INFONEWS

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

Unerwünschte Werbemails - Spam

Tagtäglich werden wir durch unerwünschte Emails gestört und verlieren Zeit für die wichtigen Emails. Unser INFONEWS 2/04 zeigt, woher Spam kommt und was Sie dagegen tun können.

Inhaltsverzeichnis

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Was müssen Sie über Spam wissen?

Spam ist eine Sammelbezeichnung für unerwünschte, belästigende Nachrichten in Form von Email oder Beiträgen (Postings) im Usenet. Bei Email spricht man auch von Junk Email ("Junk" = wertloser Mist).

Da das Versenden von Nachrichten in grosser Menge einfach und billig ist, ist es zu einem ernsthaften Problem geworden.

Europäische Mittelständler verlieren jährlich 22 Mrd. Euro durch elektronische Schädlinge und unerwünschte Email-Werbung. Jeder erfolgreiche Angriff durch Viren schlägt im europäischen Durchschnitt mit etwa 5'000 Euro durch Arbeitsausfälle und Datenverluste zu Buche. Das ergab eine Umfrage des Antiviren-Software-Herstellers Network Associates. Für das vergangene Jahr hatten die Marktforscher von Datamonitor einen durchschnittlichen Schaden von 37'000 Euro durch Virusattacken bei grossen Unternehmen ermittelt.

Bei SPAM können folgende Typen unterteilt werden:

- Kommerzielle Spams (UCE = **U**nsoliticed **C**omercial **E**- Mail: Unerbetenes Kommerzielles Email)
- Kettenbriefe/ Viruswarnungen
- Durch Viren versandte Emails

1.1 Wie gelangen Spammer an Ihre Adresse?

Immer wieder taucht die Frage auf, wie denn Spammer zu ihren Adressen kommen. Da Spammer die Herkunft ihrer Adressen nur in den seltensten Fällen preisgeben, kann man in der Regel nur Vermutungen aufstellen, die auf Beobachtungen von Systemadministratoren oder von Spamopfern beruhen. Taucht zum Beispiel eine spezielle Mailadresse, die man nur einer Firma angegeben hat, plötzlich in diversen Spams auf, kann man davon ausgehen, dass diese Firma die Adressen weiterverkauft hat.

1.1.1 Adresshandel

Es gibt Firmen, die Adressen, an die sie irgendwie gelangt sind (Newsletterabonnenten, Wettbewerbe, Betreiber von Maildiensten) an Dritte weiterverkaufen. Um solchen Firmen auf die Schliche zu kommen, könnte man jeder Firma, mit der man verkehrt, eine eigene Emailadresse angeben, so dass man den Handel mit Emailadressen verfolgen könnte.

Andererseits ist es bei vielen Gratismaildiensten üblich, dass der Anbieter selbst Werbung verschickt, oder dies von Dritten tun lässt. Entsprechende Bestimmungen befinden sich meistens in den allgemeinen Geschäftsbedingungen.

Das grösste Segment im Adresshandel dürften die Spammer selbst ausmachen, die ihre bisherigen Adressen an andere verkaufen oder mit anderen Spammern tauschen.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1.1.2 Scanning

Weit verbreitet ist das automatisierte Suchen nach Emailadressen mit speziell dafür geschriebenen Programmen, auch Harvesting genannt. Verbreitet ist das Scannen von so genannten Newsgroups oder von Webseiten. Besonders ärgerlich an dieser Sammelmethode ist, dass man ihr kaum ausweichen kann. Der Grund, wieso man eine Adresse im Usenet oder auf einer Webseite angibt, ist ja, dass andere Internetbenutzer per Email Kontakt aufnehmen können. Gibt man seine Adresse nicht oder nur verfälscht an, wird die Kontaktaufnahme für andere schwierig oder gar unmöglich.

1.1.3 Brute Force

Mit sinkenden Versandkosten wird es für die Spammer vermehrt attraktiv, durch systematisches Durchprobieren von gängigen Kombinationen (z.B. üblichen Accountnamen wie info@..., webmaster@... oder verbreiteten Vornamen) an gültige Adressen zu kommen.

1.1.4 SMTP-Harvesting

Eine Methode ist das so genannte SMTP-Harvesting. Dabei werden SMTP-Server, die für den Versand und den Empfang von Emails zuständig sind, gezielt nach möglichen Buchstabenkombinationen abgefragt. Gemäss SMTP-Standard meldet ein empfangender Server dem Sender, wenn er ein Mail nicht ausliefern kann, weil die Adresse nicht existiert. Spammer können nun je nach Antwort des Servers darauf schliessen, ob eine angegebene Emailadresse existiert oder nicht.

1.2 Wie verdienen Spammer Geld?

Ein besonderes Merkmal von Spam ist, dass fast sämtliche Kosten nicht vom Spammer, sondern von den Empfängern, den Unternehmen mit eigenem Mailserver und den Providern bezahlt werden müssen.
Möglich macht dies die Eigenheit des SMTP- Protokolls (mit welchem Emails versandt werden), welches erlaubt, dass der Versender von Emails den Text des Spams zusammen mit einer Liste von 100 Emailadressen schicken kann und der Mailserver dann diese Liste abarbeitet. Der Spammer trägt somit nur rund 1/100 der anfallenden Kosten. Auch fällt beim Spamming keinerlei Arbeit an. Es existieren Programme, die den vollautomatischen Versand von Millionen von Emails ermöglichen.

Aufgrund der geringen Kosten rechnet sich Spamming für den Spammer schon bei sehr wenigen positiven Reaktionen. Wenn auf 5 Millionen Spams 5 Personen ein Produkt für Fr. 100 kaufen, lohnt sich das Geschäft bereits. Für die beim Versand tatsächlich anfallenden Kosten, muss der Spammer ja nicht aufkommen.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

2 Was kann man gegen Spam tun?

Den allermeisten von uns ist Spam lästig. Kaum jemand will Spam lesen. Es bieten sich verschiedene Möglichkeiten an, etwas dagegen zu tun. Die häufigste Methode ist das "Wegklicken". Das Problem löst diese Methode jedoch nicht. Prognosen gehen davon aus, dass in Zukunft das Spamaufkommen weiter ansteigen wird.

Je nachdem, welche Dienste man im Internet tatsächlich braucht, gibt es ein unterschiedliches Risiko, Spam-Mails zu erhalten. Zuerst sollte man sich darüber im Klaren sein, wieso man überhaupt Spam zugeschickt kriegt. In den allermeisten Fällen ist es notwendig, dass der Spammer die Emailadresse kennt. Häufig vorkommende Emailadressen wie admin@....ch, info@....ch oder webmaster@...ch werden vom Spammer erraten. In der Regel können Sie davon ausgehen, dass eine Adresse nur dann mit Spam eingedeckt wird, wenn Sie oder Dritte diese bekannt geben.

Quellen von Emailadressen können sein:

- Eingabeformulare
- Usenet
- Bekannte, die Ihre Emailadresse weitergeben
- Emailverzeichnisse
- Webseiten
- Email
- Homepage

2.1 Eingabeformulare

Für den normalen Internetbenutzer dürften vor allem Eingabeformulare ein Problem sein. Beachten Sie, dass sich viele Dienste in Ländern befinden, in denen keine oder nur schwache Datenschutzregelungen gelten. Die "Privacy Statements", die viele Dienstleister auf ihren Webseiten anbieten, sagen im Kleingedruckten oft aus, dass die Adresse beliebig weitergegeben werden darf. Grundsätzlich müssen Sie bei der Angabe einer Emailadresse damit rechnen, dass Sie nun Spam erhalten, auch bei scheinbar seriösen Dienstleistungen. Sie sollten sich immer fragen, ob die Angabe einer Emailadresse in einem Formular wirklich notwendig ist. Auf keinen Fall sollten Sie in solchen Formularen eine private Emailadresse angeben.

2.2 Usenet

Wenn Sie das Usenet benützen, werden sie mit grosser Sicherheit mit Spam konfrontiert. Newsgroups sind ein einfaches Ziel für Programme, die Emailadressen suchen. Vielfach wird dazu geraten, eine falsche Emailadresse anzugeben. Dies führt jedoch dazu, dass eine Kommunikation nicht mehr möglich ist.

Für Usenet- Kommunikation ist es praktisch unmöglich, ohne einen zweiten Mailaccount zu kommunizieren. Praktisch ist ein Mailaccount bei einem Gratis-Mailanbieter. Die Filterfunktionen erlauben es, einzustellen, dass nur Emails mit "Re", "Aw", "Fw" und "Fwd" weitergeleitet werden, also solche, die sich auf eine Diskussion in Newsgroups beziehen. Spams werden so sehr zuverlässig abgeblockt.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

2.3 Mitarbeiter / Bekannte

Ein leidiges Problem sind Mitarbeiter/Bekannte, die "wichtige" Mails an alle, die sie kennen, weiterleiten und in ihrem Mitarbeiter-/ Bekanntenkreis Personen kennen, die dasselbe tun, usw. So kommt schnell eine stattliche Anzahl von Emailadressen zusammen. Einerseits werden Sie so mit Emails bombardiert, andererseits benutzt vielleicht ein Spammer die Emailadressen als erstklassige Datenbank. Abhilfe schafft die Erziehung Ihrer Mitarbeiter oder Bekanntenkreises. Senden Sie Emails an solche Gruppen immer mit den Empfänger-Adressen im BCC Feld, sobald ein Email das Unternehmen verlässt. Die Emails werden an alle verschickt - die Empfänger sind jedoch im Email nicht mehr ersichtlich.

2.4 Emailverzeichnisse

Viele Emailverzeichnisse sind ein Paradies für Spammer, der Nutzen vergleichsweise gering, denn Personen, die Sie unbedingt erreichen wollen, werden mit Sicherheit Ihre Adresse kennen oder diese sonst im Telefonbuch nachschlagen. Spammer schätzen solche Verzeichnisse jedoch, weil die Adressen mit hoher Wahrscheinlichkeit korrekt sind und oft durch systematisches Abfragen der Datenbank ausgelesen werden können. Auf solche Einträge sollte man deshalb verzichten.

2.5 Emails

Ein besonders perfider Trick, Emailadressen zu verifizieren, ist, dass Ihnen "alte Bekannte" oder "eine Verehrerin" oder jemand, der "dringend Hilfe braucht" schreibt und Sie um Antwort bittet. Ebenfalls sollten Sie nicht auf Spams hereinfallen, die an Ihr Mitleid appellieren oder auf den "für jedes Email, dass zurückgesandt wird, spenden wir 1 Franken"-Trick. Ihr Mitleid wird schamlos ausgenützt, denn eine verifizierte Emailadresse, von der man zudem noch weiss, dass deren Inhaber die Emails auch noch liest, kann im Adresshandel einiges mehr einbringen als sonstige Emailadressen.

2.6 Homepage

Geben Sie auf Ihrer Homepage die Emailadresse nicht in Klar-Text ein. Folgende zwei Methoden helfen Ihnen, Ihre Email „verschlüsselt" abzulegen.

2.6.1 Grafische Lösung

- Schreiben Sie Ihre Adressdaten, Email etc. wie gewohnt in ihrem Lieblingseditor und zeigen sie die fertige Webseite an, dann fangen sie die Webseite grafisch ein (bei Windows z.B. mit der Taste Druck, gehen dann in das Programm Paint und fügen den Inhalt der Zwischenablage ein (Shift + Ins)).
- Jetzt bearbeiten Sie das Bild und schneiden nur den Teil aus, der Ihre Adressdaten enthält.
- Das so gewonnene Bild setzen Sie jetzt anstatt Ihrer Adressdaten in Ihre Webseite ein.

Der HTML Code sieht wie folgt aus (kursive Textteile sind anzupassen):

```
<form
action="mailto:neubauer@goSecurity.example">
<input type="hidden" name="Subject" val-
ue="www.goSecurity.ch">
<input type="hidden" name="Body" val-
ue="Kommentar:">
<input
src="http://Ihre.Domain.hier/images/das_Bild
.gif" name="submit" type="image">
</form>
```

2.6.2 JavaScript Lösung:

Bei dieser Methode müssen Suchmaschinen den JavaScript Code ausführen um zu der Adresse zu gelangen. Ein Nachteil dieser Methode ist, dass evtl. manche Ihrer Besucher die Email Adresse nun nicht sehen, wenn beim Besucher die Ausführung von JavaScript nicht gestattet ist.
Der JavaScript Code anstelle der Emailadresse sieht wie folgt aus (kursive Textteile sind anzupassen):

```
<script language="JavaScript">
<!--
var name = "info";
var domain = "goSecurity";
var land = "ch";
document.write('<a href=\"mailto:' + name +
'@' + domain + '.' + land + '\">');
document.write( name + '@' + domain + '.' +
land + '</a>');
//-->
</script>
```

3 Was tun, wenn man Spam erhält?

Auf keinen Fall sollten Sie auf ein Spam-Mail direkt antworten, einen im Mail angegebenen Link besuchen oder eine im Mail beworbene Handlung vornehmen. Oft sind in Spams auch Webseiten angegeben, auf denen man sich angeblich löschen könne. Auch hier gilt: Finger weg!
Die Absenderadresse in einem Mail kann beliebig gewählt werden. Kaum ein Spammer gibt hier seine eigene Adresse an. Schlimmstenfalls wertet der Spammer die zurückkommenden Mails aus und übernimmt die Emailadressen der Antwortenden in eine Datenbank mit verifizierten Adressen, die er besonders teuer tauschen oder verkaufen kann. Einige Spammer rächen sich auch gerade noch an ihren persönlichen Feinden, indem sie in deren Namen spammen.
Die in Spams angegebene "Remove"- Funktion dient in aller Regel auch der Verifikation. Andere Spammer geben auch nur eine "Remove"- Adresse an, um die Empfänger zu beruhigen, da sie dann glauben, das Problem gelöst zu haben.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

3.1 Organisatorische Schutzmassnahmen

Massnahme	Vorteile	Nachteile
Filtern nach Merkmalen in Subjekt-Zeile oder Text (Stichworte..) Bei Internet-Provider oder Email-Provider	Filtermechanismus kann laufend angepasst werden.	Es können auch echte persönliche Mails gefiltert werden.
Bestimmte Adressen blockieren Bei den meisten Email-Programmen/ Diensten möglich	Absender mit blockierten Adressen kommt nicht mehr durch.	Spammer verwenden immer wieder andere (teilweise fiktive) Absenderadressen
Mehrere Email-Konten führen	Ein Email-Konto kann sauber gehalten werden, indem die Adresse nur sehr restriktiv herausgegeben wird.	Mehraufwand für Benutzer
Email-Adresse nicht überall eintragen (Newsgroups, Mailinglisten, Bestellungen, Homepages).		Erreichbarkeit sinkt. Bestimmte Dienste ohne Angabe einer Email-Adresse nicht nutzbar.
Email-Adresse modifiziert angeben Vor und nach dem @ Leerschlag eingeben	Von Computern nicht sogleich als Email-Adresse erkennbar	Emails können nur schwer zugestellt werden. Der Benutzer muss diese Adresse als falsch erkennen und korrigieren.

3.2 RBL Blacklists

Eine Organisation wie zum Beispiel ordb.org pflegt eine Liste von Mailservern, die Spam versenden.
Die Kriterien, welche Server gelistet werden, sind unterschiedlich. Dies kann unter anderem sein, wenn der Server keine Reverse-DNS-Adresse besitzt. Für jedes eingehende Mail werden eine oder mehrere dieser RBLs abgefragt (je nach eingesetzter Software). Abhängig von der Antwort kann das Mail anschliessend als abgelehnt, als SPAM gekennzeichnet, in eine Quarantäne oder gelöscht werden.

3.3 Lokale Blacklists

Diese werden von Administrator selber verwaltet. Darin können Sender-Emailadressen oder auch IP-Adressen enthalten sein. Auch hier können die Emails abgelehnt, in eine Quarantäne verschoben oder gelöscht werden.

3.4 Textanalyse

Bei der Textanalyse wird der Emailtext mit einer gewichteten Liste von Worten verglichen. Wenn nun ein Wort zutrifft, wird das Email als Spam bezeichnet. Es wird dabei oft zwischen zwei Teilen unterschieden, dem Sichtbaren (Mail Body) und dem Unsichtbaren (RAW Format, bei welchem auch Links analysiert werden).

3.5 Bayesische Analyse

Ein relativ junges Verfahren ist die bayesische Analyse. Hier wird der Mailtext und Aufbau durch ein Regelwerk gelassen. Mit mathematischen Algorithmen wird versucht, das Email auf Spam zu überprüfen. Viele Informationen finden Sie unter diesem Link: http://www.niedermayer.ca/papers/bayesian/bayes.html

3.6 Whitelists

Bei dieser Art werden nur die Emails durchgelassen, die auf dieser Liste eingetragen sind. Nachteilig wirkt sich natürlich aus, dass neue Kunden bzw. Interessenten keinen Kontakt mehr aufnehmen können.

White- und Blacklists sind mit einem enormen Aufwand für den Administrator verbunden. Daher werden diese Verfahren oft mit anderen kombiniert.

3.7 Orte zur Bekämpfung von Spam

3.7.1 Spam Prevention am Gateway

Der Test auf Spam wird vorzugsweise auf dem Mail-Gateway gemacht. Die vorhandenen Verfahren (siehe folgendes Kapitel) können hier zentral definiert werden. Es ist möglich, Regeln für die ganze Organisation oder Gruppen von Mailempfängern sowie einzelnen Personen einzustellen. Die als Spam erkannten Meldungen können anschliessend gelöscht, in die Quarantäne verschoben oder einer spez. Emailadresse zugestellt werden. Nachteilig wirkt sich aus, dass der Benutzer hier keinen Einfluss nehmen kann.

3.7.2 Spam Prevention auf dem Mailserver

Für viele Systeme wie z.B. Microsoft Exchange existieren Lösungen, Spam direkt auf dem Mailserver zu erkennen und zu reagieren. Zum Einsatz kommen die bereits erwähnten Verfahren. Vorteilig wirkt sich hier aus, dass der Benutzer selber sein Regelwerk verwalten kann.

3.7.3 Spam Prevention auf dem Client

Für den Client gibt es eine Vielzahl von Lösungen. Diese Software kann als lokaler Gateway verwendet werden oder als Plugin für das Mailsystem. Die Systeme können so selber eingestellt und erweitert werden. Ebenfalls existieren Lösungen, welche die Emails vor dem Download auf den eigenen Rechner auf dem POP3-Server des Providers auf Spam-Mails untersuchen. Als Spam gekennzeichnete Emails können direkt gelöscht und so Bandbreite und Downloadzeit eingespart werden.
Unter diesem Link finden Sie eine Vielzahl von kostenlosen Anti-SPAM Tools:
www.webattack.com/freeware/comm/fwspam.shtml

4 Wie sieht der Aufbau eines Emails aus?

Informationen zum Technischen Aufbau finden Sie unter nachfolgender Internetseite.
http://sites.inka.de/ancalagon/faq/headrfaq.html

Weiterführende Informationen:
Email Aufbau:
http://sites.inka.de/ancalagon/faq/headrfaq.html

kostenlose Anti-Spam Tool:
http://www.webattack.com/freeware/comm/fwspam.shtml

weitere Links zum Thema Spam:
http://www4.ncsu.edu/~aiken/antispam.html