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

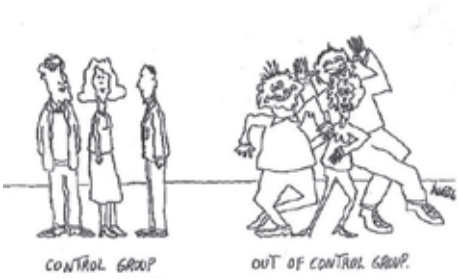
Zomerslaap

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.

Zo tegen de zomer verschuift de belangstelling vanzelf een beetje richting vakantie en lijken de IT-zaken toch op een wat grotere afstand te staan. Niet helemaal natuurlijk, want de kranten staan de laatste tijd bol van de aan IT-beveiliging gerelateerde zaken, en het is gewoon te verleidelijk om die krantenartikelen toch maar even te lezen.

In de NRC-Next van 6 juli j.l. stond een interessant artikel over de economische schade van cybercrime en gerelateerde zaken. Wat blijkt? Het middel lijkt erger dan de kwaal: de feitelijke schade bedraagt niet veel meer dan een paar dubbeltjes per persoon per jaar, en dat is een veel lager bedrag dan wat er in de bestrijding ervan wordt geinvesteerd. Da's toch boeiend, niet? Al die firewalls, spamfilters, virusbestrijdingsmethoden zijn dus eigenlijk maar flauwekul, en vallen in dezelfde categorie als de overtrokken reactie op terrorisme, waarvan de bestrijding ook veel meer kost (inclusief aantallen slachtoffers) dan het fenomeen zelf.

Het probleem met dit soort uitspraken is m.i. dat er eigenlijk altijd een controlegroep ontbreekt. Wat zou de schade zijn geweest wanneer je de beschermende maatregelen niet zou hebben genomen? Zo'n controlegroep ontbreekt meestal, in ieder geval bij 'real life' toepassingen.



In de context van de IT is zo'n controlegroep of controle-experiment nog wel uit te voeren. Een mooi voorbeeld vind ik altijd nog wat we enige jaren geleden hebben gedaan. Toen hebben we, tijdens een 'Honeypot' cursus, een 'out-of-the-box' windows systeem geinstalleerd op een computer en hebben we deze computer vervolgens, met een tot dan toe niet gebruikt IP adres, aan het Internet gekoppeld om te kijken hoelang 't zou duren voordat de 'bad guys' zich meester zouden hebben gemaakt van de desbetreffende Windows bak. Nou, binnen 40 seconden was 't gepiept.

'Real life' controlegroepen kom je minder vaak tegen. Zo vermeldt het NRC-Nextartikel dat de opbrengst bij bankovervallen in het Verenigd Koninkrijk zo gering is, dat de kosten van beveiligingsschermen ter beveiliging van de loketten daar niet tegen opwegen. Ik denk dan: de schermen waren er waarschijnlijk al, en wat zouden de bedragen zijn geweest (en de emotionele weerslag op de lokettisten) wanneer die schermen er niet waren geweest?

The lure of the honeypot ant

Laten we een door het toeval bepaalde scheiding aanbrengen tussen bankfilialen: sommige voorzien we van beveiligingsschermen en andere niet. Vervolgens wachten we een paar jaar om de overvallers een eerlijke kans te geven om hier en daar eens een overval te plegen, waarna we de ontvreemde bedragen en het ziekeverzuim onder de lokettisten van de banken met en zonder beveiligingsschermen met elkaar vergelijken. Een mooi onderzoek, maar welke banken willen hun medewerking eraan verlenen? Nog afgezien van het feit dat we dit soort onderzoek tegenwoordig al snel afkeuren als zijnde 'onethisch'.

Dit soort bevindingen maken toch dat ik niet direct met de meute meejuich wanneer iemand beweert dat beveiliging eigenlijk allemaal maar flauwekul is. In 2007 werd de RUG geconfronteerd met een grote inbraak. Zo'n 300 computers waren ten prooi gevallen aan een groep cyber-inbrekers. Als reactie op dat incident zijn er diverse extra beveiligingsmaatregelen genomen om herhaling en andere grootschalige incidenten te voorkomen. En ja, dat kost geld. Sommige faciliteiten hebben we moeten aanschaffen, maar alle extra maatregelen kosten extra inzet. Leveren die maatregelen nou meer op dan ze kosten? Dat weet je dus niet, want er is nou eenmaal geen control-CIT. Maar er is in ieder geval een aantoonbare spin-off: we weten sinds 2007 wat er speelt in ons netwerk, en we kunnen, ook geruime tijd nadat een incident heeft plaatsgevonden, nog achterhalen wat er precies is gebeurd. Meer in het algemeen: we houden de vinger aan de pols en dat heeft ons sinds 2007 bij herhaling de mogelijkheid gegeven om snel en adekwaat te reageren op feitelijke incidenten of verdachte omstandigheden. Wat dat betreft is de functie van een beveiligingsgroep natuurlijk toch wat bijzonder: als 't goed is merk je er niks van, simpelweg doordat alles goed gaat. En ja, daaraan is ook een risico gekoppeld: het is niet altijd duidelijk of een genomen maatregel niet enigszins 'over the top' is. Om dat te voorkomen zorgen we regelmatig voor onafhankelijke 'peer reviews': security audits door onafhankelijke instellingen of door SurfNET.

Economische schade voorkomen is natuurlijk belangrijk, maar voor de meeste gebruikers van IT-voorzieningen geldt natuurlijk toch ook, en misschien wel primair, dat 'hij het gewoon moet doen'. Waarmee dan wordt bedoeld dat de werkzaamheden die men met de computer wil uitvoeren, onbelemmerd moeten kunnen worden uitgevoerd. Virussen, afgeleid worden door spam, ongeauthoriseerd gebruik van de computer doordat de computer een slaafje is geworden in een botnet, etc., etc., worden doorgaans niet geassocieerd met het onbelemmerd gebruik maken van computers.

Veel misbruik van computers wordt uiteindelijk veroorzaakt door de gebruiker zelf, die zelf trojaanse paarden binnenhaalt door schijnbaar aantrekkelijke software te installeren, die in feite geinfecteerd is met 'malware', of die gedachtenloos onbekende attachments opent. Veel misbruik kan zo worden verklaard; maar niet alle misbruik. Voor die laatste categorie geldt dan weer dat – wellicht - de beveiligingsmaatregelen die 'aan de poort' zijn genomen ertoe bijdragen dat ons netwerk relatief 'schoon' blijft, dat onze computers in het algemeen gewoon kunnen worden gebruikt, en dat we bij een incident vrijwel altijd snel in staat zijn het probleem te isoleren en te verhelpen.

Of dat alles de kosten van de beveiliging waard is? Wie het weet mag het zeggen.

Frank B. Brokken,
genietend van zijn zomerslaap....