# Cyber security versus cyber crime:
# Kat en muis in een digitale oorlog

Collectieve 'digibewust-wording' en regulering zijn nodig om het internet te beschermen tegen cyber-aanvallen die ons leven dreigen te ontwrichten, aldus oud-generaals Dick Berlijn (NL) en Harry Raduege (VS) die zich nu bij Deloitte inzetten voor onze virtuele veiligheid.

*Dick Berlijn en Harry Raduege*

Nu het internet tot in alle hoeken en gaten van de privé- en werksfeer is doorgedrongen en onmisbaar is voor de internationale handel, communicatie en vervoer, zou een wereldwijde uitval van het internet door een cyberaanval desastreus kunnen uitpakken. "De digitale infrastructuur ondersteunt veel kritieke functies en faciliteiten in ons dagelijks leven", beaamt Harry Raduege, oud-generaal van de Amerikaanse luchtmacht en hoofd van het Center for Cyber Innovation van Deloitte US. "Via het internet kun je de stroomvoorziening en kritische informatiesystemen lamleggen. Opeens zou je geen geld meer uit de pinautomaat kunnen halen, het eten in je koelkast en in de supermarkt zou bederven en in ziekenhuizen gaan op de intensive care de machines uit, met alle gevolgen van dien."

**Enorme buit**

De belangen zijn dus enorm, maar waar komt het gevaar precies vandaan? En belangrijker nog: hoe kunnen we ons ertegen beveiligen, zonder de vrijheid en rechten van gebruikers al te zeer aan te tasten? Voor de technische kant van het internet bestaan internationale regels, maar niet voor de toegang, het gebruik en de beveiliging. "Cruciaal is dat het wereldwijde web – naast land, zee, luchtruim en ruimte het 'vijfde domein' – geen grenzen kent en niet onderworpen is aan wet- en regelgeving", aldus Dick Berlijn, voormalig Commandant der Strijdkrachten van het Nederlandse leger en sinds september 2009 senior board advisor bij Deloitte Nederland met veiligheid als belangrijk onderdeel van zijn portefeuille.

Vanwege de hoge opbrengsten en lage pakkans neemt de internetcriminaliteit overal ter wereld toe. "Naar schatting is in 2008 wereldwijd via het internet voor zo'n biljoen dollar aan data gestolen," vertelt Harry Raduege. "Deze vorm van criminaliteit is aantrekkelijker dan het beroven van een bank – de kosten en pakkans zijn laag, de buit enorm. Inmiddels streeft de omvang van internetcriminaliteit in geld gemeten de drugshandel voorbij. Bovendien ontstaan er wereldwijde syndicaten van cybercriminelen."

**Nederland favoriet bij cybercriminelen**

Het aantal cyberaanvallen neemt eveneens toe. Meestal gaat het om een denial-of-service (DOS) aanval, waarbij een server gebombardeerd wordt met loze verzoeken of e-mails tot deze bezwijkt. Een meer sinistere variant is de distributed denial-of-service (DDOS) aanval, waarbij computers van derden worden overgenomen en vervolgens ingezet om een server aan te vallen. De motieven voor deze aanvallen kunnen financieel, ideologisch of politiek zijn, of gewoon een egotrip van een hacker. Individuen, ondernemingen, organisaties en zelfs overheden kunnen slachtoffer, maar ook dader zijn. "Estland werd enkele jaren geleden door een zeer zware cyberaanval op de knieën gedwongen, naar het zich laat aanzien door een niet-welgezinde overheid," volgens Harry Raduege.

**Collectief 'digibewustzijn'**

Beide oud-generaals zijn het erover eens dat bewustwording van en voorlichting aan particulieren, ondernemingen, organisaties en overheden wereldwijd de sleutel zijn tot een veilig internet. Een collectief 'digibewustzijn' zorgt voor de nodige inzet en waakzaamheid om het internet te beschermen tegen criminelen en terroristen en hun zogenaamde *weapons of mass disruption*, die bedoeld zijn om op grote schaal chaos en paniek te veroorzaken.
Wil dit echter lukken, dan moet wel de hele wereld meedoen. "Gelukkig zijn overheden zich meestal maar al te goed bewust van de kwetsbaarheden van de maatschappij, en handelen ze daar ook naar als een dreiging zich voordoet," zegt Dick Berlijn. "Steeds meer landen hebben oog voor de schade die kan ontstaan door internetcriminaliteit en beseffen niet welk risico ze nemen door geen firewall of antivirusprogramma op hun computer te installeren. Bovendien lopen niet alleen hun eigen computer en gegevens gevaar in geval van een kwaadaardig virus. We moeten zorgen dat iedereen voldoende 'digibewust' wordt."

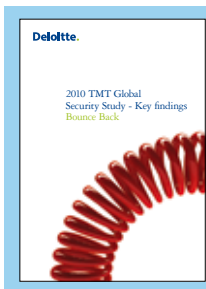
**Gebruikersidentificatie**

Het internet zelf vraagt ook om regulering: gebruikersidentificatie kan bijvoorbeeld helpen om cybercriminelen op te sporen en te ontmoedigen. "Als voertuigen een kentekenplaat moeten hebben eigenaren in geval van een verkeersovertreding op te kunnen sporen, waarom kunnen we internetgebruikers niet verplichten identificatie te voeren?", vraagt Dick Berlijn zich af. Het zal niet verbazen dat bepaalde technische mogelijkheden om de identiteit van individuen vast te stellen en te controleren het mikpunt zijn van cybercriminelen. Nu de muizen slimmer worden, moet ook de muizenval volgens Harry Raduege geavanceerder worden. Mogelijkheden zijn identificatie op basis van de persoonseigen karakteristieken van bloedvaten, of zelfs op basis van DNA. "Omdat de criminelen bovendien steeds sneller leren, raad ik veiligheidsmensen aan om ze minstens twee stappen vóór te blijven."

**Evenwichtskunst**

Een veilig internet betekent ook meer regulering en bepaalde beperkingen ten aanzien van informatie. Hoe hiermee om te gaan? Dick Berlijn: "We willen geen controles invoeren die de vrije geest van het internet de kop indrukken. Maar de maatschappij legt al bepaalde beperkingen op, bijvoorbeeld om jongeren af te schermen voor porno, dus waarom kan dat niet ook op internet?" Harry Raduege is meer filosofisch: "Meestal is vrijheid goed, soms regulering."

## 'Er ontstaan wereldwijde syndicaten van cybercriminelen'




**Cybercrime steeds grotere bedreiging voor nationale veiligheid**

Het rapport 'Bounce Back: 2010 TMT Global Security Study', dat Deloitte op 26 mei heeft gepubliceerd, bevat de uitkomsten van interviews met security executives van 150 TMT-multinationals. Een van de hoofdconclusies gaat over de dreiging van cybercrime. Deze dreiging wordt steeds groter, zowel voor het bedrijfsleven als voor de nationale veiligheid. Van de ondervraagde technologie-, media- en telecombedrijven zegt 37% dat de toegenomen complexiteit van cyberaanvallen het op een na grootste probleem vormt bij effectieve informatiebeveiliging.

Hoe groot het land is waar de cyberaanvallen vandaan komen doet er niet altijd toe. Zo is Nederland, door de hoge penetratie van breedband internet en de aanwezigheid van een belangrijk internetknooppunt, favoriet geworden bij cybercriminelen. Gemeten naar het aantal aanvallen dat hiervandaan wordt gelanceerd, staat Nederland nummer 9 op de ranglijst van cybermisdaadlanden.

**Meer informatie**

Dick Berlijn