

Schutz von Netzwerken vor E-Mail-Gefahren

Warum umfassende E-Mail-Sicherheit auf Server-Basis so wichtig ist

In diesem White Paper wird erläutert, warum Anti-Viren-Software nicht ausreicht, um Ihr Unternehmen vor aktuellen und zukünftigen Viren und Gefahren, die per E-Mail übertragen werden, schützen zu können. Informieren Sie sich über die verschiedenen Arten E-Mail-basierter Angriffe und Probleme, die eine potenzielle Bedrohung für Ihr Unternehmen darstellen. Erfahren Sie auch, warum sich Netzwerke nur mit einer Server-basierten Lösung zur Inhaltskontrolle zuverlässig schützen lassen.

Einführung

Dieses White Paper erläutert, warum Anti-Viren-Software nicht ausreicht, Ihr Unternehmen vor heutigen und zukünftigen Viren umfassend zu schützen. In diesem Dokument werden verschiedene Arten E-Mail-basierter Gefahren und Angriffsmethoden erläutert. Erfahren Sie, warum eine zuverlässige Absicherung Ihres Unternehmens vor E-Mail-Viren und -Angriffen nur mit einer Server-basierten Lösung zur Inhaltskontrolle möglich ist.

Einführung	2
Bedrohung durch E-Mail-Viren und -Trojaner	2
Sicherheitsgefahr Geheimnisverrat	3
E-Mails mit böswilligen oder beleidigenden Inhalten	3
Methoden zur Kompromittierung von E-Mail-Systemen.....	3
Virenerstellung leicht gemacht	5
Warum Anti-Viren-Software oder eine Firewall nicht ausreicht.....	5
Die Lösung: Ein proaktiver Ansatz	6
Über GFI MailSecurity for Exchange/SMTP.....	6
Über GFI.....	7

Bedrohung durch E-Mail-Viren und -Trojaner

Die mittlerweile weit verbreitete Kommunikation per E-Mail bietet Hackern und anderen Internet-Kriminellen neue, einfache Möglichkeiten, böswillige Inhalte in interne Netzwerke zu schleusen. Hacker können den Schutz einer Firewall mit Hilfe einfacher Tunneling-Methoden durch das E-Mail-Protokoll problemlos umgehen, da E-Mail-Inhalte von dieser Sicherheitsbarriere nicht analysiert werden.

Berichten von CNN vom Januar 2004 zufolge hat der Virus MyDoom bei Unternehmen Produktivitätseinbußen und Support-Kosten in Höhe von ca. 250 Millionen US-Dollar verursacht. Laut von NetworkWorld im September 2003 zitierten Studien beläuft sich der Schaden durch Blaster, SoBig.F, Wechia und andere E-Mail-Viren allein für US-Unternehmen auf rund 3,5 Mrd. US-Dollar.

Des Weiteren lassen sich mit Hilfe von E-Mails auch Trojaner installieren, die der zielgerichteten Ausspionierung eines Unternehmens dienen, um an vertrauliche Informationen zu gelangen oder die Kontrolle über Unternehmens-Server zu übernehmen. IT-Sicherheitsexperten nennen diese Sicherheitsbedrohung auch "Spionage-Viren", die in Zukunft vermehrt zur Industriespionage eingesetzt werden könnten. Bereits im Oktober 2000 wurde das Unternehmensnetzwerk von Microsoft per E-Mail angegriffen und von Microsoft als "eindeutiger Akt der Industriespionage" bezeichnet. Das System wurde angeblich über einen Backdoor-Trojaner gehackt, der per E-Mail an einen Netzwerk-Anwender geschickt worden war.

Sicherheitsgefahr Geheimnisverrat

Unternehmen sind sich oftmals nicht der Gefahr durch interne Mitarbeiter bewusst, die sich widerrechtlich unternehmenskritische Daten aneignen und verbreiten. Mehrere Studien haben ergeben, dass vertrauliche Unternehmensinformationen aus verschiedensten Gründen von Mitarbeitern per E-Mail an Außenstehende verschickt werden. Ursache für die Veröffentlichung sensibler Daten ist neben Unzufriedenheit und Rache enttäuschter Mitarbeiter auch Unwissenheit. Manche Mitarbeiter sind sich nicht bewusst, welche Gefahren der E-Mail-Versand vertraulicher Daten birgt, die nur zur internen Verwendung bestimmt sind.

In einer im Jahr 2003 in Großbritannien gestarteten Umfrage bei Behörden und der BBC wurde festgestellt, dass selbst Regierungsbeamte und ranghohe BBC-Mitarbeiter als vertraulich eingestufte Informationen per E-Mail verbreitet hatten. In einem im März 1999 in der PC Week veröffentlichten Artikel wurde eine Studie mit 800 Teilnehmern zitiert, bei denen 21 bis 31% der Befragten zugaben, bereits einmal vertrauliche Informationen wie Finanz- oder Produktdaten per E-Mail an Außenstehende verschickt zu haben.

E-Mails mit böswilligen oder beleidigenden Inhalten

E-Mails mit rassistischen, anzüglichen oder anderen beleidigenden Inhalten, die von Mitarbeitern eines Unternehmens verschickt oder auch empfangen werden, können auch für den Arbeitgeber schwer wiegende rechtliche Folgen haben und ihn somit angreifbar machen. Im September 2003 wurde das britische Unternehmen Holden Meehan Independent Financial Advisors von einer ehemaligen Mitarbeiterin auf £10.000 Schadenersatz verklagt, weil das Unternehmen sie nicht vor beleidigenden E-Mails geschützt hatte. Auch das US-Unternehmen Chevron geriet in die Schlagzeilen, weil es vier seiner Mitarbeiter 2,2 Millionen US-Dollar zahlen musste, die sexuell belästigende E-Mails erhalten hatten. Nach britischem Recht können Arbeitgeber für E-Mails rechtlich belangt werden, die Mitarbeiter während ihrer Unternehmenszugehörigkeit verfassen – unabhängig davon, ob die Nachricht mit Einverständnis des Arbeitgebers verschickt wurde oder nicht. Das Versicherungsunternehmen Norwich Union musste als Ergebnis einer außergerichtlichen Einigung 450.000 US-Dollar Schadenersatz zahlen, weil es sich widerrechtlich per E-Mail zu Mitbewerbern geäußert hatte.

Methoden zur Kompromittierung von E-Mail-Systemen

Um sich besser auf die verschiedenen Arten aktueller E-Mail-Angriffe einstellen und geeignete Abwehrmaßnahmen ergreifen zu können, sollten Administratoren über alle gängigen Angriffsmethoden informiert sein. Hierzu zählen:

Anhänge mit böswilligen Inhalten

Die Viren Melissa und LoveLetter waren die ersten Schädlinge, die Anwender vor Augen geführt haben, dass vermeintlich vertrauenswürdige E-Mails mit angeblich harmlosen

Anhängen eine große Gefahr darstellen. Diese Viren nutzten das Vertrauensverhältnis aus, das zwischen Freunden oder Kollegen besteht, um sich ungehindert zu verbreiten. Welcher Anwender zweifelt schon an der Integrität einer Mitteilung, die von einem Freund empfangen wird und dazu auffordert, den beigefügten Anhang zu öffnen? Diese Vorgehensweise verfolgten unter anderem die E-Mail-Würmer Melissa, AnnaKournikova und Sircam. Wird ein solcher Wurm aktiviert, versendet er sich selbst an sämtliche E-Mail-Adressen, die er im Adressbuch des befallenen Rechners findet, an Adressen aus verschickten Mitteilungen, an auf dem lokalen Rechner gespeicherte Webpage-Caches, oder er bedient sich ähnlicher Methoden. Virenschreiber sind vor allem darauf bedacht, dass ihre Opfer auf jeden Fall den Anhang öffnen. Sie spielen dabei mit den Erwartungen der Empfänger und versehen Anhänge mit verlockenden Namen wie SexPic.cmd oder me.pif.

Viele Anwender versuchen, das Risiko, ihr System mit E-Mail-Viren zu infizieren, indem sie nur solche Dateien öffnen, die bestimmte Dateierweiterungen wie JPG oder MPG besitzen. Es gibt jedoch einige Viren, wie den AnnaKournikova-Wurm, die sich mit mehreren Erweiterungen tarnen, um Anwender zu täuschen. So wurde der Schädling AnnaKournikova als E-Mail-Anhang mit dem Namen "AmmaKournikova.jpg.vbs" übertragen. Die doppelte Dateierweiterung mit "JPG" als eine der Endungen für eine harmlose Bilddatei sollte Empfänger darüber hinwegtäuschen, dass es sich tatsächlich um ein Visual Basic Script mit böswilligem Code handelt – und nicht etwa um ein Bild des berühmten Tennis-Stars.

Zudem können Hacker mit der Class ID-Erweiterung (CLSID) die eigentliche Erweiterung der Datei verbergen und somit die Tatsache verschleiern, dass es sich bei der Datei cleanfile.jpg um eine verheerende HTA-Datei handelt (HTML-Applikation).

Mit Hilfe diese Methode werden zurzeit auch verschiedene Content-Filter-Lösungen überlistet, die nur auf einfache Dateikontrollmethoden zurückgreifen – mit der Folge, dass Hacker noch Ihren Opfern noch einfacher Schaden zufügen können.

Applikations-Schwachstellen als Schlupfloch für Viren

Internet-Anwender wurden vom Nimda-Wurm vollkommen überrascht, da dieser viele E-Mail-Sicherheitslösungen einfach umging und neben Servern und Unternehmensnetzwerken auch die Rechner normaler Heimanwender befiel. Bei Nimda besteht die Besonderheit darin, dass er sich auf Rechnern mit einer ungepatchten Version des Internet Explorer oder von Outlook Express automatisch aktiviert. Nimda ist einer der ersten Schädlinge aus einer mittlerweile langen Liste, die sich Schwachstellen in bestimmten Applikationen zu Nutze machen, um sich zu verbreiten. Varianten des Bagle-Virus vom März 2004 haben z. B. eine alte Outlook-Sicherheitslücke ausgenutzt, um sich auch ohne Zutun von Anwendern zu verbreiten.

HTML-Mails mit eingebetteten Skripten

Alle aktuellen E-Mail-Clients sind in der Lage, Mitteilungen im HTML-Format zu empfangen und zu verschicken. HTML-Mails können Skripten und Active Content enthalten, mit denen sich

Programme oder Code auf den Client-Rechnern ausführen lassen. Outlook und andere Produkte verwenden zur Anzeige von HTML-Mails Komponenten des Internet Explorer – und weisen dadurch auch automatisch für die gleichen Schwachstellen auf wie der IE.

Auf HTML-Skripten basierende Viren bergen zudem die Gefahr, dass sie automatisch gestartet werden, sobald die Mitteilung geöffnet wird. Der Schadteil steckt somit nicht länger im Anhang – mit der Konsequenz, dass Filter zur Anhangskontrolle, die in gängigen Anti-Viren-Lösungen zum Einsatz kommen, bei der Abwehr unbekannter HTML-Skript-Viren versagen.

Der Virus BadTrans.B beispielsweise setzt zur Verbreitung auf eine Kombination aus E-Mail-Exploit und HTML. Der infizierte Anhang wird automatisch per HTML-Skript geöffnet, sobald die E-Mail beim Empfänger eingeht.

Virenerstellung leicht gemacht

Mit nur wenig Visual Basic-Erfahrung lässt sich bereits viel Unheil anrichten, indem einfach Viren programmiert werden, die bereits bekannte Sicherheitslücken häufig verwendeter E-Mail-Clients und Produkte ausnutzen. Um sich über Schwachstellen zu informieren, genügt ein kurzer Aufruf der SecurityFocus-Website, die Auskunft über verschiedene verfügbare Exploits gibt, z. B. für Microsoft Outlook. Böswillige Script-Kiddies, die einen Virus erstellen wollen, brauchen lediglich den Exploit-Code zu modifizieren – der öffentlich zugänglich ist – um eigenen Code zur Ausführung zu bringen.

Auf der Site Guninski.com wird beispielsweise ein Exploit für den Internet Explorer und Microsoft Access beschrieben, der auch problemlos auf Outlook und Outlook Express anwendbar ist. Virenschreiber können sich dies zu Nutze machen, um Visual Basic-Code auszuführen, sobald das Opfer eine infizierte E-Mail öffnet. HTML-Dateien würden infiziert sein, und der Virus verschickt sich selbst an alle im Adressbuch des Empfängers verzeichneten Kontakte. Das Hauptmerkmal dieses Virus' besteht jedoch darin, dass es schon gestartet wird, sobald der Anwender einfach die mit böswilligem HTML-Skript versehene E-Mail öffnet.

Warum Anti-Viren-Software oder eine Firewall nicht ausreicht

Einige Unternehmen wiegen sich in falscher Sicherheit, wenn sie denken, dass sie durch die Installation einer Firewall bereits ausreichend geschützt sind. Dieser Schritt ist auf jeden Fall ratsam, um das Intranet eines Unternehmens zu schützen, aber er reicht längst nicht aus: Firewalls können zwar verhindern, dass unautorisierte Anwender auf ein Netzwerk zugreifen, aber sie kontrollieren z. B. nicht den Inhalt von E-Mails, die von autorisierten Netzwerk-Anwendern verschickt und empfangen werden. Dies bedeutet, dass E-Mail-Viren diese Sicherheitsbarriere immer noch überwinden können.

Zudem schützt Anti-Viren-Software auch nicht vor ALLEN E-Mail-basierten Viren und Angriffen:

Anti-Viren-Hersteller können ihre Signaturen nicht immer rechtzeitig auf den neuesten Stand bringen, um Anwender vor zerstörerischen Viren zu schützen, die sich binnen weniger Stunden weltweit per E-Mail verbreiten und Systeme infizieren (wie die aktuellen Würmer MyDoom, NetSky.B und Beagle). Unternehmen, die lediglich eine einzige Scan-Engine zur Virenabwehr einsetzen, sind somit bei Ausbruch eines neuen Virus' nicht in jedem Fall zuverlässig geschützt. Eine von der britischen Regierung Anfang 2004 in Auftrag gegebene Studie ergab, dass 99% der großen Unternehmen in Großbritannien Anti-Viren-Produkte einsetzen, aber 68% von ihnen im Jahr 2003 dennoch mit Viren infiziert wurden. Diese Anfälligkeit wurde im Jahr 2003 durch eine Studie der Forschungslabors von Hewlett-Packard in Bristol bestätigt. Das Methode der Erkennung und Abwehr neuer Viren durch Signatur-Updates ist grundsätzlich unausgereift: Viren und Würmer verbreiten sich immer schneller, als aktualisierte Virensignaturen verteilt werden können.

Die Lösung: Ein proaktiver Ansatz

Wie können sich Anwender nun vor diesen E-Mail-Gefahren schützen? Nur durch einen proaktiven Ansatz, d. h., die Inhalte sämtlicher eingehender und ausgehender E-Mails sind schon auf Server-Ebene zu überprüfen, bevor sie an Anwender weitergeleitet werden. Hierdurch wird garantiert, dass nur wenn potenziell böswillige Inhalte aus einer infizierten oder verdächtigen Mitteilung entfernt worden sind, diese an Empfänger weitergeleitet wird.

Unternehmen können sich durch einen auf ihrem E-Mail-Server installierten Gateway, der umfassende Inhaltskontrolle von E-Mails und Virenabwehr bietet, vor potenziellen Schäden und Produktivitätsverlust durch aktuelle und zukünftige Viren schützen.

Über GFI MailSecurity for Exchange/SMTP

GFI MailSecurity for Exchange/SMTP ist eine umfassende E-Mail-Sicherheitslösung und bietet Inhaltskontrolle, Exploit-Erkennung, Gefahrenanalyse und Anti-Viren-Schutz für elektronische Post. Sämtliche schädlichen Elemente, die sich per E-Mail übertragen lassen, werden beseitigt, bevor sie E-Mail-Anwender erreichen. Zu den wichtigsten Leistungsmerkmalen von GFI MailSecurity zählen unter anderem mehrere Virus-Engines für eine höhere Erkennungsrate und schnellere Gegenmaßnahmen bei neuen Viren, eine E-Mail-Inhalts- und Anhangskontrolle, um gefährliche Inhalte und Anhänge unter Quarantäne zu stellen, ein Exploit-Schutz zur Abwehr von aktuellen und zukünftigen auf Exploits basierenden Viren, eine HTML-Threats-Engine zum Deaktivieren von HTML-Skripten sowie ein Trojan & Executable Scanner zum Aufspüren potenziell gefährlicher exe-Dateien. Weitere Informationen und eine Test-Version stehen zum Download bereit unter <http://www.gfi-software.de/de/mailsecurity>.

Über GFI

GFI (www.gfisoftware.de) ist ein führender Entwickler und Anbieter von Produkten für Netzwerk- und Inhaltssicherheit sowie von Kommunikationslösungen. Das Produktportfolio von GFI umfasst unter anderem den Netzwerk-Fax-Server GFI FAXmaker for Exchange/SMTP, die Sicherheitslösung GFI MailSecurity for Exchange/SMTP zur Überprüfung von E-Mail-Inhalten und zum Schutz vor E-Mail-basierten Exploits und Viren, die Server-basierte Anti-Spam-Software GFI MailEssentials for Exchange/SMTP, GFI LANguard Network Security Scanner (N.S.S.) für Sicherheits-Scans und Patch-Management, GFI Network Server Monitor zum automatischen Versand von Warnmitteilungen und zur Fehlerbehebung bei Netzwerk- und Server-Problemen, GFI LANguard Security Event Log Monitor (S.E.L.M.) zur Ereignisprotokoll-basierten Eindringlingserkennung und netzwerkweiten Verwaltung von Ereignisprotokollen sowie GFI LANguard Portable Storage Control (P.S.C.) zur netzwerkweiten Kontrolle wechselbarer Speichermedien. GFI-Produkte sind im Einsatz bei Microsoft, Telstra, Time Warner Cable, Shell Oil Lubricants, NASA, DHL, Caterpillar, BMW, der US-Steuerbehörde IRS und der USAF. GFI unterhält Niederlassungen in den USA, Großbritannien, Deutschland, Zypern, Rumänien, Australien und Malta und wird von einem weltweiten Netzwerk von Distributoren unterstützt. GFI ist "Microsoft Gold Certified Partner" und erhielt die Auszeichnung "Microsoft Fusion (GEM) Packaged Application of the Year". Weitere Informationen erhalten Sie unter <http://www.gfisoftware.de>.

© 2004 GFI Software Ltd. Alle Rechte vorbehalten. Die in diesem Dokument aufgeführten Informationen geben den von GFI zum Zeitpunkt der Veröffentlichung vertretenen Standpunkt zum Thema des White Papers wieder. Änderungen aufgrund von veränderten Marktbedingungen sind vorbehalten. Die in diesem Dokument präsentierten Informationen stellen keine Verpflichtung seitens GFI dar, und für ihre Genauigkeit wird nach dem Datum der Veröffentlichung keine Garantie übernommen. Dieses White Paper dient nur der Produktinformation. GFI ÜBERNIMMT KEINE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE HAFTUNG FÜR DIE IN DIESEM DOKUMENT PRÄSENTIERTEN INFORMATIONEN. GFI, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI LANguard, GFI Network Server Monitor, GFI DownloadSecurity und die zugehörigen Produkt-Logos sind eingetragene Marken oder Marken von GFI Software Ltd. in den Vereinigten Staaten und/oder anderen Ländern. Alle in diesem Dokument aufgeführten Produkte oder Firmennamen sind Eigentum der jeweiligen Inhaber.

