

Protéger votre réseau contre les menaces email

Le besoin d'une sécurisation email complète au niveau du serveur

Ce livre blanc explique pourquoi un logiciel antivirus seul n'est pas suffisant pour protéger votre organisation contre les attaques et menaces virales de messagerie actuelles et futures. Il décrit la nécessité d'avoir une solution de sécurisation de messagerie de serveur solide pour la protection de votre réseau, en analysant les différents types d'attaques email et les problèmes qui menacent les entreprises d'aujourd'hui.

Introduction

Ce livre blanc explique pourquoi un logiciel antivirus seul n'est pas suffisant pour protéger votre entreprise contre les attaques et menaces virales de messagerie actuelles et futures. Il décrit la nécessité d'avoir une solution de sécurisation de serveur de messagerie fiable pour la protection de votre entreprise contre les virus email et les attaques ainsi que les fuites d'informations, en analysant les différents types d'attaques email et les problèmes qui menacent les organisations d'aujourd'hui.

Introduction.....	2
La menace posée par les virus email et des chevaux de Troie	2
Le danger des fuites d'informations	3
La menace des emails malicieux ou au contenu offensif.....	3
Les méthodes utilisées pour attaquer votre système de messagerie	3
La création d'un virus avec une étonnante facilité	5
Pourquoi un seul logiciel antivirus ou un pare-feu ne sont pas suffisants	5
La solution : Une approche dynamique.....	6
A propos de GFI MailSecurity for Exchange/SMTP	6
A propos de GFI Software.....	7

La menace posée par les virus email et des chevaux de Troie

L'usage répandu des emails a rendu la distribution de contenus dangereux à des réseaux internes plus facile pour les hackers et les pirates informatiques. Les hackers peuvent aisément contourner le système de protection qu'offrent les pare-feux en parcourant le protocole de messagerie, car celui-ci ne procède pas à l'analyse des contenus d'emails.

CNN a rapporté en Janvier 2004 que les compagnies, à cause du virus MyDoom, ont perdu plus de \$250 millions (US) en termes de baisse de productivité et de dépenses en support technique. Alors que NetworkWorld (Septembre 2003) a mentionné des études qui plaçaient le coût de la lutte contre Blaster, SoBig.F, Wechia et autres virus email à \$3.5 milliards (US) seulement pour les compagnies américaines.

De plus, un email peut aussi être utilisé tout particulièrement pour installer des chevaux de Troie, ayant pour cible votre organisation afin d'obtenir des informations confidentielles ou afin de prendre le contrôle de vos serveurs. Décrit comme « virus instructifs » ou comme « virus espions » (spy viruses) par les experts de sécurité informatique, ils constituent des outils importants de l'espionnage industriel. Un exemple serait l'attaque sur le réseau de Microsoft en Octobre 2000 qui a été décrite par l'un des porte-parole de Microsoft Corp comme « un acte d'espionnage industriel pure et simple ». Selon les rapports, le réseau de Microsoft a été piraté

au moyen d'un cheval de Troie dangereux en backdoor envoyé dans un email à un utilisateur du réseau.

Le danger des fuites d'informations

Les entreprises ont souvent du mal à reconnaître le fait que des données cruciales puissent être en danger d'être volées par un de leurs employés. Plusieurs études ont montré comment les employés font usage d'emails pour transmettre des informations confidentielles. Soit par vengeance ou par mécontentement ou encore parce qu'ils ne voient pas les conséquences désastreuses de telles actions, les employés utilisent les systèmes de messagerie électronique pour partager des données qui sont à usage interne uniquement.

Comme l'a bien montré le rapport Hutton en 2003 au Royaume-Uni, il s'est avéré que des représentants du gouvernement et les cadres de la chaîne de télévision BBC avaient communiqué par email pour révéler des informations confidentielles. Un article paru dans PC Week en Mars 1999 fait référence à une étude dans laquelle, 21-31%, des 800 employés interrogés, ont admis transmettre des informations confidentielles par email – telles que des données financières ou des renseignements sur des produits – à des destinataires en-dehors de la compagnie.

La menace des emails malicieux ou au contenu offensif

La compagnie est légalement tenue responsable pour le contenu des emails envoyés par ses employés ; qu'ils contiennent des commentaires racistes, sexistes ou tout autre matériel offensif. En Septembre 2003, la compagnie anglaise Holden Meehan Independent Financial Advisors a dû dédommager une de ses employés de £10,000 pour ne pas l'avoir protégée contre le harcèlement d'emails dont elle était victime. La compagnie Chevron est notoire pour avoir payé \$2.2 millions à quatre de ses employés qui, supposément, avaient reçu des emails constituant du harcèlement sexuel. Selon le système législatif anglais, les employeurs sont tenus responsables pour tout email écrit par leurs employés et ce pour la durée de leurs contrats, qu'ils aient ou non consenti aux messages. La compagnie d'assurances Norwich Union a dû payer \$450 000 lors d'un accord amiable pour avoir fait des commentaires via emails sur la compétition.

Les méthodes utilisées pour attaquer votre système de messagerie

Pour arriver à contrôler les menaces emails d'aujourd'hui, il est préférable d'avoir un aperçu des méthodes actuelles d'attaques virales. Cela inclut :

Des pièces jointes au contenu malicieux

Melissa et LoveLetter étaient parmi les premiers virus qui ont illustré le problème de faire

confiance aux emails et à leurs pièces jointes. Ils ont abusé la confiance qui existait entre amis et collègues. Imaginez que vous avez reçu une pièce jointe de la part d'un ami qui vous demande de l'ouvrir. C'est ce qui s'est passé avec Melissa, AnnaKournikova, SirCam et d'autres vers similaires. Activés, ce genre de vers s'emparent des adresses emails enregistrées dans l'annuaire de la victime, d'un message précédent, des caches de documents Internet de la machine locale et par d'autres méthodes similaires, s'envoient dans la forme d'un email. Les créateurs de virus mettent l'accent sur la pièce jointe de façon à ce que la victime l'ouvre. Ils utilisent donc des titres attirants tels que SexPic.cmd et me.pif.

Plusieurs utilisateurs essaient d'éviter des infections en ne cliquant double que sur des fichiers à certaines extensions telles que JPG et MPG. Cependant, des virus tels que le ver AnnaKournikova, utilisent des extensions multiples pour tenter d'inciter l'utilisateur à ouvrir le fichier. Le virus AnnaKournikova a été transmis sous la forme d'une pièce jointe appelée 'AnnaKournikova.jpg.vbs' qui a amené les destinataires à croire que ce qu'ils recevaient n'était rien d'autre qu'une image JPG inoffensive de la célèbre joueuse de tennis, plutôt qu'un Visual Basic Script contenant un code infecté.

De plus, l'extension Class ID (CLSID) permet aux pirates de cacher la véritable extension du fichier, et donc de déguiser la vraie nature du fichier cleanfile.jpg, un fichier HTA (HTML application) infecté.

Cette méthode contourne actuellement plusieurs solutions de filtrage de contenu d'emails qui utilisent des méthodes de vérification de fichier simples, rendant le pirate informatique capable d'atteindre l'utilisateur visé bien plus aisément.

Des emails déclenchant des exploits connus

Le ver Nimda a pris Internet par surprise, contournant beaucoup d'utilitaires de sécurisation d'emails, pénétrant sur les serveurs et les réseaux d'entreprise et infectant le système du particulier. Nimda s'exécute automatiquement sur les ordinateurs ayant une version vulnérable de Internet Explorer ou de Outlook Express. Nimda était l'un des premiers virus à exploiter une faille ou une autre pour se propager. Les variantes du virus Bagle qui sont apparues en Mars 2004, par exemple, exploitaient une vieille faille d'Outlook pour se propager sans attendre l'intervention de l'utilisateur.

Du courrier HTML aux scripts incorporés

De nos jours, tous les clients email peuvent envoyer et recevoir des emails HTML. Le courrier HTML peut inclure des scripts et Active Content, qui permettent aux programmes ou aux codes d'être exécutés sur la machine client. Outlook et autres produits utilisent des composants Internet Explorer pour afficher les emails HTML, ce qui veut dire qu'ils héritent des vulnérabilités de sécurité rencontrées dans Internet Explorer.

Les virus basés sur des scripts HTML sont plus dangereux car ils sont exécutables automatiquement dès l'ouverture du message malicieux. Ils ne s'en remettent pas aux pièces

jointes ; d'où, l'inutilité, dans la lutte contre les virus au script HTML inconnus, des filtrages de pièces jointes trouvés dans les programmes antivirus.

Le virus BadTrans.B, par exemple, associe un exploit d'email à un HTML pour se propager, utilisant HTML pour automatiquement lancer une pièce jointe une fois le message reçu.

La création d'un virus avec une étonnante facilité

N'importe qui, ayant des connaissances même minimales de Visual Basic, peut créer un désastre en exploitant des vulnérabilités bien connues de plusieurs des clients email et des produits très utilisés. Une visite sur le site SecurityFocus, par exemple, vous montrera plusieurs exploits disponibles pour Microsoft Outlook. Un gamin du script (*script kiddie*) malveillant qui a l'intention de produire un virus peut simplement modifier le code d'exploit - qui est à la disposition de tous ! - pour exécuter son code.

Par exemple, un exploit pour Internet Explorer et MS Access, qui peut facilement être appliqué à Outlook et Outlook Express, est décrit sur Guninski.com. Un créateur de virus pourrait aisément l'exploiter pour exécuter un code Visual Basic dès que la victime ouvre le message infecté. Cela infecterait tous les fichiers HTML et il pourrait se répandre à tous les contacts contenus dans l'annuaire électronique de la victime. Une fonction clé de ce virus, cependant, est qu'il s'exécute simplement lorsque l'utilisateur ouvre l'email contenant un script HTML malicieux.

Pourquoi un seul logiciel antivirus ou un pare-feu ne sont pas suffisants

Certaines organisations sont persuadées qu'elles sont en sécurité après avoir installé un pare-feu. Cela est un bon moyen pour protéger leur intranet, mais n'est pas suffisant : les pare-feux empêchent des intrus de pénétrer sur votre réseau sans en avoir la permission. Toujours est-il, ils ne vérifient pas le contenu du courrier envoyé et reçu par ces personnes non autorisées à utiliser le système par exemple. Cela veut dire que les virus email peuvent toujours passer au travers de cette mesure de sécurité.

De même qu'un logiciel de scans antivirus ne protège pas contre TOUS les virus et attaques email : les vendeurs d'antivirus ne peuvent pas toujours à temps, mettre à jour leurs signatures contre les virus fatals qui sont distribués mondialement par un email en quelques heures (tel que récemment les vers MyDoom, NetSky.B et Beagle). Les compagnies qui utilisent un moteur de scan viral unique ne sont pas nécessairement protégés quand un nouveau virus apparaît. En 2004, une étude du gouvernement Britannique a trouvé que, par exemple, bien que 99% des grandes compagnies anglaises utilisent des produits antivirus, 68% d'entre elles étaient infectées par un virus en 2003. De même, une étude menée en 2003 dans les laboratoires de recherches de Hewlett-Packard à Bristol, a trouvé que l'approche des mises à

jour des signatures à la détection et l'élimination des virus peut être gravement faussée, tout simplement parce que les vers se répandent plus vite que les mises à jour des signatures antivirus ne sont distribuées.

La solution : Une approche dynamique

Comment donc se protéger contre les menaces email ? Une approche dynamique est nécessaire, ce qui implique la vérification de contenu de tous les emails entrants et sortants au niveau du serveur, avant la répartition aux utilisateurs. De cette façon, tous les contenus éventuellement dangereux sont enlevés de l'email infecté ou douteux, et à ce moment là seulement le message est-il transféré à l'utilisateur.

En installant une vérification de contenu intelligente et une passerelle antivirus sur leur serveur de messagerie, les compagnies peuvent se protéger contre les dommages éventuels et les pertes de temps de travail que les virus actuels et futurs peuvent causer.

A propos de GFI MailSecurity for Exchange/SMTP

GFI MailSecurity for Exchange/SMTP est une solution de vérification du contenu, de détection d'exploits, de scanneur de chevaux de Troie et d'exécutables, d'analyse de menaces et d'antivirus, qui enlève tout type de menaces basées sur les emails avant qu'elles n'affectent vos utilisateurs de messagerie. Les fonctions clés de GFI MailSecurity comprennent des multiples moteurs d'anti-virus, pour garantir un taux de détection plus élevé et une réponse plus rapide face aux nouveaux virus ; une fonction de vérification du contenu et des pièces jointes de messagerie, pour mettre en quarantaine les pièces jointes et les contenus dangereux ; un bouclier contre les exploits, pour se protéger des virus existants et futurs basés sur des exploits ; un moteur anti-menace HTML, pour désactiver les scripts HTML ; un scanneur de chevaux de Troie et d'exécutables, pour détecter les exécutables dangereux, et bien d'autres. Pour un complément d'information, lisez et téléchargez une version d'évaluation sur <http://www.gfsfrance.com/fr/mailsecurity/>.

A propos de GFI Software

GFI est l'un des leaders dans le domaine de la réalisation de logiciels qui fournit une seule source intégrée permettant aux administrateurs de résoudre les problèmes de sécurisation de réseaux, de contenu et de messageries. Grâce à sa technologie innovatrice, une stratégie agressive de commercialisation et sa concentration sur le marché de petites et moyennes entreprises, GFI répond aux besoins de continuité d'affaires et de productivité des entreprises et d'autres organisations sur une grande échelle. Fondée en 1992, GFI est une entreprise internationale qui possède des bureaux à Malte, à Londres, Raleigh, Hong Kong, Adelaïde et à Hambourg avec plus de 200.000 installations de ses logiciels à travers le monde. GFI est une entreprise spécialisée et possède un réseau de plus de 10.000 partenaires à travers le monde. Partenaire stratégique de Microsoft, GFI est membre certifié du partenariat Microsoft Gold Certified Partner. Pour plus d'informations à propos de GFI, visitez le site <http://www.gfsfrance.com>.

© 2007 GFI Software. Tous droits réservés. L'information contenue dans ce document représente le point de vue actuel de GFI sur les questions abordées à la date de sa publication. Etant donné que GFI doit répondre aux conditions dynamiques du marché, il ne devrait pas être interprété comme un engagement de la part de GFI, et GFI ne peut pas garantir l'exactitude d'aucune information présentée après la date de la publication. Ce livre blanc est seulement à titre informationnel. GFI NE FAIT AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, DANS CE DOCUMENT. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor et leurs logos de produit sont des marques déposées ou des brevets commerciaux de GFI Software aux Etats-Unis et/ou dans d'autres pays. Tous les noms de produit ou d'entreprises mentionnés ci-dessus peuvent être les marques déposées de leurs propriétaires respectifs.