Problematisch internetgebruik

Frank Brokken
f.b.brokken@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.

Heeft u wel eens van CERT-NL gehoord? Zo niet, dan is dit een mooie gelegenheid om daar eens over te worden geïnformeerd, zo aan het einde van het jaar.

www.CERT.nl

CERT-NL is de Nederlandse tak van het 'Computer Emergency Response Team'. Eigenlijk zijn er meerdere van dat soort teams, ook de RUG heeft zo'n team, dat onder de vlag van Terena is geïnstalleerd.

Ernstige klachten

Hoewel de RUG dus zelf zo'n CERT-team heeft, hebben we ook te maken met de landelijke CERT-NL. Onze relatie met CERT-NL is eigenlijk een heel eenvoudige, omdat we door onze relatie met SURF(net) ook nauw betrokken zijn bij SURFnet-CERT. SURFnet-CERT vermeldt op haar website (merk op dat ook SURFnet-CERT net zoals wij met gepaste trots vermeldt dat het als een 'Level 2 CSIRT' is geregistreerd):

> "SURFnet-CERT is het Computer Emergency Response Team van SURFnet, de Internet provider voor het hoger onderwijs en vele onderzoeksinstellingen in Nederland. SURFnet-CERT onderzoekt en coördineert alle gevallen van beveiligingsinbreuken, die afkomstig lijken te zijn van de SURFnet-klanten of waarbij SURFnet-klanten het slachtoffer zijn geworden."

SURFnet CERT

De manier waarop SURFnet die coördinatie uitvoert, is eigenlijk tamelijk eenvoudig: stel er komt een officiële klacht binnen bij SURFnet-CERT. Het SURFnet-CERT team onderzoekt welke organisatie de klacht lijkt te hebben veroorzaakt en stuurt de klacht dan door naar de desbetreffende SSC (Site Security Contact). De SSC zorgt ervoor dat de klacht wordt verholpen, en meldt de klacht dan af bij SURFnet-CERT.
Dergelijke klachten zijn eigenlijk altijd van ernstige aard. Een computer die op grote schaal spam verspreid, of waarvan 'Denial of Service Attacks' worden uitgevoerd, kan aanleiding zijn tot een klacht die ons vanaf SURFnet-CERT bereikt. In het algemeen zijn dit de wat 'ernstiger' klachten, die het niveau van een doorsnee 'abuse'-melding overstijgen.

Actieve beveiliging

We krijgen ongeveer twee keer per week zo'n klacht vanaf SURFnet-CERT toegespeeld. Soms zijn het er meer, zoals aan het einde van afgelopen voorjaar toen plotseling een groot aantal RUG-computers besmet waren met een virus dat verantwoordelijk was voor de verspreiding van spam.

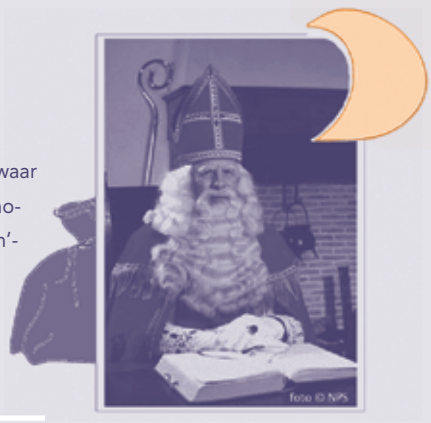
Meestal is het voldoende om de gebruiker van de computer die de overlast veroorzaakt op het ge-

constateerde probleem te wijzen, waarna in goed overleg het probleem wordt verholpen. Dat gaat vrijwel altijd goed, en illustreert de positieve instelling die de meeste universitaire gebruikers ten aanzien van beveiliging hebben. Die posititieve instelling is mogelijk

niet altijd manifest, maar vaak op z'n minst latent aanwezig. Vooral nadat iemands computer het slachtoffer is geworden van een beveiligingsincident zie je dat men bereid is een actievere rol in de beveiliging van de eigen computer te spelen.

Maar het is natuurlijk niet alles goud wat er blinkt. Soms zit er ook wel eens wat blik tussen het goud. De zogenaamde rotte appel.

In het geval van 'rotte appels' krijgen we bij herhaling een klacht over dezelfde computer. Wanneer dat ernstige vormen aanneemt, kan SURFnet besluiten de desbetreffende computer af te koppelen van het internet. Uiteraard vinden we dat niet prettig, want zo'n situatie doet ons als universiteit ook weinig goeds.
Onlangs deed zich zo'n situatie voor. Nadat bij herhaling een klacht over een computer was ontvangen, besloot SURFnet dat de maat wel vol was, en werd de desbetreffende computer enige tijd van het internet afgekoppeld. Zoiets wil natuurlijk wel helpen, zou je denken. Maar nee: de aansluiting was nog niet hersteld of de klachten begonnen opnieuw.
Wat kunnen we daar nou tegen doen? Na alle goede woorden, na het wijzen op onze 'Gebruiksregels', nadat op ruime schaal hulp en ondersteuning is aangeboden, gaat op een gegeven ogenblik het RUG-belang zo zwaar wegen dat de 'wie niet horen wil, moet maar voelen'-procedure van stal moet worden gehaald. Helaas, maar waar.



Mee naar Spanje

In nauw overleg met de juridische afdeling van de RUG is daarom een procedure opgesteld waarmee we dergelijke situaties, wanneer ze zich voordoen, kunnen bestrijden. De procedure gaat ongeveer als volgt:

1. Bij de eerste klacht wordt de gebruiker op de gebruikelijke manier geïnformeerd en gevraagd het probleem te verhelpen. Daarbij kan natuurlijk assistentie door helpdesk en/of IT-Team worden geboden.
2. De computer wordt van het internet afgesloten wanneer daarvoor, gezien de aard van de klacht, aanleiding bestaat. Nadat het probleem is verholpen, wordt de aansluiting weer hersteld.
3. Wanneer echter bij herhaling klachten over dezelfde computer worden ontvangen, wordt deze voor langere tijd van het internet afgekoppeld. Ook kan onderzoek van de computer en mogelijk herinstallatie van de software noodzakelijk worden geacht, uit te voeren door leden van het RUG-Crashteam. Aan dit onderzoek en herinstallatie zijn dan kosten verbonden, die tot € 600 kunnen oplopen.

Maar, zoals opgemerkt, zo'n situatie doet zich in de praktijk natuurlijk zelden of nooit voor. Het is een beetje zoals we ons dat uit onze kindertijd kunnen herinneren: Sinterklaas komt eigenlijk altijd alleen maar langs met kadootjes. Gevallen waarin onze vriendjes en vriendinnetjes of - o, griezel - wijzelf door de Sint werden uitgenodigd om maar eens in de zak mee naar Spanje te gaan kunnen we ons toch eigenlijk niet herinneren, nietwaar? Zo moet het ook maar blijven....

Ik wens iedereen een prettig en veilig nieuwjaar toe,

Frank B. Brokken
(heeft van alles in Spanje meegemaakt)

Links

- CERT-NL:
  www.cert.nl
- Terena:
  www.ti.terena.nl
- CERT-team van de RUG:
  http://security.rc.rug.nl/about/achtergrond.php
- SURFnet-CERT:
  http://cert.surfnet.nl
- Denial of Service Attacks:
  http://news.com.com/Security+from+A+to+Z+DDoS/2100-7349_3-6138447.html
- De Gebruiksregels:
  https://security.rc.rug.nl/docs/aup/aupnl.php
- Procedure problemen pc-gebruik bij de RUG:
  https://security.rc.rug.nl/docs/probleemgebruik.php
- Meer informatie over het RUG-Crashteam:
  http://security.rc.rug.nl/crashteam