Het gevaar uit cyberspace

Terroristen en criminelen die containers in de haven hacken, het is allang geen filmscenario meer. Cyberexpert Jaap Schekkerman legt uit waar de gevaren zitten en wat havens kunnen doen om de zwakke plekken te versterken.

'In april 2013 heeft een tot nog toe onbekende groep het eerste deel van de beveiliging van een elektriciteitsonderstation in de VS onklaar gemaakt. Daarna zijn met zware wapens 37 isolatoren tussen de hoogspanningsmasten uitgeschoten, met kortsluiting en stroomuitval tot gevolg. Dat is onlangs bekend geworden; de autoriteiten hebben het lang stil gehouden, omdat ze geen aanknopingspunten voor de daders hadden. Er is alleen speculatie – misschien was het wel een proefaanval van terroristen, om te kijken hoe de overheid zou reageren, en willen ze zoiets herhalen maar dan op meerdere plekken tegelijk.'

Aan het woord is Jaap Schekkerman (61), director global cyber security voor de internationale consultancyfirma CGI. Infrastructuur kan zo het doelwit van een aanval zijn, wil hij maar zeggen met het voorbeeld. Zijn boodschap: scherm ook de digitale kant goed af. 'Ik kan geen namen van klanten noemen, want daar willen ze zelf meestal niet mee te koop lopen uit oogpunt van marketing. Bovendien zijn er altijd hackers die als ze zo'n bedrijfsnaam zien, dat meteen willen testen... Er zitten multinationals onder, maar ook kleinere bedrijven, overheden en defensie.'

Maar wat houdt zijn werk eigenlijk in? 'Voor CGI houd ik me vooral bezig met de beveiliging van critical infrastructures. Dat is namelijk fundamenteel anders dan hoe bijvoorbeeld banken en websites worden aangevallen. Het grootste verschil is dat de technologie die achter procesautomatisering zit, bijvoorbeeld van de kranen in de haven, of van onbemande voertuigen, niet altijd maar soms gedateerde ICT bevat. Iedereen heeft het nu over Windows XP, maar ik kom nog geregeld MS-DOS tegen. Dat is goed verklaarbaar, omdat het van oorsprong min of meer geïsoleerde processen zijn.'

Inmiddels worden die processen gekoppeld aan logistieke systemen, zoals een enterprise resource planning (ERP), zodat meteen ook de voorraden of grondstoffen in de gaten gehouden kunnen worden. 'Dat houdt een risico in, omdat industriële processen van een andere orde zijn. Die werken niet alleen met gegevens, maar ook met besturingscommando's – bijvoorbeeld dat kleppen iets moeten doen', aldus Schekkerman.

Je zou toch zeggen dat iedereen, na alle onthullingen over hackers en de NSA, zich nu wel bewust is van die gevaren? 'Het bewustzijn begint te groeien, maar de industrie weet vaak niet wát ze moeten doen. Het is ten dele ook een ontwerpvraagstuk: de systemen zijn niet *designed with security in mind*, zoals het heet. Dat compliceert het nemen van maatregelen: zo is er vaak nog sprake van proprietary ofwel eigen industriële protocollen, in plaats van ingekochte IP (internet protocol, red.) bij grote software-aanbieders, of zitten ze op een smalbandig netwerk.'

In de haven spelen bovendien nog specifieke zaken, stelt Schekkerman. 'Daar zie je twee vraagstukken. Zo is in het najaar 2013 in de haven van Antwerpen het containerlogistieke systeem gehackt, met als doel om drugs containers te laten passeren. Daarbij speelt dataprotectie een rol, ofwel het voorkomen van het manipuleren dan wel stelen van gegevens. Het andere vraagstuk speelt op niveau van de procesbesturing, en daar gaat het om het frustreren van industriële processen, bijvoorbeeld het stopzetten of verplaatsen van hele groepen containers. Dat laatste kan zelfs uitgevoerd worden met een terroristisch oogmerk, door een terreurgroep. Soms zitten daar zelfs landen achter, dan wel *nation state sponsored groups*. Die landen hebben dan belang bij het uitschakelen van de infrastructuur, onder meer door aanvallen op de elektriciteitsvoorziening.'

Problematisch

Volgens de CGI-consultant is het problematisch wie verantwoordelijk is voor de elektriciteitsvoorziening, want dat zijn – net zoals in het geval van de logistieke keten in de haven – voor het grootste deel private partijen. 'Vorige week heb ik een werkgroep van de Europese Commissie hierover gesproken, dat er weliswaar regulering is, maar geen controle over de grenzen heen.'

Niet dat er nog helemaal niets gebeurt. 'Defensie loopt altijd voorop in dit soort zaken, en voor Nederland geldt dat zeker. Zo beschikt ons land al over een cyber defense-eenheid in het leger. Een van de redenen waarom veel Navo-landen zo'n eenheid opzetten is de verwachting dat in een conflict een fysieke aanval altijd voorafgegaan zal worden door een cyberaanval op de critical infrastructure, zoals de energievoorziening, maar ook het transport en de logistieke keten.'

> Ze zeggen dat het prima beveiligd is, maar ik heb er geen beeld van.
>
> **Jaap Schekkerman, director global cyber security CGI**

Het roept de vraag op hoe het in de Rotterdamse haven is geregeld. 'In Rotterdam is er een prachtig systeem voor informatie-uitwisseling in de haven, het Port Community System, waar zo'n 2500 bedrijven bij zijn aangesloten. Maar de beveiliging staat of valt met de zwakste schakel van die 2500. Ze zeggen dat het prima beveiligd is, maar heel eerlijk: ik kan daar geen duidelijk beeld van krijgen. Ik heb in Rotterdam nog geen voorbeeld gezien zoals die drugs-hack in Antwerpen, maar we moeten ons ook realiseren dat in Europa ook heel weinig in de openbaarheid komt. In Amerika daarentegen hebben ze een speciale instantie in het leven geroepen, de ICS-CERT (Industrial Control Systems – Cyber Emergency Response Teams), en die rapporteren over 2013 zo'n 600 gevallen. Van de aanvallen heeft 58% betrekking op de energiesector, 19% op critical manufacturing en 5% op transportation and logistics.'

'En dat is nog maar het topje van de ijsberg', stelt Schekkerman fijntjes. 'Als CGI beveiligen we veel netwerken van bedrijven en organisaties, en wij krijgen dagelijks rond de 43 miljoen alerts in onze Security Operations Centers. Dat zijn meldingen van alles wat afwijkt van de standaardprocedure, dus het overgrote merendeel heeft niet betrekking op een hackerspoging, maar het geeft wel een beeld van de omvang.'

Uitwaaierend

'Wat de zaken nog eens compliceert in de haven, is dat goederen binnenkomen via zeetransport, maar via andere kanalen doorgaan naar het achterland. Dat is een uitwaaierende keten, die je in zijn geheel in de gaten dient te houden. Neem die drugszaak in Antwerpen: het was uiteindelijk de bedoeling om die containers ook met vrachtwagens van het terrein af te krijgen.'

De vraag dringt zich op hoe je dat nou kunt beveiligen. 'Wij hebben een methode ontwikkeld om industrial control systemen (ICS) te beschermen tegen cyberaanvallen, SECURE-ICS geheten,' vertelt Schekkerman. 'Dat betekent dat je het systeem opsplitst in functionele lagen en die dan afzonderlijk beschermt, beginnend bij het laagste niveau, de meetsensoren, tot en met

FOTO XXX

de besturing en de koppelingen met het corporate netwerk.'
'Wij adviseren een Cyber Security Management Framework aanpak. Dat houdt in dat je planmatig te werk gaat en op basis van risicoanalyse maatregelen neemt om bedreigingen te detecteren, om te beschermen en ook om de respons te organiseren. Stel dat alle systemen door hackers niet meer bruikbaar zijn, wat is dan je recovery-mogelijkheid? Het is aan te bevelen een zogeheten recovery plan achter de hand te hebben, zodat je álle technologie-instellingen één op één kunt terugzetten aan de hand van actuele image back-ups.'
'Daarnaast is een goede cyber security referentie architectuur van groot belang. Daarmee ontwerp je een soort blauwdruk voor al je beveiligingsprocessen. Dat doen we ook voor grote productieomgevingen in de chemie, waar soms wel honderden processen draaien die je niet allemaal stuk voor stuk compleet kunt doorlichten. Daar gebruik je de blauwdruk voor, waarin de spelregels staan hoe om te gaan met proces-, data- en netwerksecurity.'
Klinkt indrukwekkend allemaal, maar zijn we er dan? 'Je moet het fysieke beveiligingsproces overigens niet vergeten', erkent hij. 'Fijn als je computers ook online veilig staan, maar als een medewerker de achterdeur open laat staan en een kwaadwillende kan zo het gebouw of de fabriek binnen, dan heb je daar nog niets aan.'

PETER WIERENGA

BEDRIJFSNIEUWS

J. Stam Transport b.v. is met 35 eenheden gespecialiseerd in het geconditioneerd vervoer van bloemen, planten en stukgoederen naar en van Duitsland. De onderneming heeft onlangs twee Volvo's FH 460 pk 4x2 trekkers en een Volvo FH 460 pk 6x2 bakwagen aangeschaft. Met deze nieuwe Euro VI-trucks hoopt het bedrijf op termijn, bijvoorbeeld qua tolheffing, een voordeel te behalen.

Een nieuwe naam, een nieuwe huisstijl en een nieuwe web portal. **T Comm Tracking & Tracing** gaat voortaan als **T Comm Telematics** door het leven. Met de nieuwe naam wil het bedrijf duidelijker aangeven dat de focus ligt op het realtime monitoren van ladingdragers en de grote variatie aan sensoren die afgelezen kunnen worden.
T Comm Telematics is specialist in het draadloos meten, registreren en realtime inzichtelijk maken van de locatie en staat van trailers, motor- en aanhangwagens en de conditie van de lading hierin.

J.L. Mijnders Transport heeft onlangs zes Volvo FH 460 Light Concept trucks in gebruik genomen. De nieuwe vrachtwagens zijn een uitbreiding op het bestaande wagenpark van 85 eenheden en 120 opleggers. J.L.Mijnders is een belangrijke speler binnen de containertransportsector met als specialisaties tank/box-containertransport (chemie & foodproducts) en koelcontainers met genset aansluiting. Het bedrijf heeft vestigingen in Melissant, Duisburg en Antwerpen.

Norbert Dentressangle krijgt de leiding over het nieuwe verscentrum van **Albert Heijn** in Nieuwegein. Dit zogeheten Shared Fresh Center (SFC) moet volgend jaar gaan draaien. Via Nieuwegein worden straks ongeveer negenhonderd Albert Heijn-supermarkten beleverd. Het nieuwe centrum moet zorgen voor een snellere en efficiëntere belevering met verse producten, minder voorraad en minder transportbewegingen. Albert Heijn is van plan nog een tweede verscentrum op een centrale plek in Nederland te bouwen. Beide vervangen de bestaande verscentra die in Nieuwegein en Utrecht zijn gevestigd.

Heeft u ook logistiek of transportnieuws over uw bedrijf? Mail naar:
redactie@nieuwsbladtransport.nl