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

Het gevaar van ransomware

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.

Berichtgeving over organisaties die het slachtoffer geworden zijn van een ransomware-aanval, keert helaas steeds vaker terug in het nieuws. Ransomware is kwaadaardige software die er op gericht is een groot aantal bestanden onbruikbaar te maken door deze te versleutelen.

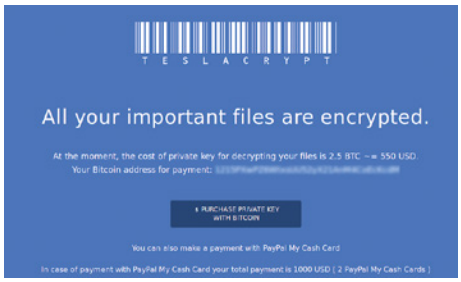
Het slachtoffer krijgt vervolgens het aanbod om tegen betaling de toegang terug te krijgen tot die bestanden. Wie betaalt, krijgt de sleutel om de bestanden mee te ontcijferen, althans, dat is de belofte. Niet altijd wordt deze belofte waar gemaakt. Analisten hebben zelfs ransomware gezien, waarbij het helemaal niet mogelijk is na een infectie de bestanden ooit nog te ontcijferen.

De impact van een ransomware-aanval hangt af van het aantal geïnfecteerde computers en de hoeveelheid en het belang van de getroffen bestanden. Ook hangt het af van de mogelijkheid om bestanden vanuit het backupsysteem weer te herstellen, en de hoeveelheid tijd die daarmee gemoeid is.

Soms is deze impact zo groot, dat dit het voortbestaan van een organisatie in gevaar brengt. In het meest gunstige geval blijft de schade beperkt tot ongemak en verlies van tijd. Beheerders en gebruikers moeten daarom alert zijn om de kans op het slagen van zo'n aanval zo klein mogelijk te houden.

Waarschuwingsvenster

De eerste stap in de verdediging tegen ransomware is het zorgen dat de werkplek zo goed mogelijk is beschermd door voortdurend de



software up-to-date te houden, alle beveiligings-updates te installeren en een geactualiseerd anti-malware programma te gebruiken. De RUG-beheerders houden de UWP-machines up-to-date.

Wie echter geen UWP-machine gebruikt, maar zelf zijn werkplek beheert, moet hiervoor zelf zorgen. Zorg dan voor een goed antivirusprogramma, met de laatste updates en zorg ook voor de updates van het besturingssysteem en alle gebruikte software.

Een tweede stap is het verantwoord gebruik van de computer. Klik niet zomaar op linkjes in mailtjes en let goed op wanneer een waarschuwingsvenster verschijnt. Klik dit niet zo maar weg, zonder deze eerst te lezen.

Zero-days

Soms lukt het een ransomware-programma om toch een computer te infecteren, ondanks dat alle updates geïnstalleerd zijn, bijvoorbeeld door het gebruik van nog onbekende zwakheden in het besturingssysteem of in een van de applicaties (zogenoemde zero-days). De ransomware versleutelt na infectie de bestanden. Dit kunnen bestanden op het systeem zelf zijn (bijvoorbeeld op de C-schijf), maar ook bestanden die centraal zijn opgeslagen, op de X- en de Y-schijf. De laatste worden door het backup-systeem van de RUG beschermd tegen verlies. U kunt voor het herstel van die bestanden de CIT-Servicedesk benaderen.

Het backup-systeem van de RUG maakt echter geen reservekopie van bestanden op de C-schijf. Ook wanneer u voor de opslag van uw bestanden andere media gebruikt, doet u er goed aan na te gaan of en hoe deze via een backup-systeem zijn beschermd. Wanneer er niet automatisch en geregeld door een backup-systeem reservekopieën van de bestanden worden gemaakt, kan de impact van een mogelijke ransomware-aanval groot zijn. Niet alleen door ransomware, maar ook door andere oorzaken kunnen bestanden of een bestandssysteem corrupt raken.

Datalek

Wanneer een geslaagde ransomware-infectie tot versleuteling van bestanden heeft geleid, dient u dit altijd te melden. De ransomware kan naast de bestanden op de lokale harde schijf ook bestanden op de X- en Y-schijf hebben versleuteld. De Autoriteit Persoonsgegevens heeft bepaald dat wanneer persoonsgegevens door ransomware zijn versleuteld, dit altijd moet worden aangemerkt als datalek. In dat geval is de RUG verplicht dit binnen de gestelde termijn van 72 uur te melden. Bent u het slachtoffer van ransomware, meldt dit daarom zo snel mogelijk bij de Servicedesk. Wanneer mogelijk ook persoonsgegevens betrokken zijn, meldt dit dan meteen bij het centrale meldpunt datalekken van de RUG, via **cert@security.rug.nl**.