

# NEDERLAND KWETSBAAR VOOR CYBERCRIMINALITEIT

Het Stuxnet-virus maakt duidelijk hoe kwetsbaar de gedigitaliseerde samenleving is geworden voor aanvallen vanuit cyberspace. Ook voor Nederland is het een 'wake up call'. Het kabinet-Rutte kondigde al de oprichting van het Nationaal Cyber Security Centrum en de Cyber Security Raad aan. Maar voorlopig moet Govcert.nl, de cyberwaakhond van de Nederlandse overheid, het met zeventien werknemers opnemen tegen een criminele sector die dagelijks in omvang groeit. 'Omdat Stuxnet eigenlijk bij toeval ontdekt is, vraag ik me af: wat circuleert er allemaal al waar we niets van weten?'

TEKST RENÉ ZWAAP

**H**et afscheidsfeestje van de Israëliische generaal Gabi Ashkenazi, in februari dit jaar, werd volgens de Israëliische krant *Haaretz* opgevolgd met een videofilm over de loopbaan van de hoogste man van de Israëliische strijdkrachten, waarin onder meer een cyberaanval met het computervirus Stuxnet op een nucleaire installatie in Iran werd gememoreerd. Dat was hoogst opmerkelijk, want formeel heeft Israël nooit de verantwoordelijkheid genomen voor het Stuxnet-virus, dat vanaf 2010 wereldwijd voor grote paniek zorgde. Weliswaar hadden computerspecialisten al het vermoeden geuit dat Israël (eventueel in samenwerking met de Verenigde Staten) achter Stuxnet zat, maar evengoed waren er beschuldigende vingers uitgestoken naar China, dat zich de laatste jaren ook bepaald niet vies heeft getoond van oorlogvoering in cyberspace. China werd bijvoorbeeld verantwoordelijk gesteld voor de lancering van het Aurora-virus, een andere *cyber attack*, die gericht was op industriële spionage. Stuxnet, een wormvirus dat zich via Windows toegang verschaft in computers, bleek bij nadere analyse speciaal zijn te ontworpen om industriële besturingsapparatuur ontwikkeld door het Duitse elektronicaconcern Siemens plat te leggen. Deze systemen waren onder meer gekocht door Iran, dat ze gebruikte voor de uraniumverrijkinginstallatie bij Natanz, die in 2010 plat kwam te liggen als gevolg van de Stuxnet-besmetting. Beweerd wordt dat het Iraanse atoomprogramma jaren

achterop schema raakte als gevolg van de Stuxnet-aanval.

Of Israël daadwerkelijk achter Stuxnet zit, zal waarschijnlijk nooit voor de volle honderd procent vast te stellen zijn. Andere dadertheorieën vloeien dan ook rijkelijk op het internet. Het computerbeveiligingsbureau Symantec rekende uit dat bij de ontwikkeling van Stuxnet vijf tot tien goed getrainde programmeurs betrokken moeten zijn geweest, die er minimaal een jaar aan hebben gewerkt. Kortom, er moeten ettelijke miljoenen zijn geïnvesteerd in de ontwikkeling van Stuxnet, dat zich via usb-sticks verspreid naar het doel. Het bestaan van het Stuxnet-virus werd eigenlijk per toeval ontdekt door een Wit-Russische leverancier van anti-virus software. Als dat niet was gebeurd, was de wereld mogelijk nooit achter het bestaan van Stuxnet gekomen. Het virus is zodanig vormgegeven dat het zichzelf niet meer verspreidt na 24 juni 2012.

Ook aan Nederland ging de Stuxnet-aanval niet onopgemerkt voorbij. Volgens beveiligingsbedrijf Symantec zijn in Nederland enkele honderden PC's met een Stuxnet-besmetting aangetroffen. Dit is minder dan één procent van het totaal (in Iran was dat 60 procent). Een van de Nederlandse bedrijven die het virus daadwerkelijk opliep omdat het gebruik maakte van Siemens-apparatuur was het Nederlandse Vanderlande Industries, dat bagagesystemen aan vliegvelden levert. Ook de kerncentrale in Borssele was na de ontdekking van Stuxnet extra alert.

Volgens Chris Verhoef, hoogleraar informatica aan de Vrije Universiteit, moet Stuxnet bovenal worden beschouwd als een 'game changer' en een 'wake up call'. Verhoef: 'Ongetwijfeld is Stuxnet ontwikkeld voor de aanval op de atoomcentrifuge in Iran. Omdat het om een *semi-targeted attack* gaat, is er ook *collateral damage*: de Siemens-apparatuur die hier in het geding is, zit in tal van industriële toepassingen, ook in Nederland. Dat kunnen kerncentrales zijn, maar ook sluizen, stormvloedkeringen, bruggen en tunnels, oliepipleidingen, het gasnet, chemische fabrieken, staalfabrieken en papierfabrieken, centrales voor het wegverkeer en het treinverkeer, noem maar op. Stuxnet toont aan hoe groot de kwetsbaarheid is van al deze installaties, die je veelal niet even uit kunt zetten om te kijken of er geen besmette computers in het spel zijn. In die zin is het verontrustend dat de Nederlandse autoriteiten die zijn gemoeid met het monitoren van cyberaanvallen, zoals Govcert.nl en de Nationaal Coördinator Terrorismebestrijding (NCTb), pas erg laat reageerden op



De IT'ers van de kerncentrale in Borssele waren extra alert toen bekend werd dat het Stuxnet-virus via beveiligingssoftware van Siemens werd verspreid

dit nieuwe gevaar. Zelf kreeg ik vrij snel de eerste informatie over Stuxnet, die ik vervolgens in een factsheet heb doorgegeven aan diverse beheerders van NCTb-alertsystemen bij de overheid. Omdat Stuxnet werkt via besmette usb-sticks heb ik onder meer het advies gegeven aan instellingen en bedrijven geen usb-sticks meer toe te laten tot de systemen, want voorkomen is uiteindelijk beter dan genezen. Voor de beheerders kwam mijn factsheet als nieuws, maar je zou toch verwachten dat instanties zoals Govcert.nl en de NCTb dit allang hadden gecommuniceerd. Mogelijk waren Govcert.nl en NCTb wel op de hoogte, maar de beheerders van de alertsystemen niet, en dat heeft bij mij wel tot verbazing geleid.

Aart Jochem, teamleider bij Govcert.nl, de organisatie van het ministerie van BZK die zich bezighoudt met het voorkomen en bestrijden van cyberaanvallen, bestrijdt dat zijn bureau te laat op de hoogte zou zijn gekomen van het bestaan van Stuxnet. 'De eerste meldingen kwamen na de ontdekking van Stuxnet bij ons ook binnen in de zomer van 2010,' zegt hij. 'Zodra we op de hoogte waren van de dreiging hebben we direct een waarschuwing uitgestuurd naar belangrijke partijen en onze deelnemers. De periode daarna hebben we Stuxnet verder onderzocht. Tot dan toe was dit type van *malware* onbekend en het kostte ons – net als de hele wereld van de informatiebeveiliging – tijd voordat we precies wisten waar we mee te maken hadden. Daarna hebben we direct een bericht doen uitgaan om de partijen

op de hoogte te houden van de ontwikkelingen rond Stuxnet.'

Stuxnet zit zo geavanceerd in elkaar dat het wel tot stand gekomen moet zijn met heel veel geld en dat er een staat of meerdere staten bij betrokken zijn geweest staat wel zo goed als vast, zo vertelt Jochem. 'Verder kun je daar niet veel mee, want geen land zal toegeven achter zo'n virus te zitten. Het Aurora-virus kwam uit China, maar toen de Chinese autoriteiten daarop werden aangesproken was de reactie dat cybercriminaliteit ook in China strafbaar is en

## 'HET OORSPRONKELIJKE DOEL VAN STUXNET LEEK BEDRIJFSSPIONAGE'

dat de Chinese overheid er dus niets mee van doen had. Daar is de kous dan mee af.'

### SCHOT HAGEL

Govcert.nl schat dat er wereldwijd inmiddels honderdduizenden computers zijn besmet met Stuxnet. Maar daarvan staat het overgrote deel niet in een omgeving met industriële systemen. Jochem: 'Je moet dit virus zien als een worm die op diverse plekken wordt losgelaten en dan langzaam naar zijn werkelijke doel kruipt.' Stuxnet maakt gebruik van een aantal kwetsbaarheden in Windows en

verbergt zijn aanwezigheid, kent verschillende manieren van verspreiding en maakt gebruik van het gegeven dat de aan te vallen procescontrole-systemen van Siemens met hard-gecodeerde wachtwoorden kunnen werken. Onderdeel van Stuxnet is een elektronisch ondertekende driver, die ondertekend is met gestolen certificaten (de digitale handtekening). Niet alleen procescontrolesystemen zijn door Stuxnet besmet. Ook andere Windows-computers kunnen worden besmet. Omdat Stuxnet op zoek is naar specifieke Siemens-systemen, houdt besmetting echter niet per definitie in dat gegevens verdwijnen of processen worden verstoord. 'Het oorspronkelijke doel van Stuxnet leek bedrijfsspionage,' aldus Jochem. 'Wanneer een proces-

## 'HET HELE CYBER SECURITY-VAK IS STEEDS ACHTER DE FEITEN AANHOLLEN'

controlesysteem is besmet is het echter eveneens mogelijk de besturing van industriële processen te beïnvloeden en te verstoren, waaronder de aansturing van apparatuur zoals pompen en motoren. Stuxnet is daarom te beschouwen als een uiterst serieus te nemen waarschuwing wat betreft de kwetsbaarheid van procescontrolesystemen.'

De Nederlandse softwarespecialist Rob Hulsebos was nauw betrokken bij het ontcijferen van de Stuxnet-code. In nauw contact met het IT-bedrijf Symantec, dat zich aan het kraken van de Stuxnet-code had gezet, ontdekte Hulsebos meer details over de precieze werking van het virus. Hulsebos: 'Wat me eigenlijk het meest heeft verbaasd aan deze

zaak is dat Siemens zo weinig informatie heeft willen delen met de mensen die het Stuxnet-virus wilden ontleden. In hun plaats zou ik erg benieuwd zijn naar de manier waarop mijn producten misbruikt worden, om vervolgens maatregelen te bedenken hoe herhaling kan worden voorkomen. Sowieso was de industriële wereld niet echt behulpzaam. Ik neem aan dat de angst is dat andere partijen nu ook door krijgen hoe Stuxnet in elkaar zit en dat industriële installaties een makkelijk doelwit zijn vanwege hun achterstand. Ook publicatie van het boek *Hacking scada*, dat beschrijft hoe industriële systemen beveiligd moeten worden, wordt op alle mogelijke juridische manieren tegengehouden. De auteurs, diverse beveiligingsexperts uit de VS, hebben inmiddels de publicatie afgeblazen.'

De vrees dat Stuxnet een bron van inspiratie zal zijn voor andere *malware*-auteurs, is volgens Hulsebos zeker niet onterecht. 'Opeens is duidelijk welke risico's we lopen. Het is een geluk bij een ongeluk dat Stuxnet, afgezien van Iran, niets deed. Maar omdat Stuxnet eigenlijk bij toeval ontdekt is, vraag ik me af: wat circuleert er allemaal al waar we niets van weten? Er ligt een belangrijke taak bij de bewustwording van bedrijven dat er iets gedaan moet worden. In de watersector, vliegvelden en procesindustrie is er al het nodige gebeurd, maar in een sector als de machinebouw gaat het helemaal niet zo hard en bij leveranciers hoeft je al helemaal niet aan te komen. Ook qua opleidingen zou er iets moeten gebeuren. Het hele *cyber security*-vak is steeds achter de feiten aanhollen. Het zou beter zijn als software meteen vanaf dag één onkraakbaar geschreven zou zijn.' ●

## DAVID TEGEN GOLIATH

Met zeventien werknemers is Govcert.nl, het cyber security-bureau van de Nederlandse overheid, een David die het moet opnemen tegen de Goliath van de georganiseerde criminaliteit in cyberspace. Toch is teamleider Aart Jochem trots op de prestaties van de dienst. 'We werken maar met zeventien man, maar die zijn wel tot op het bot gemotiveerd en zijn ook niet te beroerd om nachten door te werken als de situatie daarom vraagt.' Govcert.nl boekte in samenwerking met het KLPD veel succes met het ontmantelen van het Bredolab-netwerk, dat door cybercriminelen werd gebruikt om volledige controle over een besmette computer te verkrijgen en de instellingen van het systeem te wijzigen of te verwijderen. Bovendien kunnen wachtwoorden en financiële gegevens, zoals creditcardnummers, met Bredolab worden gestolen. De Oost-Europese bende die achter het virus zat, maakte gebruik van in Nederland gehuurde servers. Zo konden

in een maand tijd 3 miljoen computers worden besmet en eind 2009 waren er dagelijks ongeveer 3,6 miljard e-mailberichten met schadelijke software van Bredolab in omloop.

Jochem: 'We vergroten onze slagkracht door intensief samen te werken met nationale en internationale partijen. Het Team High Tech Crime van het KLPD is bijvoorbeeld een belangrijke partner. Zo is verleden jaar een Armeniër opgespoord die door middel van cyberaanvallen vanuit Nederland een eigen dienstverleningsbedrijf ten behoeve van de criminele sector had opgestart. Hij had ongeveer 800 klanten, die gespecialiseerd waren in zaken als bancaire fraude. Hij ving daar ongeveer een ton per maand voor. De cybercriminaliteit stelt je telkens weer voor nieuwe verrassingen. Zo moest het bureau voor emissierechten van de Europese Commissie een tijd dicht omdat cybercriminelen erin waren geslaagd in te breken in de

computers van reële partijen in deze markt en zo geld achterover wisten te drukken op grond van niet-bestaande emissies. Govcert vervulde een belangrijke rol in de bestrijding hiervan.'

Govcert.nl richt zich op versterking van de informatiebeveiliging binnen de Nederlandse overheid en doet dat door het monitoren van bronnen via internet, het uitgeven van adviezen over ICT-kwetsbaarheden en waarschuwingen bij dreigingen en door ondersteuning te bieden aan overheidsorganisaties bij de afhandeling van ICT-gerelateerde incidenten. Dit bureau van het ministerie van BZK wordt in de loop van volgend jaar uitgebreid en ondergebracht in het nieuw te vormen Nationaal Cyber Security Centrum. Het kabinet streeft ernaar dat ook private partijen onderdeel worden van deze nieuwe organisatie. Daarnaast roept het kabinet een Cyber Security Raad in het leven, waarin op strategisch niveau vertegenwoordigers van alle relevante partijen zitting zullen hebben. Deze raad, die wordt gefaciliteerd door de overheid, zal 1 juli dit jaar van start gaan.