kunt u lezen waarom antivirussoftware alleen niet genoeg is om uw organisatie adequaat te beschermen tegen aanvallen van e-mailvirussen en andere dreigingen. Dit paper beschrijft de noodzaak voor een degelijke servergebaseerde e-mailbeveiliging om uw netwerk te beschermen tegen e-mailaanvallen en andere bedreigingen voor organisaties in de 21^e eeuw.

Inleiding

In dit white paper kunt u lezen waarom antivirussoftware alleen niet genoeg is om uw organisatie adequaat te beschermen tegen aanvallen van e-mailvirussen en andere dreigingen. In dit paper wordt uitleg gegeven over diverse soorten e-maildreigingen en manieren waarop uw netwerk kan worden aangevallen. Dit paper maakt duidelijk waarom een degelijke servergebaseerde content-checking gateway noodzakelijk is om uw bedrijf te beschermen tegen zowel e-mailvirussen en andere e-maildreigingen, zoals informatielekken.

Inleiding	2
E-mailvirussen en Trojaanse paarden.....	2
Informatielekken	3
E-mails met kwaadaardige of beledigende inhoud	3
Manieren waarop uw e-mailsysteem kan worden aangevallen	3
Het gemak waarmee virussen worden gecreëerd.....	5
Waarom antivirussoftware of een firewall niet genoeg is	5
Over GFI MailSecurity voor Exchange/SMTP	6
Over GFI.....	7

E-mailvirussen en Trojaanse paarden

Door de hoge populariteit van e-mail hebben hackers en crackers tegenwoordig volop gelegenheid om schadelijke bestanden op uw netwerk te verspreiden. Hackers kunnen uw firewall gemakkelijk omzeilen door middel van inkapseling in het e-mailprotocol. Dit protocol analyseert immers niet de inhoud van e-mails.

CNN heeft in januari 2004 bekendgemaakt dat het MyDoom-virus bedrijven circa \$250 miljoen (€217 miljoen) heeft gekost aan verloren productiviteit en technische onderhoudskosten. Volgens NetworkWorld (september 2003) bedragen alleen in de Verenigde Staten de kosten van de bestrijding van Blaster, SoBig.F, Wechia en andere e-mailvirussen al \$3,5 miljard (€3 miljard).

E-mail wordt tevens gebruikt voor het installeren van Trojans. Deze dringen uw organisatie binnen om vertrouwelijke informatie te bemachtigen of de controle over uw servers over te nemen. Deze virussen, die door beveiligingsexperts wel "instructieve virussen" of "spionnenvirussen" worden genoemd, spelen een belangrijke rol in bedrijfsspionage. Een goed voorbeeld hiervan is de aanval op het netwerk van Microsoft in oktober 2000. Een woordvoerder van Microsoft beschreef deze aanval als "een duidelijk geval van bedrijfsspionage". Volgens de berichten werd het netwerk van Microsoft gekraakt door een Trojaans paard dat met kwade opzet naar een netwerkgebruiker was gemaild.

Informatielekken

Veel organisaties beseffen niet dat het risico bestaat dat insiders cruciale informatie stelen. Onderzoek heeft uitgewezen dat werknemers soms e-mail gebruiken om vertrouwelijke informatie te versturen. Of het nu is omdat ze ontevreden en wraakzuchtig zijn of omdat ze zich niet realiseren dat ze iets gevaarlijks doen, feit is dat werknemers e-mail gebruiken voor het verzenden van vertrouwelijke informatie die officieel het bedrijf niet had mogen verlaten.

Uit het Britse Hutton-onderzoek van 2003 bleek dat ambtenaren en stafmedewerkers van de BBC via e-mail vertrouwelijke informatie hadden verspreid. In een artikel in *PC Week* uit maart 1999 werd een onderzoek beschreven waarin tussen de 21 en 31 procent van de 800 respondenten toegang vertrouwelijke informatie (zoals financiële gegevens of productinformatie) te hebben gemaïld naar mensen buiten het bedrijf.

E-mails met kwaadaardige of beledigende inhoud

Werknemers die racistische, seksistische of anderszins beledigende e-mails versturen kunnen uw bedrijf in juridische problemen brengen. In September 2003 moest de Britse firma Holden Meehan Independent Financial Advisors een voormalige werknemer £10.000 (€15.220) betalen omdat het bedrijf er niet in was geslaagd haar te beschermen tegen intimidatie via e-mail. Berucht is de zaak van Chevron. Dit bedrijf moest vier werknemers \$2,2 miljoen betalen nadat ze via e-mail seksueel geïntimideerd waren. Volgens de Britse wet zijn werkgevers verantwoordelijk voor e-mails die door hun werknemers zijn geschreven, ongeacht of de werkgever heeft ingestemd met de e-mail. Verzekeringsmaatschappij Norwich Union werd in een schikking gevraagd \$450.000 (€389.948) te betalen vanwege e-mails betreffende concurrentie.

Manieren waarop uw e-mailsysteem kan worden aangevallen

Om u een idee te geven van de verschillende e-maildreigingen die er zijn zal in dit hoofdstuk een beknopt overzicht worden gegeven van de belangrijkste manieren waarop uw e-mailsysteem kan worden aangevallen. Bedreigingen zijn onder andere:

Attachments met schadelijke inhoud

De oudste voorbeelden van het probleem met attachments en vertrouwen zijn de virussen Melissa en LoveLetter. Deze maakten gebruik van het vertrouwen dat mensen hebben in vrienden en collega's. Stelt u zich voor dat u een attachment ontvangt van een vriend die u vraagt het te openen. Dit is wat gebeurde met Melissa, AnnaKournikova, SirCam en vergelijkbare e-mailwormen. Deze wormen zenden zichzelf naar e-mailadressen uit het adresboek en oude berichten van het slachtoffer, webpage caches op de computer, enzovoort. Schrijvers van virussen doen hun best om het slachtoffer het attachment te laten openen.

Daarom geven ze hun attachments aantrekkelijke namen, zoals Sex.Pic.cmd en me.pif.

Veel gebruikers proberen virusbesmetting te voorkomen door alleen te dubbelklikken op bestanden met bepaalde extensies, zoals JPG en MPG. Sommige virussen, zoals de AnnaKournikova-worm, maken echter gebruik van verscheidene extensies om de gebruiker te verlokken het bestand te openen. Het AnnaKournikova-virus werd verspreid via een attachment met de naam 'AnnaKournikova'.jpg.vbs'. Hierdoor dachten ontvangers dat ze een onschuldig JPG-bestand met een foto van de beroemde tennisspeelster binnenhaalden in plaats van een Visual Basic Script met een besmettelijke code.

Bovendien kunnen hackers dankzij de Class ID (CLSID)-extensie de echte extensie van het bestand verbergen. Op die manier hebben ontvangers niet in de gaten dat cleanfile.jpg in feite een vervelend HTA (HTML-applicatie)-bestand is.

Deze aanvalsmethode omzeilt momenteel diverse contentfilters die eenvoudige manieren van bestandscontrole gebruiken. Zo kan de hacker zijn doelwit gemakkelijker bereiken.

Emails die gebruik maken van beveiligingsfouten

De Nimda-worm verrastte iedereen. De worm omzeilde vele beveiligingstools en onder de slachtoffers waren zowel bedrijfsnetwerken als consumenten. De truc van Nimda is dat het automatisch wordt uitgevoerd op computers met een kwetsbare versie van Internet Explorer of Outlook Express. Nimda was een van de eerste virussen die gebruik maakten van een of andere beveiligingsfout om zich te verspreiden. De diverse varianten van het Bagle-virus uit maart 2004 maakten bijvoorbeeld gebruik van een oude beveiligingsfout in Outlook in een poging zich te verspreiden zonder interventie van gebruikers.

HTML-mail met ingebedde scripts

Tegenwoordig kunnen alle e-mail clients HTML-mail verzenden en ontvangen. HTML-mail kan scripts en Active Content bevatten. Hierdoor kunnen programma's of codes worden uitgevoerd op het werkstation. Outlook en andere producten gebruiken Internet Explorer om HTML-mail te laten zien. Dit betekent dat ze lijden onder de beveiligingsfouten in Internet Explorer.

Virussen die gebaseerd zijn op HTML-scripts zijn extra gevaarlijk omdat ze automatisch actief worden zodra het kwaadaardige mailtje wordt geopend. Ze leunen niet op attachments; de attachmentfilters in antivirussoftware zijn dus zinloos bij het bestrijden van onbekende HTML-scriptvirussen.

Het BadTrans.B-virus bijvoorbeeld combineert een e-mailbeveiligingsfout met HTML om zich te verspreiden: door middel van HTML wordt er automatisch een attachment gelanceerd zodra de e-mail is ontvangen.

Het gemak waarmee virussen worden gecreëerd

Iedereen die wat van Visual Basic weet kan chaos veroorzaken door gebruik te maken van welbekende beveiligingsfouten in diverse veelgebruikte e-mail clients en andere producten. Op de site van SecurityFocus staan bijvoorbeeld verschillende exploits die beschikbaar zijn voor Microsoft Outlook. Iedere kwaadwillende die een virus wil maken kan gewoon de exploitcode (die openbaar is!) aanpassen om zijn code uit te voeren.

Bijvoorbeeld: een exploit voor Internet Explorer en MS Access, die gemakkelijk toegepast zou kunnen worden op Outlook en Outlook Express, is te vinden op Guninski.com. Een virusmaker kan dit gemakkelijk gebruiken om Visual Basic-code te runnen zodra het slachtoffer het besmette mailtje opent. Deze besmet vervolgens alle HTML-bestanden en stuurt zichzelf naar alle adressen in het adresboek van de ontvanger. Een cruciaal aspect van dit virus is echter dat het eenvoudigweg wordt uitgevoerd wanneer de gebruiker het mailtje met schadelijke HTML opent.

Waarom antivirussoftware of een firewall niet genoeg is

Sommige organisaties installeren een firewall en denken vervolgens ten onrechte dat hun netwerk nu goed beveiligd is. Het installeren van een firewall is verstandig, maar niet voldoende. Firewalls kunnen voorkomen dat ongeautoriseerde gebruikers toegang tot uw netwerk verkrijgen. Ze controleren echter niet de inhoud van mail die wordt verstuurd en ontvangen door geautoriseerde gebruikers, om maar een voorbeeld te noemen. Dit betekent dat e-mailvirussen op dit beveiligingsniveau toch nog doorgelaten kunnen worden. Ook beschermen virusscanners niet tegen ALLE e-mailvirussen en aanvallen: Verkopers van virusscanners kunnen hun signatures niet altijd op tijd updaten voor de nieuwste fatale virussen die in een paar uur over de hele wereld verspreid kunnen worden (zoals de recente MyDoom, NetSky.B- en Beagle-wormen). Bedrijven die alleen een enkele virusscan-engine gebruiken zijn niet noodzakelijkerwijs veilig wanneer er een nieuw virus wordt gelanceerd. Uit een onderzoek van de Britse overheid uit 2004 is gebleken dat hoewel 99% van de grote bedrijven in Groot-Brittannië antivirusproducten gebruiken, 68% van hen in 2003 met virusbesmettingen te maken heeft gehad. Ook bleek uit onderzoek in de Hewlett-Packard laboratoria in Bristol dat de signature update-methode voor virusdetectie en -eliminatie ernstig tekortschiet aangezien wormen zich sneller kunnen verspreiden dan antivirus signature-updates.

De oplossing: Een proactieve aanpak

Hoe kunt u zich beschermen tegen deze e-maildreigingen? Wat u nodig heeft is een proactieve aanpak waarbij de inhoud van alle inkomende en uitgaande e-mail op serverniveau wordt gecontroleerd voordat de mail bij uw gebruikers belandt. Op deze manier wordt alle schadelijke content uit besmette of verdachte e-mails verwijderd. Daarna worden de mailtjes pas naar de gebruikers doorgestuurd.

Met een degelijke e-mail content checking en antivirus gateway op hun mailserver kunnen

bedrijven zich beschermen tegen eventuele schade en tijdsverlies door bestaande en toekomstige virussen.

Over GFI MailSecurity voor Exchange/SMTP

GFI MailSecurity voor Exchange/SMTP is een tool voor content checking, exploitdetectie, dreigingsanalyse en virusbestrijding die alle soorten dreigingen verwijdert voordat ze uw gebruikers kunnen bereiken. GFI MailSecurity biedt de volgende essentiële beveiligingsmogelijkheden: met meer dan één virusscan-engine is de detectiekans hoger en de reactie sneller; de inhoud van e-mailberichten en bijlagen wordt gecontroleerd, waarbij gevaarlijke bijlagen en inhoud in quarantaine worden geplaatst; exploitbeveiliging voor bescherming tegen huidige en toekomstige virussen op basis van exploits; een engine die HTML-scripts uitschakelt; een Trojan & Executable Scanner die kwaadaardige uitvoerbare bestanden opspoor; en meer. Kijk voor meer informatie en een trialversie op <http://www.gfi.nl/nl/mailsecurity/>.

Over GFI

GFI is een toonaangevende ontwikkelaar van software voor netwerkbeveiliging, inhoudsbeveiliging en messaging. Dankzij bekroonde technologie, een agressieve prijsstrategie en een sterke focus op MKB-bedrijven helpt GFI bedrijven over de hele wereld om maximale continuïteit en productiviteit te bewerkstelligen. GFI is opgericht in 1992 en heeft kantoren in Malta, Londen, Raleigh, Hong Kong, Adelaide en Hamburg die wereldwijd meer dan 200.000 installaties ondersteunen. GFI is een kanaalgericht bedrijf met meer dan 10.000 partners over de hele wereld. GFI is ook een Microsoft Gold Certified Partner. Meer informatie over GFI is te vinden op <http://www.gfi.nl>.

© 2007 GFI Software Ltd. Alle rechten voorbehouden. De informatie in dit document geeft het standpunt van GFI weer betreffende de besproken onderwerpen op de datum van publicatie. Aangezien GFI moet reageren op veranderende marktomstandigheden, moet dit document niet als een toezegging van GFI worden geïnterpreteerd. Na de publicatiedatum kan de correctheid van de informatie niet worden gegarandeerd. Dit white paper dient puur ter informatie. GFI GEEFT IN DIT DOCUMENT GEEN ENKELE GARANTIE, EXPLICIET NOCH IMPLICIET. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor en de bijbehorende logo's zijn ofwel geregistreerde handelsmerken of handelsmerken van GFI Software Ltd. in de Verenigde Staten en/of andere landen. Alle product- en bedrijfsnamen in dit persbericht zijn mogelijk handelsmerken van hun respectievelijke eigenaren.

