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

Het moet werken

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.

Gebruikers van IT-voorzieningen vinden primair, zo blijkt uit de onlangs uitgevoerde gebruikersenquête, dat IT-voorzieningen 'moeten werken'. Dat is natuurlijk een geweldige bevinding...

"Met de helpdesk, zegt u het maar..."
"Hij doet 't niet."
"Kunt u uw probleem misschien iets nader specificeren?"
"Ja, ik heb net een computer gekocht en druk op de 'aan'-knop, en hij doet 't niet."
"Aha. En u heeft de computer net gekocht?"
"Ja, vanmorgen gekocht, uitgepakt, maar hij doet 't niet."
"Zit de stekker wel in het stopcontact?"
"Euhh... nee..."
"Probeert u dat eens, waarschijnlijk werkt-ie dan wel."

'Het moet werken'. Natuurlijk een begrijpelijke en veelal terechte wens, maar soms is het handig wanneer de gebruiker zelf ook even nadenkt. Vlak voordat deze Pictogrambijdrage werd geschreven, werd bekend dat de voicemail van veel mobiele telefoons die door de overheid zijn verstrekt eenvoudig door derden konden worden afgeluisterd.

Gebruikersgemak

Terzijde vraag je je dan natuurlijk af of dat ook heeft bijgedragen aan het mislukken van de helikopterevacuatiemissie in Libië, maar afgezien daarvan: hoe is het mogelijk dat zoiets gebeurt?

"Dag Vodafone, met Mark Rutte. Waarom kan iedereen zomaar mijn voicemail afluisteren?"
"Ja meneer Rutte, wij begrijpen uw vraag, maar dat komt doordat wij de afweging hebben gemaakt dat gebruikersgemak vóór beveiliging gaat."

Oops... Maar ook werd er door Vodafone fijntjes op gewezen dat in de handleiding wordt benadrukt dat een eigen pincode dient te worden gekozen. Tja, RTFM noemen we dat, 'Read The Fucking Manual' (**http://en.wikipedia.org/wiki/RTFM**). Maar helaas, niet veel mensen doen dat, want het 'gebruiksgemak' prevaleert, nietwaar?

Gelukkig geldt dat niet voor iedereen en zijn er nog steeds mensen die zelf een beetje nadenken, en daardoor dit soort onwenselijke situaties voorkomen. Een voorbeeld bij het Vodafone-incident is Fred Teeven, momenteel staatssecretaris van Veiligheid en Justitie. Toevallig? In ieder geval leek hij niet erg onder de indruk te zijn van het Vodafone-beveiligingslek. Hij had TFM wel gelezen en prompt z'n pincode aangepast. Complimenten!

Je ziet hier opnieuw dat beveiliging nauwelijks een technische kwestie is. 'Het moet werken' in beveiligingsland is een kwestie van 'the right stuff' (**http://en.wikipedia.org/wiki/The_Right_Stuff**), maar dan 'tussen de oren': een mentaliteitskwestie. Wie die mentaliteit heeft, verdient een compliment.

Digitale therapie

Dat geldt bijvoorbeeld voor Jos Karssies, studentendecaan bij het Studenten Service Centrum van de RUG. Hij vraagt zich af wat te denken van de manier waarop 'digitale therapie' voor studenten wordt aangeboden.

Een leuk onderwerp, ook al actueel omdat de Eerste Kamer onlangs het Elektronisch Patiënten Dossier naar de prullenmand heeft verwezen. Wat mij betreft voornamelijk 'hoera' vanwege de onvoldoende garanties op vertrouwelijkheid van het materiaal dat daarbinnen zou worden opgeslagen.

De 'digitale therapie' zou met behulp van Blackboard (BB) worden geïmplementeerd. Om verschillende redenen moet je dat natuurlijk niet willen:

- Ten eerste is de verbinding met BB standaard onbeveiligd (mogelijk kan dat anders, maar dat zou moeten worden onderzocht), waardoor in principe iedereen tussen de patiëntcomputer en het BB-systeem kan meeluisteren;
- Ten tweede staat expliciet in het BB-contract dat alle medewerkers van BB wanneer dat naar het inzicht van BB nodig is toegang tot de informatie hebben;
- Ten derde is het nog maar de vraag of het Nederlands recht van toepassing is. Door de RUG is dat wel bedongen, maar of dat elders ook zo is? Maar wat dat betekent in het licht van het vorige punt weet ik niet zo goed....
- Ten vierde heeft BB een opmerkelijk zwakke (slechte?) 'track record' op het gebied van handhaving van de beveiliging van hun product. Kortom: wie allemaal bij de informatie kan, is voor patiënt en therapeut een vraag, maar zeker geen weet.

Jos verdient een compliment omdat hij zich realiseert dat hier vertrouwelijkheid en integriteit issues zijn. Hij blijkt daarmee ook te beschikken over 'The Right Stuff'!

Beveiliging of gebruiksgemak? Een verkeerde vraag. Beide zijn natuurlijk belangrijk. Ik denk wel dat beveiliging uiteindelijk juist leidt tot gebruiksgemak. Maar voordat die idee breed wordt gedragen, zijn we, vrees ik, nog wel even bezig. Goed voorbeeld doet goed volgen, hoop je dan. Helaas ontbreekt dat goede voorbeeld vaak daar waar dat wel zou moeten en kunnen worden gegeven. Daar kan ook weer het nodige over worden geschreven. Maar dat doe ik in een volgende Pictogrambijdrage.

Frank B. Brokken
(niet altijd even gemakkelijk in het gebruik)