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

Baas in eigen pc

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.

Zelf de eigen computer beheren, dat lijkt soms wel aantrekkelijk. Zelf het besturingssysteem kiezen en zelf bepalen welke software wel, en welke niet op het systeem komt. Echter, ieder voordeel heeft zijn nadeel. Wie zelf het computersysteem beheert, moet ook zelf zorgen dat dit systeem veilig is, goed werkt en geen data verloren kan raken. Dit beheer kost aandacht, tijd en moeite. Past dat wel naast het eigenlijke dagelijkse werk?

Privé

De universiteit is een organisatie die de medewerkers veel vrijheid geeft. Dat geldt ook voor de inzet van ICT-apparatuur. Bij veel andersoortige organisaties ontbreekt die vrijheid, daar kiest de organisatie het apparaat waarop men het werk moet doen, worden centraal de systemen geconfigureerd en beheerd en hebben de gebruikers geen alternatieve mogelijkheden.

Bij de universiteit kan men kiezen om te werken op een centraal beheerde desktopcomputer, maar medewerkers kunnen er ook voor opteren zelf het besturingssysteem te kiezen en zelf het systeem te beheren. Daarnaast staat het medewerkers vrij privéapparatuur voor het werk te gebruiken, zoals bijvoorbeeld tablets.

Open deur

Wanneer een medewerker zelf zijn systeem beheert en zelf zijn privéapparatuur voor het werk gebruikt, dan moet die medewerker ook zelf voor de veiligheid van die systemen en de daarop verwerkte informatie zorgen. Dit betekent dat op tijd de beveiligingsupdates worden geïnstalleerd, dat het systeem veilig is geconfigureerd en alleen veilige software wordt gebruikt en dat de data tegen dataverlies is beschermd. Dit klinkt als een open deur, maar helaas blijkt dit in de praktijk vaak een lastig onderwerp.

Regelmatig komen we bij de universiteit systemen tegen, die ver achterlopen met de beveiligingsupdates of waarvan de configuratie onveilig is. Hierdoor zijn deze systemen onnodig kwetsbaar en helaas komt het ook voor, dat derden daadwerkelijk misbruik van deze kwetsbaarheden hebben gemaakt. Een derde heeft zich dan ongeautoriseerd toegang tot het systeem verschaft.

Soms krijgen we klachten van buiten de universiteit, omdat een systeem binnen het universiteitsnetwerk misbruikt wordt om kwaadaardige activiteiten uit te voeren. Iemand buiten de universiteit is dan het slachtoffer van een binnen de universiteit minder goed beheerd systeem. Cybercriminaliteit wordt een steeds ernstiger probleem, waardoor het beheer van de computer écht dagelijks aandacht nodig heeft.

Voorkomen van dataverlies

De informatie die op de systemen staat, wordt steeds belangrijker voor ons werk en ook steeds waardevoller. Die informatie moet goed worden beschermd, niet alleen tegen de dreiging van criminelen, maar ook tegen het risico van dataverlies. Jammer genoeg gebeurt het nog steeds dat het lokaal beheerde opslagsysteem van de computer beschadigd raakt en waardevolle informatie verloren gaat.

Wie zelf zijn systeem beheert, moet daarom ook zelf goed over een backup-strategie nadenken. Een belangrijke voorwaarde voor een goede backup-strategie is dat deze volledig automatisch plaatsvindt. Zodra menselijk handelen nodig is, bijvoorbeeld om af en toe een kopie op een USB-schijf te zetten, bestaat het risico dat op het moment dat de backup echt nodig is, blijkt dat de laatste kopie te oud is en net dat ene kritische bestand ontbreekt.

Vulnerability scan

Het CIT scant maandelijks het universiteitsnetwerk met behulp van een vulnerability scan-systeem. Dit systeem herkent computers met zwakheden zoals achterstallig onderhoud en bepaalde configuratieproblemen. Het netwerk is te groot om in één keer te scannen, daarom wordt elke maand steeds een ander deel van het netwerk gescand.

Wanneer de scanner zwakheden in een gebruikerssysteem meldt, dan wordt contact gezocht met de betreffende gebruiker, met het verzoek deze zwakheden te verhelpen. Op deze manier wordt het systeem van die gebruiker minder kwetsbaar, wat bijdraagt aan de veiligheid van het gehele netwerk.

Bij het zelf beheren van de werkplekcomputer of een server, komt vaak meer kijken dan wat men op het eerste gezicht verwacht. De tijd, energie en aandacht die men daaraan besteedt, kan men niet aan het eigenlijke werk besteden. Een onoplettendheid kan leiden tot compromittatie van het systeem en/of verlies van data. Het kan geen kwaad daar nog eens bij stil te staan en regelmatig na te gaan of alles nog goed geregeld is. Schakel bij twijfel gerust het CIT in.