Cyberwantrouwen

Prins, J.E.J.

Published in:
Nederlands Juristenblad

Publication date:
2011

Document Version
Peer reviewed version

Cyberwantrouwen

Heeft u ooit de webpagina www.fiod.nl bezocht? Vast niet. En mocht u de pagina hebben opgeroepen, dan is uw bezoek waarschijnlijk van zeer tijdelijke duur geweest. “Under construction” is alles wat er te lezen valt. Maar aan de pagina wordt allesbehalve gewerkt. Het webadres bestaat enkel en alleen omdat er iemand is die maar al te graag het emailadres @fiod.nl in handen heeft.[1] En dat is iemand anders dan de betreffende overheidsinstantie zelf. Een medewerker van de Belastingdienst vertelde me dat de persoon zich als de FIOD voordoet om belastingplichtigen in verwarring te brengen, onder druk te zetten of mogelijk af te persen. Fraude dus met de ‘identiteit’ van een overheidsinstelling.

Twee weken geleden presenteerde het kabinet de in het regeerakkoord al aangekondigde integrale aanpak voor cyberveiligheid. Met deze “Nationale Cyber Security Strategie” beoogt de regering de veiligheid van de digitale samenleving te versterken. Ambitie is de Nederlandse overheid slagvaardiger en vooral ook in samenwerking met andere partijen te laten werken aan de veiligheid en betrouwbaarheid van de digitale samenleving. Laat ik voorop stellen het kabinetsinitiatief toe te juichen. Samenwerking is cruciaal nu digitale ellende zich niets aantrekt van schotten tussen overheid en bedrijfsleven. Ook is het hoog tijd dat kennis, kunde en capaciteit aanzienlijk worden vergroot. Toch valt een aantal zaken op. Allereerst komt het beeld naar voren dat cyberveiligheid in de ogen van het kabinet primair een kwestie van het bestrijden van incidenten is. Incidenten die zich op een bepaald moment voordoen en waar vervolgens met een heel concrete actie op gereageerd dient te worden. Alle scenario’s ontwikkeld in de Nationale Risicobeoordeling (de rapportage over 2010 werd op 22 februari j.l. naar de Kamer gestuurd) gaan van deze perceptie uit. Ze beschrijven een cyberaanval, een moedwillige verstoring van ICT dan wel plotselinge uitval van een netwerk. Echter, kenmerkend voor veel verschijningsvormen van cyberrisico’s is nu juist dat ze een sluipend karakter hebben. Een veenbrand, aldus de mooie vergelijking van Ybo Buruma. Effecten en daarmee ellende duiken telkens opnieuw weer ergens op. Jaren later nog, zoals diverse identiteitsfraudezaken illustreren. Cruciaal is daarom dat wordt gedifferentieerd in kenmerken en oorzaken van cyberrisico’s. Dat betekent dat het denken niet alleen in termen van kwetsbare techniek (concrete en tastbare systemen) gaat, maar juist ook vanuit risicovolle informatie (ongrijpbare, stromende en daarmee voortwoekerende ellende).

Dit brengt me bij het tweede punt: de reikwijdte van de strategie. Deze stelt cyberveiligheid centraal: “het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.” Door ook te spreken over ‘gevaar of schade veroorzaakt door misbruik van ICT’ en ‘schending van de vertrouwelijkheid en integriteit van opgeslagen informatie’ schuurt de strategie aan tegen het fenomeen cybercrime. Niet alleen het FIOD-voorbeeld komt daarmee binnen de reikwijdte van de strategie. Cyberafpersen en bij een ruime interpretatie van ‘misbruik van ICT’ ook haat zaaien en kinderpornografie vallen eronder. Tegelijkertijd is het opvallend dat de gepresenteerde maatregelen primair het beeld oproepen van een aan te pakken wereld van hightech-criminelen, whizzkids en internationale bendes die met één enkele actie grote aantallen slachtoffers maken of schade aanrichten. Onderzoek van Wouter Stol e.a. uitgevoerd in opdracht van de KLPD laat echter zien dat cybercrime van het volk is.

[1] Technisch is het verband tussen domeinnaam en mailadres eenvoudig te leggen, namelijk door de domeinnaam te laten verwijzen naar een IP-adres van een computer waar niet alleen de server voor de webpagina op draait, maar ook die voor het mailadres.

Hacken, eens voorbehouden aan whizzkids, is ‘gedemocratiseerd’. Rommelen met iemand z’n account of profiel is geen technisch hoogstandje maar een onder jongeren alledaagse manier om de ander een hak te zetten. Deze conclusie heeft zeker betekenis voor preventie en bewustwording. De oorzaak van de ellende kan immers soms heel dicht bij huis liggen.

Het laatste opvallende punt is dat de strategie weliswaar een beroep op burgers, bedrijfsleven en organisaties doet om zelf het nodige te doen, maar de verantwoordelijkheidskwestie niet aankaart. Toch is het hoog tijd het debat te entameren over de vraag waar we verschillende betrokkenen op mogen afrekenen. Wat bijvoorbeeld mag van de overheid (ook in politiekbestuurlijke zin) en het bedrijfsleven worden verlangd als het om de veiligheid van grootschalige informatie-uitwisseling gaat? Of als het op het (kunnen) afleggen van verantwoording daarover aankomt? De Eerste Kamer debatteert 15 maart a.s. wederom met de minister over de beveiliging van het elektronisch patiëntendossier. Ook dat is cyberveiligheid. Ondanks vele expertmeetings en ontelbare uren debat blijft nog altijd schimmig of met het ontwikkelde systeem de veiligheid van miljoenen patiëntgegevens voldoende valt te waarborgen. En of daarover wel toetsbare verantwoording valt af te leggen. Ondanks alle inspanningen van het College Bescherming Persoonsgegevens mag bijvoorbeeld een geïnformeerd openbaar debat over de beveiliging van regionale systemen niet worden gevoerd omdat belangen van systeemleveranciers (die hun specificaties niet prijs willen geven) kennelijk nog steeds kunnen blijven prevaleren boven cyberveiligheid als maatschappelijk belang.

Juist voor cyberveiligheid geldt: kwetsbaarheid moet je actief zoeken. Een open oor en oog hebben voor faciliterende factoren die op het eerste gezicht nauwelijks iets met kwetsbaarheid en dreigingen van doen lijken te hebben. Een houding die concreet van de fiscale opsporingsautoriteit verlangt dat ze alert is op misbruik met de domeinnaam www.fiod.nl en zonodig maatregelen neemt.[2] Een houding bij ons allemaal die zich kenmerkt door een gezonde dosis cyberwantrouwen.

[2] Bijvoorbeeld op grond van art. 2.1 van de geschillenregeling SIDN.