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

Vertrouwen

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.

Onlangs werd ik gevraagd aanwezig te zijn bij een bijeenkomst die was gewijd aan privacy. Ik vind dat moeilijk. Privacy is niet mijn terrein. Waar ik me wel mee bezig houd, is - om een bekende Engelstalige afkorting te gebruiken - CIA: Confidentiality, Integrity en Availability. Mogelijk dat confidentiality nauwe banden onderhoudt met privacy, maar daar kun je waarschijnlijk over twisten.

Te vuur en te zwaard

De meeste mensen die ik spreek, vinden overigens wel dat bijvoorbeeld bij medische gegevens vertrouwelijkheid een rol speelt. En artsen verdedigen hun medisch beroepsgeheim doorgaans te vuur en te zwaard. Wat je bij je huisarts zoal opbiecht, hoort de volgende dag niet in de krant te staan. Is dat nou privacy of vertrouwelijkheid?

Ik hou het op vertrouwelijkheid: informatie die tot mijn persoonlijke levenssfeer hoort, wil ik daar graag houden (privacy?) en ik vertrouw erop dat dat zo blijft wanneer ik in een vertrouwelijk gesprek de vertrouwelijke informatie over mijn persoonlijke levenssfeer ventileer. Dat vertrouwen is naïef, dat weet ik ook wel. Maar het voelt zo prettig wanneer je dat vertrouwen koestert.

Valsheid in geschrifte

Onlangs organiseerden we een bijeenkomst over de vertrouwelijkheid en authenticiteit van e-mail. Mijn collega Mark Meinema liet in een overtuigend voorbeeld weer eens zien hoe ongelooflijk eenvoudig het is om e-mail namens iemand anders te sturen. Waarom is het niet vreemd dat dat zomaar kan?

Het antwoord is simpel: ik kan ook zomaar een brief schrijven namens een van mijn collega's. Wanneer ik die brief dan per post bij weer een andere collega laat bezorgen, dan zal de geadresseerde op z'n minst enige tijd veronderstellen dat de brief in feite afkomstig was van de namaakafzender.

Is hier nou sprake van vertrouwelijkheid? Dat is nog niet zo gemakkelijk te beantwoorden. Vertrouwelijkheid heeft te maken met de vraag of anderen dan de bedoelde lezers de brief kunnen lezen. In die zin is er sprake van vertrouwelijkheid, want de brief is verstuurd in een enveloppe.

Voorlopig gaan we er maar even vanuit dat de post de enveloppe niet open stoomt om eens te lezen wat er nu weer wordt verstuurd.

Is er sprake van integriteit? Dat heeft te maken met de vraag of iemand de informatie zou hebben kunnen wijzigen. Opnieuw veronderstellend dat de post niks onbehoorlijks met mijn enveloppe doet, is de integriteit van de brief ook gewaarborgd.

Waar het mis gaat, is bij de authenticiteit: ik pleeg valsheid in geschrifte door mij voor te doen als mijn collega, en schrijf namens hem of haar een brief aan een andere collega. Wordt dat dan niet ontdekt? Niet eenvoudig als ik de bijbehorende handtekening goed kan namaken.

Zo'n enveloppe kan dus nogal wat waarborgen leveren: vertrouwelijkheid en integriteit. Ik kan natuurlijk ook de informatie per briefkaart versturen. Dan is die informatie voor iedereen die de briefkaart in handen krijgt te lezen (geen vertrouwelijkheid) en zelfs te wijzigen (geen integriteit).

Elektronische briefkaart

Laat me even terugkeren naar de e-mail. Iedereen gebruikt e-mail, en bewaart die e-mail doorgaans in zijn/haar computer - mogelijk zelfs in een backup - en hetzelfde geldt voor de ontvanger van de e-mail. Wat gebeurt er eigenlijk wanneer we e-mail versturen? Volgens welingelichte bronnen binnen bijvoorbeeld het UMCG, sturen artsen elkaar regelmatig e-mail, ook over patiënten. Van arts naar arts, dat is natuurlijk binnen de context van Hippocrates (**http://nl.wikipedia.org/wiki/Eed_van_Hippocrates**).

Dat kan goed gaan, maar meestal is dat niet zo. E-mail is niet anders dan het versturen van een briefkaart. Iedereen die de briefkaart in handen krijgt, kan de informatie lezen. Dat kan onderweg, maar ook binnen de computers van afzender en geadresseerde. Een arts die een e-mail verstuurd naar een collega over een patiënt, hanteert de elektronische variant van de briefkaart. Is daar nou sprake van aantasting van onze privacy of niet? Ik vind van wel, vooral omdat het zo niet hoeft te gaan.

Wie vertrouwelijke e-mail wil versturen, moet maatregelen treffen om dat te realiseren. Dat kan door gebruik te maken van versleuteling en een elektronische handtekening. De bijeenkomst met collega Mark Meinema over vertrouwelijkheid en authenticiteit van e-mail was daaraan gewijd. Gezien het gemak waarmee e-mail (en andere informatie) kan worden beveiligd tegen toegang door onbevoegden en gezien het gemak waarmee de authenticiteit van e-mail kan worden geverifieerd, is er geen goed excuus om daar geen gebruik van te maken.

Elektronische handtekening

Het veilig gebruik van e-mail was nog niet zo lang geleden een moeizame zaak. Ik kan me herinneren dat het ten tijde van Pegasus mail erg moeilijk was om e-mail veilig en geauthenticeerd te versturen. Met de komst van Thunderbird en de Universitaire werkplek (UWP) is dat allemaal veel eenvoudiger geworden, en daarop was de bijeenkomst over vertrouwelijkheid en authenticiteit dan ook gebaseerd. Beide zijn goed te realiseren, maar het verhaal rondom authenticatie is wat lastiger goed voor het voetlicht te krijgen.

Ook hier bestaat een duidelijke parallel met het versturen van brieven. De authenticiteit zit in de handtekening, en in sommige situaties moet je je handtekening zelf authenticeren door de handtekening ter plekke te maken en je paspoort of ander identiteitsbewijs te tonen. Zoiets geldt ook voor de 'elektronische handtekening'. Een elektronisch gesigneerde e-mail is nog niet automatisch ook van de kennelijke afzender afkomstig. Dat geldt pas wanneer we de echtheid, de authenticiteit, van die handtekening hebben geverifieerd.

Uiteraard kan in deze column de ins en outs van het veilig gebruik van e-mail niet uitgebreid worden behandeld. Daarom een overzicht met informatie en een aantal links:

De afdeling Opleidingen van het CIT verzorgt regelmatig korte trainingen over veilig e-mailgebruik (de PGP-cursus, zie de cursus 'Security: Gegevensbeveiliging' op **www.rug.nl/cit/onderwijs/rooster**);

Op verzoek wordt een promotiebijeenkomst samen met Mark Meinema georganiseerd;

Een toelichting over het gebruik van PGP in combinatie met Thunderbird is te vinden op **www.rug.nl/cit/security/adviezen/email**.

En uiteraard, voor alle verdere vragen op het gebied van veilig e-mailen kan altijd contact worden opgenomen met

Frank Brokken
(voor alle authentieke adviezen)