Kampf dem Werbemüll

Als ob Spam und Viren noch nicht ausreichend für Ärger sorgten, sehen sich E-Mail-Anwender mit einer weiteren Erscheinung konfrontiert – der Spyware. Doch es gibt wirksame Abhilfe, dass das erfolgreiche Kommunikationsmittel E-Mail nicht am eigenen Erfolg scheitert.

von Aldo Britschgi

Längst ist Spam mehr als ein blosses Ärgernis: es vermindert die Mitarbeiter-Produktivität und belastet Netzwerke, Server und die elektronischen Postfächer mit ungewolltem und oftmals anstössigem Inhalt. Mit dem unaufhaltsamen Wachstum des Werbemülls nehmen auch die negativen Auswirkungen auf Unternehmen zu – und ein Ende der Misere ist nicht in Sicht. Vordergründig scheint dies kein Problem zu sein. Aber bei durchschnittlich 96 Spam-Mails pro Tag, geht der Schaden rasch einmal in die Tausenden von Franken. Rechnet man durchschnittlich fünf Sekunden pro E-Mail für Sortierung, Analyse und anschliessende Löschung, so ergibt das bereits mehr als acht Minuten unproduktiver Arbeitszeit pro Tag und Mitarbeiter. In einer Firma mit 150 Angestellten gehen so wöchentlich schnell einmal über hundert Arbeitsstunden verloren.

Darin nicht eingerechnet sind Zeitaufwand und Ärger, etwa wenn die gesuchte E-Mail in der Spamflut nicht mehr auffindbar ist oder gar irrtümlicherweise gelöscht wurde. Zusätzlicher Schaden entsteht, wenn ein

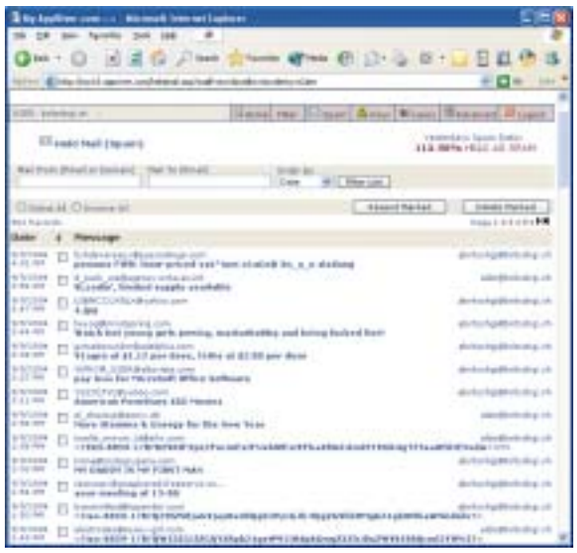
LESER FRAGEN – ICT KOMMUNIKATION ANTWORTET:

«Mittlerweile sind auch Firewalls mit integrierter Intrusion-Detection-(IDS-)Funktionalität erhältlich. Ist diese Multifunktionalität wirklich das Non-Plus-Ultra, wenn man nur gerade den Datenverkehr zwischen Intra- und Internet kontrollieren und schützen will? Welche Erfahrungen haben Anwender solcher Firewalls mit integriertem IPS gesammelt?» *(R. L. aus B.)*

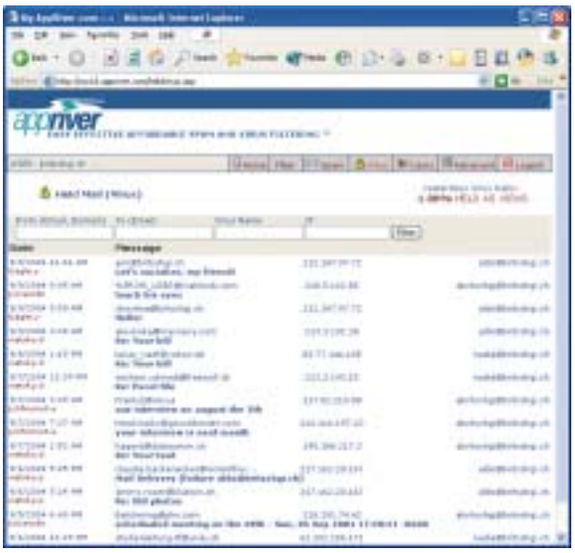
Eine Firewall regelt den Verkehr zwischen der internen Netzwerk (LAN) und dem externen Internet-Anschluss (WAN) aufgrund definierter Regeln, beispielsweise der Öffnung des Port 80 für den WWW-Zugriff oder die Sperrung des Port 21, falls aus definierten Gründen FTP-Verbindungen verboten sind.

Unter «Intrusion» versteht man die absichtliche Verletzung der Sicherheitsmassnahmen eines Systems. Das Ziel der Intrusion Detection (ID) ist es, diese Verletzungsversuche zu erkennen und mittels Intrusion Gegenmassnahmen (Intrusion Response System, IRS) geeignete Gegenmassnahmen zu treffen, beispielsweise die Sperrung der IP-Adresse des Angreifenden oder die Alarmierung zuständiger Sicherheitsfachleute. Intrusion-Funktionen ergänzen die Firewall in sinnvoller Weise, indem sie sämtliche Daten-Pakete einer eingehenden Analyse unterziehen und zwischen zulässigem Datenverkehr und echten Angriffen unterscheiden, die sowohl von innen als auch von aussen erfolgen.

Die ständig zunehmenden Sicherheitsbedrohungen und raffinierteren Hacker-Aktivitäten verlangen nach modernen Systemen und Firewalls mit integriertem IDS-Funktionalität. Mit Hilfe der Intrusion-Detection-Systeme ist es möglich, anhand von verdächtigen Aktivitäten im Netzwerk Angriffe schon im Vorfeld zu erkennen und abzuwehren.



Bei einer externen Antispamlösung hat der E-Mail-Benutzer über eine Web-Oberfläche den Zugriff auf alle gefilterten E-Mails.



Moderne Antispam-Lösungen verfügen über integralen Virenschutz und halten sämtliche E-Mails mit Virenanhängen zurück.

Mailserver unter der Spamflut zusammenbricht oder ein Mailversand gar nicht mehr möglich ist, weil ein «Spammer» die gesamte Bandbreite des Postausgangsservers (SMTP) beansprucht.

Warum gibt es Spam?

Die meisten Spammails sind kommerzieller Natur. Der Versand erfolgt in Massen, also gleichzeitig an Hunderttausende oder gar Millionen Empfänger. Die Kosten des Versands sind gering. Das Hauptproblem stellen die Zieladressen dar: Spezialisierte Programme generieren systematisch E-Mail-Adressen und senden diese mit fremden Absendern an Internet-Server. Das Ergebnis sind unzählige Unzustellbarkeitsmeldungen, die wiederum in die Postfächer ahnungsloser E-Mail-Anwender schwappen.

Als besonderes Merkmal von Spam bezahlt der Empfänger die Kosten und nicht der Versender. Das SMTP-Protokoll, das Standardprotokoll für die Kommunikation zwischen E-Mail-Servern, erlaubt den Versand an zahllose Empfänger per Mausklick. Für den Versender, Spammer genannt, lohnt sich das Geschäft in jedem Fall. Kauft auf Millionen von Versendungen nur eine Handvoll Empfänger ein Produkt, sind die Werbekosten bereits gedeckt.

Wie gelangen aber Spammer in den Besitz der Empfänger-Adressen? Ganz einfach: Suchprogramme – vergleichbar mit herkömmlichen Suchmaschinen wie Google oder Search.ch – indizieren Websites und sammeln E-Mail-Adressen. Weit verbreitet ist etwa die «Brute Force»-Methode, die systematisch E-Mail-Adresse ausprobiert. Am erfolgreichsten ist aber das blosse Scannen des E-Mail-Verkehrs im Internet, fluten E-Mails doch wie offene Postkarten durchs Netz. Die so gefundenen Adressen lassen sich automatisch kopieren und in zweifelhaften Datenbanken für den weltweiten Adressenhandel speichern.

Viren und Spam sind Verbündete

Spam-Versender und Virenprogrammierer arbeiten Hand in Hand. Das verschärft die Probleme für Firmenverantwortliche dramatisch. Immer öfter enthalten Spam-E-Mails nämlich Vi-

SCHUTZSCHILD AM INTERNET-GATEWAY

Der kalifornische Security-Spezialist McAfee hat den Launch seiner Sicherheitslösung WebShield 3.0 bekannt gegeben. WebShield ist eine Komponente der Secure-Content-Management-Lösung und bietet Virenschutz, Content-Scanning-Funktionen sowie Anti-Spam-Funktionen direkt am Internet-Gateway.

AD-AWARE KOMPLETTIERT SECURITY-PORTFOLIO

Der norwegische Sicherheitsanbieter Norman Data Defense hat eine strategische Partnerschaft mit dem schwedischen Anbieter von Antispyware-Lösungen Lavasoft geschlossen. Durch die Kooperation ergänzt Norman sein Produkt-Portfolio aus Antiviren-, Antispam- und Personal Firewall-Lösungen um das Produktfeld der Antitrackware-Lösungen.

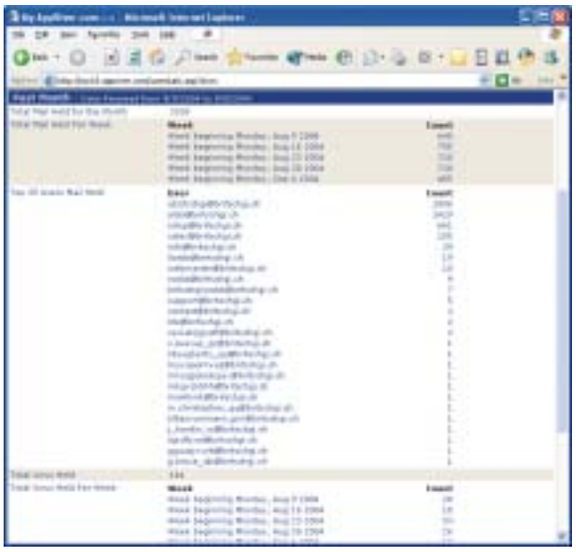
MICROSOFT: EINE MRD. DOLLAR GEGEN HACKER

Die steigende Anzahl an Angriffen von Hackern und Viren hat Microsoft veranlasst, eine Mrd. Dollar in das Upgrade von Windows-Computer zu investieren. 300 Mio. Dollar investiert Microsoft allein in die weltweite Update-Kampagne, die CDs mit Service Pack 2 (SP2) auf Nachfrage frei zur Verfügung stellt. Das Unternehmen behauptet, dass Windows durch die Verbesserungen im Internet Explorer und Outlook Express sicherer ist als je zuvor.

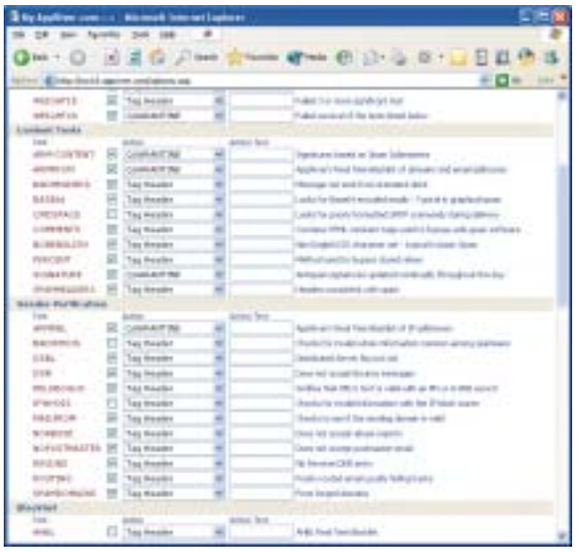
START-UPS FINDEN KEINE MANAGER

Investoren entdecken die Hightech-Branche wieder. Diese sieht sich aber einem unerwarteten Problem gegenüber: US-Start-ups aus dem Technologie-Umfeld finden keine Manager, wie das Wall Street Journal berichtet. Damit büsst die Branche für die negativen Erfahrungen, die viele Spitzenleute beim Platzen des Dotcom-Hypes gemacht haben. Andererseits haben viele der damaligen Manager derart gut verdient, dass sie jetzt viel lieber das süsse Nichtstun geniessen.

(ICT/Agenturen)



Die übersichtliche Weboberfläche zeigt die erreichte Effizienzsteigerung dank der Antispamlösung: Hunderte von Spam-Mails und Viren entlasten die Mailbox.



Die ausgeklügelte Kombination verschiedener Antispam-Kriterien filtert Spam-E-Mails sowie Viren und verhindert «False-Positives».

ren und Würmer, die trotz ausgeklügelter Firewall-Lösung mit Intrusion Detection in Firmennetzwerke eindringen und sich rasch ausbreiten.

Im Trend liegt die Benutzung verseuchter E-Mail-Server für den Massenversand, wo Virenautoren durch trojanische Pferde befallene Rechner Spammern gegen Bezahlung zur Verfügung stellen. So können Spammer – von den eigentlichen Computer-Besitzern unbemerkt – von deren Systemen ihre Werbeflut versenden, um damit Antispam-Tools zu umgehen.
Ein aktuelles Beispiel hierfür ist der Virus «Randex». Dessen Autoren nutzen den Virus um auf Tausenden von Rechnern ein so genanntes trojanisches Pferd zu installieren und damit weit reichende Kontrolle über die befallenen Systeme zu erlangen. Über IRC, ein Internet-Chat-Programm, steuern die Virenautoren die Schadsoftware auf den fremden Rechnern, suchen nach CD-Keys von PC-Spielen oder laden weitere Software auf die infizierten PCs, um die befallenen Systeme für den Spam-Versand zu missbrauchen.

LESER FRAGEN – ICT KOMMUNIKATION ANTWORTET

«Was ist in Zukunft nebst Firewall (Software, Hardware) geplant, um die Spamflut in den Griff zu bekommen?» *(M. L. aus L.)*

Es gibt drei Hauptansätze zur erfolgreichen Bekämpfung der Spam-Flut:

- **Antispam-Filter:** Die erste haben Sie bereits genannt, nämlich kombinierte Hardware- und Softwarelösungen. Diese technischen Ansätze haben wenig mit der klassischen Firewall gemeinsam, die typischerweise am Firmenstandort steht. Antispam-Technologien filtern unerwünschte E-Mails nach einer Vielzahl von Kriterien heraus, damit diese erst gar nicht zum firmeneigenen Mailserver oder Internet-Anschluss gelangen. Diese Technologien sind in der Zwischenzeit sehr ausgereift und erreichen Erfolgsquoten bis zu 99 Prozent.

- **Gesetzliche Massnahmen:** Das Bundesamt für Kommunikation (Bakom) plant Massnahmen zur Stärkung des Konsumentenschutzes. Das Verbot von unverlangten Massenwerbesendungen per E-Mail oder SMS ist gemäss Bakom Informationsblatt Nummer 4 vom 1. Juni 2004 in der Revision des Bundesgesetzes über den unlauteren Wettbewerb vorgesehen. Bei der Verletzung bestehender Gesetze sind bereits heute rechtliche Schritte möglich, beispielsweise wenn ein «Spammer» trotz Aufforderung weitere E-Mail-Zustellungen nicht unterlässt. Der eidgenössische Datenschutzbeauftragte gibt Empfehlungen ab: www.edsb.ch

- **Verhalten des Anwenders:** E-Mail-Benutzer können mit einer Reihe von Massnahmen der Spam-Flut entgegenwirken: Auf Spam-Mails nicht antworten, weil dann eine E-Mail-Adresse erst recht dem gezielten Versand dient; Verzicht auf Ketten-E-Mails; Virenwarnungen (Hoax statt Virenwarnungen) nicht weiterleiten; E-Mail-Adressen nicht offensichtlich im Internet publizieren, statt dessen in anderer Schreibweise wie vorname-at-domain.ch statt vorname@domain.ch veröffentlichen.

PROGRAMME FÜR DIE ENTFERNUNG VON SPYWARE:

Adware Spyware: www.noadware.net (Englisch)
Ad-Aware: www.snapfiles.com (Englisch)
Spybot Search & Destroy: www.spybot.info/de (Deutsch)
Spyware Removal: www.spybot-spyware-removal.com (Englisch)

Spyware macht die Sache noch schlimmer

Immer öfter wird Spyware eingesetzt, um Produkte scheinbar kostenlos anzubieten, wie dies in Spam-Mails oft der Fall ist. Als Spyware wird Software bezeichnet, die persönliche Daten des Benutzers ohne dessen Wissen oder gar Zustimmung an den Hersteller der Software oder an Dritte sendet. Der Benutzer klickt auf einen harmlosen Internet-Link und schon ist ein Cookie auf der Festplatte gespeichert.
Meist dienen die Spyware-Programme dazu, das Surf-Verhalten im Internet zu analysieren, um gezielt Werbebanner oder Pop-ups einzublenden, die den Interessen des Benutzers angepasst sind. Firmen erhoffen sich daraus eine Steigerung der Wirksamkeit ihrer Werbemethoden.
Spyware ist längst keine Randerscheinung mehr. Der US-Provider Earthlinks hat in Zusammenarbeit mit einer spezialisierten Software-Firma

während dreier Monate über eine Million Computer nach Spyware gescannt. Das Resultat ist erschreckend: Laut dem Report sind auf jedem PC durchschnittlich 28 Spyware-Programme gespeichert.
Kann man die harmloseren Varianten der Spyware-Familie noch als ärgerliche und penetrante Formen des Internet-Marketings abtun, müssen bei deren gefährlicheren Vertretern die Alarmglocken läuten: So genannte System-Monitoring-Programme werden mit betrügerischer Absicht auf PCs installiert. Diese Wanzen können Tasteneingaben, Chats und E-Mails aufzeichnen – private und geschäftliche Daten sind damit in Gefahr.

Spam-Bekämpfung ist äusserst komplex

Die Spam-Bekämpfung ist eine komplexe Angelegenheit. Als oberstes Gebot ist zu vermeiden, dass legitime Nachrichten versehentlich herausgefiltert werden (False-Positives). Andererseits sollen möglichst keine unerwünschten E-Mails zu den Benutzern gelangen – abonnierte und willkommene E-Mail-Newsletter hingegen schon.
Natürlich muss die Spam-Bekämpfung in Echtzeit erfolgen, denn Benutzer dulden keine Verzögerung in der E-Mail-Zustellung. Im geschäftlichen Umfeld haben sich die angebotenen Desktop-Programme als ungeeignet erwiesen. Die Installation ist aufwändig; die Programme belasten den Computer zusätzlich und verursachen Abstürze. Auch lässt die Erfolgsrate schon nach kurzer Zeit zu wünschen übrig.
Aus technischer Sicht muss die Spam-Bekämpfung folglich beim E-Mail-Server ansetzen. Wenn Spam gar nicht bis zum E-Mail-Server gelangt, lassen sich viele Vorteile erreichen: Die Internet-Zugangsleitung wird nicht mit Spam blockiert, die Mailserver-Infrastruktur benötigt keine zusätzliche Ressourcen und der Zugriff auf die Mailbox ist unabhängig vom Standort möglich, also auch mittels eines Webbrowser-Zugriffs. In der Praxis bedeutet dies, dem E-Mail-Server eine effektive Antispam-Filterung voranzustellen. Ähnlich wie bei Antivirenprogrammen muss eine erfolgreiche Antispamlösung permanent über die aktuellsten Antispam-Technologien verfügen, ansonsten ist die Bekämpfung unbefriedigend (siehe Kasten).
Für Unternehmungen gestaltet sich der Betrieb einer eigenen Antispamlösung oft als unwirtschaftlich. Immer mehr spezialisierte Firmen und Internetprovider bieten daher gegen eine Monatsgebühr externe Management-Lösungen an. Sämtliche E-Mails durchlaufen in Echtzeit eine zentralisierte Antispam- und Antivirenkontrolle, bevor die elektronische Post den firmeneigenen Mailserver erreicht. Der Endbenutzer verfügt mittels einer Weboberfläche jederzeit über die volle Kontrolle und kann sämtliche zurückbehaltenen E-Mails einsehen. Antispam-Lösungen kosten Geld. Fehlende Antispam-Massnahmen verursachen aber direkt und indirekt höhere Kosten. Mit den erreichten Vorteilen und Sicherheitsvorzügen lassen sich laufende Ausgaben für sinnvolle Abwehrmassnahmen problemlos rechtfertigen. ◆

ANTISPAM-TECHNOLOGIEN

Moderne Antispam-Lösungen kombinieren eine Vielzahl von Technologien und erreichen eine Erfolgsquote von 97 bis 99 Prozent. Das hört sich nach viel an, bei gegenwärtig knapp hundert täglichen Spam-Mails pro Empfänger macht dies pro Jahr immer noch über 1000 unerwünschter und gefährlicher E-Mails. So arbeiten moderne Antispam-Lösungen:

- **Heuristische Analyse:**
  Regelbasierende Scanmethode, die bestimmte Merkmale einer E-Mail erkennt. Merkmale wie «Remove-link» und bestimmte Wörter wie «Viagra» deuten auf Spam hin und werden «Schlechtpunkten» zugeordnet. Nach der Analyse werden die Punkte addiert; ab einem definiertem Grenzwert gilt eine E-Mail als klassifizierter Spam.
- **Analyse von manipuliertem Text:** Spams ersetzen Zeichen in den bekannten Wörtern, z. B. 0ffer statt Offer (eine Null statt des Grossbuchstabens O). Diese Methoden werden mittels Analyse erkannt, was aber eine ständige manuelle Aktualisierung verlangt.
- **Lexikalische Textanalyse:**
  Untersuchung nach ganzen Textstellen und Verknüpfung mittels Operatoren OR, AND, NOT etc.; beispielsweise Verkaufsangebote und die Aufforderung zum Besuch von Websites.
- **Bayer'sche Textanalyse:**
  Vergleich mit Statistiken, die aufgrund der Spam-Analyse entstanden sind. Die Qualität hängt stark von der Datenbankgrösse und Erfahrung des jeweiligen Antispam-Anbieters ab.
- **Anti-Spoofing:**
  Erkennung von Spammern, die E-Mails offiziell von externen Domains aber zur Tarnung mit internen Absender-Adressen versenden.
- **Header-Analyse:**
  Überprüfung der E-Mail-Header, um Abweichungen von festgelegten E-Mail-Standards zu ermitteln.
- **Analyse der Betreffzeile (Subject):** Viele Spam-Mails verfügen über einschlägig bekannte Betreffzeilen oder neu versandte Spam-Mails können gezielt gefiltert werden.
- **Unterbindung von «Directory Harvesting Attacken»:**
  Spammer versuchen direkt über den SMTP-Server an gültige E-Mail-Adresse zu kommen – dies wird unterbunden.
- **Real-Time Black-Lists (RBL):**
  Listen im Internet, die IP-Adressen von Mail-Server enthalten, von denen Spam versandt wurde. Mit RBL akzeptiert der Firmenserver keine E-Mails von solchen einschlägig bekannten IP-Adressen. Es kommt aber vor, dass Mail-Server irrtümlich auf dieser Liste enthalten sind, wenn Firmenserver ungewollt zum Spam-Versand missbraucht wurden.
- **Schutz vor Mail-Bombing:**
  Massive Zustellung von automatisch generierten E-Mails auf einen Mailserver (DoS, Denial of Service); dieser Schutz reguliert den E-Mail-Fluss, um eine Überlastung zu verhindern.
- **Antispam-Datenbank:**
  Vergleich von E-Mails mit einer Antispam-Datenbank.
- **Internal Black Lists und White Lists:**
  Liste mit Domain-Namen und Adressen, die eindeutig gesperrt sind. White Lists sind das Gegenstück, also klare Spezifizierungen von erwünschten E-Mails.
- **Anti-Relay-Funktion:**
  Schutz des Mailservers, damit dieser nicht als Spam-Versender missbraucht werden kann. Damit wird eine Auflistung in den Real-Time Black-Lists verhindert.