Matto Fransen / m.j.fransen@rug.nl

Tablets

Matto Fransen is security manager bij het CIT. Met deze functie probeert de RUG het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen.

Cloudproviders maken het werken op mobiele apparatuur zoals tablets en smartphones steeds aantrekkelijker. Denk aan het gebruik van Google e-mail en de calender, maar ook aan Google Docs. Voorheen was het gebruik van de universitaire huisstijl nog lastig, maar inmiddels is dit ook in de Google Docs-omgeving beschikbaar.

Wie privé een tablet aanschaft, kan daarbij van de universiteit een tegemoetkoming in de kosten krijgen. Het gevolg is dat steeds meer medewerkers een privé-tablet voor het werk inzetten. Voor elk mobiel apparaat, of dit nu een laptop, een tablet of een smartphone is, gelden een aantal veiligheidseisen.

De toegang tot het apparaat is beveiligd, bijvoorbeeld met een wachtwoord of vingerafdrukherkenning. Dit is meestal vrij eenvoudig in te stellen. De opslag op het apparaat is versleuteld. De verschillende besturingssystemen bieden allen de mogelijkheid tot sterke encryptie, maar veelal wordt de opslag pas versleuteld nadat de gebruiker dit activeert. Kies waar mogelijk altijd voor two-factor authentication.

Cloud applicaties

Bedenk dat veel cloudapplicaties al snel vertrouwelijke informatie bevatten. Het is heel prettig om altijd en overal, onderweg en thuis, bij de e-mail te kunnen, maar waar e-mail is, is vertrouwelijke informatie. De Autoriteit Persoonsgegevens ziet bijvoorbeeld e-mailadressen, ook als deze zakelijk zijn, als persoonsgegevens. Het gebruik van e-mail op een mobiel apparaat leidt vanzelf tot een gevuld adresboek, terwijl ook inhoud van de e-mailberichten soms vertrouwelijk is.

Verder biedt toegang tot uw Google e-mailaccount ook vaak toegang tot uw Google Drive. Verlies van een mobiele telefoon of tablet kan daardoor vergaande gevolgen hebben. Om dit risico zo klein mogelijk te houden, is het raadzaam voor elk apparaat en applicatie, waar mogelijk, een device specific wachtwoord in te stellen. Hierdoor kan bij verlies van het apparaat snel voor het ene specifieke apparaat de toegang tot bijvoorbeeld Google Mail, Google Calendar en Google Drive worden geblokkeerd.

Apparaat specifieke wachtwoorden

Het instellen van een device specific wachtwoord vereist bij Google wat laveren door de verschillende schermen. Start in de mail bij 'Settings', ga door naar 'Accounts', en kies daar voor 'Google Account settings', en dan voor 'Sign-in & security'. In het blok 'Password & sign-in method' is tenslotte de menukeuze 'app passwords' te vinden.

Voeg hier een apparaat toe, bijvoorbeeld uw tablet, door onderin bij 'Select app' bijvoorbeeld Mail te kiezen en bij 'Select device' een apparaat te selecteren, of voer zelf de naam van een apparaat in.

Via het knopje 'Generate' wordt een nieuw wachtwoord gegenereerd, dat specifiek voor dat apparaat bedoeld is. Dit wachtwoord neemt u over in de account-instellingen op dat specifieke apparaat. Google toont het wachtwoord daarna niet meer, alleen het bestaan er van.

Het is vooral van belang dat u later nog kunt herkennen, welke apparaten in dit scherm gepresenteerd worden, zodat u, ingeval van nood, snel en zonder twijfel de toegang voor een specifiek apparaat ongedaan kunt maken. Gebruik dus voor u zelf goed herkenbare namen van apparaten.

Vreemde wifi-netwerken

We zijn zo gewend dat we overal netwerk hebben, dat we er nauwelijks nog bij stil staan wie de netwerkverbinding aanbiedt en hoe veilig die is. Binnen de universiteit is overal draadloos wifi-netwerk aanwezig. Aanmelding op dit netwerk gaat via Eduroam, een fantastische voorziening.

Wie eenmaal het gebruik van Eduroam op zijn laptop, tablet of smartphone heeft geconfigureerd, kan binnen heel Europa, maar soms ook ver daarbuiten, moeiteloos gebruik maken van veilige, lokale educatieve draadloze netwerken.

Buiten Eduroam wordt het moeilijker. Het is makkelijk om de naam van een wifi-netwerk te fingeren en we weten nooit wie er meeluisteren. Gebruik daarom bij voorkeur geen publieke netwerken en kies liever voor de 3G- of 4G-verbinding van de telefoonprovider.

Melden verlies of diefstal

Wanneer uw laptop, tablet of smartphone verloren of gestolen is en dit apparaat gaf toegang tot RUG-gegevens, zoals bijvoorbeeld uw e-mail of agenda, meld dit dan altijd. Ook wanneer het een privé-apparaat betreft. U meldt dit per e-mail op het centrale meldpunt voor (vermoedelijke) datalekken: **cert@security.rug.nl.**