Spam - Ursache, Auswirkungen und Bekämpfung

oder: Hau wech die Scheiße!

Ulli Horlacher - framstag@belwue.de

Was ist Spam?

Spam ist ursprünglich gepökeltes Dosenfleisch der US-Firma Hormel mit schlechtem Ruf: salziges Fastfood in Dosen ohne jeglichen Nährwert.

"The Spam Sketch" in Monty Python's Flying Circus #25 1970-12-15
(http://www.geocities.com/Pipeline/4285/montyspam.htm):

"Spam spam spam spam. Lovely spam! Wonderful spam!"
"I don't want ANY spam!"

Spam ist im Netz ein Sammelbegriff für

- Kettenbriefe
- Unerwünschte Werbung jeder Art: kommerziell, politisch, religiös
- "Get Rich Quick", "Make Money Fast (MMF)"
- Bettelbriefe
- Massenmails
- Junkmails

im Usenet (News) und via E-Mail. Im WWW (**W**elt-**W**eites **W**erbefernsehen) gibt es den Begriff "Spam" nicht.

Der erste Spam kam von den Rechtsanwälten Canter+Siegel 1994-04-12:
Das Werbeposting Green Card Lottery in allen (>10.000) Newsgruppen.

Begriffe:

- UCE: Unsolicited Commercial E-Mail
- UBE: Unsolicited Bulk E-Mail
- EMP: Excessive Multiple Posting (News)
- MMF: Make Money Fast
- MML: Multi Level Marketing

From: nike@indirect.com (Laurence Canter)
Subject: Green Card Lottery- Final One?
Date: 12 Apr 1994 07:53:17 GMT

Green Card Lottery 1994 May Be The Last One!
THE DEADLINE HAS BEEN ANNOUNCED.

The Green Card Lottery is a completely legal program giving away a certain annual allotment of Green Cards to persons born in certain countries. The lottery program was scheduled to continue on a permanent basis. However, recently, Senator Alan J Simpson introduced a bill into the U. S. Congress which could end any future lotteries. THE 1994 LOTTERY IS SCHEDULED TO TAKE PLACE SOON, BUT IT MAY BE THE VERY LAST ONE.

PERSONS BORN IN MOST COUNTRIES QUALIFY, MANY FOR FIRST TIME.

The only countries NOT qualifying are: Mexico; India; P.R. China; Taiwan, Philippines, North Korea, Canada, United Kingdom (except Northern Ireland), Jamaica, Domican Republic, El Salvador and Vietnam.

Lottery registration will take place soon. 55,000 Green Cards will be given to those who register correctly. NO JOB IS REQUIRED.

THERE IS A STRICT JUNE DEADLINE. THE TIME TO START IS NOW!!

For FREE information via Email, send request to cslaw@indirect.com

--
****
Canter & Siegel, Immigration Attorneys
3333 E Camelback Road, Ste 250, Phoenix AZ 85018 USA
cslaw@indirect.com telephone (602)661-3911 Fax (602) 451-7617

Spam: das Problem, die Seuche

Spam...

- belästigt den Empfänger
- ist zu 99% Müll: Pornos, Glückspiele, Pyramiden-Marketing, etc - virtuelle Kaffee-Fahrten-Produkte
- ist in vielen Ländern illegal
- verstopft Datenleitungen, Server, User-Mailboxen oder macht sie durch Überlastung unbrauchbar
- ist für den Versender praktisch kostenlos, aber verursacht beim Empfänger Kosten (Umkehrung des Verursacherprinzips)
- wird meistens (illegal) über Fremd-Relays ausgeliefert
- und Spamcancel machen in News >80% der Artikel aus!
- bindet wertvolle Arbeitskraft, vor allem bei den Providern, Administratoren
- ist *Ressourcendiebstahl*

Aktuelle Situation

- entgegen allen Erwartungen nahm das Spamproblem im letzten Jahr nicht mehr exponentiell zu
- in Deutschland gibt es inzwischen einige Gerichtsurteile, die Spam für illegal erklären
- viele bekämpfen inzwischen aktiv Spam, vor allem einige große Provider (http://spam.abuse.net/goodsites/index.html)
- es stehen immer noch zu viele große Provider (AOL, Compuserv, Mogelcom) auf der *dunklen Seite der Macht* oder sind ihr zumindest gegenüber tatenlos-indifferent
- neue Spamwelle aus "Newbie"-Staaten: z.B. China, Thailand, Taiwan, Chile, Japan(!)
- es gibt "bunti-klicki" Spamsoftware inklusive Adressdatenbank auf CD zu kaufen

Spambekämpfung

The Empire strikes back!

durch den User

- lokales Filtern
- Verwendung von Spam-proofed E-Mail-Adressen (z.B. GMX)
- news:de.admin.net-abuse.* lesen oder mitdiskutieren
- Beschwerden via Mail
    - Adresssuche manuell mittels Headeranalyse (nicht trivial, aufwendig)
    - Adresssuche via WWW-CGI (einfach, aber aufwendig)
    - forward via abuse.net (erfordert zuvor korrekte Adresssuche)
    - automatische Beschwerdegeneration mittels lokaler Software (einfach, schnell, aber systembedingt nicht fehlerfrei)
    - forward an den eigenen Admin (sofern der gewillt ist)
- mit Kleinbus und Lötkolben eine gute Tat vollbringen

durch den Admin, Provider

- vertragliches Verbot mit Konventionalstrafe
- bessere Software (Filter, Konfiguration)
- Abdichten von offenen Mail- und Newsservern
- Exekution oder andere geeignete Massnahmen gegen "eigene" Spammer
- Teergruben einrichten
- Cancels, UDP, Blacklists unterstützen
- aktive Mitarbeit in news:de.admin.net-abuse.* und Admin-Mailinglisten

durch andere

- Zeitschriften, Provider, etc: politische Lobbyarbeit
- Network Underground (Hacker): Sabotage von Spam-Sites und andere kreative Maßnahmen die Spaß machen :-)

Was man *nicht* machen sollte

Als User

- "remove me" Aufforderungen nachkommen oder sich in "Robinson" Listen eintragen: dies dient nur der Verifikation von Adressen
- seine Adresse verfälschen: ist völlig kontraproduktiv
- mit Mail-Bombing antworten: es trifft in 99% aller Fälle eh die Falschen
- bei der **`From`** Adresse beschweren: die ist sowieso gefälscht

Als Admin

- Spambeschwerden ignorieren: Blacklists drohen
- offene Mail Relays betreiben: Blacklists drohen noch schneller
- Spam einfach wegfiltern: ist illegal!

MTAs (Mail Transport Agents) und Fremd-Relaying

Spam wird auf zwei Arten ausgeliefert:

1. direkt, d.h. über den eigenen Provider:
   Diese Spammer bzw Spam-Provider lassen sich leicht bekämpfen bzw abklemmen.

2. via Fremd-Relaying, d.h. ein Dritter MTA wird als Relay missbraucht (Spammer --> Relay --> Opfer):
   Dies ist ein Riesenproblem, weil der eigentlich Spammer sich hinter unschuldigen Opfern verstecken kann.
   Dazu schickt der Spammer seine Mail nur einmal an das Relay, aber mit einer gigantischen Adressliste. Das missbrauchte Relay macht dann die eigentlich "Arbeit".

Erlaubtes Relaying sollte sein:

- von WORLD an eigene E-Mail-Adressen
- von eigenen ip-Adressen an WORLD
- von eigenen Adressen an eigene Adressen

`sendmail` ist der mit 90% "Marktanteil" am meisten verwendete MTA im Internet und erst seit relativ kurzer Zeit gegen Fremd-Relaying resistent:

- 1996-09-26
  sendmail 8.8.0 bietet zum ersten mal optional Schutz gegen Fremd-Relaying, alle Versionen davor dazu unfähig

- 1998-05-19
  sendmail 8.9.0 hat jetzt Anti-Relaying-Konfiguration als Default aktiviert.

Bitte unterlassen Sie es, mir und vielen Anderen unverlangte E-Mails zu schicken. Empfang, Speicherung und Verarbeitung solcher E-Mail verursacht auf unserer Seite Zeit- und Kostenaufwand. Im uebrigen bin ich in keinster Weise interessiert an "**[Subject]**".

Fuer Benutzer eines "elektronischen Briefkastens" entsteht durch unverlangte Werbesendungen eine Belaestigung und verstoesst gegen die guten Sitten. Das Landgericht Traunstein hat am 14.10.1997 festgestellt, dass das Versenden von unverlangtem Werbematerial via E-Mail wettbewerbswidrig und somit unzulaessig ist (Az: 2HK O 3755/97). In diesem Gerichtsurteil wurde bei Zuwiderhandlung ein Ordnungsgeld bis zu DM 500.000,- pro Einzelfall festgesetzt.

Das Landgericht Berlin (Beschluß vom 14. Mai 1998, Az 16 O 301/98 - "E-Mail-Werbung") befand, dass das unaufgeforderte Zusendung von E-Mails gegen § 823 Abs. 1 BGB verstoesst. Bei Zuwiderhandlung wurde ein Ordnungsgeld von 500.000 DM, ersatzweise Ordnungshaft bis zu sechs Monaten festgesetzt.

Nach der staendigen Rechtsprechung des Bundesgerichtshofs verstoesst ein Verhalten im Wettbewerb nicht nur dann gegen die guten Sitten, wenn es dem Anstandsgefuehl der redlichen und verstaendigen Mitbewerber widerspricht, sondern auch dann, wenn die in Frage stehende wettbewerbliche Massnahme von der Allgemeinheit, insbesondere von den durch die Werbemassnahme angesprochenen Verkehrskreisen, missbilligt und als untragbar angesehen wird; denn § 1 UWG soll auch die Allgemeinheit vor Auswuechsen des Wettbewerbs bewahren (BGHZ 59, 317, 319 = NJW 1973, 42 - Telexwerbung; vgl. auch BGHZ 54, 188, 189 = NJW 1970, 1738 - Fernsprechwerbung m. w. N.). (BGH, Urteil vom 03.02.1988 - I ZR 222/85)

Eine Kopie dieser Beschwerde wurde an Ihre Systemverantwortlichen geschickt.

Aus gegebenem Anlaß: Einige Hinweise des CCC Ulm zu dieser Seite.

Da Ihre E-Mail an mich persönlich adressiert ist, fordere ich Sie hiermit gemäß Bundesdatenschutzgesetz (BDSG) auf:

1. Sie haben mir gegenüber unverzüglich offenzulegen, welche Daten ausser Name und E-Mail-Adresse Sie über meine durch diesen Namen/diese Adresse identifizierte Person gespeichert haben, und aus welchen Quellen diese Daten stammen.
   § 19 Abs. 1, § 34 Abs. 1 BDSG

2. Sie haben den Verwendungszweck dieser Daten ebenfalls unverzüglich mir gegenüber offenzulegen.
   § 19 Abs. 1, § 34 Abs. 1 BDSG

3. Sie haben **sämtliche** meine Person/meine E-Mail-Adresse betreffenden Daten unverzüglich zu löschen und mir diese Löschung zu bestätigen.
   § 20 Abs. 2 Satz 1, § 28 Abs. 3, § 30 Abs. 3, ferner § 4 Abs. 1 BDSG

4. Ich untersage Ihnen jedwede zukünftige Speicherung meine Person bzw. meine E-Mail-Adresse betreffenden Daten ohne meine vorherige ausdrückliche schriftliche Genehmigung.
   § 14 Abs. 2 Satz 2, § 4 Abs. 2 BDSG

5. Ich untersage Ihnen die Übermittlung dieser Daten an Dritte. Für bereits an Dritte übermittelte Daten fordere ich eine unverzügliche Sperrung.
   § 28 Abs. 3 BDSG

Ich setze Ihnen zur Erfüllung dieser Forderung eine Frist von zwei Wochen beginnend mit dem Datum dieses Schreibens. Nach Ablauf dieser Frist werde ich den Vorfall unserer Rechtsabteilung übergeben, um gegebenenfalls ein Strafverfahren gegen Sie zu eröffnen.

automatische Beschwerdegeneration mit *nadc*

```
Complain in German? [n]
Is it a chain letter? [n]
Add US legal warning? [n] y

jed will now be started with the auto-generated complain-mail. Please
verify it and look for correct headers. If this is the first time you are
using nadc then enter "?", otherwise hit ENTER:
```

```
To: abuse@aol.net,mail.ims1.com@abuse.net,www.privategold.com@abuse.net
Bcc: framstag
Subject: COMPLAINT: Re: Information
References: <1287128688-11573106@ims1.com>

Please advise this user to discontinue sending unsolicited commercial or
broadcast mail (spam) to my e-mail address. My site must pay to receive
and store them.In addition, I'm not interested in "Re: Information" at
all.

By US Code Title 47, Sec.227(a)(2)(B), a computer/modem/printer meets the
definition of a telephone fax machine. By Sec.227(b)(1)(C), it is unlawfull
to send any unsolicited advertisment to such equipment. By Sec.227(b)(3)(C),
a violation of the aforementioned section is punishable by action to recover
actual monetary loss, or $500, whichever is greater, for each violation.


--------forwarded message--------
...
```

```
#!/client/bin/perl -w

#       They invade our newsgroups - and we fall back!
#       They assimilate entire mailing lists - and we fall back!
#       Not again! The line must be drawn here!
#       This far - no farther!
#       AND WE WILL MAKE THEM PAY FOR WHAT THEY'VE DONE!

# This is nadc-19980624 written in Perl 5.
```

Aus gegebenem Anlaß: Einige Hinweise des CCC Ulm zu dieser Seite.

Links

- **(Anti) Abuse Net**
  "the best anti-spam site on the net" und Beschwerdeweitervermittlung
  http://abuse.net/
  http://spam.abuse.net/

- **The Net Abuse FAQ**
  http://www.cybernothing.org/faqs/net-abuse-faq.html

- **E-Mail-Header lesen und verstehen FAQ**
  http://www.rhein-neckar.de/~ancalago/headrfaq.html

- **de.admin.net-abuse.mail E-Mail-Missbrauch FAQ**
  http://www.unix-ag.uni-hannover.de/faq/de.admin.net-abuse.mail.html

- **FAQ: Falsche E-Mail-Adressen**
  http://home.pages.de/~gerlo/falsche-email-adressen.html

- **de.admin.net-abuse.news Fremdcancel-FAQ**
  http://babelon.virtualave.net/fremdcancel.html

- **Teergruben FAQ**
  http://www.iks-jena.de/mitarb/lutz/usenet/teergrube.html

- **MAPS Realtime Blackhole List**
  http://maps.vix.com/

- **GMX**
  freie E-Mail-Accounts mit Spam-Filterung
  http://www.gmx.de/

- **spamblock**
  mein Spam-Filter für UNIX Users
  http://www.belwue.de/wwwservices/hilfestellungen/spamblock.html

- **nadc (new adcomplain)**
  mein automatisches Beschwerde-Programm
  ftp://ftp.belwue.de/belwue/software/nadc

- **kommerzielle Anti-Spammer Software für Windows**
  http://www.cnet.com/Content/Reports/Shootouts/Spam0727/

- **freie Anti-Spammer Software für Windows**
  http://www.cix.co.uk/~net-services/spam/spam_hater.htm
  http://www.blighty.com/products/spade/

- **Get that spammer!**
  WWW Tools Sammlung um Spam-Autoren aufzuspueren
  http://kryten.eng.monash.edu.au/gspam.html

- **Transport Security Initiative**

MTA sichern gegen Fremd-Relaying
http://maps.vix.com/tsi/

- **S.P.U.T.U.M. : SubGenius Police, Usenet Tactical Unit (Mobile)**
  "Anti-Spam Tactical Operations Headquarter by the Church of the SubGenius"
  http://www.sputum.com/

- **junkbuster**
  freier WWW Werbeblocker für UNIX und Windows
  http://www.junkbuster.com/

- **Spam Rechts-Analyse für Deutschland**
  http://www.digital-law.net/artikel5/artikel/bgh-uce.html

- **Verbot von Mail-Filterung durch den Provider**
  http://www.lrz-muenchen.de/~rgerling/rfra_txt.htm#Heading9

- **EU-Parlament Online-Petition von c't magazin & politik-digital**
  http://www.politik-digital.de/spam/

- **The European Coalition Against Unsolicited Commercial Email**
  Nicht-kommerzielle politische agierende Anti-Spam Organisation
  http://www.euro.cauce.org/

- **Canter & Siegel Green Card Lottery Net Spam Case**
  http://www.eff.org/pub/Privacy/Crypto_misc/Digital_money/Crypto_misc/Computer_security/Hacking_cracking_phreaking/Legal/Cases/Canter_Siegel/
  http://www.forum.swarthmore.edu/news.archives/geometry.college/article124.html

- **Vortrags-Folien**
  ftp://ftp.belwue.de/pub/doc/spamvortrag/

1. Wir weisen an dieser Stelle darauf hin, daß die Seiten unterhalb von http://ulm.ccc.de/chaos-seminar/ keine Meinungsäußerung des Chaos Computer Club darstellen sondern ausschließlich dazu dienen die im Chaos Seminar gehaltenen Vorträge zu dokumentieren.
2. Wir wurden darauf aufmerksam gemacht, daß die unter Links verlinkte Seite zu freier Anti-Spammer Software für Windows auf ein Programm (whoisi.exe) verweist welches mit "timesink" "verseucht" sei.
   Mit timesink werden Windowsprogramme dazu gebracht auch noch andere Funktionen als die erwarteten auszuführen und zB Werbung anzuzeigen. Manche Leute bezeichnen dies als "spyware".
   freewareguide.de schreibt über timesink:

   > In alten Versionen wurde die unangenehme steige Laufzeit des Roboters durch das Programm TSADBOT.EXE geleistet. Die Lauffähigkeit des "Wirtsprogrammes" wurde zumeist nicht dadurch beeinflusst, wenn dieser Roboter entfernt wurde (s.u.). Aktuelle Versionen von "TimeSink" verzichten ganz auf die Installation dieses Roboters und somit läuft der Werbemechanismus nur, wenn auch das "Wirtsprogramm" aktiv ist. Dafür ist dann aber der verbleibende Mechanismus (soweit ich weiß) nicht entfernbar, ohne die Lauffähigkeit des "Wirtsprogrammes" zu beeinträchtigen.
   > Das Programm TSADBOT.EXE befindet sich im Ordner "TimeSink" innerhalb des "Programme"-Ordners um es löschen zu können. Hierzu löscht man in der Registrierung unter "\HKEY_LOCAL_MACHINE\ Software\ Microsoft\ Windows\ CurrentVersion\ Run\" den Schlüssel "TimeSink Ad Client" (z.B. mit Hilfe des Startup Control Panel) und startet das System neu. Eine andere Möglichkeit ist das Beenden des Prozesses mit einem entsprechenden Programm (z.B. Another Task Manager) vor der Löschung.

   Wir weisen deshalb darauf hin, daß wir keinen Einfluß auf den Inhalt verlinkter Seiten haben und erst recht nicht auf Programme die nicht im Source Code vorliegen. Wir empfehlen freie Software aus vertrauenswürdigen Quellen zu verwenden.

3. Die unter BSDG Aufforderung verlinkte Seite hat inzwischen den Namen FFFF (Framstags freundlicher Folter-Fragebogen) bekommen und erfreut sich zunehmender Beliebtheit, ist aber rechtlich umstritten. Es gibt auch noch eine Variante samt Kommentaren von Thomas Goerlich

   Wir weisen deshalb darauf hin, daß wir keinen Einfluß auf die Rechtsprechung in irgendeinem Land der Erde haben. Um Beachtung der Diskussionen in de.admin.net-abuse.mail wird gebeten.