Internet / Neue Medien / Trends

Dipl.-Ing. Dr. techn. Stefan Grünwald

Lästiges, teures „Dosenfleisch" – Spam

In den 1930er Jahren wurde der Name Spam für Schweinefleisch in Dosen geboren, eine Abkürzung für Spiced Ham. Heute verbindet man statt dieser Kriegsdelikatesse unerwünschte Werbemails. Mehr als 50 Prozent der E-Mails sind Spam und zusätzlich noch an die sieben Prozent mit Viren verseucht. Wenn Sie jetzt ungläubig den Kopf schütteln, dass bei Ihnen nur selten ungewollte Mails den Posteingang erreichen, dann danken Sie Ihrem Mail-Administrator, der seine Hausaufgaben gewissenhaft erledigt. Ein Eliminieren der Störenfriede ist vor allem über Filterung möglich, wobei es dabei Grenzen gibt. Diese sind dann erreicht, wenn erwünschte und vielleicht wichtige E-Mails nicht ihren Weg zum Empfänger finden. Das kann dann nicht nur lästig sein, sondern sehr unangenehme Auswirkungen haben.

Wie erreichen diese Mails ihre Empfänger? Versender von Spam sammeln entweder selbst E-Mail-Adressen oder kaufen diese zu. Unseriöse Unternehmen sammeln über ihre Webseiten (z.B. E-Shops) Kundendaten, um ihre nicht funktionierenden Geschäftsmodelle zumindest temporär am Leben zu erhalten, und verkaufen diese Daten weiter. Ebenso werden Newsgroups und Chats nach verwertbaren E-Mail-Adressen gescannt und diese gesammelt. Oder die Adressen werden über augenscheinlich seriöse Wege wie „Marketing-CDs" oder ähnliche Angebote beschafft. Ein Schutz stellt ein Eintrag in die so genannte Robinsonliste dar, die eine Weitergabe der persönlichen Daten verhindert. Der sorgsame Umgang mit der eigenen E-Mail-Adresse stellt einen weiteren Schutz dar.

Warum ist Spam zum Massenphänomen geworden? Eine der Ursachen für das Problem ist, dass die Absenderadresse gefälscht werden kann und standardmäßig keine Benutzer-Authentifizierung im Mailprotokoll vorgesehen ist. Diese Maßnahme ist bisher nur optional und viele Provider verzichten darauf und lassen darüber hinaus noch beliebige Angaben als Absenderadresse zu. Daher ist selbst bei geeigneten gesetzlichen Rahmenbedingungen ein Verstoß nur schwer zu verfolgen.

Gefährlich und auch teuer kann es werden, wenn durch Spam Anwender auf nachgebaute Webseiten von Banken gelockt werden und so versucht wird, an sensible Daten heranzukommen (Passwörter, TANs). Dieses unter dem Begriff Pishing (Passwort fischen) bekannte Vorgehen wird durch Sicherheitslücken des Internet-Explorer zusätzlich erleichtert. Unternehmungen kann durch Fälschungen des Absenders Schaden entstehen, wenn dadurch kritische Informationen an vermeintliche Kollegen gelangen.

Maßnahmen gegen Spam können nur gemeinschaftlich durch das Zusammenwirken von Gesetzgeber, Betreibern von Mailservern, Administratoren und Anwendern wirkungsvoll sein. Internet Service Provider (ISP) sollten vermehrt die zur Verfügung stehenden Werkzeuge nutzen (Authentifizierung, keine Verwendung ungültiger bzw. gefälschter Absenderadressen). Administratoren stehen vor der Herausforderung, ihre Filter und Virenabwehr in den Griff zu bekommen. Die Praxis zeigt, dass die Betreuung eines Mailservers sehr hohe Qualifikation voraussetzt und nicht im „Vorbeigehen" möglich ist. Weiters ist die Auswahl der Applikationen (E-Mail-Client, Webbrowser) ein entscheidendes Kriterium, um Anwender einen möglichst sicheren Umgang mit dem Internet zu gewährleisten. Anwender können vor allem durch Information über die Gefahren und vorsichtigen Umgang mit persönlichen Daten und dem Medium E-Mail zur Lösung beitragen. So wie es aber lange gedauert hat, bis z. B. ein überwiegender Teil der Nutzer so genannte Hoaxes ignoriert und nicht weiterleitet, wird auch das angepasste Verhalten zur Vermeidung von Spam noch Jahre dauern.

Stefan Grünwald