

VELDWIJK

Certificaat van Onvermogen



Terwijl de deadline voor deze column nadert explodeert het DigiNotar schandaal. Het begon met de klassieke reactie van de overheid op vragen van een journalist: ontkennen ... bagatelliseren ... liegen. Normaliter zou de doofpot hebben gewerkt, maar nu gebeurde er iets opmerkelijks. Minister Donner kwam binnen vier dagen twee keer met een persco. Misschien heeft de topbestuurder Donner iets geleerd dat zijn voorlichters nog niet begrijpen. Misschien is er iets verschrikkelijks gebeurd dat Donner wel weet en wij nog niet. Mocht dat zo zijn dan lijkt Donners plotselinge haast te zijn ingegeven door het beperken van aansprakelijkheid: ordinaire *damage control*. Dat er 300.000 Iraniërs door hun wrede overheid zijn afgetapt en er vermoedelijk doden gaan vallen staat sowieso niet centraal.

Uiteindelijk doet het er niet eens toe wat er precies is gebeurd. Het doet er evenmin toe of het bedrijf DigiNotar echt zo onbekwaam is als het nu lijkt. Er zijn wereldwijd nog honderden van dit soort *Certificate Authorities* dus DigiNotar zal niet de enige rotte appel zijn. Wat het DigiNotar schandaal belangrijk maakt is dat het laat zien dat de wereld is veranderd en dat we dat niet goed beseffen. Denk eens terug aan het einde van de vorige eeuw. Hele volksstammen dachten toen dat de wereld vol stond met onderling verbonden ICT-voorzieningen en dat één Y2K bug op de verkeerde plek zou leiden tot een cascade van uitvallende systemen. Op 1/1/00 bleek dat de wereld er anders uitzag en sindsdien wil niemand herinnerd worden aan de niet uitgekomen voorspellingen. Maar sinds Y2K is de wereld wel ingebed in een netwerk van onderling verbonden ICT-voorzieningen. Als het nu niet 2011 was maar 1999, zou de wereld op 1 januari a.s. nog steeds niet vergaan. Maar wat wel is veranderd is dat we afhankelijk zijn geworden van specifieke, globale ICT-voorzieningen waaraan allerlei andere voorzieningen zijn opgehangen in *tightly coupled* modus. Wat zou er gebeuren als volgend jaar – het is dan *solar max* – een zonnevlam de GPS-voorzieningen en de helft van de communicatiesatellieten plat legt? Wat zou er gebeuren als er door de een of andere extreme blunder een Windows update met een *bootbug* wordt uitgerold? Maar verreweg de grootste verandering sinds het jaar 2000 is de mogelijkheid om ICT-voorzieningen op afstand te manipuleren, te plunderen of uit te schakelen. En dat kunnen we allemaal weten als we het nieuws volgen. Russische nationalist (lees: de post-KGB) hebben het Internet van Estland al eens platgelegd. Maar de mooiste stunt is de actie van 'onze' veiligheidsdiensten die met een speciaal virus voor

Siemens apparatuur de hardware van de Iraanse uranium-centrifuges hebben gesaboteerd. De Ayatollahs nemen nu wraak op de zwakste westerse partij – *c'est nous!*

Laat mij als amateur John Le Carré voorspellen wat er tussen nu en tien jaar te gebeuren staat. Een slimme (China?) of desperate (Noord-Korea?) staat of een puur criminele organisatie (Spectre?) investeert in het opzoeken van zwakke plekken en verzamelt in een periode van een jaar of vijf een grote hoeveelheid *soft spots*. Alleen al het dreigen met het tegelijk activeren van alle ICT-bermbommen, waarschijnlijk voorafgegaan door een kleine demonstratie, is in 2020 al voldoende voor het creëren van een ICT-armageddon waar we in 1999 alleen maar van konden dromen. Kunnen hoogtechnologische landen daar wat aan doen? Nauwelijks. We realiseren ons niet hoe enorm complex ICT is geworden en dat complexiteit altijd leidt tot zwakke plekken. We doen alsof we gegevens van A naar B verplaatsen terwijl gegevens van A naar B worden *gekopieerd* zodat, als B een boef is, A normaliter niet eens merkt dat er iets is gebeurd. En wat helemaal bijna niemand buiten de AIVD wil toegeven is dat je mensen kunt omkopen met geld, seks of dreigementen tegen familieleden in het thuisland. Nee, we kunnen hooguit de systemen van landen als Iran en China ondermijnen om, net als in de koude oorlog, wederzijdse afschrikking te organiseren. We kunnen ook dreigen om cyberaanvallen te vergelden met ouderwetse kogels en bommen en inderdaad is dat sinds kort bij de Amerikanen officieel beleid. En tenslotte kunnen we natuurlijk systemen vereenvoudigen, ontkoppelen, desnoods off-line halen. Laten we dat vooral doen, maar het zal de integratietrend niet keren.

Als u deze column leest dan weet u meer dan ik nu. Nu weten we van Donner dat ook de UWV-polisadministratie kan zijn leeggetankt (code Iran = '315'). Gelukkig heeft u in DB/M kunnen lezen dat alles wordt gelogd. Wel verontrustend om te horen dat die logging is uitgezet omdat men bij UWV niet aansprakelijk zou willen zijn. Ik hoop dat het niet waar is en dat UWV anders dan DigiNotar "*gelukkig hebben we de logfiles nog*" kan zeggen. Gelukkig ook dat Donner een kopie van de bevolkingsadministratie opslaat bij vrienden in de USA: *priceless*. Zoals ze zeggen in Iran: wordt vervolgd!

René Veldwijk

Dr. R.J. Veldwijk (rene.veldwijk@faapartners.com) is partner bij FAA Partners, een onderdeel van de Ockham Groep.