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

It's now or never

Frank Brokken is security manager bij het CIT. 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.

Nou, dat was een onverwacht grote oogst. RUG-medewerkers en -studenten kregen een door de projectgroep Risk Awareness gecomponeerde phishing mail.

Er zijn ruim 11.000 e-mails verzonden. Ruim 3.000 ontvangers hebben de mail ook daadwerkelijk gelezen, waarvan ruim 2.500 keer de phishing-link is gevolgd, terwijl het phishing-formulier zelf, waarin gebruikers onder andere naar hun wachtwoord werd gevraagd, ongeveer 900 keer is ingevuld. Dat laatste hoeft natuurlijk niet te betekenen dat ook de feitelijke login-gegevens zijn ingevuld. Er zijn ook gebruikers die onzininformatie hebben ingevuld omdat het hen duidelijk was dat het hier een phishing-poging betrof.

Toch heeft de actie ertoe geleid dat kort na de het versturen van de mail ruim 150 passwords zijn gewijzigd, terwijl dat op een doorsneedag zo'n dertig keer gebeurt. Hulde wat mij betreft aan de projectgroep Risk Awareness, die deze fraaie phishing-poging heeft bedacht en gerealiseerd.

Ook de nazorg was goed geregeld. De telefoons bij de CIT-Servicedesk stonden roodgloeiend, extra medewerkers waren nodig om alle verontruste (en soms ook geïrriteerde) telefoontjes te beantwoorden.

Grote schoonmaak

Diverse leden van de RUG-gemeenschap namen de mail voor waar aan en hebben acuut hun (volgens de phishing mail overvolle) mailbox opgeruimd. Dan denk ik al snel: zo nu en dan kan een grote schoonmaak geen kwaad, maar sommige 'slachtoffers' waren kwaad dat ze de phishing mail niet op waarde hadden geschat en prompt een deel van de inhoud van hun mailbox hadden verwijderd. Voornamelijk kwaad op zichzelf, hoop ik, want - wees reëel - dit is niet de eerste keer dat we met phishing mails te maken hebben gekregen. Sterker nog: al geruime tijd sturen we waarschuwingen uit om vooral alert te zijn op phishing mails, en eerst eens goed te kijken waar je je login-gegevens invult voordat je die informatie ook feitelijk verstrekt.

Adviezen phishing

SURFnet, en ook de projectgroep, geven een aantal aanwijzingen om phishing mails te kunnen herkennen (zie bijvoorbeeld **http://www.surfnet.nl/nl/Thema/cybersafe/identiteit/Pages/Phishing.aspx)**.

De projectgroep noemt de volgende nuttige adviezen:

1. Geef nooit je inlogcode of wachtwoord.
   Dat is een voor de hand liggend advies. Maar het betekent ook dat logingegevens niet zomaar op een webpagina moeten worden ingevuld. Voor de RUG geldt dat logingegevens alleen maar via beveiligde verbindingen worden gevraagd. Een beveiligde verbinding begint altijd met https://. Let op: de 's' moet erbij staan. Is dat niet het geval, vul je logingegevens dan niet in.

2. Gebruik een sterk wachtwoord.
   Een sterk wachtwoord is zelfs niet te raden door mensen die je kennen. Het is altijd een combinatie van letters, cijfers en tekens.
   Ook hiervoor biedt SURFnet een pagina met adviezen (**http://www.surfnet.nl/nl/Thema/cybersafe/wachtwoorden/Pages/Stappenplan.aspx**). Neem de moeite deze pagina eens te bekijken en vraag je af: is mijn wachtwoord wel veilig genoeg?
3. Wees voorzichting met 'links' in e-mails, typ liever zelf een weblocatie in.
   Op zich een juist advies, maar wie wel eens goed naar een aantal locaties heeft gekeken, weet ook dat die vaak niet eenvoudig te typen zijn. Neem bijvoorbeeld een korte locatie zoals deze op YouTube: **http://www.youtube.com/watch?v=ui442IDw16o**
   Op zich geen onmogelijk lange locatie, maar de merkwaardige tekst achter het vraagteken maakt het toch lastig om in te typen. Nou is dat YouTube, maar onze eigen webfaciliteiten kunnen er wat van:
   http://myuniversity.rug.nl/gadgets/ifr?url=http%3A%2F%2Fgadgets.rug.nl%2Fgadgets%2Fmodules%2Frugmail%2Frugmail.xml&container=default&view=home&lang=en&country=%25country%25&debug=1&nocache=1&sanitize=%25sanitize%25&v=da6ab91cd4530de9e6334b589b606782&st=default%3AwFYdNc_0lg6f6b439iykI7uk3_Kxf_jz40j_QBPmDdOI67_2F2Sh0gklBbzkXJ8Y2ZvVjIBrTH72VZXdtKCDw1MYV_3p_ETjq7_fbXjpB2BGyAyQ0xCot0ojT3be4IhbBiiyqEInbc_AOrVQKM_iv3SJWVqrLfh4CtAJQ5jLgltt5pTaQp7G6O8E-_4aJtuivx9YA&testmode=0&parent=http%3A%2F%2Fmyuniversity.rug.nl&mid=0#
   Ga dat maar eens intypen (voor de geïnteresseerde: ik heb het niet zelf bedacht, maar deze link vond ik bij een aankondiging voor een colloquium bij Technische Bedrijfskunde).
   Nee, er moet een andere manier zijn om een locatie over te nemen.
   Nou zijn deze http://-locaties interessant omdat je nu al a-priori weet dat je logingegevens er niet in moeten worden ingevuld. Sommige browsers laten http:// ook gewoon weg, wat synoniem is met: dit is een onveilige verbinding.

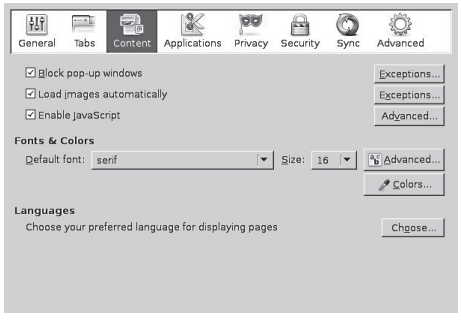
Urgentie

4. Een beveiligd webadres begint met 'https' en heeft een intact slotje.

Een prima advies! Wanneer kun je je logingegevens wel invullen? Twee eisen:

- de link moet beginnen met https://
  Als dat het geval is, weet je zeker dat de verbinding beveiligd is en dat de informatie tussen webbrowser en webserver niet kan worden afgeluisterd.
- voor de RUG geldt dat het eerste deel (achter https://) tot aan de eerste 'slash' (/) moet eindigen in 'rug.nl'. Niet 'rug.nl.cn', niet 'rug.ru', niet 'rug-mail.de', etc. Alleen: 'rug.nl'. Er staat dan dus 'https://xxx.yyy.rug.nl/etc/etc
  ^ ^^^^^
  Let op de 's' bij 'https', let op de tekst tot aan de eerste / na https://, dat moet eindigen in 'rug.nl'.

5. Betrouwbare organisaties vragen nooit om SNELLE reactie via een link of snelle installaties van programma's. Er is nooit sprake van urgentie bij informatie die door de RUG verstuurd wordt. Het is nooit 'it's now or never'; er is altijd voldoende tijd om, bijvoorbeeld, de CIT-Servicedesk eerst te bellen (363 3232).
6. Sluit popups altijd af met een kruisje, en niet door op OK te drukken.
   Webbrowsers geven je ook de optie om popups te blokkeren (met de mogelijkheid om uitzonderingen aan te geven)



7. Bij twijfel kun je bijvoorbeeld de website **www.virustotal.com** gebruiken om (kleinere) bestanden en url's te checken.

Strijd nog niet gestreden

Nou zou je verwachten dat deze actie tot flink wat bewustwording op het gebied van phishing zou hebben geleid. Maar een paar weken na de actie ontvingen RUG-medewerkers de volgende prachtige (hier iets ingekorte) tekst (met dank aan CIT-collega Jan Jonkman):

We wish to inform you that the United Nations (UN) has authorized us to remit to you a total amount of 1,500,000.00 USD (One Million Five Hundred Thousand United States Dollars). This amount is to be paid to you because of the fact that you were selected as a beneficiary in the Last E-mail ballot promotion Held in Malaysia, by United Nations Poverty Alleviation Program. This Program is inline with the Social responsibility of the United Nations Organization, which is held once Every year to change the living status of five (5) lives around the Globe. This year, yourself and Four (4) other people were randomly selected. On behalf of the United Nations Organization, we wish to congratulate you formally. The funds was paid out to us, by the United Nations, And they have successfully succeeded in depositing your whole funds with us Here at Western Union Malaysia. They have now ordered us to take full Responsibility in the transfer process of your funds and thus commence the Immediate remittance of your funds to you.

Be strongly informed that because Of our Western Union transfer policy, your funds will be paid to you via our Western Union Daily Transfer limit of 7,600.00 US Dollars. This means that you will Continuously receive a daily amount of 7,600.00 US Dollars from us, and this amount Can be collected from any of our numerous Western Union outlets in your Current location.

To begin receiving your daily payment as stated above, we need you to provide Us with; Your Full Name, Address, and Phone Number. Upon receipt of the Requested details, your first transaction will be activated by you, before we can proceed to provide you with the Money Transfer Control others after 24 hours of Receiving each payment.

Een gewaarschuwd mens telt voor twee, zou je verwachten? Binnen een uur waren er minstens vijf medewerkers die hierop hadden gereageerd. Ziende blind? Naïef? Hebzucht? Geen idee, maar het is duidelijk dat de strijd tegen de vissers nog niet is gestreden.

Frank Brokken,
Vangt liever vissers dan vis.