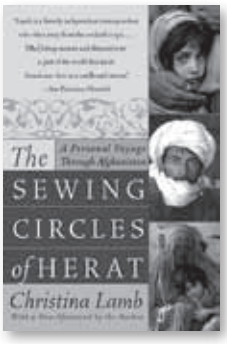
Frank Brokken / f.b.brokken@rug.nl

Default Deny

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.



Afgelopen september was ik in Kabul, Afghanistan. Het is 29 januari wanneer ik dit schrijf en over twee dagen ben ik daar opnieuw. Een interessante ervaring. Er gebeuren spannende dingen in Afghanistan en het is bijzonder om dat van nabij mee te maken.

Uiteraard horen we hier alleen indianenverhalen, maar er worden ook serieuze pogingen ondernomen om het land uit de greep van de Taliban te houden. Ik vind dat een goede zaak: ik kan weinig sympathie opbrengen voor een filosofie die stelt dat handen van vrouwen moeten worden afgehakt wanneer zij hun nagels lakken (Christina Lamb, The Sewing Circles of Herat (Harper, 2004)).

Wederopbouw kennisinfrastructuur

Ook door het CIT is medewerking verleend aan de wederopbouw van Afghanistan. De situatie daar moet je niet onderschatten: na zo'n 30 jaar oorlog is de infrastructuur ter plekke zo ongeveer helemaal vernietigd (en dat geldt dan niet alleen voor de fysieke infrastructuur, maar ook voor de kennisinfrastructuur).

Een paar jaar geleden werd een groep Afghaanse systeembeheerders in de gelegenheid gesteld om bij het CIT de fijne kneepjes van het vak te leren op de wijze waarop we dat ook vrijwel jaarlijks in Nuffic-verband doen. Het bezoek van de Afghanen werd gesubsidieerd door de Nato, die naast een militaire poot ook een afdeling kent die zich actief richt op de wederopbouw van door oorlogsgeweld getroffen landen. Zoiets kunnen wij ons in Europa, na net de nobelprijs voor de vrede te hebben gekregen natuurlijk helemaal niet meer voorstellen: getroffen door oorlogsgeweld...

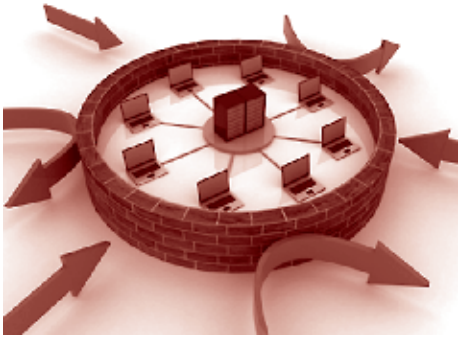
Basisprincipe

Ik ga in deze Pictogram-bijdrage niet uitgebreid in op mijn eigen ervaringen in Afghanistan. Maar de introductie over Afghanistan brengt me als vanzelf bij het hoofdonderwerp van deze bijdrage. Hopelijk verbaas ik de lezer niet teveel wanneer ik nu al vertel dat dat onderwerp over beveiliging gaat.

In Kabul kun je niet zomaar overal naar binnen. Hoe vriendelijk je er ook uitziet, voordat je ergens naar binnen kunt, zul je bewakers voorzien van automatische wapens moeten passeren. Ze inspecteren je bagage en vragen je door metaaldetectiepoortjes te stappen. De foto laat de wachtpost zien bij het Cedar House Guesthouse. Hier vond in september het symposium plaats waar ik een paar presentaties verzorgde.

Het bijzondere aan deze Cedar House-foto is dat het een essentieel kenmerk van beveiliging illustreert: je komt er niet zomaar in. Daar hebben we natuurlijk ook een mooie naam voor bedacht: 'default deny'.

Het default deny-principe stelt dat je ergens niet naar binnen mag, tenzij je er iets te zoeken hebt. Een eenvoudig en algemeen gehanteerd beveiligingsprincipe. Wie wel eens heeft gevlogen weet dat je pas toegang hebt tot de 'gate' nadat je je hebt geïdentificeerd en je 'boarding pass' hebt laten controleren. Andere voorbeelden zijn makkelijk te bedenken; het basisprincipe is steeds default deny.

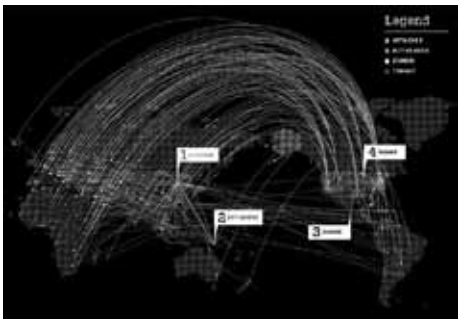


Duizenden connecties

Welk risico loop je wanneer je dat principe niet volgt? In een land als Afghanistan is dat duidelijk: als de kwajongens zomaar binnen kunnen komen kan dat je hele dag bederven. En bij onze IT-infrastructuur? Nog niet zo lang geleden kreeg ik via de webcoördinator van de RUG, Wybe van Dijk, een klacht toegespeeld van iemand uit Denemarken die zich beklaagde dat zijn computer werd gepest door een RUG-computer. Uiteindelijk bleek de situatie iets complexer dan de klager veronderstelde.

Omdat wij standaard verkeersgegevens registreren van al het internetverkeer dat de RUG binnenkomt of verlaat, kon mijn collega Hopko Meijering al snel achterhalen dat de bewuste RUG-computer duizenden connecties per uur afhandelde. Computers verspreid over de hele wereld maakten verbinding met onze computer. Wanneer onze computer nou www.rug.nl was geweest dan was dat misschien nog te begrijpen, maar het betrof hier een gewone computer met een standaard Universitaire werkplek (UWP). Wat was er aan de hand?

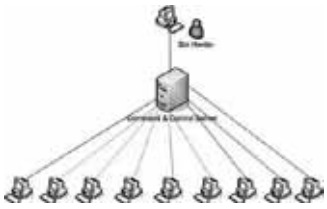
Computers die zonder duidelijke reden zo veel connecties verwerken als de bewuste UWP-computer zijn zeer waarschijnlijk onderdeel van een botnet.



Spin het botnet

Een botnet bestaat uit soms wel duizenden computers die vanuit een of enkele computers worden aangestuurd. De 'botnetmaster' stuurt het botnet aan, meestal met illegale bedoelingen. Zo kunnen de duizenden computers massaal een aanval uitvoeren op een bedrijf ten gevolge waarvan de IT-infrastructuur van dat bedrijf niet meer functioneert.

Voor veel bedrijven is dat een onwenselijk scenario, en het bedrijf kan worden gedwongen om voor een afgesproken tijdstip een fors bedrag over te maken op een niet traceerbare bankrekening, om zo de aanval te voorkomen. Het verkeer dat door zo'n botnet wordt gegenereerd is wereldomspannend, en de bron, de botnetmaster, kan niet eenvoudig worden getraceerd.



Onze computer was waarschijnlijk een spin in een groter botnet. Computers die elders in de wereld zijn opgesteld (waaronder die van onze Deense klager) zijn 'drones' die doen wat de 'botnetmaster' ze opdraagt. Gebruikelijk daarbij is dat de drone de botnetmaster vraagt wat er moet gebeuren.

Zo'n drone moet dan de botnetmaster natuurlijk wel kunnen bereiken. Op dit moment staan we zoiets gewoon toe. Maar een default deny policy sluit deze mogelijkheid effectief af, omdat de drones de botnetmaster dan niet meer kunnen bereiken.

Win-winsituatie

Default deny betekent dat onze computers geen verbindingen meer van buitenaf kunnen accepteren. Voor sommige computers (denk aan webservers of mailservers) is dat natuurlijk niet wenselijk. Maar voor praktisch alle werkstations zal een default deny policy bij de RUG-firewall geen enkel merkbaar effect hebben. Tenzij je voor je werk nou eenmaal inkomend verkeer moet toestaan. Dat is een uitzonderlijke situatie. Maar daarvoor kan eenvoudig een webpagina worden ingericht waarbij een gebruiker aangeeft voor welke computer welk type inkomend verkeer moet worden toegestaan. Naar schatting zal 99% van de RUG-gebruikers deze faciliteit niet nodig hebben, en de resterende 1% zal waarschijnlijk prima overweg kunnen met de mogelijkheid om specifiek verkeer naar zijn/haar computer toe te staan. Een win-winsituatie: ons netwerk wordt veiliger, en gebruiksfaciliteiten worden niet verminderd.

De plannen zijn er, de voordelen worden ook door de CIT technisch directeur Haije Wind, gezien. Er wordt aan gewerkt, maar voor het zover is zal er nog wel wat water door het Reitdiep zijn gestroomd.

Frank B. Brokken.
('default deny', ook zonder Kalashnikov)