SPAM - den Datenmüll bekämpfen.

Ein Artikel von M.Rogge ©Juli 2003

Oftmals wundert man sich, dass man E-Mails von Frauen bekommt, die man gar nicht kennt oder man wird permanent von irgendwelchen Internetangeboten z.B. für potenzfördernde Mittel belästigt.
Kurz und werbefrei möchte ich Ihnen in diesem Artikel erklären woher SPAM kommt, wie man sich schützen und wehren kann.

Ziemlich weit verbreitet sind derzeit Nachrichten wie diese:

"Hallo XXXXXXXXXXX,
Jemand hat Dir eine Video-Botschaft in unserem System aufgenommen.
Um die Nachricht anzuschauen klicke bitte auf den unten angezeigten Link.
Wir wünschen Dir viel Spaß mit Deiner persönlichen Botschaft !
Zum Anzeigen der Nachricht hier klicken, Automatische Nachricht von Message-Online"
Die URL lautet dann:
http://members.tripod.com.pe/lucky/messagorig.txt?sid=19140218135E1001000159020724025516 4F0304084545500B415B5044054E0A5044025E42534A0652.

Dabei taucht nicht nur das Problem der SPAM Mail auf, sondern zugleich noch das große Übel mit den bekannten 0190-Dialern oder Dialern anderer Länder.
Ein Trick dabei ist auch, dass der Absender "Nadja Weber@web.de" heisst, jedoch der Ursprung dieser E-Mail sich von der angezeigten Adresse unterscheidet: "Nadja Weber@web.de" <sxeeuy@centurytel.net>.
Hallo, jemand hat für XXXXXXXXX eine Livecam-Botschaft in unserem System hinterlegt.
Bitte schauen Sie in unseren Chat und rufen Sie diese dort ab.
Video-Botschaften werden generell 48 Stunden gespeichert.zur LiveCam-Botschaft.
Auch hier wieder ein sehr merkwürdiger Link:
http://345k34j5h235235bklzu45634dgt435dtu435jfhjf4533ser654@c005.tripod.com.br/mmm.txt?sid=19140218135E1001000159020724025516 4F03040843445E0D475B5B40054E0A5043065D42534A0652.
Ein Spamer ist vor wenigen Wochen gefasst worden, jedoch geht das Massenmailen munter weiter, also sollte z.B. earthlink.net auf jeder Spamliste stehen.
(hier die Meldung auf heise.de: http://www.heise.de/newsticker/data/see-15.05.03-001/)

So werden unter anderem veröffentlichte E-Mail Adressen abgescannt, die irgendwann einmal in Gästebüchern oder öffentlichen Foren zu lesen waren.
Werden beispielsweise E-Mails oder E-Mail Adressen gefunden, die z.B. basicprojekt@xxxxx lauten, so werden neue E-Mails erstellt, die an alle denkbaren basicxxx@xxx Adressen verschickt werden.
Auch werden zum Beispiel E-Mail Adressen von E-Mail Providern wie GMX oder WEB.de gefälscht, um die Empfänger in falscher Sicherheit zu wiegen: Automatic Mail@gmx.de" <BvtomaticMbil@tiscali.it>.
Angezeigt wird hier nur Automatic Mail@gmx.

Zum Schutz vor SPAM kann man einiges tun!

Sie sollten einfach auf den Absender einer E-Mail achten, die Ihnen zugestellt wird.
Die meisten Menschen mit denen man im Internet kommuniziert kennt man namentlich oder per E-Mail Adresse und so kann SPAM bereits hier erkannt werden.
Programme helfen da schnell und schaffen Abhilfe, indem diese Briefköpfe, Header und Inhalte von E-Mails prüfen und anhand von langen Auswertungen eine Erkennung ausgeben können.
Weiterhin würde ich Ihnen empfehlen, sich eine geschäftlich genutzte E-Mail Adresse und mindestens eine andere, nicht geschäftliche E-Mail Adresse zuzulegen.
Dann würde ich mir genau überlegen, wo und wem ich die geschäftlich genutzte E-Mail Adresse bekannt gebe.
Der E-Mailprovider WEB.de setzt dabei auf ein 3-Wege System.
Zum anderen bietet WEB.de den Nutzern des WEB.de Dienstes eine erweiterte ANTI-SPAM Lösung an, die in der Freemail nicht enthalten ist.

Spamschutz beginnt wie vieles in der Internetsicherheit im Kopf.

Spam ist nicht nur ein Problem eines Betroffenen, der eine oder zehn Spam-Mails bekommt, sondern Spam verstopft die Internetwege, blockiert Mail- und Web-Server des Internet.
Natürlich sind wir Vertreter der Internetkultur, die die schnellen Kommunikationswege schätzen.
Diese Wege werden aber in jeglicher Richtung immer wieder durch verschiedene Formen von Werbung und SPAM sabotiert oder gestört werden.
Wie und vor allem wo finden SPAM-Betreiber E-Mail Adressen?
Oft werden einfachste Methoden genutzt, um E-Mails für Datenbanken zu sammeln, die dann im Anschluss Werbe-Mails versenden die hinlänglich als SPAM bekannt sind. (Sofern unerwünscht!)
Hier muss eine Möglichkeit erwähnt sein: Betreiber von Newslisten, Mailinglisten oder von Portalen nutzen die E-Mail Adressen der User, die sich registrieren um eine Datenbank zu füllen und diese entsprechend zu verkaufen.
Sehr oft ist es in allgemeinen Geschäftsbedingungen von Freemaildiensten verankert, dass Werbemails von Drittanbietern erstellt werden und somit die Weitergabe der E-Mail Adresse mit der man sich registriert hat, garantiert ist.
Weiterhin gibt es sehr viele Programme auf dem Markt, mit denen man Newsgroups und Webseiten scannen kann, um nach E-Mailadressen zu suchen.
Diese Technik nennt man in Fachkreisen Harvesting und ist derzeit weit verbreitet, da Programme die auf diese Art arbeiten viele zusätzliche Funktionen anbieten.
Eine abgewandelte Form hiervon ist das SMTP-Harvesting, bei der dann alle Formen vor einem @Zeichen an einem Server abgefragt werden.
Gesendete E-Mails die ohne eine Fehlermeldung zurück kommen sind zu 99% existend und können entsprechend

weiterverwendet werden.
Im anderen Fall (so schreibt das SMTP Protokoll vor) sendet der Server eine Fehlermeldung und die E-Mail Adresse die nicht existend ist kann verworfen werden.

Welche Schritte kann man einleiten, um gegen SPAM vorzugehen und sich zu schützen?
Zum einen hat man immer die Möglichkeit, sich an den E-Mailprovider direkt zu wenden und eine sachlich formulierte Beschwerde einzureichen.
Weiterhin besteht eine Möglichkeit sich direkt an den Provider der Absendermail zu wenden, die den Verlauf der E-Mail nachvollziehen können.
Es besteht ebenfalls die Möglichkeit, wenn man mit Outlook oder Outlook Express arbeitet einen Empfänger zu sperren wenn von dort eine E-Mail eintrifft.
Auf keinen Fall sollte man auf eine SPAM Mail direkt mit einer Beschwerde antworten, da somit gewährleistet ist, dass die E-Mail als SPAM angekommen ist.
Sehr wichtig erachte ich E-Mails so zu versenden, dass bei mehreren Empfängern die einzelnen Adressaten nicht sehen, wer diese E-Mail noch erhalten hat.
Hierzu setzt man die weiteren Empfänger auf BCC (Blind Carbon Copy) und sich selbst in die TO Leiste ein.
Eine weitere Schutzmöglichkeit ist, die E-Mail auf einer Homepage im UniCode einzugeben und somit unlesbar für Harvesting-Methoden machen.
Dies kann unter anderem dann so aussehen: (Quellcode in HTML einbetten)

```
<a href="&#109;&#97;&#105;&#108;&#116;&#111;&#58;&#109;&#114;&#64;&#98;&#114;&#97;&#105;
&#110;&#45;&#112;&#114;&#111;&#46;&#100;&#101;">E-Mail an Brain-Pro Marko Rogge senden</a>
```

Auf der Internetseite ist dann nur "E-Mail an Brain-Pro Marko Rogge senden" zu lesen und im Quelltext ist die E-Mail nicht erkennbar.
Diesen automatischen Generator finden Sie auf dieser Internetseite:
http://www.lerneniminternet.de/htm/tip_spam-email.html

Folgendes Kleine JavaScript bietet ebenfalls Abhilfe:

```
<script language="JavaScript">
<!--
var name = "Test";
var domain = "testdomain.de";
document.write('<a href="mailto:' + name + '@' + domain + '">');
document.write(name + '@' + domain + '</a>');
//-->
</script>
```

Ein weiteres Programm hierfür ist das Mailto-Verschlüsselungsprogramm von Peter Hahm.
Sie finden es unter: http://www.ib-hahm.de

Ich möchte Ihnen als eine weitere Schutzmaßnahme NoHTML empfehlen.
Dieses kleine Script, in Outlook oder Outlook Express importiert, sorgt dafür, dass Sie keine E-Mails mehr im HTML-Format erreichen,
und gleich in Klartext dargestellt werden.
Dies ist sehr nützlich, da sehr viele SPAM Mails mit Dialerlinks versehen sind die man sonst nicht erkennen kann:
http://ntbugtraq.ntadvice.com/download/Nohtml.zip

Ein weiteres Produkt was ich einige Tage lang getestet habe kommt von der **Firma Eleven GmbH** mit dem Gründer R.Rothe.
Die Firma hat das Produkt eXpuregate entwickelt, dass Serverseitig die E-Mails bereits dort nach verschiedenen Kategorien filtert und entsprechend dann weiterleitet.
Der Service ist für private Kunden ein kostenloser Dienst und geschäftliche Nutzer können auf eine kostengünstige Variante zurück greifen.
Das Programm bietet verschiedene Einstellungsmöglichkeiten an, wie mit SPAM verfahren werden soll:
Einstellen, an welche E-Mail-Adresse eine Kategorie gesendet werden soll.
Individuelle Kopfzeilen (Header) hinzufügen.
Kopfzeilen (Header) löschen.
Ändern der Betreffzeilen (Subjectheader).
Gleichbehandlung verschiedener Kategorien.
Weiterhin ist eine sehr ausführliche Hilfe dazu angeboten, die das Konfigurieren sehr einfach und leicht macht.

:: SPAM den Kampf ansagen ::

Statistik Zeitraum: 4.7.2003 - 4.8.2003 (Mailanzahl)

Statistik erzeugt am: 4.8.2003 17:06:16

Statistik über:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Download Excelfile

Mailtypen	Anzahl	%
Clean	6	5.0
Suspect	2	1.7
Spam	106	87.6
Bulk	7	5.8
Dangerous	0	0.0
Bulk.Advertising	0	0.0
Bulk.Porn	0	0.0
Dangerous.Virus	0	0.0
Total	121	

Sehr schön im Bild ist erkennbar, wie einzelne E-Mails behandelt wurden und in welche Kategorie diese eingeteilt sind. Welche Kategorie was genau beinhaltet wird entsprechend in einer Legende dargestellt und man kann selbst bestimmen, wie mit welchen E-Mails verfahren werden soll und wohin die E-Mails weitergeleitet werden.
Weitere Informationen zu eXpuregate: http://www.eleven.de

Weiterführende Links und Infos:
Hacking Intern - Kapitel 7, ab Seite 397: 0190-Dialer von seriös bis illegal & Spam und Flaming - wenn das Postfach platzt

Produkteauswahl auf PC-Welt, englisch:
http://www.pcworld.com/downloads/browse/0,cat,1447,sortIdx,1,00.asp

Öffentliche Veranstaltung der SPD-Fraktion:
http://www.spdfraktion.de/perl/dbdoc?category=events&subcat=aktuell&id=28987&type=event&locator=/veranstaltungen/xx#

E-Mail Header erkennen und verstehen:
http://sites.inka.de/ancalagon/faq/headerfaq.php3

Wiederruf der Genehmigung zur Speicherung von Daten für werbliche Zwecke:
http://www.schnappmatik.de/TFFFFF/

Harvestinginformation:
http://www.openarchives.org/OAI/2.0/openarchivesprotocol.htm

Yahoo gegen SPAM:
http://de.docs.yahoo.com/spamguard/use/index.html

Programme gegen SPAM:
SAProxy: http://saproxy.bloomba.com/
SPAMNet: http://www.cloudmark.com/
SPAMPal: http://www.spampal.org/
MailShield Desktop: http://www.lyris.com/store/mailshield/desktop/download.html
SPAM Assassin: http://spamassassin.org/index.html
K9-Spam Filter: http://www.8ung.at/thebatinfo/spam/k9.htm

Beste Grüße, Marko Rogge - Security Consultant
Brain-Pro Security : www.brain-pro.de
10.07.2003 // Update 04.08.03
Danke an U.Laumann und A.Peter für Hilfe und Korrektur