TRENDS

Jaap Schekkerman, director global cyber security CGI

PRODUCTIEOMGEVINGEN EN KRITISCHE INFRASTRUCTUUR ZIJN DOELWIT CYBERAANVALLEN

Een elektriciteitsleverancier die ‘op zwart’ gaat en honderdduizenden huishoudens en bedrijven niet meer van energie kan voorzien. Waterbedrijven die letterlijk droogvallen. Nucleaire centrales waar de temperatuur in rap tempo en onvoorzien omhoog gaat doordat de koeling is uitgeschakeld. In alle gevallen gaat het om hackers die hetzij rechtstreeks inbreken of via speciaal geschreven malwaresoftware toegang krijgen tot cruciale systemen. De rampscenario’s lijken regelrecht uit een Hollywood-rampenfilm afkomstig. Helaas behoren zij echter wel tot de huidige realiteit, zegt Jaap Schekkerman, director global cyber security CGI.

Tekst: Paul Teixeira

De gemiddelde gebruiker heeft anno 2014 op zijn minst wel eens gehoord van Denial of Service-aanvallen (DoS) of hackersdreigingen. Het gros heeft ook al in slecht Nederlands opgestelde mailtjes gekregen waarin ‘hun bank’ vraagt om vooral te klikken op de ingebedde link en vervolgens in te loggen op hun account. Deze vormen van cybersecurity zijn inmiddels gesneden koek voor CIO’s en andere directieleden. Maar er is nog een andere belangrijke cyberdreiging waar minder bewustwording voor is: aanvallen gericht op de procesautomatisering. Over deze dreiging wordt echter niet veel geschreven of gezegd. Jaap Schekkerman, director global cyber security CGI, heeft daar een verklaring voor: “ Als ik door een DoS-aanval niet bij mijn bankgegevens kan en ik meld dat vervolgens via Twitter, dan krijgt het massale aandacht in de pers. Als er echter een industriële omgeving wordt gecompromitteerd, dan wordt dat feit door de getroffen onderneming angstvallig binnenskamers gehouden. Pas als het incident te groot is om te verzwijgen, komt de bewuste organisatie er mee naar buiten. De reden daarvoor is simpel: de imagoschade voor het betreffende bedrijf is groot en de eventuele vervolgschade kan eveneens groot zijn.”

Een complicerende factor is dat het in de praktijk niet zo eenvoudig blijkt om het een en ander in dergelijke productieomgevingen afdoende af te schermen tegen cyberaanvallen, aldus Schekkerman. “De ervaring leert dat er in industriële omgevingen vaak zogenoemde ‘achterdeuren’ open staan. Productieomgevingen zijn immers nooit ontworpen met cyberveiligheid in het achterhoofd. Verder speelt mee dat de Chief Information Officer van dergelijke ondernemingen vaak een minder grote invloed heeft op de productieautomatisering. Daar hebben veelal andere leidinggevenden, zoals de plant managers, meer zeggenschap over. En, ook niet onbelangrijk: als je een effectieve cyberverdediging in productieomgevingen wilt opzetten, dan vergt het kennis van zowel de industriële procesautomatisering, als de koppeling van industrieel automatisering naar die van de kantooromgeving.”

IMPACT OP ECONOMIE EN SAMENLEVING

Dat de dreiging van cyberaanvallen op infrastructuur onderbelicht blijft, is volledig ten onrechte, stelt Schekkerman. De mogelijke gevolgen van een geslaagde aanval op cruciale infrastructuur zijn immers bijzonder groot. Daarbij gaat het om energie- en watervoorziening, wegtransport, luchtvaart, spoorwegen, grote evenementen (denk aan de recente nucleaire top in Den Haag), financiële transactienetwerken (betalingsverkeer) en fysieke infrastructuur (dijken en bruggen). “Een dergelijke aanval raakt de economie en/of de samenleving direct”, aldus Schekkerman.

Waar het bij DoS-aanvallen vaak nog om zogenoemde ‘script kiddies’ gaat (relatief onervaren onverlaten die met behulp van gekochte of gedownloade tools aanvallen uitvoeren op websites), zijn de hackers van kritische infrastructuur van een geheel ander (lees: hoger) niveau. Schekkerman: “Het gaat om een ander soort aanvallen en een ander soort hackers. Zij zijn heel bewust op zoek naar kwetsbaarheden om hun doel te bereiken. Dat hoeft overigens niet alleen het verstoren van het productieproces zelf te zijn, maar het kan ook gaan om de diefstal van intellectuele eigendommen. Die zijn bijvoorbeeld in de olie- en gas-fabricage al verankerend in de productiesystemen van de bewuste bedrijven. Er is een bekend Canadees voorbeeld van dergelijke praktijken: een aantal Chinese fabrikanten hebben destijds intellectueel eigendom van Nortel, een telecomfabrikant van mondiaal formaat, gestolen. Op basis van de verkregen informatie hebben de bewuste Chinese concurrenten de Nortel-apparatuur nagebouwd en vervolgens nagenoeg dezelfde spullen voor veel lagere prijzen op de markt gebracht. Het heeft er mede voor gezorgd dat Nortel failliet is gegaan.”

Daar waar de diefstal van intellectuele eigendommen een enkele onderneming tot de bedelstaf kan brengen, hebben aanvallen op kritische infrastructuur verstrekkendere gevolgen. In potentie kan een samenleving volledig ontwricht raken en de economie van een land in negatieve zin beïnvloeden. “Iedereen merkt de gevolgen als een cruciale infrastructuur, zoals de elektriciteitsvoorziening, wordt verstoord. In sommige gevallen kan het ook mensenlevens kosten”, aldus CGI-topman Schekkerman.

ENERGIESECTOR ALS DOELWIT

De vraag dringt zich op of er zich vaak hackincidenten in de cruciale infrastructuur voordoen. Het grote publiek hoort en ziet er immers weinig van. “Op dit moment is er wereldwijd maar één land dat dergelijke aanvallen registreert: de Verenigde Staten. Daar is een Industrial Control Systems Cyber Emergency Response

‘De vraag is niet *of* je ooit wordt aangevallen maar de vraag is *wanneer* zal het gebeuren’

Team opgericht dat ernstige incidenten bijhoudt en rapporteert. Daarbij gaat om aanvallen die een directe impact kunnen hebben op de samenleving. In 2013 heeft het ICS-CERT gemeld dat de Amerikaanse energie sector met 58 procent aan kop ging als het ging om het aantal gerichte cyberaanvallen. Volgens mijn bronnen is in Europa eenzelfde beeld te zien: ook hier is de energiesector het grootste doelwit van hackers.”

Schekkerman betreurt het dat er geen Europese tegenhanger bestaat van het Amerikaanse ICS-CERT. “Het zou goed zijn als wij hier ook een dergelijke instantie zouden hebben. Al was het alleen al om de bewustwording te vergroten. Overigens gaat de Amerikaanse situatie ook op voor Nederland. Volgens de Nationaal Coördinator voor Terrorismebestrijding en Veiligheid ligt de energie sector hier onder het vergrootglas van hackers. De energie-keten heeft door zijn vele schakels, van de opwekking tot het transport, ook nogal wat zwakheden die hackers kunnen uitbuiten. Daarbij komt dat nieuwe ontwikkelingen, zoals smart meters en smart grids, de kwetsbaarheid van de energievoorziening alleen maar groter maken. Het vraagt om goede samenwerking tussen partijen in de gehele keten zodat er geen zwakke schakels meer overblijven.” Hij ziet hier ook een rol weggelegd voor de overheid én de wetenschap. De overheid kan voor meer regelgeving en naleving daarvan zorgen, terwijl de academische wereld het nodige onderzoek kan verrichten naar maatregelen om cyberaanvallen vroegtijdig op te sporen en vervolgens te bezweren. “Ik zie dat er in Nederland door de overheid al stappen in de goede richting worden gezet. Maar het mag wat mij betreft wel wat sneller en doortastender. Bijvoorbeeld door net als de Amerikaanse overheid workshops te organiseren waarin partijen afkomstig uit verschillende sectoren hun ervaring op het gebied van cybersecurity delen.”

ASSESSMENT

De aanvallen op kritische infrastructuur worden niet alleen door schimmige hackers uitgevoerd, weet security-expert Schekkerman. Ook overheden maken zich hier schuldig aan, al is het dan wat lastiger om de beschuldigende vinger te kunnen wijzen. Feit is echter wel dat dergelijke aanvallen plaatsvinden. “In Navo-verband is ieder land al op zijn minst bezig om een task force cyber op te zetten die zowel defensief als offensief kan opereren.” Iran kan er over meepraten. Het land heeft enkele jaren geleden een geslaagde cyberaanval op enkele Iraanse nucleaire faciliteiten voor de kiezen gekregen. Naar verluidt, zijn de Amerikaanse en Israëlische overheden daar in gezamenlijkheid te werk gegaan. De vrucht van de samenwerking, door security experts ‘Stuxnet’ gedoopt, was een bijzonder ingenieus malwareprogramma dat Iraanse ultracentrifuges buiten werking heeft weten te stellen. Schekkerman: “Enige tijd geleden, tijdens de crisis op de Krim, is een variant van de Stuxnet-malware gesignaleerd in Oekraïne. Die software, ‘Snake’ gedoopt, was in staat om netwerken duurzaam te ontwrichten.”

Bij de broodheer van Schekkerman, CGI, is inmiddels een set hulpmiddelen ontwikkeld voor organisaties die hun productieomgevingen of kritische infrastructuur kritisch willen laten doorlichten op eventuele zwakheden waar hackers gebruik van kunnen maken. “Die assessments doen wij op geregelde basis voor onze klanten en geïnteresseerde organisaties”, aldus de security-man. Dat het in ieder geval geen kwaad kan om een dergelijke ‘check up’ te laten verrichten, staat wat Schekkerman betreft als een paal boven water. “De vraag is niet of je ooit wordt aangevallen maar de vraag is wanneer zal het gebeuren.” •