

So kann man Spam-Mails eindämmen

Private Internetanwender sind gleichermaßen von Spam e-mails betroffen wie Unternehmer. Einige Sicherheitstipps können helfen, sich ziemlich wirkungsvoll von SPAM zu schützen.

Bis zu 90 Prozent aller weltweit versandten E-Mails rühren von so genannten Spammern her. Sie machen mit den Massenmails gutes Geld. Betroffene Unternehmen haben unnötige Investitionen zur Abwehr der e-Mail-Flut; Privatanwender vergeuden unnütz Zeit mit Löschaktionen.

Zu den größten Herausforderungen im Bereich IT-Sicherheit in der Wirtschaft gehört die Abwehr von Spam-e-Mails, also von unerwünscht zugeschickten Massenmails.

Bis zu 90 Prozent aller weltweit versandten Mails sind so genannte Spam oder Junk Mails. 2007 waren es im Schnitt 75 Prozent aller Mails; zu besonderen Anlässen, etwa um die Weihnachtszeit, verstärkten die professionellen Spammer ihre Aktivitäten auf 83 Prozent, beschreibt der aktuelle Spam-Report des IT-Security-Spezialisten Symantec die Situation.

30 Prozent unerwünschte Werbung

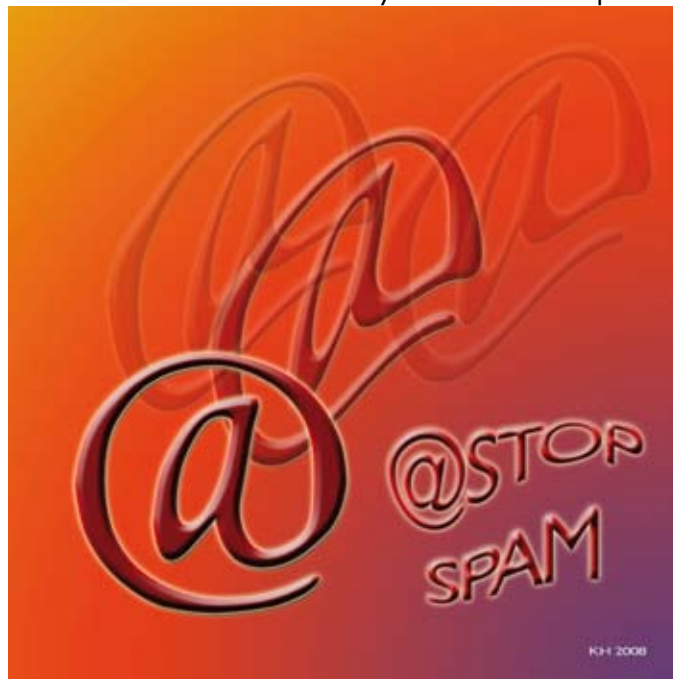
Bei den meisten Massenmails handelt es sich nach Angaben des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) um Werbemails für dubiose Produkte - von Diätmitteln bis hin zu Potenzpillen.

Der jährliche Gesamtschaden durch Spams betrug in den USA schon im Jahr 2005 geschätzte zehn Milliarden USD, in Europa wird von mindestens drei Milliarden EUR Schaden gesprochen. Spam-Mails kosten nicht nur Arbeitszeit (löschen), sondern können den Mailverkehr

von Unternehmen erheblich stören bzw. sogar lahm legen. Dies dann, wenn die Firmen-Mailserver regelrechten Spam-Attacken ausgesetzt sind.

Hohe Abwehrkosten

Laut BSI (www.bsi.de) entstehen einem Einzel- oder Kleinunternehmen - nach Einführung von Anti-Spam-Schutzmaßnahmen - noch immer jährliche Kosten von bestenfalls 325 €, einem mittelständischen Unternehmen bis zu 60.000 € und Grosunternehmen Gesamtkosten von rund 320.000 € - Tendenz steigend. Heruntergerechnet kostet einem Kleinunterneh-



men jede Spam-Mail trotz Schutzprogramm vier Cent, ohne entsprechende Maßnahmen sogar 66 Cent.

Die Jagd beginnt am Gateway

Um eine möglichst hohe Effizienz zu erzielen, muss man Spam schon an den Mail-Gateways, die die Mails annehmen, abfangen, zwischenspeichern und dann an den Mailserver weiterschicken. Der nächste

Spam-Checkerfolgt dann durch den Mailserver. Hier wird auch ein Viren-Check durchgeführt. Beliebt und bewährt ist der kostenlose „Spam Assassin“ ein Programm mit sehr hohem Wirkungsgrad, das zum Einsatz kommt, wenn die Gateways auf einer Linux-Lösung basieren. Bei kommerziellen Lösungen wird dieses Filterprogramm in der Regel dahinter angehängt. Außerdem werden die e-Mails mit Spam-Adressen-Blacklists abgeglichen – schwarze Listen also, in denen Spammer erfasst werden. Notgedrungen musste ein Grossteil der privaten Netze aus China gesperrt werden. Über sie operieren Spammer mit Vorliebe. Laut Symantec haben es Spammer

aus China immer öfter auf freie Web-Blogs abgesehen, in die sie ihre zweifelhaften Produktwerbungen kostenfrei und massenhaft ablagern.

Anti-Spam-Software

Neben Spam Assassin (spamassassin.apache.org) gibt es noch eine Reihe anderer Anti-Spam-Software, aber auch E-Mail-Programme verfügen über Mail-Filter für den Einsatz am heimischen PC. Das

e-Mail Programm „Thunderbird von Mozilla“ hat eine sehr gut funktionierende Spam-Engine eingebaut. MS Outlook bietet die Möglichkeit Junk-Mail Absender listenmäßig zu erfassen und dann zu blocken. Das ist allerdings eine Sisyphos Arbeit, denn Spammer ändern ihre Adressen permanent. Mutmaßliche Spam-Mails werden u.a. von solchen Filtern aufgefangen und in einen eigenen Ordner (Junk) transferiert, wo sie vor dem Löschen noch einmal durchgeschaut werden können.

Sorgsamer Umgang

Die wichtigste Maßnahme gegen Spam ist ein sorgsamer Umgang mit der eigenen E-Mail-Adresse. Das heißt: Die eigene E-Mail-Adresse sollte möglichst gar nicht bzw. nicht wahllos im Internet veröffentlicht werden, damit sie nicht von Spammern mittels „Robotern“, so genannten Harvestern, ausgelesen werden kann. So können Mailadressen auch auf der eigenen Homepage so verschleiert werden, dass sie im Html-Quelltext nicht ohne weiteres als solche zu erkennen sind, aber für die Nutzer der Website transparent bleiben. Auch sollte die Zahl öffentlicher Firmen-Mail-Adressen beschränkt sein. Oft genügt eine Adresse wie `info@firma.at` oder `office@firma.at`, damit Homepage-Besucher Kontakt aufnehmen können. Wichtig ist zudem: niemals auf eine Spam-Mail antworten, da gültige E-Mail-Adressen für Spammer Gold wert sind.

Und wer sind diese ungeliebten Spammer?

Untersuchungen haben gezeigt, dass es weltweit etwa 500 Mailserver gibt, von denen aus unerwünschte e-Mails, sog. SPAM, versendet werden. Eine unbekannte Anzahl von klei-



Verschiedene e-Mail Programme, wie etwa MS Outlook (TM) oder Mozilla Thunderbird haben Vorkehrungen eingebaut und sammeln Spam in eigenen Ordnern.

neren Spammern fällt daneben praktisch nicht mehr ins Gewicht. Doch auch als Privater kann man zum Spammer werden, wenn man seinen PC nicht ausreichend vor bösar-

tigen Angriffen schützt. Solche Angreifer, meist Trojaner, lesen das persönliche Adressbuch aus und verschicken im Namen des privaten Anwenders unerwünschte e-Mails. Das ist

nicht nur lästig, sondern auch strafbar. In Österreich ist für den Versand von kommerziellen e-Mails die ausdrückliche Zustimmung des Empfängers nötig (Geldstrafe bis zu 36.000 EUR). Doch in den Herkunftsländern wirkt diese Drohung leider nicht.

Richtig schlimm wird es aber, wenn man als missbrauchter Spammer auf eine „Blacklist“ gerät und mit seiner eigenen e-Mail Adresse keine Post mehr versenden kann, weil man weltweit gesperrt ist.

Was tun?

Als Homepagebetreiber setzt man seine e-Mail Adresse nicht leichtfertig auf die Site, sondern verschlüsselt sie, damit sie für Webroboter, sog. Spider, unlesbar wird.

<http://www.skoom.de/service/email-verschlueseln.xtc>

<http://www.dw-formmailer.de/?action=mailcoded>

Wer seine e-Mail Adresse bei Gewinnspielen, Firmenkontakten oder in Foren leichtfertig bekannt gibt, braucht sich nicht wundern, wenn er schon bald mit SPAM zugeschüttet wird.

Und eines sollte man zu guter Letzt auch noch bedenken: aufgrund der vielen Spam-Filter ist keineswegs gewährleistet, dass seriöse e-Mails ihren Empfänger erreichen. Dagegen ist leider noch kein Kraut gewachsen.

Klaus HERBERT