Woensdag Gehaktdag?

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.

Onlangs werd een werkstation binnen het RC 'gehacked'. Een vervelende en in potentie gevaarlijke gebeurtenis, niet alleen voor de desbetreffende gebruiker. Het is overigens nog maar de vraag of de gebruiker er zoveel last van heeft gehad, want hij was op het moment dat het gebeurde afwezig, genietend van een welverdiende vakantie.

Waarom vond deze 'hack' plaats, waarom was deze nou zo potentieel gevaarlijk, en hoe kun je voorkomen dat hackers toegang krijgen tot onze computers? Voor de RUG geldt dat er twee elementen zijn die ons tot een aantrekkelijk doelwit voor hackers maken. In de eerste plaats is dat de 10 Gb grote bandbreedte waardoor de inbreker een bijzonder snelle toegang krijgt tot het internet: leuk voor 'Denial of Service'-aanvallen, waarbij de aangevallen persoon of organisatie effectief van het internet wordt afgesloten doordat men plotseling wordt gebombardeerd met een enorm groot aantal connecties, die dan (uiteraard) niet alle kunnen worden afgehandeld. Het resultaat is dan dat bijvoorbeeld de mail niet meer aankomt en de webserver 'down' gaat.

Een tweede element dat ons aantrekkelijk maakt voor hackers is de grote dataopslagcapaciteit van de RUG. In het verleden hebben we gezien dat bijvoorbeeld printers werden gebruikt voor de opslag van illegaal gekopieerd werk. Wie een printer open toegankelijk aan het internet koppelt, vraagt om dit soort moeilijkheden.

Binnen een minuut

Het is gemakkelijk om jezelf in slaap sussen met de gedachte dat het wel heel toevallig zou zijn wanneer nu juist jouw computer of printer het slachtoffer zou worden van een aanval, maar dat is naïef. Wie een Windows-systeem 'out of the box' installeert en aan het internet hangt, kan ervan uitgaan dat dat systeem binnen een minuut (meestal gaat het sneller, zoals bleek tijdens de indertijd georganiseerde Honeynet-cursus) is gekraakt.

Wie zich afvraagt hoe dat kan: het antwoord is dat een enorm leger van 'script kiddies' constant bezig is het internet af te stropen naar 'open computers'.

Deze script kiddies doen niet veel meer dan het starten van een klein programmaatje (een script) dat het werk voor ze doet. Kennis en inzicht zijn niet vereist. Zo verging het waarschijnlijk ook onze gehackte computer. De script kiddie vond een opening en de inbraak was een feit.

Onze gehackte computer werd echter primair gebruikt door een medewerker die vanuit zijn werkplek een aantal productiesystemen van de RUG moest kunnen bereiken, zoals het webplatform. Om toegang tot het webplatform te krijgen, worden gebruikersnamen en wachtwoorden gebruikt. Doordat Windows de neiging heeft het leven van de gebruiker te veraangenamen, probeert Windows om deze informatie intern op te slaan, zodat het 'vervelend intypen van username en password' niet telkens opnieuw wordt vereist.

Een aardig gebaar, zeker, totdat iemand zich ongewenst toegang tot de computer verschaft, de toegangsinformatie vindt en vervolgens toegang heeft tot weer andere computers (die dan ook kunnen worden gecompromitteerd). Veel fantasie is niet vereist om te bedenken wat er dan zoal op de RUG-website zou kunnen komen te staan.

Tegen zo'n doemscenario zijn goed maatregelen mogelijk, onder andere door usernames en passwords niet in de computer op te slaan, maar in je hoofd (kijk bijvoorbeeld eens op **https://security.rc.rug.nl/apply/password.php**).

Kwetsbaar voor inbraak

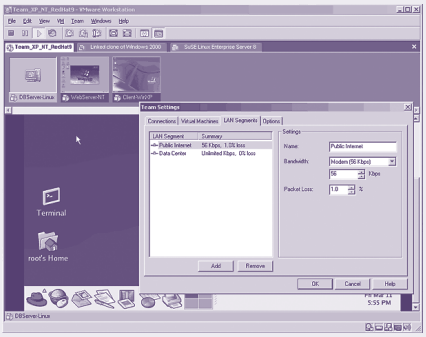
Zo'n 'fan-out' van een hack is absoluut niet denkbeeldig, en de script kiddie heeft ook de mogelijkheid om toegangsinformatie op een computer met behulp van een script op te zoeken. Maar een computer laat het natuurlijk niet zomaar toe dat iemand van buitenaf toegang krijgt, toch?
Zou dat wel zo zijn? Hoe zit dat met uw computer, beste lezer? Langs welke weg kan een script kiddie (of wie dan ook) toegang krijgen tot uw systeem? Wie het antwoord niet weet is in principe kwetsbaar voor inbraak. Maak eens de vergelijking: u weet toch ook of u bijvoorbeeld uw huis en auto fatsoenlijk heeft afgesloten? Waarom weet u dat dan niet voor uw computer?

In het geval van de RC-computer bleek het probleem te zijn ontstaan door een niet goed beveiligde testapplicatie die de medewerker uit de aard van zijn werkzaamheden zo nu en dan moest gebruiken. De job moet af en al te veel ruimte voor het goed configureren van zo'n applicatie is er dan niet; zo werkt dat nou eenmaal.
Een spannende ontwikkeling, waarvan je je afvraagt hoe zoiets in de praktijk kan worden voorkomen. Tenslotte moet de medewerker z'n werk kunnen doen, maar willen we aan de andere kant ook voorkomen dat dat werk tot schade op eigen of andere computers leidt.
In zo'n geval is het een goed idee om een beveiliging te realiseren die uit een paar gevarieerde lagen bestaat. Niet een enkele firewall, maar meerdere. Verschillende vormen van beveiliging toepassen heeft het voordeel dat de inbreker meerdere barrières moet nemen waardoor detectie makkelijker wordt en de vereiste inspanning groter, wat weer leidt tot grotere onaantrekkelijkheid voor de script kiddie. Daarnaast kan bij een beveiliging in lagen een enkele laag (bijvoorbeeld voor onderhoud) even worden uitgezet, zonder dat het direct consequenties heeft voor de beveiliging van de computer waar het allemaal om gaat. Redundantie dus.

Virtuele besturingssystemen

Zo'n gevarieerde beveiliging hebben we gerealiseerd door toegang tot de computer te beperken tot systemen die binnen het RC zijn opgesteld. Zo'n toegangsbeperking kan aan de (switch) poort eenvoudig worden gerealiseerd.
Een volgende laag bestaat uit een lokale firewall. De lokale firewall kan worden gebruikt om redundantie en 'fine-tuning' te bewerkstelligen, door bijvoorbeeld alleen de directe collega's en het systeembeheer toegang te verlenen. Windows Service Pack (SP) II bevat standaard een firewall, dus waarom zou u daar geen gebruik van maken?

Ai, dat leidde tot een nieuwe complicatie. De medewerker zei geen gebruik te *kunnen* maken van SP II vanwege de testapplicatie. Omdat we echter van alle markten thuis zijn, werd ook daar een goede oplossing voor gevonden (en een oplossing die op grote schaal navolging verdient): het is mogelijk om binnen een computersysteem extra (virtuele) besturingssystemen te gebruiken. De benodigde programmatuur wordt geleverd door VMWare (**www.vmware.com**). Een VMWare-omgeving kan worden gebruikt om Windows binnen Windows, Windows binnen Linux, Linux binnen Windows of Linux binnen Linux te installeren. In het plaatje wordt een



voorbeeld gegeven van RedHat Linux (**www.redhat.com**) binnen een Windows-systeem.

De VMWare-installatie kan volledig worden afgeschermd van de buitenwereld, maar het is ook mogelijk om geselecteerde delen van de buitenwereld toegang te geven. In ons geval kon e.e.a. zo worden ingericht dat de directe collega's toegang kregen tot de *testomgeving*, maar niet tot de *primaire* werkomgeving van de medewerker (dus het onderliggende Windows-systeem).
Tenslotte werden de systemen onderworpen aan een 'security scan', om te controleren of er nog ergens een onbedoelde opening buiten schot was gebleven. Zo'n security scan kunnen we op verzoek voor elk RUG-systeem uitvoeren.
Het aardige van de oplossing vind ik zelf dat de oplossing enerzijds generiek is (toegang op poortniveau werd met een paar zeer generieke regels gerealiseerd); weinig extra kosten met zich meebrengt (aan het gebruik van een VMware virtuele omgeving zijn geen kosten verbonden); terwijl er ook ruimte is voor individuele aanpassingen door de lokale firewall-configuratie. Door een in lagen en soort gevarieerde beveiliging te hanteren, is bovendien een opzet gerealiseerd waar de script kiddies zeer waarschijnlijk hun vingers niet aan zullen willen branden.

Frank B. Brokken
(Bekend met alle variaties)