SPAM : Ongevraagde E-mail

De kreet
Spam® is de naam van een blikje met een vleesproduct van de fabrikant Hormel die in de zestiger jaren een ieder zodanig tot vervelends toe belaagde met ongewenste reclameuitingen dat dit in de reclame-wereld een vakterm is geworden. In de jaren zeventig speelde Monty Python een sketch in een studio cafetaria waarin ieder menu item is vervangen door het woord "spam". Daardoor raakt de hele conversatie in steeds meer "spam, spam spam and spam". De treffende overeenkomst met het fenomeen is verdere aanleiding geweest om deze kreet in het digitale tijdperk over te nemen.

Spam-mail
Spam (junk-mail) is ongevraagde, vaak commerciële e-mail die in grote hoeveelheden over het Internet wordt verspreid. Een belangrijke groep die verantwoordelijk is voor spam zijn de verkopers.

Spam is een generieke naam waaronder twee begrippen worden geplaatst:
Excessive Multi-Posting (EMP) wat zoveel inhoudt als teveel separate copieën van een in hoofdzaak identiek bericht.
Excessive Crossposting (ECP) betekent dat hetzelfde of meermalen hetzelfde bericht naar te veel groepen ontvangers wordt gestuurd.
Veel eindgebruikers hanteren een hele ruime definitie, die vinden alle ongewenste e-mail spam.

Waarom spam slecht is
E-mail en Newsgroepen zijn populaire media vanwege de lage kosten voor de zender en het grote bereik. Zo liggen de kosten van het kopen van een e-mail adreslijst met 300.000 adressen rond de USD 40. De kosten van deze spam zijn zo voor de zender bijna nihil, in tegenstelling tot de ontvanger en de Internet Service Providers (ISP) die voorzien in het datatransport en de opslag. In het fysieke (papieren) domein ligt dit geheel anders, daar komen de kosten voor het drukken en verspreiden bij de adverteerder.

De opslagkosten zijn voor een ISP enorm. Voorbeeld: Een beetje bericht is zo'n 10Kbyte. Wanneer één ISP voor 10.000 klanten wordt geraakt is dat zo'n 100Mbyte. Zelfs bij een normale harde schijf van 120Gbyte betekent dat het bij 400 spam's een service onderbreking gaat ervaren, terwijl 4000 spam's per dag per ISP aan de lage kant is.

Het dagelijks e-mail gebruik ondervindt hinder van spam. Gebruikers ervaren het als ongewenst dat het ophalen van post via inbellen bij de ISP langer dan noodzakelijk duurt vanwege deze non-informatie.

Er is geen afstemming van de boodschap op de wensen van de ontvanger, zo goed als niemand is geïnteresseerd. Vanwege de lage kosten wordt echt iedereen gemaild, dit in tegenstelling tot folders. De dubbeltjes kosten geven enige doelgroep- of regio-beperking. Niet bij e-mail.

Verder wordt spam vaak expres via omwegen verstuurd, waarbij de Internet-mail gateways van nietsvermoedende bedrijven worden gebruikt als tussenstations (spam-relay). Dit geeft een dergelijk bedrijf een slechte naam en kan zoveel capaciteit vragen dat de eigen mail niet of veel trager wordt afgehandeld.

SPAM en ander typen ongewenste e-mail
* **Commerciële uitingen**
Doel: attentiewaarde te creëren voor een bepaalde site, product, actie.
Get a loan, how to get rich, meet more women;
* **Mail bom**
Doel is het beïnvloeden van de performance van een netwerk of het systeem van de gebruiker.
Vaak wordt een mailtje verstuurd met in de header een virus waarschuwing, dat via een e-mail (met een specifiek onderwerp) een virus verspreidt wordt. Gevraagd wordt het bericht door te sturen naar je vrienden, collega's etc. Het gevolg is dat het netwerk overbelast raakt.
*** Letter bomb**
Een Letter Bomb is een e-mail of word processing document welke actieve code

bevat bedoeld om schade toe te brengen aan de ontvanger, bijvoorbeeld door de harddisk van de computer te wissen. De virussen TechWeb Encyclopedia en Melissa zijn voorbeelden van dergelijke documenten met macro-instructies!

Dit een limitatieve opsomming. Er mag worden verwacht dat organisaties in de toekomst steeds vaker geconfronteerd zullen worden met een vorm van spam. Dit resulteert in lagere productiviteit en grotere ergernis.

De maatregelen
Er zijn duidelijk maatregelen nodig om spam tegen te kunnen houden nu en in de toekomst. Een aantal maatregelen zijn reeds in Internet standaarden (RFC's) verwoord.

Concrete voorgestelde maatregelen komen onder andere neer op:
1) Controleren of in de route een spam-relay zit. Voor het identificeren van een spam-relay zijn een tweetal speciale organisaties ontstaan. Een organisatie die een spam-aanval heeft gehad, kan deze daar aanmelden. Bij het meermalen voorkomen van deze naam zal de betreffende organisatie een verzoek krijgen de configuratie te wijzigen. Wordt dit niet (adqueaat) gedaan dan zal deze organisatie op een "spam-lijst" komen. Veel organisaties staan dan geen mail meer van deze adressen toe, waarmee de mogelijkheid legitieme e-mail te versturen tussen deze organisaties komt te vervallen.
2) Controleren van het bron-adres. Via het Domain Name System (DNS) is voor SMTP-servers te achterhalen of dit adres vanuit een bestaand domain is verstuurd. Hoewel DNS niet vrij is van beveiligingslekken, zal de introductie van Secure DNS dit een goede controle maken. Het zal duidelijk zijn dat de makers van spam-software inmiddels op deze ontwikkeling inspelen en echte adressen zijn gaan gebruiken als bron-adres.
3) SMTP-server opties op "veilig" instellen. Binnen de protocol standaardisatie rondom SMTP zijn er een aantal commando's waarvan de aanwezigheid verplicht is, maar noodzaak om deze op het Internet te bieden er niet is, waaronder:

- mail-lijst expansie (SMTP-commando:EXPN)
- verify adres (SMTP-commando:VRFY)
- remote queueing (SMTP-commando:ETRN)

Inmiddels zijn er passende foutcodes waarmee de acceptatie van dergelijke verzoeken kunnen worden geweigerd op basis van configuratie-optie instellingen van de SMTP-server.
4) Intelligentere client-protocollen (bijvoorbeeld het Internet Mail Access Protocol - IMAP4) waarbij de header-tekst (het Subject: veld) separaat opgehaald kan worden. Dit geeft enige verlichting maar vraagt meer ervaring bij de eindgebruiker.

Bah, last van spam, wat nu?
Het is niet plezierig om een mail te ontvangen, waarom je niet hebt gevraagd. Het is nog onplezieriger als je de hogere telefoonrekening moet betalen om al die spam op te halen bij je ISP.

Tip 1 : probeer eens een keer te "unsubscriben" maar alleen bij een gerenommeerd bedrijf zal dat helpen, bij alle andere bevestigd dit alleen maar dat dit e-mail adres werkt. Gevaarlijk maar het KAN werken.
Tip 2 : direct weggooien, niet mee zitten. Makkelijk en veilig maar het biedt geen garantie dat het niet meer voorkomt.
Tip 3 : gebruik een betere mail-client die eerst headers haalt en daarna op aanwijzing pas de rest. De ISP moet dit wel ondersteunen.
Dit voorkomt dat naast de rest ook de spam moet worden opgehaald.
Tip 4 : persoonlijk filters toepassen. Hoewel van beperkte waarde zijn er hulpmiddelen (plugin's) die ervoor zorgen dat je dan persoonlijk paal en perk kan stellen aan dit soort mail. Het spaart de tijd om dergelijk mail te lezen.
Tip 5 : vraag de ISP hulp bij het filteren. Het kan goed zijn dat de ISP in staat is de spam te filteren als zij op het verschijnen ervan attent worden gemaakt. Na afspraken met een servicedesk kan het forwarden ervan naar een technische dienst behulpzaam zijn.

Tip 6 : mail-client regels toepassen
Recentere versie van mail-clients zijn in staat een set aan regels toe te passen voor het afhandelen van binnenkomende post. Indien er vaker spam komt van een enkele zender of domein kan deze in een speciale folder worden geparkeerd.
Tip 7 : probeer de bron te benaderen
Een enkele keer wil een bedrijf dit mechanisme hanteren om reclame te uiten en geeft het een telefoonnummer erbij. Bellen en aankondigen dat je nooit zal kopen bij het toepassen van dergelijke praktijken wil wel eens helpen.

Literatuur

RFC 2196 Site Security Handbook. B. Fraser. September 1997. (Format: TXT=191772 bytes) (Obsoletes RFC1244) (Also FYI0008) (Status: INFORMATIONAL)

RFC 2505 Anti-Spam Recommendations for SMTP MTAs. G. Lindberg. February 1999. (Format: TXT=53597 bytes) (Also BCP0030) (Status: BEST CURRENT PRACTICE)

RFC 2635 DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*). S. Hambridge, A. Lunde. June 1999. (Format: TXT=44669 bytes) (Also FYI0035) (Status: INFORMATIONAL)

Stopping Spam, Schwartz, Alan and Simson Garfinkel, O'Reilly and Associates, 1998.

Internet-verwijzingen

http://www.ietf.org/html.charters/run-charter.html
The working group of the Internet Engineering TaskForce on Responsible Use of the Network (RUN)
Archive: ftp://ftp.intel.com/pub/ietf-run

http://spam.abuse.net/
Fight Spam on the Internet! Help Stamp Out Spam. Anti-junk mail filters, IP blocking, blacklists, other boycot tools to keep the net useful for everyone.

http://spam.gunters.org/
News, tools, links, and other info about how to fight spam (junk email). Emphasis on end-user and server-level mail filters using tools such as procmail, maildrop, and perl scripts.

http://pw2.netcom.com/~ix537260/antispam/index.html
Anti-spam Intelligence Center; Web clearinghouse for anti-spamming resources and information.

http://www.killfile.org/~tskirvin/faqs/spam.html
Current Spam thresholds and guidelines, Lewis, Chris and Tim Skirvin.

http://www.blighty.com/spam/docs.html
The Art of Hunting Spam - A library of texts for the serious spam hunter. Includes lots of ways of filtering spam of all flavours from your account or an entire site.

Dit artikel is eerder gepubliceerd in het Handboek Netwerkmanagement van WoltersKluwer Ten Hagen Stam, door Ir. E.J. Mellink. Publicatie met toestemming.

De Auteur

Ir. Ernst J. Mellink is IT Security Architect en eigenaar van More-Secure BV. Hij adviseert grotere en kleinere organisaties over de wijze waarop IT-beveiliging (technisch en organisatorisch) een onderscheidende factor kan zijn in de markt en in de bedrijfsvoering. Hij is bereikbaar op e.j.mellink@more-secure.nl

Contact

More-Secure BV
Da Costalaan 14
3767GH Soest
T: +31 (0)6 5357 9338
F: +31 (0)35 524 7587
E: info@more-secure.nl
W: www.more-secure.nl