Spam-E-Mails und von Viren und ähnlichen Schadprogrammen erzeugte E-Mails

Neues von der Netiquette von Dr. Bernd Bäse, Braunschweig

Massenhaft und unerbeten versandte Werbe-E-Mails, im Fachjargon als "Spam"[2] bezeichnet, entwickelten sich in den letzten Jahren von einer lästigen Randerscheinung zu einem echten Ärgernis. **Spam-E-Mails** werden im günstigsten Falle für das Direktmarketing genutzt. Sie erhalten beispielsweise seriöse oder unseriöse Informationen zu Hypothekenangeboten, Gesundheitsthemen oder Möglichkeiten, akademische Grade käuflich zu erwerben. Typisch sind aber eher die Spam-E-Mails, die - im technischen Sinne ebenfalls Direktmarketing - für Viagra, Pornoseiten (oft mit einem Link auf einen z. T. extrem kostenintensiven 0190-Dialer), Vergrößerungen sehr ausgewählter Körperteile usw. werben.

Noch neuer als Spam-E-Mails sind automatisch **von Viren und ähnlichen Schadprogrammen erzeugte E-Mails.** Der Virus gelangt auf den eigenen Rechner, sobald eine E-Mail empfangen, geöffnet und auch der enthaltene Anhang (ein Programm mit Erweiterungen wie *.exe, *.com, *.bat, *.pif, *.scr usw.) aktiviert wird. Erst das Öffnen dieses Anhangs erweckt den Virus zum „Leben“. Ein E-Mail-bezogener Virus analysiert dann das E-Mail-Adressbuch und versendet sich an beliebige Adressaten weiter, unter Umständen unter Verwendung eines falschen Absenders, der ebenfalls dem Adressbuch entnommen wird. Dabei wird ein möglichst interessant und/oder harmlos klingender, meist englischsprachiger Betreff gewählt.

Gegen Spam- und Viren-E-Mails kann man sich nur recht schwer schützen. Allgemein gilt der Grundsatz, bei der Bekanntgabe der eigenen E-Mail-Adresse restriktiv vorzugehen. Sofern man sich bei bestimmten Softwareherstellern oder Online-Angeboten unter der Angabe einer E-Mail-Adresse anmelden muss, ohne dass man je wieder von dem Anbieter hören möchte, so können kostenlose "Wegwerf-E-Mail-Adressen" genutzt werden, die sich nach einer gewissen Anzahl eingegangener E-Mails selbst löschen. Eine solche Taktik vermindert die Wahrscheinlichkeit, Spam-E-Mails zu erhalten, schließt sie aber bei weitem nicht aus, da die E-Mail-Adressen zum Teil nach Zufallsprinzipien erzeugt werden oder anderweitig an alle Kunden eines E-Mail-Anbieters geleitet werden.

Es ist grundsätzlich möglich, E-Mail-Filter zu aktivieren oder zusätzlich zu installieren, die anhand von Absendern oder Schlüsselwörtern im Betreff unerbetene E-Mails von Ihrem Rechner fernhalten. Solche Filter können Sie selbst installieren, oder sie können von Anbietern von E-Mail-Diensten betrieben werden. Jede Computerzeitschrift behandelt ein- bis zweimal im Jahr dieses Thema, z. B. die Zeitschrift PC-Magazin (Heft 10/2003, S. 24 - 27). Es soll deshalb an dieser Stelle nicht näher auf die verschiedenen technisch-organisatorischen Möglichkeiten eingegangen werden - das würde den Rahmen dieses Artikels sprengen und über den Themenbereich dieser Zeitschrift hinausgehen.

Prinzipiell könnte man also

- nur E-Mails von vertrauten Absendern zum Empfang zulassen,
- nur E-Mails von Absendern annehmen, die nicht auf im Internet allgemein zugänglichen schwarzen Listen mit Spam-Versendern (kurz Spammer genannt) verzeichnet sind oder
- nur solche E-Mails annehmen, die nicht Schlüsselwörter wie "Sex" im Betreff aufweisen.

Wer mit dem Gedanken spielt, nur E-Mails von ausgewählten und bekannten Absendern zu empfangen, sei gewarnt: E-Mail-Adressen von Bekannten und Freunden können sich ändern. Sie würden nie von der neuen E-Mail-Adresse erfahren; denn der neue Absender würde ja herausgefiltert werden. Diese Option einer Positivliste - neudeutsch im Gegensatz zur

schwarzen Liste (black list) als „white list“ bezeichnet - ist also in aller Regel zu verwerfen.

Die schwarzen Listen mit den Internet-Adressen von Spam-Versendern helfen erst dann weiter, wenn ein Spammer bereits einmal in Erscheinung getreten ist. Problematisch wird es, wenn einmal ein seriöser Absender versehentlich in eine dieser Listen aufgenommen wird - die eigentlich gut gemeinten Listen, die von Filterprogrammen automatisch ausgewertet werden, können gelegentlich ein gewisses Unheil anrichten. Gelegentlich wird angeboten, schwarze Listen und Positivlisten miteinander zu kombinieren: Absender, von denen man auf jeden Fall E-Mails erhalten möchte, können also in der Positivliste vorsichtshalber von dem Bann ausgenommen werden, der sich aus den schwarzen Listen ergeben könnte. - Sie ahnen wahrscheinlich, dass dieses Verfahren technisch ziemlich aufwändig und wohl nur für große Institutionen geeignet ist.

Auch die Schlüsselworttechnik ist problematisch. So berichtete die BBC im Februar 2003 (Quelle: s. o.), dass Abgeordnete wegen eines solchen Filters E-Mails zu einem geplanten Gesetz gegen *sex*uelle Belästigung nicht erhalten hätten. Eine E-Mail wegen eines Rezension*sex*emplars hätte wohl ebenfalls keine Chance. Auch das Schlüsselwort "Brust""breast" hat schon dazu geführt, dass Internetseiten und E-Mails zum Thema "Brustkrebs" geblockt wurden. Wenn Sie das Wort "Porno" ausschließen, werden Sie mit Gewissheit früher oder später eine E-Mail mit dem Betreff "P0rn0" (mit Nullen anstatt des Buchstaben "o") erhalten. Außerdem ist die Phantasie der Spam-E-Mail-Versender unerschöpflich. Dies musste auch der Autor dieser Zeilen feststellen, als er die E-Mail mit dem Betreff "nice Grannies" = "schöne Omas" bekam. Über den Inhalt der E-Mail dürfen Sie selbst spekulieren ...

Automatisierte Verfahren zur Abwehr von Spam-E-Mails können also nicht perfekt arbeiten, sie können nur eine Vorauswahl treffen. Vermutliche Spam-E-Mails werden deshalb in vielen Fällen schon nicht mehr gelöscht, sondern nur in ein separates Verzeichnis verschoben, dessen Inhalt von dem E-Mail-Empfänger vor dem Löschen tunlichst geprüft werden sollte. Lassen Sie uns einen Vergleich zur normalen Post anstellen: Die unerbetenen Werbeblättchen und -briefe, das Pendant zu Spam-E-Mails, würden dann von vornherein in der Altpapiertonne landen. Diese müsste aber vor der endgültigen Leerung noch einmal auf den Schreibtisch geschüttet werden, um die Entsorgung von wichtiger, aber fehlgeleiteter Post zu vermeiden. Klingt inakzeptabel, nicht wahr?

Eine Radikalkur gegen Spam-E-Mails besteht darin, sich eine veränderte E-Mail-Adresse zuzulegen und nur diejenigen darüber zu informieren, die davon Kenntnis haben sollen. Gerade bei einer größeren Zahl von Personen, mit denen mehr oder weniger häufig korrespondiert wird, ist das ein nicht ganz unerheblicher Arbeitsaufwand, aber im Privatbereich durchaus zu leisten. Da E-Mail-Adressen über Schadprogramme ausgespäht werden können, ist die Lösung dieses Problems u. U. nur temporärer Art: Sobald Ihre neue E-Mail-Adresse wieder ausgespäht (oder gar verkauft) wurde, erhalten Sie wieder unerbetene E-Mails. Im Bereich von Behörden oder Unternehmen muss dieser Ansatz versagen - hier kommt es sehr auf das langfristig unveränderte Bestehen einer E-Mail-Adresse an.

Am erfolgversprechendsten ist der Ansatz, sich die E-Mails in einem ersten Arbeitsschritt gar nicht auf den eigenen Rechner zu laden, sondern sich nur Absender und Betreff anzeigen zu lassen. Unwillkommene E-Mails werden dann direkt auf dem E-Mail-Server (dem Zentralrechner, auf dem die E-Mails gespeichert werden, bevor Sie sie herunterladen) gelöscht. Das E-Mail-Programm von T-Online z. B. ist von vornherein so ausgelegt, dass die E-Mails auf dem Server kontrolliert werden müssen. Sofern Ihr E-Mail-Programm diese Option nicht bietet, können Sie kleine, kostenlose Zusatzprogramme wie den POP3-Manager nutzen.

Entscheidend ist bei diesem Vorgehen die kaum zu automatisierende Prüfung, ob eine E-Mail mit ihrer Kombination aus Absender, Betreff und Sendezeitpunkt Sinn macht. Das soll an einigen Beispielen verdeutlicht werden: Wenn Sie von Ihren Eltern, die kaum Englisch können,

eine E-Mail mit dem für den Sobig.F-Virus typischen Betreff "See the attached file for details" bekommen, sollten Sie höchst misstrauisch werden und die E-Mail gleich auf dem Server löschen (und möglichst die Eltern warnen). Im weiteren Sinne sind alle gänzlich unerwarteten Betreffinhalte, wie z. B. "Rechnung" oder "Die Polizei warnt", von bekannten E-Mail-Absendern unter dieser Gruppe zu subsumieren. Auch E-Mails von Unbekannten mit kryptischen, weil automatisch erzeugten Betreffinhalten - z. B. "syxcxoidfk" - sollten unbesehen gelöscht werden ("syxcxoidfk" wird von keinem E-Mail-Filter als schädlich erkannt und wird deshalb zum Download auf den Rechner zugelassen).

Seien Sie auch vorsichtig, wenn Sie E-Mails von Unbekannten erhalten, deren Betreff an Ihr Mitgefühl oder an Ihr Sicherheitsempfinden appelliert: Da jede Behörde eine eigene, sicher der Behörde zuzuordnende E-Mail-Adresse hat, sollten Sie eine E-Mail von einer unbekannten Privatperson (z. B. mit der Adresse tom.meier@gmx.de) mit dem Betreff "Die Polizei warnt" gar nicht erst annehmen. Es sollte Sie auch misstrauisch machen, wenn Sie E-Mails z. B. von den Eltern erhalten, die mitten in der Nacht - zur üblichen Zeit der Bettruhe - versandt wurden.

Diese Prüfungen wären übrigens auch vorzunehmen, wenn Ihre E-Mail durch Filterprogramme vorsortiert würde, und zwar in Spam-verdächtig und vermutlich einwandfrei ...

Was ist der langen Rede kurzer Sinn? Versehen Sie **jede E-Mail** mit einem **aussagekräftigen Betreff,** dem der Empfänger mit Sicherheit entnehmen kann, dass es sich um eine ernst gemeinte E-Mail und nicht um eine Virus-Attacke oder um eine Spam-E-Mail handelt. Seien Sie **so spezifisch wie möglich.** Bezogen auf den Internet-Auftritt der Forschungs- und Ausbildungsstätte könnte das z. B. bedeuten, dass einer E-Mail, in der um Informationen zu einer Veranstaltung gebeten wird, der Betreff "Bitte um Info zur Veranstaltung am 17. November 2003" anstatt nur "Info?" mitgegeben wird. Die als wichtigste aller Netiquette-Regeln unter dem oben genannten Link aufgeführte Regel - Hinzufügen eines Betreffs - wird damit noch wichtiger, wenn Ihre E-Mail auch tatsächlich ankommen soll. Kündigen Sie im Extremfall eine E-Mail mit potentiell zweifelhaftem Inhalt telefonisch oder über eine Vorab-E-Mail (die wiederum einen aussagekräftigen Betreff aufweisen sollte) an.

Abschließend sei der Hinweis erlaubt, dass eine seriöse und aussagekräftige E-Mail-Adresse ebenfalls die Wahrscheinlichkeit erhöht, dass eine E-Mail ernst genommen wird. Der Autor erhielt vor kurzem (seriöse) Anfragen von einem Interessenten mit dem E-Mail-Namen "tampongalvanik". Nur der einigermaßen aussagekräftige Betreff hatte diese E-Mails davor bewahrt, ungelesen gelöscht zu werden. Der Eindruck beim ersten Kontakt - das war das Lesen der E-Mail-Adresse des Absenders - war jedenfalls nicht überzeugend!

[1] Nach Duden, Die deutsche Rechtschreibung, 22. Auflage, ist die Netiquette die Gesamtheit der Regeln für soziales Kommunikationsverhalten im Internet.

[2] Spam ist eigentlich der geschützte Markenname für ein Frühstücksfleisch in Dosen und leitet sich wohl aus "spiced ham", gewürzter gekochter Schinken, ab. Da Dosenfleisch keine ausgeprägte Delikatesse ist und entsprechend wenig beliebt ist, wurden ungefragt eingehende Massen-E-Mails ebenso bezeichnet.