Honeypots

ICT-security

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

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.

Toen ik ongeveer zeven jaar was, kreeg ik van mijn ouders een elektrische trein. Een prachtig cadeau, waar ik nog jaren plezier van zou hebben. Ik was onmiddellijk gefascineerd door de ongekende mogelijkheden die mij werden geboden: gevoed door een 4.5 V batterij die was ondergebracht in een schakelkastje, kon ik een locomotief met een paar wagonnetjes in een cirkeltje met constante snelheid voor- en achteruit laten rijden.

Prachtig! Van alles is ermee gedaan: het spoortje werd onder het bijzettafeltje geleid, onder de bank, achter een kast: je kunt het zo gek niet bedenken, of ik heb het gedaan.

Het mooie van zo'n cadeau is natuurlijk dat 't nooit 'af' is. Er is altijd wel een wagon waar je helemaal verliefd op raakt, of een prachtige locomotief. En een paar jaar later had ik dan ook een aardige verzameling rails, wissels en treinen bij elkaar gesprokkeld. Mijn ouders en ik woonden tot mijn twaalfde in een tamelijk kleine bovenwoning, maar daarna verhuisden wij naar een eengezinswoning, met een zolder. Die zolder werd direct geconfisqueerd ten behoeve van de elektrische trein.

Een elektrische trein is een prachtig bezit. Je kunt natuurlijk treintjes doelloos laten ronddollen en zó hard door bochten sturen dat ze massaal ontsporen, maar daar gaat de lol eigenlijk erg snel van af. Vanaf een bepaald moment begon ik me dan ook wat meer te verdiepen in het spoorwegbedrijf. En ik vond in de speelgoedwinkel al snel een paar boeken waarvan de inhoud me wel aansprak.

In één van die boeken werd uitgebreid beschreven hoe een dienstregeling eruit ziet, hoe je er zelf eentje kunt maken, en hoe je, met andere woorden, het 'echte' spoorwegbedrijf kunt modelleren met behulp van je elektrische trein.

Bijzonder boeiend wordt het, wanneer je je gaat richten op de spoorwegautomatisering. Al die treinbewegingen zijn te complex om 'met de hand' in te gaten te houden, en je hebt hulpmiddelen nodig die je het werk ten dele uit handen nemen. Nou praten we begin jaren 60, en op dat moment waren computers nog niet zo alom tegenwoordig als dat momenteel het geval is. Dus als je je rond die tijd als kwajongen op de spoorwegautomatisering stort, dan maak je gebruik van elektromechanische relais, sleepcontacten, mechanische sensoren en draadjes om al die onderdelen aan elkaar te knopen. Zie de 'relais'-foto voor een paar voorbeelden van relais die daarbij zoal werden gebruikt.

Voorbeelden van relais

Wat ik nog steeds erg knap vind van het boek dat mij toen op het pad van de automatisering heeft gebracht, is dat er de waarschuwing in staat om toch vooral niet te veel te automatiseren. Zodra je modelspoorweg volledig is geautomatiseerd, is het net zoals bij die twee beren die broodjes smeren: je staat erbij en je kijkt ernaar. Na te hebben geconstateerd dat alles soepel en op rolletjes loopt, kun je vervolgens niet veel meer dan toekijken en constateren dat alles naar wens verloopt. Zó saai....

Bovenstaande waarschuwing is in zekere zin ook van toepassing op de inrichting van de beveiliging van onze computers. Wanneer we onze computers goed beveiligen (bijvoorbeeld: we installeren goede virusscanners; we houden die up-to-date; we installeren geen onveilige services zoals de beruchte Microsoft webserver; we verversen zo nu en dan passwords (wanneer ook al weer voor 't laatst?); wellicht plaatsen we een firewall voor onze computer; we zorgen voor goede encryptie-faciliteiten zoals Gnu's GPG (**www.gnu.org/gph/en/manual.html**, **www.pgpi.org**), dan komen we vanzelf in een toestand van saaie gelukzaligheid: hoezo is het Internet een gevaarlijke omgeving? Hoezo hackers? Hoezo misbruik van onze computers?

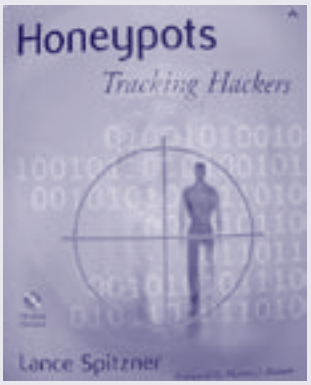
Eerstejaars psychologen leren al dat wij mensen niet goed in staat zijn constante fenomenen waar te nemen. Dat geldt ook voor ICT security. Wanneer je je systemen goed beveiligt tegen misbruik, gebeurt er niks schokkends, en verslapt je aandacht. Passwords worden niet meer ververst, 'security-patches' niet meer aangebracht, en vroeg of laat heeft de hacker vrij spel.
Maar ook al is de hacker nog zo snel, uw Security Manager achterhaalt 'm wel: met behulp van de Dienst Digitale Expertise van de Regiopolitie Groningen, en met ondersteuning van de Officier van Justitie werden onlangs twee inbrekers getraceerd die ernstig misbruik hadden gemaakt van de universitaire ICT-voorzieningen. Met deze hackers, afkomstig uit Heerenveen en Tilburg, is inmiddels door Justitie een 'indringend gesprek' gevoerd.

Hoe voorkom je nou dat de aandacht verslapt, waardoor de hacker vroeg of laat weer vrij spel krijgt? Lance Spitzner suggereert daarvoor de aanpak die je ook goed kunt gebruiken om vliegen te vangen: Honeypots.

Ergens in je netwerk plaats je een aantal computers, die geen andere operationele functie hebben dan er te zijn. Er worden geen security patches op geïnstalleerd, er worden geen speciale beveiligingsmaatregelen op toegepast. Maar ze worden wel nauwkeurig in de gaten gehouden. Omdat deze systemen geen internetverkeer horen te genereren, is elk verkeer in principe verdacht en het begin of gevolg van een inbraak.

De hacker, nietsvermoedend, breekt in op een honeypot-computer. Dit wordt gedetecteerd, waarna een aantal acties kunnen volgen:

- De activiteiten van de hacker worden gelogd, en in de gaten gehouden: dat leert ons het nodige over de bedoelingen van de hacker.
- De hacker's locatie kan worden getraceerd, zoals dat met behulp van Justitie is gebeurd bij de hackers die hun onwenselijke activiteiten vanuit Heerenveen en Tilburg uitvoerden.
- De logs van de activiteiten kunnen worden gebruikt om te voorkomen dat onze aandacht voor ICT-beveiliging afneemt: immers, de logs geven aan dat het RUGnet nog steeds wordt bezocht door onwelkome gasten. Er is geen sprake meer van constante waarneming, en we blijven alert.
- Op het moment dat het ons uitkomt, kunnen we besluiten tegenmaatregelen te nemen: we informeren de desbetreffende internetprovider en/of doen aangifte van 'computervredebreuk', zoals dat zo mooi heet. Inmiddels heeft een aantal hackers al kunnen constateren dat dat geen holle woorden zijn.



Iedereen die meer wil weten over het fenomeen 'Honeypots' kan ik Lance Spitzner's 'Honeypots' ter lezing aanbevelen. Uiteraard kan men ook met vragen en opmerkingen bij mij terecht.

Succes met het vliegen vangen!