De strijd tegen spam: challenge-response-systemen

In de strijd tegen spam kunt u werken met een spamfilter om spam te scheiden van uw 'echte' post, maar een relatief nieuw systeem is het zogenaamde challenge-response-systeem. Antispamsoftware die op deze manier werkt, beschouwt elk binnenkomend mailtje bij voorbaat als spam totdat het tegendeel bewezen is. Fabrikanten zeggen dat het 100% waterdicht is. Dat is wat rooskleurig. Er kleven ook nadelen aan dit systeem.

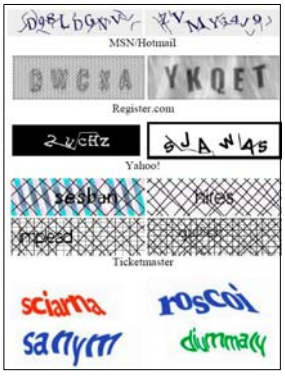
Wat is challenge-response?
Een challenge-response-systeem is een vorm van authenticatie. Het idee achter het challenge-response-systeem kent u al van telebankieren. De bank laat u een code zien (de challenge) die u op een apparaatje van uw bank moet intikken. Dit apparaatje geeft vervolgens een code terug die u weer terugzendt aan de bank (de response). De bank weet dan dat u inderdaad degene bent die u zegt te zijn.

Traditioneel spamfilter

Veel mensen hebben een conventioneel spamfilter op hun computer. Dit spamfilter gaat bij elk binnenkomend mailtje na of het om spam gaat of niet. Dat doet het filter aan de hand van diverse criteria. Het nagaan van kenmerkende woorden in de e-mail is de bekendste vorm van filtering, bijvoorbeeld 'erectie' en 'Viagra'. U kunt als gebruiker het spamfilter laten leren van zijn fouten, bijvoorbeeld door regelmatig aan te geven dat een mail die het filter heeft onderschept toch geen spam was of andersom. Het filter wordt hierdoor intelligenter en gaat steeds beter zijn werk doen. Voorbeelden van goede en gratis spamfilters zijn te vinden op www.spamfighter.com en www.spamexperts.com.

Challenge-response-systeem

Een spamfilter op basis van het challenge-response-systeem doet zijn werk heel anders. Een cr-systeem verklaart elk mailtje van een onbekende bij voorbaat tot spam totdat het tegendeel bewezen is. Het cr-systeem stuurt meteen een bericht terug naar de onbekende afzender met daarin een plaatje met schots en scheef geplaatste cijfers en letters (de challenge). Pas als de afzender de code goed overtypt en terugstuurt (de response) zal het cr-systeem de afzender als betrouwbaar registreren en voortaan e-mail van deze persoon doorlaten. Het gebruik van dergelijke plaatjes voor authenticatie noemt men Human Interaction Proof (HIP).



Voorbeelden van Human Interaction Proof (HIP), een authenticatietechniek die ook gebruikt wordt op websites, bijvoorbeeld bij het aanmaken van een account, het aanmelden van een hyperlink of het achterlaten van een bericht in een gastenboek.

De gedachte achter deze manier van authenticatie door een cr-systeem is dat iemand die spam verstuurt dergelijke plaatjes niet zal overtypen en terugsturen. Sterker, vaak wordt spam verzonden via zogenaamde spamrobots en die kunnen dit soort plaatjes niet zomaar lezen. In principe hoeft uw relatie maar één keer zo'n challenge te beantwoorden. Is dat eenmaal gebeurt dan zal het cr-systeem mail van uw relatie voortaan doorlaten.

Bij een cr-systeem kunt u meestal zelf een witlijst aanleggen van relaties (lees: e-mailadressen) die u bij voorbaat vertrouwt. Daarbij kunt u ook volstaan met alleen het gedeelte na het apenstaartje. Ofwel, alle mail vanaf bijvoorbeeld @uwprovider.nl wordt dan door het cr-systeem bij voorbaat vertrouwd en doorgelaten. Dat is vooral handig bij nieuwsbrieven. Die worden vaak automatisch verzonden door computers. Deze computers zouden niets kunnen met een challenge die ze van uw cr-systeem terug zouden krijgen.

Iets mooier dan de realiteit
Hoewel het cr-principe een interessante techniek is die zich hopelijk verder zal ontwikkelen, kleven er ook wel bezwaren aan.

- Het per se moeten beantwoorden van een challenge door uw relatie voordat deze u kan mailen, is vervelend voor iemand die u kent en komt zelfs wantrouwend over. Sommige mensen zullen niet eens goed begrijpen wat er van hen verlangd wordt en de challenge niet beantwoorden of als iets 'SPAM-achtigs' wegdoen. De kans op dit laatste neemt toe als een Engelstalig cr-systeem de challenge heeft verstuurd.

- Het feit dat mailtjes pas binnenkomen als de afzender de juiste letter- en cijfercode heeft terug gestuurd, kan ertoe leiden dat belangrijke berichten vertraagd in uw mailbox komen. Dat kan in het zakelijke verkeer zelfs geld kosten.

- Als u zich abonneert op een nieuwsbrief moet u zelf zorgen dat het e-mailadres op de witlijst komt. Doet u dat niet dan is er een reële kans dat de nieuwsbrief u niet bereikt.

- Heeft u een domein zoals @uwprovider.nl aan uw witlijst toegevoegd dan hangt een nieuw probleem in de lucht. Immers, spammers verzenden niet zelden e-mail waaraan zij als afzender volstrekt willekeurige namen en e-mailadressen koppelen. Zo kan het gebeuren dat ook spam verzonden wordt dat eindigt op @uwprovider.nl. U snapt het al, deze spam passeert ongestoord uw cr-systeem, omdat u @uwprovider.nl op de witlijst had gezet.

- Afzenders kunnen een nieuw e-mailadres in gebruik nemen. U raadt het: uw cr-systeem kent het nieuwe e-mailadres niet en van het een op het andere moment krijgt u van uw relatie geen e-mail meer totdat deze opnieuw een challenge van uw cr-systeem heeft beantwoord.

- Ook mensen die u een digitaal kaartje sturen via een website kunnen hun wens beter op een andere manier overbrengen. Immers, uw cr-systeem kent de afzender niet (vaak een e-mailadres dat eindigt op de domeinnaam van de betreffende kaartjeswebsite) en een bevestiging zit er ook niet in, omdat de betreffende website wel wat anders te doen heeft dan challenges beantwoorden.

- Stel: Piet en Linda wisselen voor het eerst elkaars e-mailadressen uit. Piet stuurt Linda daarop een mailtje. Linda blijkt echter ook een cr-systeem te gebruiken dat vervolgens een challenge verstuurt naar Piet. Omdat Piets cr-systeem Linda ook nog niet kent, stuurt deze weer een challenge terug naar Linda enzovoorts. Goede cr-systemen vangen dit scenario op door iedereen aan wie in dit geval Piet een mailtje stuurt direct op de witlijst te zetten. Daar zit ook een nadeel aan: als Piet zonder dat hij dat weet een antwoordformulier op een malafide website invult en verstuurt, komt dat e-mailadres in de witlijst te staan en komt spam vanaf die malafide website voortaan direct binnen.

- Een probleem van geheel andere orde kan zich voordoen als een spammer honderdduizenden spammailtjes verzendt met als gefingeerde afzender een e-mailadres dat eindigt op @uwprovider.nl. Probleem één is dat u deze mail binnenkrijgt, want u had @uwprovider.nl immers op uw witlijst opgenomen. Erger is het als andere gebruikers van

een cr-systeem dat niet hebben gedaan. Al die cr-systemen gaan massaal een challenge verzenden naar, u raadt het al, @uwprovider.nl. De computers van uw provider worden zwaar belast door alle deze challenges per mail en de server dreigt op hol te slaan wat hetzelfde effect heeft als een denial-of-service-aanval (meer uitleg op nl.wikipedia.org/wiki/Denial-of-Service). Het is niet ondenkbaar dat uw provider daardoor bereikbaarheidsproblemen krijgt waar u op uw beurt weer last van heeft.

- Mensen die blind of slechtziend zijn gebruiken software die mailtjes voorleest of omzet in braille. Een cr-systeem dat een challenge verzendt in de vorm van een plaatje (HIP) is voor hen een probleem. Zij kunnen mogelijk niets met deze challenge met als gevolg dat hun e-mail niet aankomt bij de geadresseerde.

- Uit wetenschappelijk onderzoek (www.ceas.cc/papers-2005/160.pdf) blijkt dat computers steeds beter in staat zijn om plaatjes met een cijfer- en lettercombinatie te interpreteren. Het lijkt dus een kwestie van tijd eer de spammer in staat is om automatisch een challenge te beantwoorden.

- Naast een lokaal cr-systeem dat op uw eigen computer zijn werk doet, bestaan ook cr-systemen op afstand, bijvoorbeeld ergens op een webserver. Afzenders die nog niet op uw witlijst staan moeten een webpagina bezoeken waar ze hun naam, e-mailadres én de reden waarom ze u willen mailen moeten invullen. Deze methode is ronduit onvriendelijk.

CONCLUSIE

In de strijd tegen spam zijn cr-systemen absoluut een interessant wapen. Er kleven echter ook bezwaren aan die iedereen voor zichzelf moet beoordelen. Verder zit er kwaliteitsverschil tussen het ene en het andere cr-systeem. Geen enkele fabrikant kan volhouden dat het 100% waterdicht is. Alleen al het feit dat spammers hun technieken voortdurend verbeteren geeft aan dat elk type spamfilter, ook het cr-systeem per definitie achter de feiten aan loopt. 100% waterdicht is onmogelijk.

Is uw interesse gewekt? U kunt sommige cr-systemen gratis testen:

XToMe: www.xtome.com/nl/ (Nederlandstalig en gratis “single user licentie”)
emailAI: www.spamresearchcenter.com (Eng.)
Spam Arrest: www.spamarrest.com (30 dagen trial - Eng.)

Bronnen:

- www.nrc.nl/krant/article60402.ece/Het_laatste_idee_tegen_spam
- linuxmafia.com/faq/Mail/challenge-response.html
- www.molensky.com/aboutme/antispam.php
- www.pcmweb.nl

Meer informatie:

- Een overzicht van de gangbare methoden in de spambestrijding (PDF-document)
- www.nrc.nl/krant/article77112.ece/Mail_versturen_Dat_is_dan_tien_seconden
- research.microsoft.com/research/sv/PennyBlack/spam-com.html