

Spam adé - Wie Sie sich und Ihr Unternehmen vor unerwünschten E-Mails schützen

Genau 38 Jahre ist es her, dass Ray Tomlinson ein Programm entwickelte, das es ermöglichte, Nachrichten von einem Computer zum anderen zu verschicken. Heute ist die E-Mail aus dem Geschäfts- und Privatleben nicht mehr wegzudenken. Nach Schätzungen des Instituts für Internet-Sicherheit der Fachhochschule Gelsenkirchen, werden mittlerweile mehr als 200 Milliarden E-Mails pro Tag verschickt. Untersuchungen zufolge sind aber 90 bis 95 Prozent aller E-Mails unerwünschter Werbe-Müll.



SPAM

Den Privatanwender kosten diese Spam-Mails Zeit und Nerven und bereits kleinen Unternehmen kosten sie ohne ausreichende Schutzmaßnahmen viele Tausend Euro pro Jahr. Neben den kommerziellen Absichten der Spammer kann die unerwünschte Post auch Viren, Würmer und andere Schädlinge verbreiten. So werden Arbeitsplatz-PCs in vielen Unternehmen infiziert und fungieren später für den Besitzer zumeist unbemerkt selber als Werbe-Müll-Schleuder.

► **Schützen Sie sich mit Sicherheitsupdates!**

Um sich vor Viren, Würmern und Trojanern in unerwünschten E-Mails zu schützen, sollten Sie über ein aktuelles Antivirenprogramm verfügen. Halten Sie besonders sicherheitsrelevante Anwendungen aber auch das Betriebssystem stets aktuell. Nahezu alle Antivirenprogramme wie auch Betriebssysteme führen automatisch Sicherheitsupdates durch oder machen Sie darauf aufmerksam.

► **Antworten Sie niemals auf Spam-Mails**

Grundsätzlich gilt: Antworten Sie niemals auf Spam-Mails, auch nicht, wenn Sie am Ende der Mail zum Abbestellen des Dienstes aufgefordert werden. Beim Klick auf Floskeln wie „Wenn Sie keine weiteren Nachrichten von uns erhalten wollen, klicken Sie hier.“ bestätigen Sie nur, dass es sich bei ihrer Mailadresse um eine Aktive handelt. Gerne werden in diesem Zusammenhang auch scheinbare Statusmeldungen über Fehler in der Zustellung an Sie verwandt. Sofern Sie den in der E-Mail aufgeführten Adressaten nicht gerade beschickt haben, ignorieren Sie diese E-Mail und verschieben Sie diese in Ihren Spamordner.

► **Geben Sie Ihre E-Mailadresse nicht bei jeder Aufforderung preis!**

Generell sollten Sie Ihre Mailadresse an so wenig Stellen wie möglich hinterlassen. Benutzen Sie nicht Ihre primäre E-Mailadresse für Anmeldungen von Newslettern oder Webseiten mit Login. Besonders für Newsgroups, Foren, Blogs und Chats sollten Sie eine extra E-Mailadresse verwenden, da diese sehr häufig von Harvestern (Programme von Spammern, um E-Mail Adressen im Internet zu identifizieren) nach E-Mailadressen durchforstet werden. Trennen Sie sich von E-Mailadressen die hauptsächlich Spam an Ihre Hauptadresse weiterleiten.

► **Präsentieren Sie Ihre E-Mailadresse nicht im Klartext**

Veröffentlichen Sie auf Ihrer Webseite Ihre E-Mailadresse nicht im Klartext. Das Problem: Wird eine E-Mailadresse im Netz veröffentlicht, dauert es nicht lange bis sie in den Adresslisten der Spammer landet. Damit Sie sich davor schützen können, sollten Sie diese verfälscht darstellen. Stellen Sie dazu Teile oder die gesamte E-Mailadresse in einer Bilddatei auf Ihre Website. Wichtig dabei ist, dass die Bilddatei einen unverfänglichen Namen erhält (also nicht „at.gif“) und der Bildhintergrund mit einem leichten körnigen Rauschen hinterlegt wird. Die heutzutage beste aber auch aufwendigste Methode ist die Bereitstellung eines Kontaktformulars. Dabei muss darauf geachtet werden, dass das Kontaktformular über einen so genannten Captcha-Schutz verfügt. Dies sind kleine Bildchen mit einer zufälligen Zeichenfolge. Nur wenn der Absender die im Bild vorgegebene Zeichenfolge richtig eingibt, wird die Nachricht versandt. Dieser Schutzmechanismus ist notwendig, damit Harvester nicht automatisch Tausende von E-Mails über das Kontaktformular versenden.

► **Beschweren Sie sich beim Provider**

Eine weitere Möglichkeit, der Flut an unerwünschten E-Mails Herr zu werden, ist eine Beschwerde bei dem Provider des Absenders. Die Beschwerde-Adresse lautet für in Deutschland ansässige Provider in der Regel „abuse@...de“, Webdienste wie T-Online, AOL, GMX und andere reagieren in der Regel auf solche Beschwerden und löschen im Zweifel das Mailkonto des Spammers. Auch das Melden der E-Mails an die so genannte „Internet-Beschwerdestelle“ kann Abhilfe schaffen.

► **Benutzen Sie einen aktuellen Spamfilter**

Spam-Filterprogramme fungieren zwischen Online-Postfach und E-Mail-Programm. Wird eine E-Mail abgerufen, durchläuft Sie zunächst den Spamfilter bevor Sie letztendlich im Posteingang oder im Falle eines Spamverdachts im Spamordner landet. Die meisten Spamfilter sind heutzutage recht zuverlässig und nehmen Ihnen beim Aussortieren von unerwünschten Nachrichten viel Arbeit ab.

Damit die Filter auch nach der Installation effektiv arbeiten können, müssen Sie diese stets aktuell halten. Doch Vorsicht! Spamfilter können auch erwünschte E-Mails als Spam einstufen. Dieses Verhalten tritt besonders häufig nach einer Neuinstallation auf, da dem Filterprogramm noch Trainingsdaten fehlen. Somit geht Ihnen unter Umständen ein wichtiger Kundenauftrag verloren. Überprüfen Sie daher regelmäßig Ihren Spamordner auf fälschlicherweise als Spam eingestufte E-Mails. Moderne Spamfilter bieten die Möglichkeit einer „Whitelist“, darin können Sie alle Mailabsender hinterlegen deren Mails Sie für vertrauenswürdig halten oder das Filterprogramm mit Ihrem persönlichen Adressbuch verknüpfen. Damit ist sichergestellt, dass E-Mails von Ihren Freunden oder Geschäftspartnern nicht in Ihrem Spamordner landen.

*Autoren: Dipl.-Inform.(FH) Sebastian Spooren, Prof. Dr. Norbert Pohlmann
Institut für Internet-Sicherheit – if(is), Fachhochschule Gelsenkirchen*

Weiterführende Informationen:

<http://www.internet-sicherheit.de>

<http://www.antispam.de/>

<http://www.internet-beschwerdestelle.de>

Das Institut für Internet-Sicherheit - if(is)

Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter: <http://www.internet-sicherheit.de>

Sichere E-Geschäftsprozesse in KMU und Handwerk

Der IT-Sicherheitstipp wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: <http://www.ec-net.de/sicherheit> sowie unter: http://www.ecc-handel.de/sichere_e-geschaeftsprozesse_in_kmu_und_handwerk.php

Bildquelle: www.fotolia.de