WHITE PAPER

Keine Chance für Spam in Netzwerken

Auf welche Funktionen Sie bei Anti-Spam-Lösungen achten sollten

Dieses White Paper ist als Leitfaden für den Kauf von Software zur Abwehr von Spam in Netzwerken gedacht und informiert Sie über Leistungsmerkmale, die jede Anti-Spam-Lösung besitzen sollte.

Einführung

Dieses Dokument informiert Sie über die wichtigsten Funktionen, die zur effizienten Abwehr von Spam erforderlich sind.

Wachstum und Kosten von Spam

Laut den Forschern der US-amerikanischen Radicati Group handelt es sich bei 52% aller weltweit verschickten E-Mails um Spam-Mitteilungen – ein Wert der bis zum Jahr 2007 auf 70% ansteigen soll. Zu einer ähnlichen Einschätzung kommt die Europäische Union, die den Anteil der Spam-Mitteilungen an der gesamten E-Mail-Korrespondenz bei 50% sieht.

Dies hat zur Folge, dass Mitarbeiter einen beachtlichen Teil ihrer Arbeitszeit dafür aufwenden müssen, ihre Postfächer von Spam zu säubern. Die durch Spam verursachten Kosten schlagen sich somit in Form einer verringerten Produktivität nieder. Des Weiteren nimmt die Übermittlung von Spam wertvolle Bandbreite und Speicherkapazität in Anspruch und belastet die Netzwerk-Infrastruktur. Zuletzt darf nicht außer Acht gelassen werden, dass sich neben der Vielzahl von Spam-Mitteilungen auch erwünschte Nachrichten im Posteingang befinden. Werden die Mailboxen wegen Zeitmangels eilig von den lästigen Werbemitteilungen gesäubert, kann es somit vorkommen, dass erwünschte Mitteilungen unbeabsichtigt mit gelöscht werden.

Berechnungen von Ferris Research zufolge verschwendet ein einziger Mitarbeiter bei nur fünf Spam-Mails pro Tag und einem Bearbeitungsaufwand von jeweils 30 Sekunden jedes Jahr somit fünfzehn Stunden wertvoller Arbeitszeit. Werden die durch diese Arbeit entstandenen Kosten nun auf alle Mitarbeiter des Unternehmens hochgerechnet, bekommt man ein ungefähres Bild davon, welche Kosten der durch Spam hervorgerufene Produktivitätsausfall verursachen kann. Laut Radicati Group beliefen sich im Jahr 2003 die durch Spam verursachten Kosten auf rund 49 US-Dollar pro Mailbox. Dieser Wert, so die Experten, soll bis zum Jahr 2007 auf die Schwindel erregende Höhe von 257 US-Dollar pro Postfach ansteigen.

Aus diesem Grund muss die Flut an Spam-Mitteilungen eingedämmt werden, um Produktionszeit, Ressourcen und Bandbreite nicht weiter zu belasten. Ein wichtiger Schritt in diese Richtung besteht darin, Netzwerk-Anwender darauf hinzuweisen, dass ihre E-Mail-Adresse nicht öffentlich und an Außenstehende weitergegeben wird (z. B. über Postings in Internet-Foren). Neben diesen grundlegenden Verhaltensregeln für Anwender muss jedoch auch von technischer Seite her eine effektive Anti-Spam-Lösung auf Server-Ebene zum Einsatz

kommen.

Auswahl der richtigen Anti-Spam-Software

Zur Abwehr von Spam-Mitteilungen ist bereits eine Vielzahl von Software-Lösungen erhältlich, deren Wirksamkeit jedoch nicht in allen Fällen sehr ausgeprägt ist. Im Folgenden erhalten Sie nützliche Informationen zu den Leistungsmerkmalen, auf die Sie bei der Auswahl von Spam-Blockern achten sollten.

Server- oder Client-basiert?

Die Abwehr von Spam auf Client-Ebene nimmt weitaus mehr Zeit in Anspruch als auf Server-Ebene. Bei einer Client-basierten Lösung muss Anti-Spam-Software auf allen Workstations Ihres Netzwerks installiert werden. Dies hat zur Folge, dass die Aktualisierung der Anti-Spam-Regeln für jeden Rechner einzeln durchzuführen ist. Des Weiteren ist Ihr E-Mail-System auch weiterhin den Angriffen von Spammern ausgesetzt: Die Nachrichtenspeicher Ihrer Server werden kontinuierlich mit Spam-Mitteilungen belastet, die gelöscht werden müssen. Vor allem aber müssen Ihre Mitarbeiter wertvolle Arbeitszeit dafür aufwenden, Spam auszusortieren und Anti-Spam-Regeln zu aktualisieren: Das eigentliche Ziel, den zeitlichen Aufwand für die Beseitigung von Spam zu reduzieren, verringert sich mit einer Client-basierten Lösung somit nicht – die Belastung verschiebt sich lediglich.

Ferner bietet eine Desktop-Lösung nicht dieselben Informationen und Ressourcen, auf die eine Server-basierte Anti-Spam-Lösung zurückgreifen kann. So lassen sich z. B. Absender-Server nicht überprüfen. Nur mit einer Server-basierten Anti-Spam-Lösung ist es möglich, Spam effektiv blockieren. Diese Methode hat unter anderem folgende Vorteile:

1. Durch die Installation am Gateway lassen sich Schwierigkeiten vermeiden, die mit der Installation und Administration Desktop-basierter Produkte verbunden sind.
2. Die Lizenzierung ist weitaus kostengünstiger.
3. Spam gelangt von vornherein nicht in Ihr E-Mail-System, sodass die Nachrichtenspeicher generell von unerwünschten Werbemitteilungen verschont bleiben.
4. Server-basierte Anti-Spam-Software stehen umfangreichere Ressourcen/Datenbanken zur Verfügung, dank derer sich Spam noch effizienter herausfiltern lässt.

Bayes'sche Filter-Technologie

Bis vor ein paar Jahren vertrauten Anti-Spam-Produkte bei der Identifizierung von Spam lediglich auf Stichwortlisten. Je umfangreicher die Liste, desto mehr Spam-Mitteilungen konnten abgefangen werden. Heutzutage ist diese Methode allein jedoch nicht mehr zuverlässig genug, denn sie erzeugt zu viele Fehlalarme (“False Positives”). Zudem müssen die Listen oftmals manuell aktualisiert werden.

Mittlerweile empfehlen führende Experten und Fachpublikationen als beste Methode zur Abwehr von Spam den Einsatz von Bayes'schen Filtern. Der Bayes'sche Filter setzt zur Spam-Erkennung statistische Berechnungen ein, bei denen bekannte Spam- und Ham-Mitteilungen (erwünschte E-Mails) berücksichtigt werden. Dieser lernfähige Filter ist der veralteten, statischen Anti-Spam-Technologie überlegen, da er nicht nur nach Stichwörtern sucht oder bei der Spam-Erkennung lediglich auf regelmäßig herunterzuladende Spam-Signaturen vertraut. Weitere Informationen zur Bayes'schen Filtermethode erhalten Sie in einem weiteren White Paper von GFI, "Effektive Bekämpfung von Spam mit Hilfe der Bayes'schen Filter-Technologie", unter http://www.gfisoftware.de/de/whitepapers/why-bayesian-filtering.pdf.

Die Bayes'sche Filtermethode hat unter anderem folgende Vorteile:

1. Die Mitteilung wird als Ganzes auf Spam-Merkmale überprüft; die Erkennung erfolgt nicht nur über Stichwörter oder bekannte Spam-Signaturen.
2. Der Filter lernt von ausgehenden Mitteilungen (Ham) und reduziert somit deutlich die Anzahl von Fehlalarmen.
3. Der Filter passt sich kontinuierlich an, indem alle neuen Spam- und Ham-Mitteilungen berücksichtigt werden.
4. Jedes Unternehmen verfügt über einen eigenen Datenbestand zur Spam-Abwehr, der einen individuellen und somit unüberwindbaren Schutz bietet.
5. Die Technologie kann für mehrere Sprachen und international eingesetzt werden.

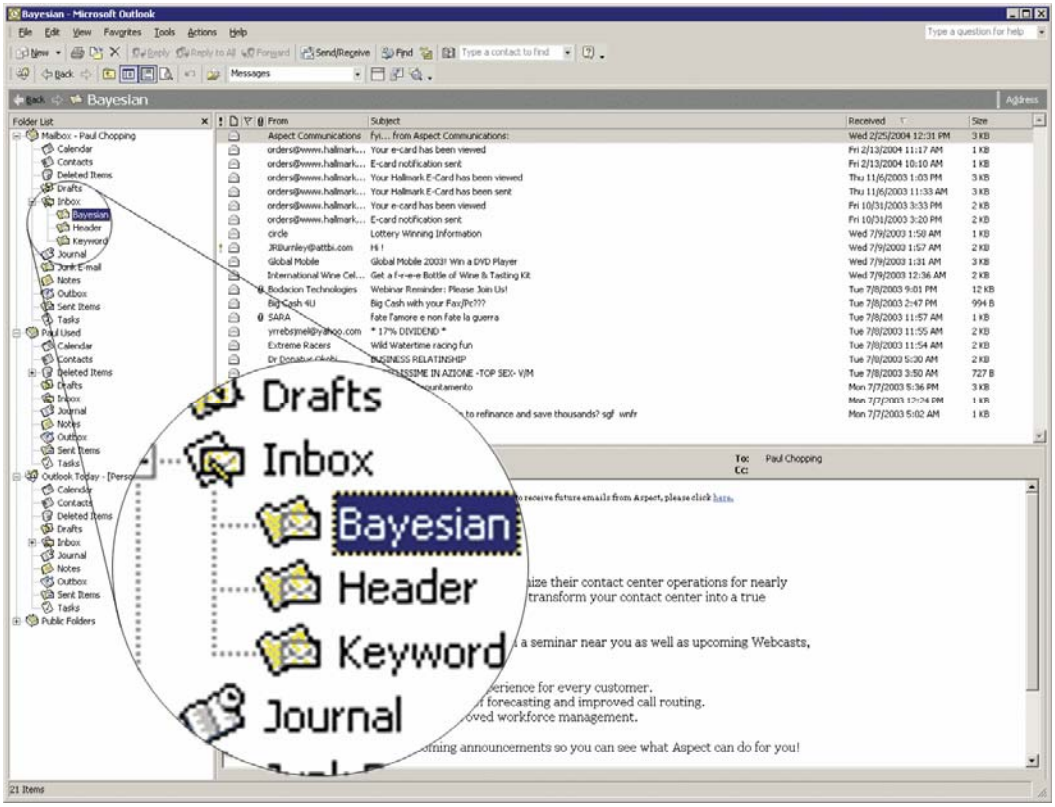
Angepasste Ham-Datei für den Bayes'schen Filter

Beim Einsatz eines Bayes'schen Filters kommt es darauf an, dass der Filter bei der Erkennung erwünschter Mitteilungen ("Ham") auf eine Datenbank zugreifen kann, die individuell an Ihr Unternehmen angepasst ist. Die Ham-Daten müssen dabei unbedingt aus Ihrer ausgehenden E-Mail-Korrespondenz stammen. Daher wird der Bayes'sche Filter mit Hilfe einer Lernphase am Anfang seines Einsatzes an Ihre Korrespondenz angepasst. Andere Anti-Spam-Lösungen verwenden hier lediglich eine allgemeine Datei mit Ham-Daten, die im Lieferumfang enthalten ist. Beispiel hierfür sind der Spam-Filter von Outlook oder der Exchange Server Internet Message Filter. Obwohl bei dieser Technologie keine Lernphase erforderlich ist, weist sie zwei grundlegende Mängel auf:

1. Die Datei mit den Ham-Daten ist öffentlich zugänglich und kann daher von professionellen Spammern gehackt und somit umgangen werden. Ist die Ham-Datei jedoch an Ihr Unternehmen angepasst und somit einzigartig, hat das Hacken der Ham-Datei keinen Sinn. Auch beispielsweise für den Spam-Filter von Outlook 2003 sind bereits Hacks aufgetaucht.

2. Der Inhalt der Ham-Datendatei ist sehr allgemein gehalten. Da die speziellen Eigenheiten der für Ihr Unternehmen üblichen Korrespondenz nicht berücksichtigt werden, ist diese Datei längst nicht so effektiv wie eine individuell angepasste Ham-Datei. Auch die Anzahl der False Positives steigt beachtlich. Beispielsweise würde die Anwendung einer

allgemeinen Ham-Datendatei auf die E-Mail-Korrespondenz eines Finanzunternehmens sehr viele Fehlalarme auslösen, da von diesem das Wort "Hypothek" sehr häufig und legitim verwendet wird, gleichzeitig aber auch bei Spammern sehr beliebt und daher in der Standard-Ham-Datei aufgeführt ist.



Einfache Überprüfung potenziellen Spams über ein Mailbox-Unterverzeichnis von Anwendern

Automatisch aktualisierte Spam-Datendatei für den Bayes'schen Filter

Die Spam-Datendatei des Bayes'schen Filters muss laufend mit den neuesten Spam-Merkmalen aktualisiert werden. Dadurch wird sichergestellt, dass der Bayes'sche Filter auch sämtliche neue Spam-Tricks erkennt und eine hohe Erkennungsrate erzielt (Hinweis: Optimale Erekennungsraten werden erst nach der zweiwöchigen Lernphase erzielt.) Wählen Sie somit eine Anti-Spam-Lösung, die diese aktuellen Spam-Daten regelmäßig für Sie abruft und Updates automatisch herunterlädt!

Effiziente Überprüfung potenzieller Spam-Mitteilungen

Ein grundlegendes Problem der Anti-Spam-Technologie sind False Positives, Fehlalarme, bei denen erwünschte E-Mail als Spam markiert wird, obwohl es sich nicht um eine Werbemitteilung handelt. Zuverlässige Anti-Spam-Software sollte es Anwendern daher problemlos ermöglichen, als Spam markierte Miteilungen einfach und effizient zu überprüfen.

Um Administratoren zusätzliche Arbeit zu ersparen, sollte die Anti-Spam-Lösung eine Option bieten, mit der als Spam klassifizierte Mitteilungen bei den einzelnen Benutzern in einen jeweils dafür bereitgestellten Junk-Mail-Ordner geleitet wird. Des Weiteren sollte die Software die Spam-Nachrichten in unterschiedliche Verzeichnisse verschieben können, je nachdem, mit welcher Erkennungsmethode die unerwünschte Mitteilung abgefangen wurde. Dank dieses schnellen Zugriffs auf als Spam markierte E-Mails können Anwender potenzielle Spam-Mitteilungen schneller überprüfen. Bei einigen Anti-Spam-Produkten ist es jedoch notwendig, dass sich Anwender bei einem Web-basierten System anmelden müssen, bevor es ihnen möglich ist, ihre Mitteilungen einzeln nacheinander zu überprüfen. Aus rein praktischen Gründen ist diese zeitaufwändige Methode nicht zu empfehlen, denn sie hält Anwender eher davon ab, ihre E-Mails zu kontrollieren.

Flexible Whitelists zur Verminderung von False Positives

Anti-Spam-Software muss eine Funktion besitzen, mit der sich umfangreiche Whitelists effizient erstellen lassen. Über Whitelists sollten alle gültigen Geschäftspartner zu identifizieren sein, um dauerhaft zu verhindern, dass ihre Mitteilungen als Spam klassifiziert werden. Gute Anti-Spam-Software sollte somit das automatische Erstellen und Aktualisieren von Whitelists unterstützen.

Spam-Abwehr mit GFI MailEssentials

Die Erkennung und Abwehr von Spam mit Hilfe von GFI MailEssentials erfolgt mit Hilfe folgender Methoden und Technologien:

1. **Abwehr von Spam auf Server-Ebene** – GFI MailEssentials wird direkt auf Ihrem Exchange 2000/20003-Server oder vor Ihrem Mail-Server installiert (bei Einsatz von Exchange 5.5 oder eines anderen Mail-Servers). So werden Spam-Mitteilungen erkannt, BEVOR sie auf Ihren Mail-Server gelangen können. Ihre E-Mail-Infrastruktur wird somit nicht mit Spam-Nachrichten belastet und Spam-Erkennungsregeln müssen nur auf dem Rechner mit GFI MailEssentials aktualisiert werden. Whitelists (Domänen/E-Mail-Adressen, von denen alle Mitteilungen erwünscht sind) und Blacklists (Domänen/E-Mail-Adressen, von denen Sie auf keinen Fall Mitteilungen erhalten möchten) lassen sich auf Server-Ebene einsetzen.

2. Analyse des Inhalts einer E-Mail mit Hilfe der **Bayes'schen Filtertechnologie** und Einsatz von auf Ihr Unternehmen zugeschnittenen Ham-Datenbanken. Aktuelle Spam-Daten werden per automatischem Download von der Web-Site von GFI regelmäßig aktualisiert. Weitere Informationen zur Bayes'schen Filtertechnologie finden Sie in folgendem White Paper von GFI: http://www.gfisoftware.de/de/whitepapers/why-bayesian-filtering.pdf.

3. **Reduzierung von False Positives durch eine automatische Whitelist** – GFI MailEssentials bietet eine zum Patent angemeldete automatische Whitelist-Verwaltung. Diese Technologie garantiert, dass alle Ihre Geschäftspartner automatisch einer Liste mit erwünschten Korrespondenzpartnern ohne weiteren Benutzereingriff oder zusätzliche

Administration hinzugefügt werden. Ihre Korrespondenz mit diesen Absendern wird nicht vom Spam-Filter kontrolliert, sodass sich Fehlalarme verhindern lassen.

4. **Flexible Verwaltung von Spam** – Nachdem eine Mitteilung als Spam identifiziert wurde, kann sie in ein Unterverzeichnis des Benutzer-Posteingangs geleitet werden. Wird bei der Kontrolle von Nachrichten festgestellt, dass eine gültige E-Mail versehentlich als Spam markiert wurde (z. B. ein abonnierter Newsletter), können Anwender den Absender ihrer Whitelist hinzufügen.

5. Zusätzlich bietet GFI MailEssentials auch die **Unterstützung der Stichwortkontrolle**, sodass Administratoren ihre Anti-Spam-Filter noch detaillierter konfigurieren können.

6. Als ergänzende Schutzmaßnahme zur Bayes'schen Filtertechnologie werden in GFI MailEssentials weitere **Technologien zur Spam-Erkennung** eingesetzt, darunter eine intelligente Funktion zur Mail-Header-Analyse und der Abgleich mit individuell festgelegten und öffentlichen Blacklists wie ORDB oder SpamHaus.

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 Fax-Connector GFI FAXmaker für Exchange- und SMTP-Mail-Server, 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, die E-Mail-Archivierungslösung GFI MailArchiver, 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, GFI LANguard Portable Storage Control (P.S.C.) zur netzwerkweiten Kontrolle wechselbarer Speichermedien sowie GFI WebMonitor zur Überwachung von HTTP/FTP-Verbindungen mit Virenschutz für ISA Server. GFI-Produkte sind im Einsatz bei Microsoft, Telstra, Time Warner Cable, 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.