Rob Kurver

Wie is hier nu de echte bad guy

Het Nederland werd onlangs opgeschrikt door een serie DDoS-aanvallen die onze grootbanken en de belastingdienst meerdere dagen platlegden. Omdat dit gebeurde vlak nadat we de wereldpers gehaald hadden met een verhaal over hoe 'onze jongens van de AIVD' jarenlang stiekem de Russische hackers in de gaten hielden die onder andere geholpen hadden president Trump in het zadel te krijgen, dacht iedereen uiteraard aan een wraakactie vanuit Rusland. Door slim recherchewerk, waaronder het lezen van de fora waar over deze DDoS-aanvallen werd gesproken, wist de Nederlandse politie echter al snel een 18-jarige puber uit een dorpje in Noord-Brabant op te pakken die deze aanvallen schijnbaar met zijn zakgeld organiseerde zodat hij daarna als expert leuk mee kon praten. Gevalletje 'brandweerman die eigen brandjes sticht' om daarna de held te zijn die ze blust, zeg maar.

Ik weet niet wat ik fascinerender vind: dat onze politiemannen en -vrouwen zo goed bezig zijn met opsporing, of dat het blijkbaar voor een puber met een krantenwijk heel eenvoudig is om miljoenen euro's schade aan te richten door banken en overheidsdiensten lam te leggen. Hebben die clubs hun security dan zo slecht op orde? DDoS is toch niet nieuw? Er bestaan toch allerlei handige oplossingen zoals de NaWaS (de Nationale Wasstraat tegen DDos-aanvallen) die dit vrij eenvoudig tegengaat? Waarom gebruiken ze die niet? Wie is hier nu de echte bad guy: de puber met de krantenwijk of de organisaties die hun zaken niet op orde hebben?

Hopelijk is het een wake-up-call voor beleidsmakers en ICT-verantwoordelijken om hun systemen beter te beveiligen. Niet alleen tegen DDoS-aanvallen – die vervelend zijn maar waarbij niets gestolen of beschadigd wordt – maar ook tegen echte hacks waarbij data wordt ontvreemd of misbruikt. In mei gaat de AVG (GDPR voor de internationaal georiënteerden) in werking en worden flink hogere eisen gesteld aan de sector om zijn zaakjes op orde te krijgen. Naar verwachting zal de meerderheid van de grote organisaties niet op tijd klaar zijn met alle technische maar vooral organisatorische aanpassingen, om over het MKB nog maar te zwijgen.

En dit kan echt niet meer! We leven in een wereld waarin data het nieuwe goud is. Kennis is macht, en tegenwoordig komt kennis steeds meer uit data. In 2016 genereerden we met elkaar 7 zettabyte (een zettabyte is een miljard terabyte) data. In 2020 zal dat bijna 45 zettabyte zijn, zegt onderzoeksbureau IDC, waarvan ongeveer een derde als nuttig wordt aangemerkt (er wordt uiteraard ook steeds meer 'ruis' geproduceerd door al onze slimme koelkasten en sensoren overal). Meer dan de helft van die data is vandaag niet goed beveiligd.

Partijen als Facebook, Google en Alibaba hebben afgelopen jaren platformen gebouwd en veelal gratis aangeboden, consumenten verslaafd gemaakt aan sociale media, en gaan die data meer en meer omzetten in waardevolle informatie door middel van Machine Learning en Artificial Intelligence.

Computers worden steeds sneller en slimmer. In 2023 bereiken we 'singularity': het punt waarop een computer evenveel rekenkracht heeft als een menselijk brein. De wereld verandert steeds sneller en wij staan erbij en kijken ernaar hoe grote tech-reuzen de macht naar zich toetrekken. De gewone burger heeft geen benul van wat zich aan het voltrekken is; die wordt in onze primetime tv-programma's voorgelicht door een mevrouw die een boek over security bij elkaar gesprokkeld heeft maar door de echte experts achteraf flink gecorrigeerd moet worden.

Als ICT-sector hebben wij hier collectief mee te maken, en een verantwoordelijkheid te nemen op het gebied van voorlichting. Maar ook om te zorgen voor adequate beveiliging bij onze klanten. Technologie is te belangrijk om aan buitenlandse reuzen over te laten.

Rob Kurver *is ondernemer, consultant en trainer/coach in ICT, telecom en cloudcommunicatie.* ***Reageren?*** *rob@white-rabbit.nl*