Laat je niet pakken?

Frank Brokken
f.b.brokken@rc.rug.nl

Frank Brokken is security manager bij het RC. Met het instellen van deze functie probeert de RUG het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen. In zijn column houdt Frank ons op de hoogte van de stand van zaken met betrekking tot zijn missie.

Onder de pakkende titel *Laat je niet pakken!* lanceerde SURFnet begin maart een landelijke campagne om gebruikers van computers ertoe te brengen aandacht te schenken aan ICT-beveiliging, en met name aan de beveiliging van hun eigen computers.

De Laat je niet pakken-campagne is een prachtig initiatief, waarvoor SURFnet op z'n minst in aanmerking zou komen voor de Annual Security Award 2004, ware het niet dat SURFnet niet in de daarvoor vereiste categorie valt: de Annual Security Award is er immers voor studenten en medewerkers van de RUG, en niet voor anderen, hoe nauw ook bij de RUG betrokken.

De SURFnet-campagne is bedoeld om de bewustwording te vergroten van de veiligheidsrisico's die verbonden zijn aan het gebruik van computers en netwerken. De tijd dat computers werden gebruikt als opgetuigde typemachines in de vorm van 'personal computers' is vrijwel voor iedereen voorbij. Vrijwel iedereen wil e-mail kunnen versturen en/of ontvangen (zolang het maar geen spam is....), vrijwel iedereen wil kunnen webbrowsen.
Om dit te kunnen realiseren is het noodzakelijk om de computer te verbinden met het internet, en hier begint vaak ook de ellende: hoe goed is onze computer bestand tegen kwaadaardige software en acties die vanuit het internet tegen onze computer worden gericht?

In deze Pictogrambijdrage wordt nogmaals aandacht aan de SURFnet-campagne besteed. Ook breng ik een paar onderwerpen voor het voetlicht die direct te maken hebben met de beveiliging van computers. Nadere details kunnen bij SURFnet worden verkregen. Uiteraard is het ook mogelijk om over de details met mij van gedachten te wisselen.

De SURFnet-campagne

In de SURFnet-campagne wordt gesteld dat veel ellende kan worden voorkomen door bewust met een computer om te gaan. Dat is een goed idee, lijkt me. In de campagne staan drie gouden regels centraal die erg effectief kunnen zijn bij het voorkomen van problemen:

1. Installeer beveiligingssoftware en updates
2. Hou wachtwoorden voor jezelf
3. Maak back-ups van je bestanden

Updates

Updates zijn nodig omdat ze 'zwakke plekken' uit het systeem kunnen halen. Die zwakke plekken worden dan door de update gerepareerd: men spreekt van het *patchen* van de software. Wanneer de computer voorzien is van de laatste software en de nieuwste patches is deze veel minder kwetsbaar voor hack-pogingen, virussen, wormen en andere ongewenste software.
Updates zijn geen garantie voor veiligheid, maar zijn een soort APK-keuring voor uw computer.

Nadat mijn auto APK-gekeurd is, kan ik nog steeds worden bekeurd voor te snel rijden, en kan een inbreker nog steeds een raampje inslaan. Maar het is iets minder waarschijnlijk dat ik door de rem trap wanneer ik een noodstop moet maken.

Beantwoord nu in dit verband de volgende vraag: wanneer is uw computer voor het laatst 'APK-gekeurd'? Met andere woorden: wat was de laatste keer dat de software van uw computer werd vernieuwd?

De APK-gekeurde auto van de Security Manager

Wanneer u het antwoord schuldig blijft, is uw computer niet zozeer het probleem, maar bent u zelf het grootste veiligheidsrisico.

Virusscanners

Virusscanners kunnen een goede bijdrage leveren aan de veiligheid van uw computer. Laten we nog maar eens een vraag stellen: wanneer is uw virusscanner voor het laatst bijgewerkt?

Wanneer u het antwoord schuldig blijft en u gebruik maakt van Windows, bent u zelf het grootste veiligheidsrisico.

Maar ook wanneer u wel een virusscanner gebruikt, bent u zelf uiteindelijk de beste virusscanner die er is. Virusscanners detecteren virussen die ze kennen, niet virussen die ze niet kennen. Virussen komen in attachments, en mogelijk in software die u zelf installeert in uw computer.
Door attachments alleen te openen wanneer u 100% zeker bent van de integriteit ervan kunt u, beter dan uw virusscanner, voorkomen dat uw computer met virussen wordt besmet (het lamme excuus: 'ik dacht dat de mail van mijn collega was', is niet erg sterk, want virussen misbruiken uw e-mailadres en dat van uw collega om zich te verspreiden).

GPG-gesigneerde e-mail kan die integriteit bieden. Een telefoontje naar de afzender mogelijk ook. In alle andere gevallen bent u niet zeker van uw zaak, en wordt u vroeg of laat gepakt wanneer u een attachment opent. Hetzelfde geldt voor software waarvan niet 100% zeker is wie kan worden aangesproken voor de integriteit ervan.

Wanneer u software installeert zonder inzicht te hebben in de veiligheidsrisico's ervan, bent u zelf het grootste veiligheidsrisico.

Firewalls

Firewalls vormen een andere categorie van beveiligingssoftware. Mooi gereedschap, maar met een gebruiksaanwijzing. Wie de gebruiksaanwijzing van een firewall niet kan of wil lezen en toch een firewall toepast, is als een automobilist die denkt dat hij onkwetsbaar is omdat z'n auto voorzien is van kreukelzones.
Persoonlijk denk ik dat een 2CV veiliger is dan een Mercedes. De 2CV-chauffeur weet dat zijn/haar auto niet erg veilig is, en zal daardoor extra voorzichtig zijn....

Wanneer u een firewall installeert en dan denkt dat uw computer tegen misbruik is beveiligd, bent u zelf het grootste veiligheidsrisico.

Passwords

De standaardmanier om toegang te krijgen tot een computer is via een username/password-combinatie. Na het intypen van een username en wachtwoord wordt de wondere wereld van de computer voor ons geopend en kunnen we naar hartelust e-mailen en webbrowsen.
Erg mooi. Maar wat is uw wachtwoord? En waar is uw wachtwoord? Onlangs zijn verschillende computers binnen de RUG misbruikt door hackers die via het zogenaamde *administrator* account toegang kregen tot deze computers.

Hackers waargenomen bij het RC

Het is mij een raadsel hoe dat kan. Volgens SURFnet wachten hackers niet tot ze een wachtwoord in de schoot geworpen krijgen. Hackers maken gebruik van virussen of andere software om een wachtwoord als het ware af te luisteren. Dat hoeft niet noodzakelijk te gebeuren op uw computer zelf: wie 'op afstand' werkt, is extra vatbaar voor snuffelaars die de verbinding tussen computers afluisteren op zoek naar gebruikersnamen en wachtwoorden. Beveiligde (versleutelde) verbindingen kunnen dit probleem effectief oplossen.
Bruut zoeken naar wachtwoorden wil ook nog wel eens voorkomen. Een verbazingwekkend aantal computers is en blijft voorzien van standaard, bij software-installatie meegeleverde gebruikersnamen en wachtwoorden. Die standaard wachtwoorden zijn bij de hackers bekend, en worden regelmatig geprobeerd. Hier zijn wat *real life*-voorbeelden van zulke pogingen, afkomstig van 81.51.123.125 (ABordeaux-103-1-28-125.w81-51.abo.wanadoo.fr):

```
(81.51.123.125[81.51.123.125]) - USER anyone: no such user found from
(81.51.123.125[81.51.123.125]) - SECURITY VIOLATION: root login attempted.
(81.51.123.125[81.51.123.125]) - USER admin: no such user found from
(81.51.123.125[81.51.123.125]) - USER test: no such user found from
(81.51.123.125[81.51.123.125]) - no such user 'www'
(81.51.123.125[81.51.123.125]) - USER oracle: no such user found from
(81.51.123.125[81.51.123.125]) - USER webmaster: no such user found from
```

Pathetische pogingen om in te breken in een RUG-computer, maar niet zo pathetisch dat het niet zo nu en dan lukt. Een sterk wachtwoord (niet standaard, ook voorzien van andere tekens dan letters en/of cijfers) kan al veel goeds doen.
Wachtwoorden hebben de neiging te verouderen. Dat betekent dat vroeg of laat wachtwoorden gaan 'zwerven', en daarmee bekend worden bij anderen. Anderen kunnen misbruik maken van uw account, waardoor het lijkt dat u degene bent die een grote hoeveelheid spam heeft verstuurd, of een server voor illegaal gekopieerde muziek of films onderhoudt. Is uw wachtwoord wel goed gekozen? Is uw wachtwoord niet bekend bij anderen?

Wanneer u op deze vragen ontkennend antwoordt, is uw wachtwoord niet zozeer het veiligheidsrisico, maar bent u het zelf.

Back-ups

Een derde advies dat SURFnet biedt, is 'maak back-ups' van documenten en software. Daar is niet veel op af te dingen. Doen! Er kan van alles misgaan met een computer en niet alleen door virussen en hack-pogingen. Ook door technische mankementen kan een harde schijf onbruikbaar worden. Het is dan ook belangrijk om regelmatig back-ups te maken van je bestanden. Dat doe je door een kopie van het bestand op te slaan op een ander medium.
Wie dat niet doet: wie zijn billen brandt, moet op de blaren zitten. Eigen schuld, dikke bult. Niet piepen wanneer informatie na een crash verloren is gegaan, terwijl er geen recente back-up is gemaakt.

Tenslotte

Een computer die gekoppeld is aan het internet geeft de gebruiker toegang tot een breed scala aan mogelijkheden. Tegelijkertijd is zo'n computer ook onderdeel van het internet, en moet daarom tegenwoordig helaas beveiligd worden tegen misbruik. Wie dat aspect van het gebruik van computers negeert, gedraagt zich asociaal, en is al snel mede verantwoordelijk voor het verspreiden van spam, of al dan niet met opzet betrokken bij illegale ICT-activiteiten, zoals het ontduiken van auteursrechten.
Door de software van computers up-to-date te houden en door beveiligingssoftware te installeren, kan misbruik worden beperkt. Dit vereist dat de gebruiker van de computer zich inzet voor de beveiliging van zijn/haar eigen computer.

De belangrijkste beveiliging van uw computer bent u zelf.

Links

- *Gnu's Privacy Guard* (GPG) maakt het mogelijk om documenten en e-mail te versleutelen en te authenticeren. De commerciële variant staat bekend als PGP: **www.gnupg.org**
- Meer informatie over ICT-security bij de RUG is te vinden op de website. Hier staat informatie over o.a. de universitaire 'Acceptable Use Policy' en de 'Annual Security Award': **www.rug.nl/rc/helpdesk/security**
- De SURFkit (knowledge, instructions en tools) is een cd-rom die jaarlijks door SURFnet wordt verspreid. De cd-rom bevat praktische informatie over internettoepassingen, bijbehorende handleidingen en software. Ook wordt informatie over beveiliging gegeven: **www.surfkit.nl**
- SURFSPOT.NL is een webwinkel die wordt beheerd door SURFdiensten, de zusterorganisatie van SURFnet. Studenten en medewerkers van hogescholen en universiteiten kunnen via SURFSPOT.NL zeer goedkoop software voor eigen gebruik aanschaffen: **www.surfspot.nl**
- SURFnet is de internetprovider voor hoger onderwijs en onderzoek in Nederland. Ruim 500.000 studenten en onderzoekers maken dagelijks gebruik van het netwerk en de diensten van SURFnet: **www.surfnet.nl**