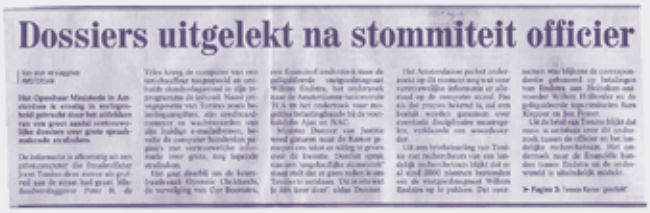
Krokodillentranen

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

ICT-security

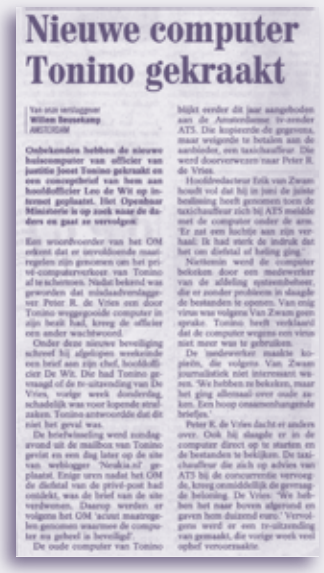
Frank Brokken is security manager bij het RC. Met het instellen van deze functie probeert de RUG het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen. In zijn column houdt Frank ons op de hoogte van de stand van zaken met betrekking tot zijn missie.



Dossiers uitgelekt na stommiteit officier

'Dit is echt diep treurig, een schande'

Reportage | Slordig omgaan met informatie over opsporingsonderzoeken kan enorme schade veroorzaken



Nieuwe computer Tonino gekraakt

Tegen de tijd dat deze Pictogram van de drukker komt en wordt verspreid, is de commotie rondom officier van Justitie Tonino natuurlijk al wat geluwd. Maar toen rond 10 oktober van dit jaar bekend werd dat mijnheer Tonino's pc bij het grofvuil op straat terecht was gekomen en was meegenomen door een voorbijganger die er nog duizend euro voor wist te vangen van de heer De Vries kon ik een glimlach toch niet onderdrukken.

Verwachtingspatroon

Waarom dan toch krokodillentranen? Omdat er ach en wee wordt geroepen in een cultuur waarin vrijwel geen aandacht wordt geschonken aan de beveiliging van computers en de daarin opgeslagen informatie. Ook illustreert dit weer eens hoe selectief mensen waarnemen: wat niet in het verwachtingspatroon valt, wordt gewoon niet opgemerkt. Daarover straks meer.

Onder de krantenkop 'Dossiers uitgelekt na stommiteit officier' wordt feitelijk verslag gedaan van het voorval: de computer staat op straat, en de inhoud van diens harddisk daarmee ook.

De tranen komen verderop in de krant: de Tweede Kamer is 'verbijsterd'. Dat horen politici natuurlijk ook te zijn in een tijdsgewricht waarin normen en waarden weer centraal komen te staan. Niet mijn normen en waarden overigens: er lijkt mij absoluut geen reden voor morele verontwaardiging.

De kracht van de cracker-beweging (dank, dank, dank voor het wrijven van zout in de wond!) wordt kort daarna nog weer eens extra duidelijk doordat Tonino's 'nieuwe huiscomputer' prompt werd gekraakt.

Geheel beveiligd?

Ik vind het boeiend. De krant schrijft: "*... het OM erkent dat er onvoldoende maatregelen zijn genomen om het privé-computerverkeer van Tonino af te schermen. Nadat (...) kreeg de officier een ander wachtwoord...*"

Hij 'kreeg' een ander wachtwoord... Tja. Kon hij er zelf geen bedenken? Maar veel heeft het niet geholpen, hè? Intrigerend vind ik de passage: "*... Onder deze nieuwe beveiliging schreef hij afgelopen weekeinde een brief aan zijn chef (…) De briefwisseling werd zondagavond uit de mailbox van Tonino gevist (…) Daarop werden er (…) acuut maatregelen genomen waarmee de computer nu geheel is beveiligd.*"

Geheel is beveiligd? Waarom ben ik hiervan niet onder de indruk? Laten we eens wat punten op een rij zetten:

Computer bij grofvuil. Officier van justitie Joost Tonino brengt door misser mogelijk strafzaken in gevaar

Kamer verbijsterd over 'blunder van de eeuw'

De kapotte computer had naar het OM moeten worden gebracht om te worden vernietigd door het bewerken met hamerslagen, citeerde minister Donner

- In Nederland (en daar niet alleen) is er vrijwel geen cultuur waarin aandacht is voor IT-Security. De RUG is, als organisatie, op dat gebied overigens een gunstige uitzondering. Een paar voorbeelden: de RUG heeft een ICT-security manager aangesteld; de RUG heeft een vastgestelde 'Acceptable Use Policy'; en de RUG reikt jaarlijks een security-prijs uit, de 'Annual Security Award'.
- De 'security awareness' van de doorsnee-computergebruiker ligt op het niveau van begin jaren tachtig, toen de IBM-Personal Computer op de markt kwam: een soort elektronische typemachine met overeenkomstige beveiligingseisen. Er was immers praktisch gezien nog geen internet, laat staan dat er crackers waren.
- Het OM dat denkt dat door het wijzigen van een password e-mailtransmissie is beveiligd, gedraagt zich hopeloos naïef. Vrijwel alle e-mail wordt in leesbare vorm verstuurd van de afzender naar de ontvanger, en dat betekent dat alle computers op het traject tussen afzender en ontvanger alle verzonden e-mail kunnen lezen. Om een indruk te geven: er zijn zo al acht tussenstations tussen mijn computer en **www.om.nl**, de computer die de website van het OM aanbiedt:

0 suffix.rc.rug.nl
1 129.125.3.251
2 Gi12-0.AR5.Groningen1.surf.net
3 PO6-0.CR2.Amsterdam2.surf.net
4 PO1-0.CR1.Amsterdam2.surf.net
5 PO0-0.CR1.Amsterdam1.surf.net
6 P0-0.BR1.Amsterdam1.surf.net
7 ams-ix.M10.AMS.we-dare.net
8 so-0-1-2.M160.RTD.we-dare.net
9 www.om.nl

Wie geïnteresseerd is in informatie die tussen mijn computer en **www.om.nl** wordt uitgewisseld, kan dus op elk van deze computers terecht. Inbreken op de eindpunten is hiervoor echt niet nodig.

- Foutje van Tonino is natuurlijk om zijn computer op straat te zetten. Dat is echt een misser, want ook hij kan weten dat grofvuil wordt gejut. Wanneer dan echter in zijn computer creditcardnummers, wachtwoorden, en documenten over grote strafzaken worden aangetroffen, passeert dat vermoedelijk het niveau van 'geen aandacht voor IT-security'. Hoewel: ik schreef het al, mensen nemen selectief waar, en wat in ieder geval niet wordt waargenomen is de informatie op de harddisk. De computer is er, maar wie heeft ooit feitelijk de informatie op zo'n harddisk gezien? De idee dat die moet worden beveiligd, kan daarom al snel aan de aandacht ontsnappen: je ziet, hoort voelt, of ruikt die informatie immers niet.
- De informatie zou eenvoudig kunnen zijn beveiligd. Een programma als Word biedt de mogelijkheid om documenten met een password te beveiligen. Een simpele beveiliging die door een doelgerichte cracker relatief eenvoudig kan worden doorbroken, maar het is beter dan niks. Waarom heeft die man dat nou niet gedaan, vraag je je dan af. En betere manier om informatie te beveiligen, die ook kan worden gebruikt voor het absoluut veilig uitwisselen van e-mail is natuurlijk gebruik maken van PGP/GPG*, waarover ik al eerder in Pictogram heb geschreven. Maar wachtwoorden en creditcardgegevens onbeveiligd op je computer laten staan? Stom!

Schokeffect

IT-security is een mentaliteitskwestie. Het voorval met Tonino's computer illustreert dat weer eens op saillante wijze. De auto-industrie heeft beveiliging inmiddels ontdekt: auto's worden aangeprezen door hun veiligheid te benadrukken: kooiconstructies, kreukelzones, airbags, ABS en wat al niet meer hebben de plaats ingenomen van topsnelheid en acceleratievermogen uit de advertenties van weleer. Iedereen sluit ook keurig na gebruik zijn of haar auto af.

De IT-wereld is zover nog niet. Persoonlijke aandacht voor de beveiliging van de eigen computer is nog ver te zoeken. IT-security is daarom afhankelijk van schokeffecten en impulsen zoals het Tonino-incident en van roependen, soms in de woestijn, zoals

Frank B. Brokken
Security Manager

(Voorzien van niet te kraken bestand met privé-data)

* **www.pgpi.org, www.gnupg.org/gph/en/manual.html**