Defensie werft slechts handvol informaticaspecialisten aan om het land te beschermen tegen cyberaanvallen

Met vier tegen de rest van de wereld

De Belgische militaire inlichtingendienst wierf onlangs vier experten in informaticabeveiliging aan, die de systemen van Defensie moeten helpen beschermen tegen eventuele militaire cyberaanvallen. Daartoe worden geregeld pogingen ondernomen, zegt defensieminister Pieter De Crem (CD&V).

DOOR RONALD MEEUS

BRUSSEL ● Volgens veiligheidsexpert Eddy Willems is een team van vier mensen te weinig om te reageren als er een grootscheepse cyberaanval wordt ingezet. 'Met het NAVO-hoofdkwartier in de buurt kunnen de Belgische militaire systemen een belangrijk eerste echelon zijn.'

Sinds een vooralsnog onbekende mogendheid – maar de slachtoffers wijzen richting Rusland – enkele jaren geleden websites en computersystemen in de voormalige sovjetstaten Georgië en Estland via het internet platlegde, is het inmiddels al zo'n vijftien jaar geleden voorspelde tijdperk van de cyberoorlog officieel ingezet. En ook de computersystemen van de Belgische overheid ontsnappen niet aan die dreiging volgens luitenant Kurt Verwilligen, woordvoerder van Defensie. "Vanwaar de aanvallen vertrekken is moeilijk te achterhalen, net als de motieven van de daders, maar ze zijn er wel." België wijkt daarin niet af van een internationale trend. 60 procent van alle overheden die eerder dit jaar over het onderwerp werden bevraagd door het Amerikaanse beveiligingsbedrijf McAfee geeft aan dat ze vermoeden dat buitenlandse overheden betrokken zijn geweest bij cyberaanvallen op kritieke infrastructuursystemen in hun land. Een even hoog percentage verwacht binnen de twee jaar een aanval te moeten incasseren die ook effect heeft. "Grote bedrijven en organisaties worden continu bestookt door aanvallen via het internet, en overheden verschillen daar niet van", zegt Eddy Willems, adviseur computersecurity bij het Duitse beveiligingsbedrijf G Data. "De aanvallen zijn zo veelvuldig dat het onmogelijk is om aan te tonen waar ze vandaan komen."

Capaciteitsproblemen

Om klaar te zijn voor eventuele ernstige aanvallen, heeft Defensie vier experten in cyberdefensie aangeworven die deze zomer in dienst treden. Volgens Willems is dat te weinig om een echte internetaanval terug te dringen. "Die mensen zijn ongetwijfeld erg bekwaam. Maar als er zich een grootschalige aanval aandient, vrees ik dat ze voor capaciteitsproblemen komen te zitten", zegt Willems. "Een viertal mensen is te weinig, zowel om proactief te werken als om erger te voorkomen wanneer er effectief een aanval bezig is."

Motieven voor een cyberaanval

Overheidssystemen worden om drie verschillende redenen via het internet aangevallen, zeggen deskundigen in cyberoorlogvoering. Een eerste motief is het verstoren van de communicatie in het land, die in toenemende mate via het internet verloopt. Een geslaagde aanval zou bijvoorbeeld de mailserver kunnen platleggen. Ook gewone computerinbraken, om vertrouwelijke gegevens te stelen uit de databaseserver – een computer in het netwerk die alle gegevens bijhoudt – zijn een mogelijkheid. En ten slotte is er het motief waar de grootste vrees voor bestaat: aanvallen die dienen om een stuk van de landelijke infrastructuur plat te leggen. Een elektriciteitsnetwerk bijvoorbeeld heeft een zogeheten SCADA-systeem (Supervisory Control and Data Acquisition), dat informatie van sensoren op fysieke plaatsen van het netwerk verzamelt in een centrale computer. Die is bij de meeste nutsbedrijven op zijn beurt aangesloten op het centrale netwerk van het bedrijf, dat vervolgens online is. Door in te breken op de server die aansluiting maakt met het internet kunnen hackers dus doordringen tot de SCADA-computer en van daaruit de infrastructuur ontregelen door valse bevelen te geven.

Als er ooit een grootscheepse cyberaanval wordt gelanceerd op de computersystemen van een landelijke overheid, zal dat hoogstwaarschijnlijk een voorbereiding zijn op een conventionele militaire inval, zeggen experten in cyberoorlog. Een manier om alvast het licht uit te doen, zodat er gebruik kan worden gemaakt van de chaos om binnen te vallen. De aanvallen op Georgische sites in 2008 kwamen ook vlak voordat het Russische leger binnenviel in de opstandige Georgische provincie Zuid-Ossetië.

> EDDY WILLEMS (ADVISEUR COMPUTERSECURITY BIJ G DATA):
> Grote bedrijven worden continu bestookt door aanvallen via internet, en overheden verschillen daar niet van. De aanvallen zijn zo veelvuldig dat het onmogelijk is om ze te traceren

Strategisch belang van België

Het belang van België als militair doel valt ook niet te onderschatten, zegt Willems. "Vergeet niet dat Brussel het hoofdkwartier van de NAVO herbergt. De Belgische militaire systemen kunnen een belangrijk eerste echelon zijn." Maar niet het enige. De experten in cyberbeveiliging van de militaire inlichtingendienst werken aan de frontlinie, maar ook daarachter zijn er beveiligingscenakels. Zoals het Computer Emergency Response Team (CERT) van Belnet, de internetprovider van de federale overheid. Die dienst richt zich op de bescherming van de overheidssystemen tegen cybercriminaliteit in het algemeen, maar puur technisch verschillen de taken weinig van die van de militaire beveiligingsexperten: heel wat daden van cyberoorlogvoering worden uitgevoerd door dezelfde hackers die door criminele organisaties onder de arm worden genomen. "Voor alle duidelijkheid: die vier mensen die we hebben aangeworven, staan niet in voor de beveiliging van alle computersystemen en -netwerken van de Belgische overheid", zegt Verwilligen, woordvoerder van Defensie. "Daarvoor zijn er nog andere instanties actief. Overheden, bedrijven en organisaties moeten ook voor hun eigen beveiliging instaan."