Op 15 en 16 november vond in het Rotterdamse WTC voor de 10e keer het internationale symposium plaats voor iedereen die in cyber security geïnteresseerd is. Dit jaar werd de bijeenkomst voor de laatste keer georganiseerd onder 'GOVCERT' vlag. Gelukkig werd op het einde aangekondigd dat het symposium blijft voortbestaan, vanaf volgend jaar onder de vlag van het nieuwe Nationale Cyber Security Center (NCSC).

Bart Jacobs,
hoogleraar computerbeveiliging Radboud Universiteit Nijmegen, lid Cyber Security Raad

Eindelijk op de agenda, na 10 jaar

Oorspronkelijk waren de GOVCERT-bijeenkomsten vooral gericht op het versterken van de onderlinge contacten tussen de internationale "ghostbusters" uit de wereld van CERT (computer emergency response team). Door naar elkaars ervaringen te luisteren en ook samen een biertje te drinken wordt de gemeenschap hechter, en is het makkelijker later Dmitri of Charles te bellen met: "Hey, remember me from the GOVCERT meeting in Rotterdam? … Yes, I had a headache too … No I did not go to the coffeeshop. But, listen, a server on your side is causing real problems over here. Can you shut it down?"

Inmiddels heeft het symposium meer dan 500 deelnemers en is het uitgegroeid tot een brede ontmoetingsplaats. Politie, justitie, inlichtingenwereld, defensie, bedrijfsleven, wetenschap en ook enkele journalisten en hackers lopen er rond. Het voor security conferenties typische mengsel van pakken en paardestaarten luistert naar uiteenlopende voordrachten en discussieert over de nieuwste ontwikkelingen, variërend van economische incentives in information security tot Russische criminelen die rijk geworden zijn met spammen en online medicijnverkoop (maar nu in de bak zitten), en internationale demografische ontwikkelingen waardoor een groot deel van de internetgebruikers in de Derde Wereld komt te zitten (en allerlei creatieve middelen zal gebruiken om er rijk mee te worden).

De zorgen om de kwetsbaarheid van onze computersystemen was de afgelopen tien jaar op GOVCERT symposia steeds aanwezig. Nieuw is dat deze zorgen nu veel breder gedeeld worden: de Tweede Kamer spreekt er het laatste half jaar bijna wekelijks over. De sfeer van zelffelicitaties rond het afhandelen van de DigiNotar-crisis was bij de overheid snel verdwenen door de dagelijkse stroom "Lektober" onthullingen. Het is duidelijk dat dergelijke kwetsbaarheden niet langer getolereerd kunnen worden en dat een combinatie van harde sancties, betere infrastructuur en effectieve (internationale) samenwerking onontkoombaar is. Privacy activisten zien de aanhoudende stroom security kwetsbaarheden als reden om gevoelige persoonsgegevens maar helemaal niet meer in databases te stoppen, terwijl hardliners menen dat juist meer gemonitord moet worden.

Algemeen werd als trend gezien dat cyberspace het nieuwe slagveld gaat worden. De Nederlandse defensie onthulde de contouren van de eigen plannen, bestaande uit een combinatie van defensieve en offensieve capaciteiten. Juist op dit offensieve vlak zullen de cyber soldaten zich dezelfde technieken aan moeten leren die cyber criminelen en spionnen de laatste jaren ontwikkeld hebben: zero day exploits, spear-phishing, botnets, denial-of-service etc. De oorspronkelijk bevrijdende krachten van internet (vrije communicatie en doorbreking van monopolies) dreigen te ontaarden in filtering, afsluiting, balkanisering, diefstal en sabotage. De onvermijdelijkheid van deze ontwikkeling wordt breed ervaren, maar is diep verontrustend.

Naast deze maatschappelijke ontwikkelingen kwamen technische zaken volop aan bod, vooral in de vele parallel sessies: over IPv6, DNSSec, quantum cryptography, advanced persistent threats (APTs), scada en smartphones. Ondanks de bredere belangstelling voor security blijft het een eigen wereld. Een fundamenteel dilemma is het volgende: heb je liever dat je computer "up" is en onveilig, of dat hij "down" is. Een security expert zal kiezen voor "down". De rest van de wereld kiest helaas nog steeds voor "up".