

Optimierte Sicherheit und reduzierte Kosten



Von Andreas Reinhard

Der Autor ist CEO der IT-Dienstleisterin Apexis AG.

38

Das Spam-Problem ist allgegenwärtig. Laut Internet Filter Review werden täglich allein 2,5 Milliarden Porno-Spam-Mails verschickt. Und das ist mit rund 30 Prozent nur ein kleines Stück des «Spam-Kuchens». Spam- und Virenproblematik rücken dabei immer näher zusammen.

zwar nicht sofort ersichtlich – sie machen sich jedoch im Nachhinein umso deutlicher bemerkbar.

Spam verschiebt die Kosten für Werbung vom Anbieter zum Empfänger der Nachricht. Im Gegensatz zu Junk-Mail, die zu Hause den Briefkasten überschwemmt, ist der Versand von Millionen E-Mails zu einem vernachlässigbaren Betrag zu bewerkstelligen. Der Empfänger jedoch bezahlt die Rechnung – in Form von Bandbreite, Zeit (sprich Geld) und Nerven.

Zentralisierte E-Mail-Filter als Lösung des Spam- und Virenproblems

In jüngerer Zeit gehen Spammer immer öfter dazu über, Einrichtungen unbeteiligter Dritter zu nutzen, um Spam-Mails über deren Mailserver zu versenden. Oft verwenden sie dazu fingierte E-Mail-Absender. Die Folge dieser unliebsamen Praxis: Fehlermeldungen und Reklamationen der Empfänger landen beim Inhaber dieser Adresse – wodurch dieser ohne eigenes Verschulden zum Opfer dieser Machenschaften wird. Diesen Prozess hat etwa die globale Sobig.f-Attacke jüngst in aller Deutlichkeit aufgezeigt. Gegenmassnahmen sind bislang ebenso umständlich wie ineffizient. Weil Spammer ihre Internetverbindung – und damit ihre elektronische Identität – häufig wechseln, sind Filter, die auf Absenderadressen basieren, meist nur kurzfristig wirksam. Werden ganze, von Spammern häufig eingesetzte Absender-Domains gesperrt, hat dies oftmals die unerwünschte Nebenwirkung, dass auch legitime E-Mail-Absender gesperrt werden. Eine Reihe amerikanischer Firmen behelfen sich inzwischen damit, Mail-Absender wie yahoo.com oder email.com ganz zu blockieren,



Das Kommunikationsmittel E-Mail ist in der privaten und geschäftlichen Korrespondenz längst zum Standard avanciert. Laut einer Untersuchung der US-Softwareherstellerin Oracle nimmt E-Mail für die Beschäftigten in den USA mittlerweile einen höheren Stellenwert ein als das Telefon. 56 Prozent der Befragten gaben an, ohne E-Mail nicht mehr arbeiten zu können – 44 Prozent waren sogar der Mei-

nung, E-Mail doppelt soviel zu nutzen wie das Telefon.

Leider gehören aber auch die Schattenseiten der «neuen» Kommunikation zur täglichen Arbeit. Dazu gehört in erster Linie die unerwünschte E-Mail-Werbung, kurz Junk-Mail oder Spam. Durch diese so genannte «unsolicited commercial email» entstehen den betroffenen Unternehmen hohe Kosten. In vielen Fällen sind diese Ausgaben

weil diese von Spammern immer wieder missbraucht werden.

Dadurch sehen sich unzählige Konsumenten, die derartige Adressen verwenden, nicht mehr in der Lage, mit den betreffenden Unternehmen in Kontakt zu treten. Viel Ärger und inakzeptable Ertragsausfälle sind die Folge. Ebenfalls keine praktikable Lösung stellt die rein inhaltliche Filterung der elektronischen Post dar. Diese Methode stellt die Anwender nämlich vor das Problem zu entscheiden, was als unerwünschten Inhalt angesehen werden soll und was nicht. Kriterien wie etwa das Wort «Sex» erweisen sich nämlich als entschieden zu simpel, möchte doch niemand E-Mails betreffend der «jüngsten Aufführung des KammerSEXtetts» oder der «Entwicklung im Bereich SEXualtherapie» im Papierkorb suchen müssen.

So wächst die Spam-Flut weiter, der administrative Zeitaufwand sorgt für rote Köpfe und die teuren, dabei aber häufig nutzlosen Schutzmassnahmen hinterlassen grosse Löcher in den Portemonnaies der Betroffenen. Sogar auf der politischen Ebene liefert Spam bereits Zündstoff: erst vor kurzem wurde in Kalifornien ein Anti-Spam-Gesetz verabschiedet, das jedoch ausser einiger Medienpräsenz noch keine konkreten Ergebnisse zeigte.

Viele schützen sich gar nicht

Effiziente Spam-Filterung auf lokaler Ebene ist ein zeitraubendes Unterfangen und mit hohen Kosten verbunden. So sind etwa Softwarelösungen oft nur mit hohem Aufwand zu installieren und binden zudem personelle Kapazitäten. Auch bietet Software nur selten aktualisierten Schutz. Sollte dies dennoch der Fall sein, stehen teure und aufwändige Updates und Lizenzerneuerungen ins Haus. Besseren Schutz bietet ein umfassender E-Mail-Filter-Service. Es kann zweifellos nicht Aufgabe des IT-Supports sein, an individuellen Filtermassnahmen zu basteln. Moderne Spam-Filterung hat zentralisiert zu erfolgen. Und: Die Spam-Filter müssen rund um die Uhr aktualisiert sein. Kleine und mittlere Unternehmen (KMU) ohne hochdotierte IT-Abteilung und Privatnutzer können aus zeitlichen und finanziellen Gründen keinen derartigen Schutz aufrechterhalten. Hier tritt ein vorgelagerter Service einer externen Einheit auf den Plan: Spam-Filter-Outsourcing.

Die Schweiz stellt im Segment der Spam-Bekämpfung und der Schutzmassnahmen einen noch wenig entwickelten Markt dar. In vielen Fällen werden Softwareprodukte aus dem Ausland ungefragt übernommen. Oftmals vertrauen Privater und KMU auf den rudimentären Spam-Schutz der Mail-Provider oder schützen sich gar

nicht. Wer sich jedoch Zeit nimmt und die Rechnung zu Ende kalkuliert, sieht dringenden Handlungsbedarf: Zentrale E-Mail-Filterung hat ganz direkt Produktivitätssteigerungen in den angeschlossenen Unternehmen zur Folge. Die Kostenersparnisse sind, sofern einmal zu Papier gebracht, ebenfalls bemerkenswert. Zusätzlich zu den Zeit- und Kosteneinsparungen darf eine weitere, wichtige Komponente nicht vergessen werden: die Sicherheit.

Spam- und Virenproblematik rücken näher zusammen

Der Technologietransfer zwischen Virenprogrammierern und Spammern funktioniert – im Gegensatz zu dem vieler Filtersoftwarehersteller – tadellos und weist in eine klare Richtung. In Zukunft ist mit Spam-Methoden à la Sobig.f immer häufiger zu rechnen. Die Zukunftsvisionen von zentralisierten und kombinierten Schutzsystemen sollten eigentlich längst überall Realität sein. Wer sich vor Spam schützen will, will auch gegen Viren geschützt sein – und umgekehrt. Zentrale E-Mail-Filterssysteme sollten daher Spam und Viren gleich in einem einzigen Schritt filtern und somit die bisher lokal installierten Virenfilter ersetzen. Die globale Sobig.f-Virenattacke im September 2003 führte, vergleichbar einer massiven Spam-Flut, mancherorts zu überlasteten Leitungen, lahmgelegtem E-Mail-Verkehr und massiven Kosten.

Mit den heutigen Mitteln kann jeder und jede zum Absender von Spam-Mail werden. Aggressive Computerviren dienen den Spammern als Aufklärer und Türöffner. «Unsubscribe»-Links entpuppen sich als Verbindung zu Virenquellen oder bestätigen den Spam-Empfang und sorgen so für noch viel mehr unerwünschter Werbung. Zudem löschen unprofessionell und schlecht konfigurierte Spam-Blocker oft wesentlich wichtige Geschäftskorrespondenz (sogenannte «false positives»). Dabei schieben sich Wirtschaft und Politik gegenseitig die Verantwortung für diese Entwicklung in die Schuhe und der Gesetzgeber tut sich schwer mit der Problematik.

Nur professionelle Filter-Anbieter verfügen über die notwendigen zeitlichen und technischen Ressourcen, um einen gut funktionierenden Schutz gewährleisten zu können. Die E-Mail-Filterung sollte daher vermehrt zentral vorgenommen werden. Während lokale Software-Lösungen ständig aktualisiert werden müssen, um den aktuellsten Bedrohungen angepasst zu sein, spart die Mail-Filterung im Outsourcing Zeit, Lizenzkosten und Speicherkapazität. Diese Rechnung geht auf – nur wird sie in der Schweiz noch zu selten gemacht. ♦

ZUWACHS BEI SICHERHEITS-ANWENDUNGEN

Der weltweite Markt für Sicherheits-Anwendungen im IT-Bereich ist im dritten Quartal 2003 gegenüber dem vergleichbaren Vorjahreszeitraum um 22 Prozent angewachsen. Das ergab eine Studie des Marktforschungs-Instituts IDC. Das Segment der Anwendungen zum Aufspüren von Hackerangriffen, Intrusion Detection, hat ein überdurchschnittliches Wachstum von 89 Prozent zu verzeichnen.

MICROSOFT GEGEN HOTMAIL-SPAMMER

Microsoft hat sich in seinem Kampf gegen Spammer mit dem New Yorker Generalstaatsanwalt Eliot Spitzer verbündet. Der Software-Konzern will gegen drei Unternehmen klagen, die unberechtigter Weise Microsoft-Computer benutzt hätten, indem sie Massenmails an Hotmail-Kunden verschickt haben.

NEUE VARIANTE VON SOBER.B ENTDECKT

Der Sicherheitsexperte H+Bedv warnt vor einer neuen Variante des Wurms Sober.B. Laut H+Bedv entpackt sich der Wurm nach dem Öffnen des Attachments mit der Fehlermeldung «Header is missing». Danach erstellt er eine Datei mit den E-Mail-Adressen, die auf den lokalen Laufwerken gespeichert sind und versendet sich mit Hilfe seiner SMTP-Engine weiter.

TRÜGERISCHE SICHERHEIT BEI VIRENSCHUTZ

Der im Rahmen von web-basierten Service-Plattformen häufig kostenfrei «mitgelieferte» Virenschutz suggeriert nach Ansicht des IT-Security-Anbieters H+Bedv dem Anwender mitunter eine trügerische Sicherheit. Insbesondere Open-Source-Virens Scanner können jedoch einem Vergleich mit Schutzprogrammen professioneller Hersteller nicht Stand halten und sollten daher noch nicht in Produktumgebungen eingesetzt werden. (pte/ICT)