Vleeswaren

Frank Brokken
f.b.brokken@rc.rug.nl

ICT-security

Frank Brokken is security manager bij het RC. Met het instellen van deze functie probeert de RUG het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen. In zijn column houdt Frank ons op de hoogte van de stand van zaken met betrekking tot zijn missie.

Onlangs kreeg ik een e-mail waarin onder meer het volgende werd geschreven:

> *Leuk van je te horen, al was het maar per circulaire. Ik wou je in deze functie ook even melden dat ik als oprit-gebruiker geen last heb gehad van virussen waarover allerlei vrienden recentelijk in paniek raakten.*
> *Ik dacht: Frank waakt over mij. Ik neem ook aan dat je de meeste junkmail tegenhoudt....*

In deze Pictogram-bijdrage ga ik niet (nogmaals) in op bescherming tegen virussen: ik neem aan dat het belang van een goede virusscanner en het up-to-date houden van de door de scanner gebruikte database zo langzaamaan genoegzaam bekend is.

Interessant is de telkens weer oplaaiende discussie over 'junk mail' (ook wel 'spam' genoemd). Naar verluid heeft spam z'n naam te danken aan het blikje 'lunchmeat' dat op grote schaal in de VS verkrijgbaar is. Veel vlees is 't niet, maar 't is redelijk acceptabel als voeding tijdens een meerdaagse trektocht in woestijngebieden, onder andere omdat 't spul nogal zout is, en je zo je zoutniveau weer op peil krijgt. Buiten deze situatie zou ik er niet aan denken om spam te consumeren, en zo gaat 't ook met veel mensen die spam- (of junk-) mail ontvangen.

Filteren

De afzender van genoemd e-mail fragment schreef: `Frank waakt over mij...'. Ik voel me natuurlijk gevleid, maar in dit geval is 't niet terecht. Spam heeft niet zoveel te maken met 'security'. In het algemeen wordt gesteld dat ICT-beveiliging zich moet richten op het in stand houden van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie die in ICT-systemen is opgeslagen. Voor zover ik kan overzien, heeft spam geen invloed op deze doelstellingen van ICT-security. Wat niet wegneemt dat het irritant is om keer op keer over ongevraagde onderwerpen e-mail te ontvangen.

Centraal filteren lukt niet goed: het volume is te groot. Bovendien kan een filter niet met zekerheid aangeven of e-mail al dan niet spam is, dus alle gefilterde mail zou ook nog eens moeten worden bewaard, voor het geval dat een niet-spam mail abusievelijk als spam wordt geclassificeerd.

Het is echter redelijk goed mogelijk om zelf binnenkomende mail te filteren op ongewenste kenmerken: ongewenste e-mail adressen of domeinen, ongewenste *subject headers*, etc.. Ik hanteer zo'n procedure nu al een paar jaar, en na een beginfase, waarin het filter moest worden voorzien van ongewenste e-mail adressen, e-mail domeinen en e-mail subject headers heb ik nu een redelijk stabiele toestand bereikt: misschien dat ik eens per week een nieuw element aan 't filter

moet toevoegen, maar er gaan ook weken voorbij waarbij dat niet nodig is.
Het resultaat van deze inspanning is dat ik vrijwel geen spammail meer in mijn mailbox aantref. Alle mail die wordt gefilterd wordt wel bewaard, en op dit moment zitten in mijn van spam verdachte mailbox 15 mailtjes. Da's dan vanaf vanochtend 9:00 uur (en 't is 11:00 uur terwijl ik dit schrijf):

Subject: AEV News n.567 ..... Energya Console
Subject: Primera
Subject: Jan, 08 1998
Subject: =?ISO-8859-3?B?ZnJhbmssSXMgZXZlcnl0aGluZyBPSz8g?=
Subject: Try Coral Calcium Risk Free
Subject: Re: Here is that sample
Subject: Get into that summer look,start now
Subject: Come see me do it all on camera!
Subject: Prescriptions online without a doctor visit
Subject: Prescriptions - Free Consultations!
Subject: new email address
Subject: new contact info
Subject: Let Us Save You Money On Your Merchant Account qpyqlt
Subject: Cash paid to everyone, no sponsoring
Subject: 0.54534

Deze troep wordt nu ongelezen verwijderd: niets wijst erop dat hier foute positieven bij zitten (dat wil zeggen: geen spammail). Ook niet de e-mail met het onderwerp 'new email address': ik ben bereid ongelezen aan te nemen dat deze mail ook spam is. Mocht dat onverhoopt niet het geval zijn, dan kan de bonafide eigenaar van het e-mail adres mij ook wel op een andere manier bereiken.
Mijn mailfilter is een echt filter: voordat inkomende e-mail in mijn mailbox terecht komt, moet de mail door het filter. Het filter besluit of de mail geaccepteerd wordt dan wel terzijde wordt gelegd in de mailbox met vermoedelijke spam. Mijn spamfilter is overigens beschikbaar voor eventuele geïnteresseerden. Het vereist dus dat het filter tussen de binnenkomende mail en de inkomende mailbox kan worden geïnstalleerd.

Fight spam

Er zijn meer agressieve manieren om spam te bestrijden: Ga bijvoorbeeld naar **www.google.nl**, en zoek naar 'fight spam'. Daarnaast is Europese wetgeving in aantocht die spam illegaal moet maken. Wellicht helpt dat, na verloop van tijd.
Hoewel spam niet echt een 'security issue' is, is het een onderwerp dat naar de mening van velen op z'n minst aan 'securiy' is gerelateerd. Ik deel die mening niet, maar zie ook wel dat spam voor veel mensen een irritant probleem is. Daarom speel ik de bal bij dezen een beetje terug: ik wil iedereen die een goede, werkzame oplossing voor het spam-probleem heeft (of denkt te hebben) uitnodigen om de voorgestelde oplossing bekend te maken op: **www.rug.nl/security/award** (Klik 'Deelnemersformulier').
Met uw oplossing maakt u ongetwijfeld een goede kans op het winnen van de Annual Security Award 2003-2004.

Frank B. Brokken

(Verwerkt alleen spam tijdens vakanties)