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

Dropbox

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.

"Is Dropbox veilig?" zo vroeg mijn collega Marijke Verheij mij onlangs. Tja... "Voor mij niet", was mijn eerste reactie. Ik ben dol op drop en de dropbox is leeg voor je 't weet.

Maar dat was uiteraard niet wat ze bedoelde. 'Dropbox' is een systeem om informatie 'in de cloud' beschikbaar te maken voor anderen, die via een toegangscode in de gelegenheid worden gesteld die informatie dan op hun computer beschikbaar te maken, te 'downloaden', in goed Nederlands.

Uit de beschrijving die Dropbox (**www.dropbox.com**) zelf geeft:

Dropbox makes sharing so easy that you'll be amazed at the things you can do. Invite your friends, family and teammates to any folder in your Dropbox, and it'll be as if you saved that folder straight to their computers. You can send people links to specific files in your Dropbox too. This makes Dropbox perfect for team projects, sharing party photos with friends, or recording your band's new album.

'In de cloud' beschikbaar... Dat betekent zoveel als: maak je nou maar geen zorgen waar die informatie is, de informatie ís er gewoon. In 't Internet, en wij (= Dropbox) zorgen er voor dat 't altijd en overal beschikbaar is.

Nou ja, bijna altijd en overal. Om bij de informatie te kunnen moet je natuurlijk wel Internet-toegang hebben, maar met uitzondering van trips naar "the middle of nowhere" is dat eigenlijk altijd wel 't geval, niet?

Dropbox zelf geeft aan voorzichtig om te gaan met de haar toevertrouwde informatie:

By using our Services you provide us with information, files, and folders that you submit to Dropbox (together, "your stuff"). You retain full ownership to your stuff. We don't claim any ownership to any of it. These Terms do not grant us any rights to your stuff or intellectual property except for the limited rights that are needed to run the Services, as explained below.

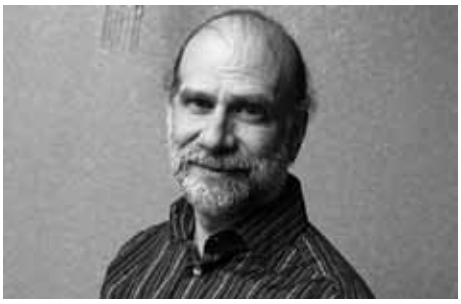
Op die 'limited rights' kom ik nog terug. Het gebruik van Dropbox op zich voldoet aan de verwachtingen die passend zijn bij een systeem als Dropbox. De verbinding met Dropbox is een https verbinding, en de installatie van het certificaat is, volgens de tests uitgevoerd door **www.networking4all.com,** up-to-date.

De vraag is nu of er een addertje onder het gras zit. Om te beginnen: hoe zit dat met die “limited rights needed to run the service”? Zoals dat zo vaak het geval is met ‘cloud services’ is het moeilijk te doorgronden wat nu eigenlijk wel en niet mag. Da’s logisch: in de ‘cloud’ is het zicht tot praktisch nul gereduceerd (een situatie die we ook wel kennen als dichte mist).

In plaats van de lange, lange tekst van de overeenkomst die we kennelijk met Dropbox aangaan wanneer we gebruik willen maken van haar diensten grondig door te spitten kunnen we ook eens kijken wat Dropbox zelf aangeeft wat we in ieder geval moeten toestaan. Het hoofdkantoor van Dropbox is in San Francisco, en dat betekent dat het Amerikaans recht van toepassing is. Denk aan de “Patriot Act” bij het lezen van het volgende:

Compliance with Laws and Law Enforcement Requests; Protection of Dropbox’s Rights. We may disclose to parties outside Dropbox files stored in your Dropbox and information about you that we collect when we have a good faith belief that disclosure is reasonably necessary to (a) comply with a law, regulation or compulsory legal request; (…) If we provide your Dropbox files to a law enforcement agency as set forth above, we will remove Dropbox’s encryption from the files before providing them to law enforcement. However, Dropbox will not be able to decrypt any files that you encrypted prior to storing them on Dropbox.

Dat lijkt me duidelijk: het gebruik van Dropbox is níet veilig, wanneer je onder ‘veilig’ rekent dat alleen personen toegang tot de informatie mogen krijgen die daartoe door de eigenaar van de informatie zijn geautoriseerd. Die eis is overigens een van de hoekstenen van wat onder ‘beveiliging’ wordt verstaan, en de faciliteiten die door Dropbox worden geboden dienen om die reden dan ook als onveilig te worden beschouwd.



Maar Dropbox zelf geeft ook een oplossing: wie gevoelige informatie heeft (en de eis om vertrouwelijk om te gaan met bedrijfsinformatie geldt a priori voor ambtenaren) dient zijn/haar spulletjes niet gedachteloos op Dropbox te plaatsen. Wie gevoelige informatie via Dropbox wil delen met anderen doet er goed aan (zoals Dropbox zelf suggereert) om de informatie eerst zelf te versleutelen en pas daarna bij Dropbox onder te brengen. Hoe je versleutelt is weer een ander verhaal. Daaraan heb ik al bij herhaling Pictogrambijdragen gewijd. De korte samenvatting is: gebruik GPG of S/MIME certificaten (**www.rug.nl/cit/security/adviezen/email**) of gebruik een versleutelingsprogramma zoals crypt (**www.wikipedia.org/wiki/Crypt (Unix)**.

Tenslotte: Bruce Schneier geeft in zijn blog eigenlijk hetzelfde advies: zodra de informatie het niveau van de vakantiefoto’s passeert, geef de verantwoordelijkheid voor de beveiliging van je informatie dan niet uit handen, maar zorg zelf voor een afdoende versleuteling. De blog verwijst ook naar een interessant artikel in ‘The Economist’. Zeker de moeite van ‘t lezen waard.

Frank B. Brokken
Verkiest, als oldtimer, andere drop.

- Het blog van Bruce Schneier:
  www.schneier.com/blog/archives/2011/05/dropbox_securit.html