



## **Spams, ein stetig wachsendes und lästiges Äœbel!**

Werbemüll in elektronischen Briefkästen nerven nicht nur die Benutzer, sondern sie überlasten auch E-Mail-Server der Unternehmen. Was kann man gegen diese Flut von ungewollten Werbebotschaften tun und wie verhält man sich als Spam-Opfer am wirkungsvollsten um nicht im zunehmenden E-Mail-Schrott zu ersticken. Eine Vielzahl von Spam-Filtern propagieren Abhilfe, bergen aber auch unliebsame Nebenwirkungen.

### **Monty Python lässt grüssen**

Spam leitet sich vom Hauptrequisit eines Monty Python-Sketches (Dosenfleisch, english spiced pork and meat) ab. Mit Spam werden solche E-Mails bezeichnet, welche man unverlangt erhält. Meist sind dies Werbebotschaften für Produkte oder sie bieten irgendwelche Links zu einschlägigen Seiten an. Zunehmend werden aber Spams auch für das Verteilen von Trojanern, welche das Ausspionieren von Computersystemen möglich machen, oder zum Einfügen von Computerviren, die sich so explosionsartig im Internet verteilen können, eingesetzt. Neben der Zeit, die man für das Durchsehen der E-Mails benötigt, wird auch viel Platz im Postfach und auf der Festplatte verschwendet.

### **Wie funktionieren Spams**

Spam ist deshalb möglich, weil die Mechanismen der Protokolle, welche die E-Mails im Internet transportieren, in ihrer Ursprungsform keine Benutzeridentifizierung vorsehen. Prinzipiell kann also jeder, der sich mit den entsprechenden Befehlen auskennt, mit einer beliebigen Absenderadresse irgendeinem Empfänger über praktisch jeden E-Mail-Server Spam-Post versenden. Da täglich mehr Menschen per E-Mail zu erreichen sind, wird der potenzielle Empfängerkreis für Spams immer grösser. Das Aufkommen solcher Spam-Mails hat in letzter Zeit problematische Ausmasse angenommen. E-Mails werden teils mit Verzögerung von bis zu 24 Stunden zugestellt. Die spezifischen Vorteile der E-Mail-Kommunikation wie Schnelligkeit oder ständige Verfügbarkeit werden damit langsam aber sicher aufgehoben. Mittlerweile hat sich ein schwunghafter Handel mit Mailadressen etabliert und es werden immer ausgefeiltere Spam-Programme entwickelt, welche das Spamming für die Versender vereinfachen.

### **Woher stammen die Adressen**

Als Quellen für E-Mail-Adressen werden sogenannte Web-Roboter-Programme (Web Robots) eingesetzt, welche Internetseiten systematisch nach Adressen absuchen und nach charakteristischen Merkmalen wie das "@"-Symbol oder in Usenet-Postings (Diskussionsforen) Ausschau halten. Als Betreiber einer Internetseite ist man darauf angewiesen, dass beispielsweise potenzielle Kunden Kontakt mit der Verkaufsabteilung aufnehmen können. Hierzu gehört auch eine Mailadresse; es gibt aber auch verschiedene Möglichkeiten, diese vor Web-Robotern zu verschleiern (siehe Kasten). Eine weitere Methode der Spammer an E-Mail-Adressen zu kommen, sind Lockangebote im Internet, beispielsweise gibt es Gewinnspiele, welche nur zu dem Zweck betrieben werden, E-Mail-Adressen zu sammeln. Des Weiteren kursieren im Internet auch diverse Angebote von Adresslisten auf CD, die von professionellen Adresshändlern bereits fixfertig für Spam-Programme aufbereitet sind. Zu guter Letzt werden E-Mail-Adressen auch nach dem Zufallsprinzip generiert.

### **Sie sind bereits Spam-Opfer**

Als Opfer von Werbemüll kann man als radikalstes Mittel natürlich die Mailadresse wechseln. Da noch frei verfügbare Ä,Ä«sprechendeÄ,Ä» Adressen aber mittlerweile selten sind und man als Nutzer nicht immer nur als Ä,Ä«NummerÄ,Ä» auftreten möchte, sollte man diesen Schritt als letztes Mittel verwenden. Viele Mailprogramme bieten sogenannte Regel- oder Filterfunktionen an. Diese kann man nutzen um selbst Mails nach Schlagworten zu durchsuchen und verdächtige Mails, beispielsweise aus dem Posteingang in einen separaten Postfachordner zu verschieben. Dieser muss dann natürlich von Zeit zu Zeit durchgesehen und bereinigt werden, da die Spam-Mails den verfügbaren Festplattenplatz einschränken. Spam-Mails beinhalten meist einen Link, um sich aus der vermeintlichen Mailingliste, in der man sich befindet, wieder auszutragen (Ä,Ä«Klick here to unsubscribeÄ,Ä») oder (Ä,Ä«Klicken Sie hier um sich aus der Mailingliste zu löschenÄ,Ä»). Dies sollte man auf gar keinen Fall tun. Der grösste Gefallen, den man Spammern tun kann ist eine direkte E-Mail-Antwort. Sollte Ihre Antwort den Spammer erreichen leitet er aus Ihrer Antwort ab, dass er auf eine gültige Adresse gestossen ist, die sich gewinnbringend weiterverkaufen lässt. Unternehmen können Spamming über ihre Rechner unterbinden, in dem sie das sogenannte Ä,Ä«RelayingÄ,Ä» abschalten, das heisst, der Server akzeptiert nur noch Mailadressen, die an seine Adresse gerichtet sind. Der beliebige Versand an alle möglichen Adressen ist damit nicht mehr möglich.

### **Abhilfe mit Spam-Filter**

Die Spamflut, die Millionen unerwünschter Mails in die elektronischen Postkästen der Unternehmen spült sorgt für einen



regelrechten Nachfrageboom nach E-Mail-Filtern. Nach Berechnungen der britischen Marktforscher von Datamonitor ([www.datamonitor.com](http://www.datamonitor.com)) soll der Markt für E-Mail-Filter-Lösungen bis zum Jahr 2008 auf insgesamt 2,87 Mrd. Dollar anschwellen. Damit sagen die Marktforscher dem weltweiten Markt eine satte jährliche Wachstumsrate von 26 Prozent voraus. Allein im vergangenen Jahr waren nach Berechnungen mehrerer E-Mail-Filter-Spezialisten zwischen 60 und 80 Prozent aller eingehenden Mails Spam. Da auch Gesetzesbeschlüsse wie der US-amerikanische Can-Spam-Act bisher ihre Wirkung verfehlten setzen die Unternehmen nun verstärkt auf E-Mail-Filter.

Es gibt sowohl kommerzielle als auch kostenfreie Filterprogramme, die in der Lage sind eingehende E-Mails zu untersuchen und (vermeintliche) Spam-Mails zu kennzeichnen oder zu löschen. Diese filtern die eingehende Post beim Abholen vom Server nach Spam-typischen Kriterien aus, beispielsweise numerische Absenderadresse, typische Schlagworte wie das Wort «Viagra», «Vi@gra» oder «V/I/A/G/R/A» geschrieben oder sonstig einschlägige Phrasen.

[zefis.ch](http://zefis.ch) - [info@zefis.ch](mailto:info@zefis.ch)

portals powered and hosted by [proswiss.ch](http://proswiss.ch)

Zentrum für Informatiksicherheit (ast) 08.04.2007

Ausgedruckt am 03.04.2025 - Seite 2/2