Eindgebruiker nog altijd laks met data

Gevaren onderschat

Laurens van Aggelen

Computergebruikers blijken nog altijd hardleers als het gaat om het veilig omspringen met data. Uit onderzoek van onderwijs ICT-innovator SURFnet kwam onlangs naar voren dat de helft van de particulieren en organisaties onvoldoende maatregelen neemt om data te verwijderen van de harde schijf van oude computers. Ook bleek het op die harde schijven te wemelen van virussen, spyware keyloggers en andere kwaadaardige bits en bytes.

"Het aantal onderzochte harde schijven is te beperkt in omvang om algemeen geldige uitspraken te doen, maar geeft wel een indicatie van hoe bedrijven en particulieren omgaan met hun data wanneer een computer is afgeschreven", aldus Rogier Spoor, Manager Middleware Services van SURFnet. SURFnet maakt deel uit van de SURF-organisatie, waarin Nederlandse universiteiten, hogescholen en onderzoeksinstellingen nationaal en internationaal samenwerken aan innovatieve ICT-voorzieningen. Volgens Spoor zou de helft van de gebruikers geen deugdelijke maatregelen nemen voor vernietiging van de aanwezige data op harde schijven, waardoor vertrouwelijke informatie in handen van derden kan vallen. Bovendien is bij een kwart van de onderzochte werkstation- en laptop harde schijven kwaadaardige software aangetroffen. "Wij kijken er niet van op en denken dat de conclusies van SURFnet nog aan de voorzichtige kant zijn. We hebben net iets te veel oude schijven in onze vingers gehad en experts gesproken om te geloven dat de overige 50 procent van de gebruikers zijn zaakjes goed op orde heeft."

Grote vangst

"Wat ons nog het meest verbaasde was dat we gegevensdragers tegenkwamen van organisaties die met veel vertrouwelijke informatie werken en waarvan je zou mogen verwachten dat men daar zorgvuldig mee omgaat. Zo troffen we complete klantenbestanden aan en zelfs de volledige informatie over de ICT-infrastructuur van een organisatie. Eén van de onderzochte serverschijven bevatte een database van een koepelorganisatie in de zorgsector. Op meerdere werkstationschijven werd vertrouwelijke informatie aangetroffen, zoals privé-documenten van acht studenten, de harde schijf van de ICT-afdeling van een luchtvaartmaatschappij, vertrouwelijke data van een communicatieadviesbedrijf en vertrouwelijke data van privépersonen", zegt Jacques Schuurman van SURFnet. Dit alles kwam aan het licht toen SURFnet software wilde testen om harde schijven te ontdoen van virussen, spyware en andere onheil. "Op de computers en harde schijven die we voor die gelegenheid her en der inkochten, kwamen we tot onze verrassing al die informatie tegen."
De schijven werden door SURFnet onderzocht met behulp van Forensics Toolkit 1.80. Om forensisch zuiver te kunnen werken is gebruik gemaakt van een writeblocker van het merk Tableau type T3U voor SATA schijven en model T5 voor schijven met een IDE/PATA-interface. Vervolgens is met behulp van hash sets van NIST NSRL en Accessdata KFF gezocht naar bekende malware en handmatig bepaald of deze malware ook werkelijk actief was.

Onzichtbaar aanwezig

"Het blijft de verantwoordelijkheid van de eindgebruiker om te zorgen dat data op een deugdelijke manier verwijderd worden voordat de harde schijven in vreemde handen terechtkomen. Wie met vertrouwelijke informatie werkt, adviseer ik deze data altijd versleuteld op te slaan. Voor het verwijderen van data zijn voldoende programma's beschikbaar, die de data zo overschrijven dat het moeilijk wordt ze terug te halen. Staan er grotere belangen op het spel en zou het anderen de moeite lonen de data toch terug te zetten, dan is overschrijven alleen niet voldoende. In dat geval is het raadzaam de gegevensdrager volledig te vernietigen", aldus Schuurman. Het overschrijven van data is namelijk maar beperkt mogelijk vanwege de aanwezigheid van een aantal verborgen sectoren. Daar blijft altijd data achter die je niet ziet. "Bij de nieuwe generaties harde schijven is het totaal verwijderen van data steeds moeilijker gemaakt", zegt Robbert Brans, expert op het gebied van datarecovery bij Norman. "Die nieuwe harde schijven zijn uitgerust met de nodige extra opslagcapaciteit om de prestaties te verbeteren. Op een hard disk van 200 gigabyte is in werkelijkheid nog eens 50 gigabyte onzichtbaar aanwezig." Deze toenemende complexiteit stelt hoge eisen aan de software waarmee data op een professionele manier gewist kunnen worden. Norman is om die reden afgehaakt met het op de markt brengen van Data Eraser. Grote nieuwe investeringen waren nodig geweest om die markt te kunnen blijven volgen en Norman wil zich de komende tijd meer richten op datarecovery.

Het onderzoek van SURFnet leidde tot opmerkelijke resultaten. Bijvoorbeeld dat veel gebruikers niet eens een poging ondernomen hadden om hun data van hun oude computer te wissen. Kennelijk is hun vertrouwen in de medemens zo groot dat zij verwachten dat anderen dit klusje wel klaren. Van gebruikers die zo met vertrouwelijke gegevens omgaan valt niet te verwachten dat ze deugdelijke security software aanschaffen.

Software

Al is de eindgebruiker zelf verantwoordelijk, het is jammer dat fabrikanten niet meer tools aanreiken voor het wissen van data. Gebruikers worden nog te vaak doorverwezen naar eenvoudige gratis tools die via internet te downloaden zijn. Maar zoals een demo van Norman eerder liet zien, blijken veel data na gebruik van deze tools nog steeds terug te halen. En ook commerciële software laat het nog al eens afweten als het gaat om totale dataverwijdering. Veel pakketten komen daarmee weg omdat de onkunde in de markt groot is. Ook gerenommeerde partijen, die zich met *refurbishment* bezighouden, houden er nog wel eens andere opvattingen op na over de wijze waarop data definitief verwijderd zouden moeten worden. Norman raadt bij monde van Robbert Brans aan om in ieder geval gebruik te maken van software zoals Ontrack Eraser of de eveneens geschikte software van Blancco. "Bedrijven die het zekere voor het onzekere willen nemen, doen er goed aan te kiezen voor een degauser. *Degaussing* is een methode waarmee de magnetische laag waarop de data van een harde schijf is gezet, wordt geëgaliseerd. Als digitaal opgeslagen data ergens niet tegen kunnen, is het wel een sterk elektromagnetisch veld." |