

Techniken zur Spambekämpfung

Froscon 2006

Alexander Wirt

25. Juni 2006

Übersicht

- 1 Einleitung
 - Unerwünschte Werbung und ihre Daseinsformen
 - Die Geschichte des SPAM
- 2 Strategien gegen SPAM
 - Die rechtliche Seite
 - Die technische Seite
- 3 Was kannst du tun

SPAM und wie er uns begegnen kann

- Vertreter
die wahrscheinlich älteste Form der unerwünschten Werbung
- Briefwurfsendungen und Reklameblätter

SPAM und wie er uns begegnen kann

- Vertreter
die wahrscheinlich älteste Form der unerwünschten Werbung
- Briefwurfsendungen und Reklameblätter
- FAX
in Deutschland eigentlich seit langem verboten

SPAM und wie er uns begegnen kann

- Vertreter
die wahrscheinlich älteste Form der unerwünschten Werbung
- Briefwurfsendungen und Reklameblätter
- FAX
in Deutschland eigentlich seit langem verboten
- SPIM
SPAM over Instant Messaging

SPAM und wie er uns begegnen kann

- Vertreter
die wahrscheinlich älteste Form der unerwünschten Werbung
- Briefwurfsendungen und Reklameblätter
- FAX
in Deutschland eigentlich seit langem verboten
- SPIM
SPAM over Instant Messaging
- SPIT
SPAM over Internet Telephony

SPAM und wie er uns begegnen kann

- Vertreter
die wahrscheinlich älteste Form der unerwünschten Werbung
- Briefwurfsendungen und Reklameblätter
- FAX
in Deutschland eigentlich seit langem verboten
- SPIM
SPAM over Instant Messaging
- SPIT
SPAM over Internet Telephony
- UCE
unverlangte kommerzielle Commercial E-Mail

Eigentlich nur Frühstücksfleisch...

- SPAM entstand aus dem Namen „**Spiced Ham**“

Eigentlich nur Frühstücksfleisch...

- SPAM entstand aus dem Namen „**Spiced Ham**“
- Frühstücksfleisch der Firma „Hormel Foods Inc.“

Eigentlich nur Frühstücksfleisch...

- SPAM entstand aus dem Namen „**Spiced Ham**“
- Frühstücksfleisch der Firma „Hormel Foods Inc.“
- *19.1.1994* - Der Anfang einer Ära.
Global Alert For All: Jesus is Coming Soon[1]

Eigentlich nur Frühstücksfleisch...

- SPAM entstand aus dem Namen „**Spiced Ham**“
- Frühstücksfleisch der Firma „Hormel Foods Inc.“
- *19.1.1994* - Der Anfang einer Ära.
Global Alert For All: Jesus is Coming Soon[1]

Der Status Quo - Willkommen im Jahr 12 a.S.

- Umsätze im Milliardenbereich

Der Status Quo - Willkommen im Jahr 12 a.S.

- Umsätze im Milliardenbereich
- International agierende Organisationen

Der Status Quo - Willkommen im Jahr 12 a.S.

- Umsätze im Milliardenbereich
- International agierende Organisationen
- 2005 - Angerichteter Schaden durch Spam ca. 40 Milliarden Euro

Der Status Quo - Willkommen im Jahr 12 a.S.

- Umsätze im Milliardenbereich
- International agierende Organisationen
- 2005 - Angerichteter Schaden durch Spam ca. 40 Milliarden Euro
- Unschuldige Rechner werden von Spamversendern mit der Hilfe von Virenprogrammierern als Geiseln und Arbeitsdrohnen gehalten

Der Status Quo - Willkommen im Jahr 12 a.S.

- Umsätze im Milliardenbereich
- International agierende Organisationen
- 2005 - Angerichteter Schaden durch Spam ca. 40 Milliarden Euro
- Unschuldige Rechner werden von Spamversendern mit der Hilfe von Virenprogrammierern als Geiseln und Arbeitsdrohnen gehalten
- Mehr als 50% aller E-Mails im Internet sind SPAM

Rechtlicher Art

- Das versenden von SPAM E-Mails ist sittenwidrig
Urteil des BGH vom 11.03.2004 (I ZR 81/01)

Rechtlicher Art

- Das versenden von SPAM E-Mails ist sittenwidrig
Urteil des BGH vom 11.03.2004 (I ZR 81/01)
- Gesetz gegen Unlauteren Wettbewerb (UWG)
Klagen/Abmahnungen können nur Mitbewerber oder Verbände

Rechtlicher Art

- Das versenden von SPAM E-Mails ist sittenwidrig
Urteil des BGH vom 11.03.2004 (I ZR 81/01)
- Gesetz gegen Unlauteren Wettbewerb (UWG)
Klagen/Abmahnungen können nur Mitbewerber oder Verbände
- Mit dem 1. März ist das neue Telemediengesetz in Kraft
getreten das Strafen bis zu 50.000 Eur für das versenden von
Spam vorsieht.

Rechtlicher Art

- Das versenden von SPAM E-Mails ist sittenwidrig
Urteil des BGH vom 11.03.2004 (I ZR 81/01)
- Gesetz gegen Unlauteren Wettbewerb (UWG)
Klagen/Abmahnen können nur Mitbewerber oder Verbände
- Mit dem 1. März ist das neue Telemediengesetz in Kraft
getreten das Strafen bis zu 50.000 Eur für das versenden von
Spam vorsieht.
- Ein Großteil des SPAMs stammt aus den USA, dicht gefolgt
von Korea und China
*Die Erfolgsaussichten für Klagen sind also verschwindend
gering*

Filtern auf SMTP Ebene

Blocken einer E-Mail auf Grund von Verstößen gegen das SMTP Protokoll (RFC 2821)

Vorteile

- In den meisten SMTP Daemons vorgesehen
- Geschieht bevor die Mail eingeliefert ist
- Kostet wenig Ressourcen

Nachteile

- Verstößt selber gegen das RFC
- Wenn die E-Mail abgelehnt wurde gibt es keine Möglichkeit diese wiederzubekommen

DNSBLs

Abfragen von externen Listen mittels des DNS Protokolls

Vorteile

- In den meisten SMTP Daemons vorgesehen
- Geschieht bevor die Mail eingeliefert ist
- Kostet wenig Ressourcen

Nachteile

- Man gibt die Kontrolle über seine SPAM Filterung aus den Händen

DNSBLs

Abfragen von externen Listen mittels des DNS Protokolls

Vorteile

- In den meisten SMTP Daemons vorgesehen
- Geschieht bevor die Mail eingeliefert ist
- Kostet wenig Ressourcen

Nachteile

- Man gibt die Kontrolle über seine SPAM Filterung aus den Händen
- Viele False Positives

Greylisting

Das Hoffen darauf das SPAM Drohnen und Massenversender mangelhaft implementiert sind

Vorteile

- Funkioniert erstaunlich gut
- Hat „theoretisch“ keine False Positives

Nachteile

- Auch Spammer werden sich anpassen
- Sorgt für Verzögerungen im Mailverkehr
- Fehlerhaft implementierte Mailserver verlieren E-Mails

Weighted Greylisting

- Minimieren der Nachteile für *gute* Nutzer
- Gegreylisted wird nur derjenige der von vornherein verdächtig ist
- Anhaltspunkte sind: DNSBL Entries, HELO Checks, Dial UP Prüfungen

Spamerkennung mit statischen Regeln

Erkennen von SPAM auf Basis von statisch aufgestellten Regeln

Vorteile

- Einfach zu implementieren
- Ergebnisse sind vorhersagbar
- Leicht anpassbar
- Bei einem guten Regelwerk wenig False Positives

Nachteile

- Leicht zu umgehen wenn das Regelwerk bekannt ist
- Steht und fällt mit der Qualität des Regelwerkes

Lernende Systeme

Erkennen von SPAM mit dynamischen Erkennungssystemen
(Bayes)

Vorteile

- Verspricht in der Theorie sehr hohe Erkennungsraten
- Stetig lernend

Nachteile

- Muss erst „angelernt“ werden
- erfordert stetiges lernen
- Ergebnisse nicht vorraussagbar

Bilderspam

Probleme

- Bilder werden durch Spammer individuell erstellt
- Reguläre Newsletter beinhalten auch Bilder
- Unschuldiger Text - völlig anderes Bild

Lösungen?

- Zerlegen von Bildern und Vergleich der Einzelbilder gegen eine Datenbank
- Vergleich über Tonwertanalyse
- Vereinfachung von Bildern mit anschließendem Vergleich

Regeln für den Nutzer im Umgang mit Spam und Viren

- 1 Kontrollieren Sie die Veröffentlichung Ihrer E-Mail Adresse
- 2 Haben Sie ein gesundes Misstrauen - bei jeder E-Mail
- 3 Seien Sie besonders Vorsichtig bei E-Mails von Banken und anderen Dienstleistern
- 4 Üben Sie besondere Sorgfalt beim Öffnen von E-Mail Anhängen
- 5 Konfigurieren Sie Ihren E-Mail Client sinnvoll
- 6 Antworten Sie **niemals** auf SPAM
- 7 Verwenden Sie elektronische Signaturen
- 8 Verwenden Sie SPAM und Virenfilter
- 9 Halten Sie Ihre Software stets aktuell
- 10 Denken Sie auch an die Alternativen zur E-Mail

References:

► Back



[Clarence L. Thomas IV]

Global Alert For All: Jesus is Coming Soon

<http://groups.google.com/groups?selm=9401191510.AA18576%40js>
19.1.1994.