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

Wie wil er nou bij mijn computer?

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 zomer was ik kort op bezoek bij vrienden in Amerika. Zoals dat dan gaat, wordt er prompt een barbecue georganiseerd en tijdens de barbecue wordt over van alles en nog wat van gedachten gewisseld. Om redenen die ik maar niet kan achterhalen, is het onderwerp van gesprek opmerkelijk vaak de beveiliging van computers. Waarom zou dat toch zo zijn?

Diepe wijsheid

Een van de opmerkingen die tijdens de barbecue werd gemaakt, hoor ik wel vaker, ook hier in Nederland of zelfs binnen het CIT: "Waarom zou ik me druk maken over de beveiliging van mijn computer? Er zijn zoveel computers in de wereld, waarom *zouden* de 'bad guys' het op mijn computer hebben gemunt?"

Daarna is het stil en word ik geconfronteerd met iets wat lijkt op een triomfantelijke blik, waarmee men kennelijk iets wil communiceren als: "Zo, dat heb ik toch maar even mooi gezegd, en nu ben ik ook mooi van dat gedoe rondom beveiliging af".

Volgens mij was de spreker daar ook al van verlost voordat hij deze diepe wijsheid met mij deelde, en ik vraag me dan op mijn beurt af wat ik met een dergelijke uitspraak moet. Soms beaam ik dan ook maar wat er is gezegd. Want zeg nou zelf: waarom *zouden* de bad guys het op jouw computer hebben gemunt?

Rat

Maar toch, zo'n uitspraak knaagt. Security is altijd een moeilijk onderwerp. Zoals mijn collega Alex Pothaar onlangs nog zei: "Van investeringen op het gebied van security zie je in de praktijk niks terug". Geen 'Return On Investment', zoals dat meen ik heet.

Dat is maar goed ook: je investeert in veiligheidsgordels, luchtzakken en kreukelzones en je hebt ze eigenlijk nooit nodig. Je doet ook geen gecontroleerd experiment, toch? Zo van: laten we eens 1.000 automobilisten loslaten in het verkeer; 500 zonder passieve veiligheidsmaatregelen en 500 met passieve veiligheidsmaatregelen. De chauffeurs worden op basis van toeval in een van de twee groepen ingedeeld en na een jaar kijken we hoeveel er nog van elke groep leven en wat hun kwaliteit van leven is: met of zonder ledematen, dwarslaesie en wat heb je allemaal.

Dat vindt men 'onethisch' en er zijn natuur-

lijk simulaties uitgevoerd die laten zien dat een dummy met een veiligheidsgordel bij een botsing beter af is dan een dummy zonder veiligheidsgordel. Dat zijn dummy's. Ben ik ook een dummy? Ach, vast wel. Ten slotte ben ik ook als de rat in een leerexperiment. Ik ben geen rat (geloof ik) maar ik gedraag me wel zo.

Helemaal niet geïnteresseerd

Maar dat was de vraag niet. De vraag was: waarom zouden de bad guys in mijn computer zijn geïnteresseerd. Hm... Misschien zit er toch wel iets interessants aan die dummy's en ratten.

Bent u wel eens verkouden geweest? Heeft u wel eens een al dan niet ernstig verkeersongeluk gehad? Wel eens griep gehad? Was u rond 2003 ook een beetje bang voor het SARS-virus? En meer recent: beducht voor het eten van groente uit Duitsland? Hele landen besloten toen geen groente meer uit Duitsland te importeren, toch? Hoeveel kippen en geiten zijn er de afgelopen periode in ons land preventief 'geruimd' (wat een mooi eufemisme is voor 'vermoord')?

Verkouden: er zijn zoveel mensen, waarom zou dat verkoudheidsvirus nou *net* bij jou willen zijn? Verkeersongelukken: er zijn elke dag weer zoveel verkeersdeelnemers, waarom zou iemand nou net bij *jou* een ongeluk veroorzaken? Zo kunnen we nog wel meer bedenken: vrijwel iedereen die ik ken doet overdag en zeker 's avonds de deur van zijn huis op slot. Nou zijn er *zoveel* huizen. Waarom zou de dief of junk het nou uitgerekend op *jouw* huis hebben gemunt?

Allemaal acties die we ondernemen omdat we denken dat wij, of datgene dat we bezitten of wat ons dierbaar is, het slachtoffer kan worden van de bad guys. Het bijzondere van deze bad guys is dat ze helemaal niet in jou zijn geïnteresseerd. Ze doen maar wat. Maar omdat het er zoveel zijn, en omdat we het de bad guys in het geval van computermisbruik wel erg makkelijk maken, is de realiteit eerder omgekeerd dan zoals door mijn geachte Amerikaanse vriend is verondersteld: "Ik zou me maar druk maken over de beveiliging van je computer, want de bad guys hebben het uiteraard op jouw computer gemunt."

Binnen een minuut

Een aantal jaren geleden, rond 2004, hebben we hier aan de RUG een cursus 'honeypots' en 'honeynets' georganiseerd. Een honeypot is een computer die nauwkeurig in de gaten wordt gehouden maar die verder 'out of the box' aan het internet wordt gekoppeld (Lance Spitzner is een van de grote namen op dit terrein, zie ook www.tracking-hackers.com).

Tijdens die cursus koppelden we een computer aan het RUGnet waarop Windows out-of-the-box was geïnstalleerd. De computer kreeg een adres binnen het RUG-domein dat niet eerder was gebruikt en dat niet bekend was bij de DNS. Toch werd de computer binnen de minuut gevonden en overgenomen door de bad guys. Er zijn zoveel computers in de wereld, waarom zouden de bad guys nou juist in *die* computer geïnteresseerd zijn?

Bingo

Tja.... Ze zijn er niet in geïnteresseerd, en *toch* wordt je gepakt. Net zomin als het verkoudheidsvirus, het griepvirus, de slechte automobilist, de dief of junk in jou als persoon of in jouw bezit als zijnde *jouw* bezit is geïnteresseerd. Er zijn weliswaar veel computers, en veel mensen, maar er zijn ook veel bad guys. Met computers is het nog vervelender gesteld: je hangt niet zomaar een computer aan het internet, maar zo'n machine is altijd onderdeel van een groter domein: de RUG, xs4all, kpn, comcast, noem maar op. Binnen zo'n domein is vaak wel wat te halen, en een beetje zichzelf respecterende hacker of groep hackers doet regelmatig een scan op de adressen binnen zo'n domein om te kijken of er nog iets nieuws te halen is.

Hackers zijn natuurlijk ook als die ratten bij de leerexperimenten: hebben ze een keer 'beet' dan werkt dat als een beloning en komen ze binnenkort weer terug. 'Beet hebben' kan al betekenen dat er een nieuw adres is gedetecteerd. Weet jij veel wat voor hackers als beloning geldt? Maar reken maar dat het feitelijk binnen kunnen dringen in een computer een belonende ervaring voor ze is. Dus als mijn hackergroep een domein in de gaten houdt en daarbinnen een computer vindt die kan worden geïnfiltreerd, dan is het 'bingo!': men komt terug om ook andere computers te grazen te nemen. En oh wee als dan je beveiliging niet op orde is.

Frank B. Brokken,
Gebruikt een zéér gewilde computer