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

Overpeinzingen ten aanzien van security

Frank Brokken is security manager bij het CIT. 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.

Heeft u zich wel eens afgevraagd wat 'security' eigenlijk is? De Webster geeft de volgende omschrijving van security:

1. The state of being or feeling secure.
2. Freedom from fear, care, danger, doubt or anxiety.
3. Protection or defense against attack, interference, espionage etc.

Safe of secure?

'Safe' is gerelateerd aan 'safety', maar heeft iets meer betrekking op de toestand volgend op een onveilige situatie. De Webster zegt bijvoorbeeld:

- Having escaped danger.
- No longer dangerous.
- Taking no risk, cautious (als een persoonseigenschap).

Dus: 'The engines of my aircraft failed and we made an emergency landing. Fortunately we're all safe.' (foto).

Er is dan ook geen 'safety manager' maar een 'security manager'; er is geen 'safety kernel group' maar een 'security kernel group'. Er zijn overeenkomsten tussen 'safety' en 'security'. In de Webster wordt bij de omschrijving van 'safe' 'secure' genoemd en omgekeerd wordt in de beschrijving van 'secure' 'safe' genoemd.

Schijnveilig

De eerste definitie van 'security', 'the state of being or feeling secure' is een interessante omschrijving. Wanneer we in 'a state of feeling secure' zijn, dan doet dat direct denken aan schijnveiligheid. We *voelen* ons veilig, maar we *zijn* het niet. Die situatie doet zich vaak voor:

- We versturen vertrouwelijke e-mail en denken dat die informatie alleen bij de ontvanger terecht komt.
- We kopen een boek bij een internetwinkel, vullen op een webpagina het nummer van onze creditcard in, en denken dat die gegevens alleen door de internetwinkel wordt gezien.
- We zijn ons bewust van de risico's die we lopen en zorgen er voor dat we creditcard-gegevens alleen invullen als we een verbinding maken met een 'https'-site.
- We gebruiken alleen onze eigen computer om vertrouwelijke informatie vanaf te versturen en denken dat we op die manier veilig zijn.

In al deze situaties gaat het om schijnveiligheid. Oh? U verstuurt geen vertrouwelijke e-mail? U gebruikt uw computer nooit voor vertrouwelijke handelingen? Tja, het zou kunnen.... Maar de RUG kan daar best eens anders over denken. De RUG heeft een Acceptable Use Policy waarin staat dat u zelf verantwoordelijk bent voor het veilig gebruik van de RUG-gerelateerde IT-faciliteiten.

Verplichte geheimhouding

Ook op andere plaatsen (bijvoorbeeld in de CAO) is vastgelegd dat u geacht wordt vertrouwelijk om te gaan met de informatie die u uit hoofde van uw functie krijgt. De CAO stelt zelfs dat u verplicht bent tot geheimhouding:

Artikel 1.16, lid 1: De werknemer is verplicht tot geheimhouding van hetgeen hem uit hoofde van zijn functie ter kennis komt, voor zover die verplichting uit de aard der zaak volgt of hem uitdrukkelijk is opgelegd. Deze verplichting geldt ook na beëindiging van het dienstverband. Nou, mooi niet dus. Zolang u e-mail over uw werk gewoon maar blijft versturen, overtreedt u mogelijk de AUP maar zeker ook de CAO.

Het kan ook anders. E-mail kan al sinds jaren op vertrouwelijke wijze worden verstuurd. Op de security-website van de RUG leest u hoe. Op die manier kan niet alleen worden voorkomen dat derden de beschikking krijgen over de verstuurde informatie, maar kan ook worden geverifieerd dat de afzender daadwerkelijk de afzender is van de verzonden e-mail. Punt 2 van de definitie van 'security' sluit daar mooi op aan: 'Freedom from doubt', in dit geval de twijfel of de afzender eigenlijk wel de afzender is.

Het signeren van e-mail is een kleine moeite en het College van Bestuur van de RUG (CvB) heeft dan ook besloten dat alle officiële mail door het CvB binnenkort elektronisch zal worden gesigneerd. Zou goed voorbeeld hier ook goed doen volgen?

Spionage?

Hoe zit dat met het gebruik van die websites? Uiteraard is een http-verbinding even onveilig als e-mail. 'Onveilig' bij http-sites heeft twee kanten. Ten eerste de kant van de lezer, ten tweede de kant van de ontvanger. De lezer die informatie krijgt van een webserver die http-pagina's aanbiedt - zoals het RUG-CMS (www.rug.nl) - heeft geen enkele garantie dat wat de lezer ziet ook datgene is wat de aanbieder (de RUG) beschikbaar wil maken. Alle informatie wordt zonder enige vorm van beveiliging tussen de aanbieder en ontvanger verstuurd en kan daarmee tussentijds worden aangepast.

Kijk nou eens naar punt 3 van de betekenis van 'security': *Protection or defense against attack, interference, espionage etc.* Ach, die spionage zijn we hier geloof ik niet zo bang voor (hoewel... Nee, daar heb ik het later nog wel eens over). Maar die 'protection against interference' is er natuurlijk absoluut niet.

Ook hier geldt: het kan ook anders (alleen nu, anno 2009-2010, nog even niet bij het RUG-CMS). Dat 'anders' heeft te maken met de wijze waarop webservers hun informatie ook kunnen aanbieden: gecertificeerd. Via de Comodo-certificaatautoriteit kan elke RUG-webserver inmiddels (gratis!) worden gecertificeerd. Binnen het Nederlandse hoger onderwijs zijn inmiddels ruim 1000 webservers gecertificeerd, en binnen de RUG zijn dat tientallen. Wanneer we verbinding maken met zo'n gecertificeerde webserver, dan staat er 'https' in plaats van 'http' in de adresbalk, bijvoorbeeld https://mijn.img.nl/internetbankieren.

Cybersafe yourself

Certificering helpt tegen 'interference'. Maar of het ook tegen 'attack' helpt, is een beetje afhankelijk van onszelf. In ieder geval is het verstandig om de eerste keer dat een gecertificeerde website wordt opgevraagd eens te kijken of er wel een verbinding is gemaakt met de bedoelde website (klik op het slotje).

Ga pas verder wanneer uit het certificaat blijkt dat er inderdaad een verbinding is met de bedoelde website en niet met een fake-website die vrijwel dezelfde naam heeft (bedenk dat de 'm' en de 'n' op het toetsenbord naast elkaar liggen; de hierboven met opzet gemaakte typefout 'img' in plaats van 'ing' is snel gemaakt).

Als alles klopt hebben we ook een redelijke bescherming tegen 'attack'. Redelijk, maar geen perfecte bescherming. Nog afgezien van de vraag of de bank haar interne IT-beveiliging op orde heeft: hoe zit dat met onze eigen IT-beveiliging? En we zijn weer terug bij af: 'Security is the state of feeling secure'.

Uiteindelijk betekent het dat we zelf alert moeten zijn op mogelijk misbruik van vertrouwelijke informatie. Controleer de echtheid van certificaten, zorg voor een computer die up-to-date is voor wat betreft software en beveiligingsmaatregelen, en 'cybersafe yourself'. Meer security-tips leest u op deze themawebsite van SURFnet.

CYBERSAVE YOURSELF CSY

Frank Brokken
(Voelt zich zeer veilig)

- Acceptable Use Policy: **www.rug.nl/cit/security/aup**
- CAO Nederlandse Universiteiten 1 september 2007 tot 1 maart 2010: **www.ru.nl/aspx/download.aspx?File=/contents/library/71/cao2007-2010.pdf**
- Informatie over het vertrouwelijk versturen van e-mail: **www.rug.nl/cit/security/adviezen/email**
- Comodo-certificaatautoriteit: **www.comodo.com**
- Cybersafe yourself is een initiatief van SURFnet: **www.surfnet.nl/nl/thema/cybersafe**