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

Verbergen

Als security manager heeft CIT-medewerker Frank Brokken de taak het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen. In zijn column doet Frank verslag van de stand van zaken met betrekking tot zijn missie.

Verbergen? Hoezo verbergen? Natuurlijk heb ik niks te verbergen. Ik ben een open boek, en iedereen mag alles van mij weten. Nou ja, misschien met uitzondering van mijn pincode dan.

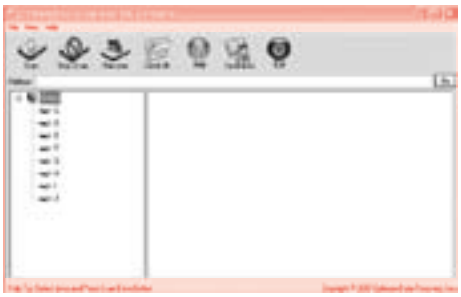
Toch is het de vraag of dat wel zo is. Nee, ik heb niks te verbergen, maar ik zou het toch niet zo leuk vinden wanneer iemand gaat joyriden met mijn auto of zich ongevraagd toegang verschaft tot mijn huis en daar wat in de kasten rommelt. Laat staan spullen meeneemt.

Intellectuele luiheid

Het standpunt dat 'je niks te verbergen hebt', komt dan ook eerder voort uit intellectuele luiheid dan dat het standpunt het resultaat is van een weloverwogen, rationele analyse van de persoonlijke situatie, zo komt mij voor. Het klinkt zo lekker open, 'Ik heb niks te verbergen'. Maar niemand had beweerd dat je iets te verbergen zou hebben.

In discussies waarbij iemand beweert dat er 'niets te verbergen valt', gaat het meestal helemaal niet om geheimen die moeten worden verborgen. Veel discussies waarbij de stelling wordt ingenomen dat 'er niks te verbergen valt', gaan over beveiliging.

Een van mijn collega's werd enige weken geleden het slachtoffer van een inbraak bij hem thuis. Had hij iets te verbergen? Tja... Zijn laptop werd gestolen, en in die computer waren wachtwoorden van diverse computers opgeslagen. Het is niet waarschijnlijk dat de junk die de computer heeft meegenomen daarin geïnteresseerd zal zijn, maar zou de 'nieuwe eigenaar' van de computer er wellicht geïnteresseerd in kunnen zijn? Dat weet je natuurlijk niet, en de waarschijnlijkheid dat de junk zo vriendelijk is om de computer eerst even goed schoon te maken voordat de laptop wordt doorverkocht, is natuurlijk niet erg groot.



Dat is ook zo'n punt dat er als raamvertelling wel even tussendoor kan. Niemand denkt toch hopelijk dat de informatie van de harddisk is verwijderd nadat de disk is geformatteerd? Wat er in dat geval gebeurt, is hooguit dat de tabel waarin staat waar welke files zich op de harddisk bevinden, opnieuw wordt geïnitialiseerd. Een beetje forensisch onderzoeker kan met een eenvoudig tooltje dan nog vrijwel alle oorspronkelijk aanwezige bestanden weer terughalen. Dat kon al onder MS-DOS en dat is nog steeds zo.

Defensie-informatie

Het Forensisch Instituut in Rijswijk kan op dat punt nog veel meer. Ook wanneer je disk volledig is gevuld met toevalsgetallen, kan men nog verbazingwekkend veel informatie weer terughalen met gespecialiseerde technieken. Kortom: het is helemaal niet zo makkelijk om iets 'te verbergen', laat staan dat het eenvoudig zou zijn om informatie te vernietigen. Flink kapot stampen met een voorhamer of goed heet maken met een snijbrander, dat komt misschien nog wel het meeste in de buurt, maar geeft nog steeds geen honderd procent garantie.

Terug naar het hoofdonderwerp. Hoe zat dat nou met de laptop van mijn collega? Paniek? Alle passwords moeten acuut worden aangepast? Nee. Niks van dat alles. Alle gevoelige informatie was opgeslagen in versleutelde files en filesystemen. Dat is dermate eenvoudig te realiseren, dat je je afvraagt waarom er nog steeds mogelijkheden zijn voor de media om te rapporteren dat er weer eens een usb-stickje of een cd'tje is gevon-

den met geclassificeerde defensie-informatie of met de namen, adressen en andere onder de wet bescherming persoonsgegevens vallende data van duizenden personen.

Omdat mijn collega op verantwoorde wijze met de aan hem toevertrouwde informatie is omgegaan, is de pijn beperkt tot het verlies van een apparaat. Uiteraard was de aan hem toevertrouwde informatie veilig opgeslagen in zijn computer en uiteraard had hij een goede backup zodat er geen informatie verloren is gegaan. Complimenten!

Top20

Dan nog zijn er computergebruikers die menen dat het allemaal zo'n vaart niet zal lopen. Nee hoor, het loopt zo'n vaart niet; al die creditcard-gegevens die je voor een prikje bij de Russische maffia kunt kopen zijn zomaar bedacht en niet het gevolg van onnadenkendheid van de rechtmatige eigenaren van die informatie; alle (ro)botnets die massaal kunnen worden ingezet om onwelgevallige organisaties en bedrijven te chanteren met het op het internet onbereikbaar maken van die organisaties en bedrijven zijn ook zomaar uit te lucht komen vallen. Dat heeft al lang niks meer te maken met de 'ik-heb-toch-niks-te-verbergen'-mentaliteit.

Op de website van SANS staat een top 20 van meest voorkomende kwetsbaarheden in computersystemen. Een bloemlezing, bestaande uit de eerst vermelde kwetsbaarheden in een paar categorieën:

- "Web Browsers: Unpatched or older versions of Internet Explorer contain multiple vulnerabilities that can lead to memory corruption, spoofing and execution of arbitrary scripts or code."
- "Office Software: Microsoft Office is the most widely used e-mail and productivity suite worldwide. It includes Outlook, Word, PowerPoint, Excel, Visio, FrontPage and Access. A large number of critical flaws were reported in MS Office applications and a few of them were zero-day issues in which exploit code was publicly disclosed before any fix became available from Microsoft."
- "E-mail: Multiple avenues of attack that can be employed through e-mail, virtually all contemporary operating systems can be used as platforms for e-mail client applications."
- "Media Players: Over the past year vulnerabilities have been released for most popular media players available today. While the severity of the vulnerabilities varies, these vulnerabilities can often be used to install malware such as viruses, botnet applications, root kits, spy-ware, and ad-ware. Operating Systems Affected:
  - Microsoft Windows
  - Linux/Unix
  - Mac OS X"

Het is maar een bloemlezing, maar het zou te denken moeten geven: is mijn computer systeem eigenlijk wel zo veilig? Veel kwetsbaarheden kunnen worden verholpen door er consequent voor te zorgen dat de laatste versies zijn geïnstalleerd, maar soms is ook dat niet genoeg (denk aan de genoemde 'zero day issues'). In die gevallen moet je dan maar hopen dat je niet gepakt wordt.

Quarantainenet
NETWORK MANAGEMENT AND SECURITY

Mensenwerk

Na een lange periode van voorbereiding zal binnenkort zal bij de RUG een proef met het Quarantainenet van start gaan. Zo'n quarantainenet zal zeker helpen om 'the day after' de 'zero day issue' de kwetsbaarheid te herkennen en te bestrijden. Maar hoe gaat dat thuis?

Uiteindelijk is beveiliging, net zoals veilig vrijen, mensenwerk. De techniek kan je helpen, maar je bepaalt uiteindelijk zelf wat je wel en niet doet en wat er wel en niet met je computer gebeurt.

Frank Brokken
(houdt de zaak het liefst zelf in handen)

- Het Nederlands Forensisch Instituut kan met gespecialiseerde technieken verbazingwekkend veel informatie terughalen van oorspronkelijke bestanden op harddisks: **www.forensischinstituut.nl**
- Wet bescherming persoonsgegevens: **www.justitie.nl/onderwerpen/opsporing_en_handhaving/wbp**
- Niks te verbergen maar toch gevoelige informatie op je computer? Kijk eens op **www.truecrypt.org**
- Niks te verbergen maar toch de mogelijkheid willen hebben om eens vertrouwelijke e-mail met iemand uit te wisselen of om de ontvanger ervan te kunnen overtuigen dat jij degene bent geweest die een e-mail heeft verzonden? Kijk eens op **www.rug.nl/cit/security/adviezen/email**
- De meest voorkomende kwetsbaarheden in computersystemen: **www.sans.org/top20**
- Meer informatie over quarantainenet: **www.quarantainenet.nl**