E-mail?

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.

E-mail is een prachtig medium. Zo prachtig dat sommigen van mening zijn dat het een bedrijfskritische voorziening is. Dat betekent dat e-mail niet mag uitvallen, omdat de bedrijfsprocessen dan gevaar zullen lopen. Ook binnen de RUG zijn er mensen deze mening toegedaan.

Zo'n belangrijke faciliteit moet natuurlijk ook overal beschikbaar zijn: niet alleen op je werkcomputer, maar ook via webmail en andere programma's waarmee we e-mail kunnen versturen, denk aan de elektronische leeromgeving Nestor.

E-mail is niet alleen voorbehouden aan de goedwillende student of medewerker, helaas krijgen we ook te maken met spam. Dat leidt weer tot de noodzaak om e-mailfilters toe te passen zodat de onverlaten die ons zomaar, ongevraagd, allerlei rommel toesturen meer moeite hebben om hun doel, onze e-mailbox, te bereiken.

Inmiddels heeft iedereen er wel eens mee te maken gehad en ondanks wet- en regelgeving op dit punt lijkt er geen einde te komen aan de stroom spam die bij ons aan de poort wordt aangeboden. Mogelijk dat draconische maatregelen die toevloed op termijn kunnen reduceren, maar dat moet nog blijken.

Honderden mailtjes

Gerelateerd aan spam is een fenomeen dat onlangs een aantal leden van onze universitaire gemeenschap overkwam. Ze werden geconfronteerd met klachten over e-mail met vervelende inhoud die ze gestuurd zouden hebben naar andere medewerkers en studenten van onze universiteit. Niet zomaar een enkel mailtje, maar honderden.

Voer voor de Security Manager? Uiteindelijk wel, maar in eerste instantie leek het daar niet direct op. De eerste reflex was de gedachte dat ofwel de betrokkene zich even niet onder controle had, ofwel slordig was geweest en zijn/haar mailprogramma 'open' had laten staan waardoor iemand anders misbruik van het account heeft kunnen maken. En eigenlijk denk je dan onwillekeurig toch aan het laatste.

Opzettelijk misbruik maken van de geboden faciliteiten is natuurlijk onbehoorlijk, maar ook voor nalatigheid die tot misbruik leidt, is de eigenaar van een account volgens de Acceptable Use Policy (zie ook **http://security.rug.nl**) verantwoordelijk.

Maar hoewel grote hoeveelheden e-mail vanaf individuele accounts werden verstuurd, was er hier toch geen sprake van nalatigheid door de eigenaren van de desbetreffende accounts. In feite was er sprake van een veel fundamenteler probleem, dat in beveiligingsland bekend staat als 'Security By Obscurity'.

Obscurity is no substitute for security.

Van Dale's groot woordenboek der Nederlandse taal geeft voor 'obscuur' de volgende betekenissen: donker, duister, vaag, onbekend, bekend in minder gunstige zin en

'wat het daglicht niet kan velen'. Een boeiende serie betekenissen, die goed passen bij de aanduiding 'Security By Obscurity'.

Met 'Security By Obscurity' wordt de schijnbare veiligheid bedoeld in een in feite onveilige situatie. De schijnbare veiligheid is een illusie, die maakt dat betrokkenen van mening zijn dat 'er niks aan de hand is' terwijl er in feite sprake is van concrete risico's. In het geval van de massale e-mail-verspreiding: er werd gebruik gemaakt van de elektronische leeromgeving Nestor, waarna de gebruiker op de voorgeschreven wijze de Nestor-sessie afsloot. Toch kon een onverlaat daarna zonder enig probleem namens de vorige gebruiker opnieuw verbinding maken met Nestor, en zo de gewraakte hoeveelheden e-mail versturen.

Werkbare omstandigheden

'Security By Obscurity': een slechte manier om te beveiligen, omdat de mogelijkheden om misbruik te plegen vroeg of laat toch aan het licht komen ('wat het daglicht niet kan velen'...). De beste manier die ik ken om 'Security By Obscurity' te voorkomen, is er niet voor weg te lopen. Het is beter om juist vanaf het begin van elk ICT-project een open oog voor de beveiligingsaspecten te hebben.

Aandacht voor de beveiligingsaspecten van een project is, zoals bij het Nestor-misbruik weer eens is gebleken, niet vanwege vergezochte mogelijkheden van misbruik, maar vanwege het realiseren van werkbare werkomstandigheden. Daar kan iedereen aan meehelpen: verstop de beveiligingsproblematiek niet, maar maak het een expliciet punt van aandacht.

Naast een Security Manager heeft de RUG ook een 'Security Kernteam'. Aarzel niet om advies van het Security Kernteam in te winnen over de beveiligingsimplicaties van een project. Dat kan altijd, en het is beter dat vroeg

in de looptijd van een project te doen dan laat, wat weer beter is dan helemaal niet.

In het geval van Nestor en (helaas) van veel andere kant-en-klaar geleverde programmatuur is er niet zoveel dat we nog kunnen doen wanneer, na aanschaf, problemen worden geconstateerd. In het geval van Nestor is bij de leverancier een urgent 'security ticket' aangemeld. Ik ga ervan uit dat het geconstateerde probleem binnen afzienbare tijd (en zeker tegen de tijd dat deze Pictogram in druk verschijnt) zal zijn verholpen. Maar in alle gevallen geldt natuurlijk 'boer pas op je kippen': misbruik is snel mogelijk, en de hackers behoren tot de slimste en vindingrijkste mensen in ICT-land.

Nou was het incident met Nestor tamelijk uniek in de zin dat Nestor op de computer van waaraf een verbinding met Nestor werd gemaakt informatie achterliet die door anderen kon worden gebruikt om opnieuw, namens de laatste gebruiker, in te loggen op het Nestor-systeem. Maar zodra er sprake is van een verbinding tussen twee computers, is alle informatie die tussen die twee computers wordt uitgewisseld onderschepbaar op elke tussenliggende computer.

Afhankelijk van de afstand tussen die computers en de organisatie van het netwerk waar de computers deel van uitmaken, kan dat variëren van enkele tot honderden computers. Webbrowsen met uw webbrowser is in dat verband niet zo'n groot probleem (even aannemend dat geen misbruik op afstand van uw webbrowser kan worden gemaakt, maar hoe aannemelijk is dat eigenlijk?).

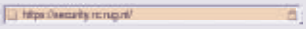
De 'bad guys' weten dat natuurlijk ook, en maken veelvuldig van dit gegeven gebruik om gebruikersnamen en wachtwoorden uit de informatie te plukken die tussen computers wordt uitgewisseld. Ook in dat soort situaties is er natuurlijk niet direct sprake van opzettelijke nalatigheid van de gebruiker. Wel van de systeembeheerder die niet heeft voorkomen dat uw login-gegevens op voor derden leesbare wijze tussen computers wordt uitgewisseld. Het resulterende misbruik van uw account is er evenwel niet minder vervelend om.

Positieve security-mentaliteit

Wat kan er nou gedaan worden om dit soort misbruik te voorkomen? Een belangrijk aangrijpingspunt zit bij de systeembeheerders. Gelukkig heeft de doorsnee systeembeheerder een positieve 'security-mentaliteit' en zal hij/zij graag meewerken aan het oplossen van geconstateerde beveiligingsrisico's op de beheerde systemen.

Maar als u zelf geen systeembeheerder bent, kunt u ook een bijdrage leveren aan het voorkomen van beveiligingsincidenten zoals met Nestor.

In principe zouden alle verbindingen die u maakt met andere computers (bijvoorbeeld die waarbij u uw browser gebruikt) versleuteld moeten zijn wanneer u uw gebruikersnaam en wachtwoord moet opgegeven. In uw webbrowser kunt u eenvoudig zien of er sprake is van zo'n beveiligde verbinding: er staat dan een slotje in het locatievenster bovenin uw browser, en de verbinding begint met 'https'.



Is dat niet het geval en er wordt u toch gevraagd uw gebruikersnaam en wachtwoord in te typen, wees dan op uw hoede: het is dan erg waarschijnlijk dat uw login-gegevens voor iedereen leesbaar over het internet wordt verstuurd. Gebeurt zoiets in RUG-verband, aarzel dan niet, en neem contact op met uw Security Manager,

Frank Brokken
(veilig communicerend)