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

Dataveiligheid

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

Cybercrime is big business. Ransomware, phisingmails, virussen en malware, backdoors- en man-in-the-middle-attacks, begrippen die de meesten van ons wel eens voorbij hebben zien komen. Het zijn zo maar wat voorbeelden die allemaal onderdeel zijn van het arsenaal en het verdienmodel van de cybercrimineel. Als computergebruiker loop je heel wat risico's.

Maar wie kan het nog, werken zonder computer, laptop of tablet? We zijn allemaal afhankelijk geworden van digitale informatie. Wanneer we niet meer bij onze gegevens kunnen, of wanneer het informatiesysteem 'uit de lucht is', dan valt er eigenlijk ook niet meer te werken. We willen dus op die computers en systemen kunnen vertrouwen, ze moeten het altijd doen en veilig en betrouwbaar zijn.

Gereedschappen

We willen niet dat onbevoegden onze gegevens kunnen inzien. Ook willen er op kunnen vertrouwen dat de informatie die uit onze systemen komt, klopt. Maar wie moet daar eigenlijk voor zorgen?

De fabrikant moet voor veilige hard- en software zorgen, en de IT-beheerders voor goede back-ups en goed beheer. Maar ook de gebruikers hebben een belangrijke rol in de dataveiligheid.

Computers, laptops, tablets, informatiesystemen, het zijn allemaal gereedschappen. Iedere klusser weet, dat de juiste keuze van de meest geëigende gereedschappen voor een klus belangrijk is voor een goed eindresultaat. Zo is het ook met onze ICT. E-mail, ongeacht de

provider of het e-mailprogramma waarin je het mailtje typt, is geen veilig medium. Door sterke encryptie te gebruiken, kun je die veiligheid wel verhogen.

Belangrijke informatiesystemen binnen de universiteit vereisen vaak een sterke tweeweg-authenticatie en een veilige verbinding om toegang te krijgen, maar wanneer je vervolgens de informatie uit zo'n systeem downloadt naar een USB-stick dan is die informatie opeens een stuk minder goed beschermd. Als gebruiker beïnvloed je dus de dataveiligheid, onder andere door de keuze van je tools en van de opslagmethode. Maar staan we daar wel voldoende bij stil?

Updates

We kennen het allemaal wel. Je bent aan een belangrijk stuk bezig, de deadline is al griezelig dichtbij. Met druppels op het voorhoofd vecht je tegen de klok. Opeens krijg je een pop-up melding dat er updates beschikbaar zijn die je moet installeren en daarna moet het systeem herstart worden.

Op zo'n moment ben je even minder goede vriendjes met je systeem en krijg je visioenen over wat je allemaal met de fabrikant zou willen doen. Wie klikt er dan nog op OK? Maar door dat niet te doen, verhinder je misschien een belangrijke update die je systeem moet beschermen tegen een bepaald type ransomware...

Ransomware is malware die alle informatie op je systeem versleutelt. Vervolgens belooft een onbekende persoon dat je bestanden weer

ontsleuteld worden, wanneer je daarvoor het losgeld betaald hebt. Dat betalen gaat via bitcoins, en dan op zo'n manier dat de ontvanger niet te achterhalen is. Of je ook echt weer de beschikking over je bestanden krijgt, en hoelang dat eventueel duurt, dat is maar de vraag.

De klos

Daarom is het ook zo belangrijk nooit gegevens op lokale opslag te zetten. Wanneer je je bestanden op X: of Y: zet, maken zij deel uit van het automatische backup-proces. In zo'n geval is het ook zonder losgeld te betalen mogelijk de bestanden te herstellen en is de ransomware-aanval vooral lastig omdat het veel ergernis, gedoe oplevert en het je veel tijd kost.

Heb je geen backup van je gegevens, bijvoorbeeld omdat je die alleen maar op de lokale schijf van je laptop of op een USB-schijf hebt opgeslagen, dan ben je de klos. Je bestanden zijn weg en het losgeld betalen is geen goed idee, omdat dit vooral een uitnodiging is aan de crimineel om de aanval later nog eens te herhalen. Bovendien is dat geen garantie dat je dan ook echt beschikking over je bestanden terugkrijgt.

Vreemd taalgebruik

Een manier waarop veel malware, inclusief ransomware, bij gebruikers op de computer komt, is via e-mail. Bijvoorbeeld doordat kwaadwillenden je een mailtje sturen met een bijlage (attachment), zoals bijvoorbeeld een Word- of pdf-document. Open je de bijlage, dan merk je misschien niets, maar op de achtergrond is de malware al geïnstalleerd.

Ook kan een mailtje een linkje bevatten naar een website. Klik je daarop, dan installeert die website tijdens het openen malware op je systeem. Vertrouw je een mailtje niet, bijvoorbeeld door de onbekende afzender of vreemd taalgebruik, open dan nooit de attachments en klik nooit op linkjes.

Wachtwoorden

Voor je het weet, heb je bij veel verschillende aanbieders een account, zoals Facebook, LinkedIn, Twitter, Instragram, Pocket, Goodreads, enzovoort. Misschien heb je privé ook nog een of meer mailaccounts, een account bij bol.com of amazon.de en een blog. Of heb je als echte kookfanaat op meerdere receptensites een account.

Bijna wekelijks komt wel weer een onlinedienstaanbieder in het nieuws, omdat die mogelijk gegevens gelekt heeft of dat kwaadwillenden zich toegang tot de gegevens verschaft hebben. Ook worden bestanden met accounts en wachtwoorden op internet gedeeld, soms van een lek van jaren geleden.

Iedere keer blijkt dan dat er nog steeds mensen zijn die op verschillende sites dezelfde gebruikersnaam hebben en hetzelfde wachtwoord gebruiken. Wanneer dat het geval is, levert een gecompromitteerd account op de ene site meteen ook een gecompromitteerd account op een andere site op.

Koekenpan, kameel en stropdas

Het is daarom ook echt belangrijk om voor elke site, voor elk account, een ander wachtwoord te gebruiken. Kies wachtwoorden die voldoende lang zijn, minstens tien tot twaalf karakters lang. Hoe langer, hoe beter. Een lang wachtwoord is een veel beter wachtwoord dan een onleesbare reeks van tekens die moeilijk te onthouden is, maar die maar zeven of acht karakters lang is.

Kies een paar woorden die niets met elkaar te maken hebben, plak ze achter elkaar en verander een paar letters door bijzondere tekens (bijvoorbeeld # of &) en voeg een of meer cijfers toe. Je kunt bijvoorbeeld van de woorden koekenpan, kameel en stropdas en heel sterk wachtwoord maken, door deze achter elkaar te plakken en wat tekens te vervangen. "Koek#npan2kameel5&str0pdas" is echt een veel sterker wachtwoord dan "#4aCfy$q". En ook veel makkelijker te onthouden!

Een zaak voor iedereen

Heb je veel accounts, dan is een wachtwoordmanager een goede oplossing. Dit is een programmaatje dat de wachtwoorden voor je onthoudt. Vaak kun je daarmee ook zonder te typen je wachtwoord invoeren, ook dat helpt weer om de veiligheid te verhogen. Maak er verder een gewoonte van om minstens één keer per jaar je wachtwoorden te veranderen. Bijvoorbeeld rond je verjaardag of in de kerstvakantie. Of prik een dag in maart en kruis die elk jaar op de kalender aan. Als het voor jou maar werkt.

Kortom, dataveiligheid is niet alleen een zaak voor de ICT-specialisten. Hier moeten we met elkaar voor zorgen. Wie met computers werkt, moet goed stil staan bij hoe je met de informatie omgaat. Wat zet je wel en wat zet je niet in een mailtje? Welke informatie kun je wel of kun je niet op een USB-stick zetten? Wanneer en hoe gebruik je encryptie?

Wees voorzichtig met ontvangen e-mail. Verder is het verstandig zo snel mogelijk nadat zij beschikbaar zijn, de updates uit te voeren, ook al komt het je eigenlijk niet goed uit. En kies voor elk account een ander wachtwoord.