Cybersecurity: de achterdeur staat open

Cybersecurity vraagt om internationale samenwerking en om concrete maatregelen. “De beveiliging van de vitale infrastructuur hoort prioriteit te krijgen, want daar staan nu veel achterdeuren open”, stelt Jaap Schekkerman van CGI.

In Nederland ligt de nadruk binnen cybersecurity nu veelal op de beveiliging tegen onder meer DDoS-aanvallen en identiteitsdiefstal. Dat is natuurlijk goed, maar Jaap Schekkerman wijst op een veel groter risico: de beveiliging van de vitale infrastructuur. “Deze beveiliging schiet tekort. We kunnen zien dat allerlei belangrijke onderdelen van deze infrastructuur via internet te benaderen zijn. Een slimme hacker of een terreurgroep kan daarmee de elektriciteitslevering of de drinkwatervoorziening in Nederland verstoren of bruggen en keringen openzetten, om maar eens wat te noemen. Dat is natuurlijk een veel ernstiger bedreiging dan dat de servers van een bank onbereikbaar worden door een DDoS-aanval.”

Schekkerman is als onderzoeker verbonden aan het Institute For Enterprise Architecture Developments en als docent aan het Delft TopTech Programma van de TU Delft. Hij werkt bij CGI als Director Global Cyber Security en Thought Leader op het gebied van veiligheid van vitale infrastructuren. Hij houdt een dringend pleidooi voor de aanpak van de zwakke plekken in de infrastructuur. “Je kunt wel een goede strategie tegen inbraak bedenken, maar als je achterdeur openstaat, heb je daar weinig aan. En er staan nog heel veel achterdeuren open.” Cybersecurity voor de vitale infrastructuur vraagt om een aanpak en maatregelen die ingrijpen in de techniek, de processen en het gedrag van de mensen in een organisatie, zegt hij. CGI ontwikkelde een specifieke aanpak voor de beveiliging van vitale infrastructuren, die is gebaseerd op internationale standaarden en best practices. Kort gezegd komen deze erop neer dat de vitale infrastructuren worden opgedeeld in zones. Alle toegang tot en al het dataverkeer tussen deze zones wordt geïsoleerd en gecontroleerd, zodat er alleen verkeer doorheen gaat dat voldoet aan de beveiligingseisen. Daarmee wordt de achterdeur goeddeels gesloten.

Het gaat erom hoe kwetsbaar men is en hoe veilig men zou moeten zijn

Het antwoord is volgens Schekkerman een raamwerk van concrete acties en maatregelen. De Nederlandse overheid onderneemt de nodige initiatieven op het gebied van cybersecurity. Eind oktober zag de tweede Cyber Security Strategie het licht en sinds twee jaar overleggen bedrijfsleven en overheid in de Cyber Security Raad. Goede initiatieven, die volgens Schekkerman echter nog niet ver genoeg gaan: “Men zou veel meer kunnen samenwerken in concrete acties en samen maatregelen kunnen nemen.” Als voorbeeld noemt hij de Verenigde Staten. President Obama noemde in zijn State of the Union in 2013 cybercrime een ernstiger bedreiging dan terrorisme en hij gaf het Amerikaanse National Institute of Standards and Technology de opdracht om binnen acht maanden een cybersecurity framework te maken. Industrie en overheid ontwikkelen dit framework samen, waarbij men leert van elkaar en best practices gebruikt. Dat resulteert in een concreet pakket van maatregelen. “Dit framework, waarbij CGI ook betrokken is, beschrijft in een aantal heel concrete stappen wat je moet beveiligen, in de volgorde identify – protect – detect. En hoe je moet reageren als je wordt aangevallen: response en recover. Aan deze stappen hangen concrete activiteiten, die zijn gerelateerd aan internationale standaarden op dit gebied.”

Een dergelijk raamwerk zou ook voor Nederland zeer wenselijk zijn, stelt hij. En daar ligt een rol voor de overheid: “Die kan werken aan de bewustwording dat cybercrime met betrekking tot vitale infrastructuren een reële dreiging is en stimuleren dat hier concrete maatregelen worden genomen. Die bewustwording zien we nu wel bij de industrie, maar bijvoorbeeld nog niet voldoende op bestuurlijk niveau bij vitale sectoren als netbedrijven.” Men kan profiteren van internationaal aanwezige kennis en best practices op dit gebied. Deze laten zien dat cybersecurity in feite een vorm van risicomanagement is. “Het gaat erom hoe kwetsbaar men is en hoe veilig men zou moeten zijn. Zet dus in op de beveiliging daarvan.”

Cybersoldaten

Cybersecurity is een internationaal thema, want de dreiging komt over het algemeen van buiten onze landsgrenzen. Bovendien kan er veel geleerd worden van andere landen als samen wordt opgetrokken. Bij het ministerie van Defensie erkennen ze dat. Defensie is onder meer lid van het NATO Cooperative Cyber Defence Centre of Excellence. “We bundelen hierin onze krachten en versterken onze kennispositie”, zegt Hans Folmer, commandant Task Force Cyber bij het ministerie. Doel van deze taskforce is om Defensie optimaal te laten opereren in cyberspace, zowel defensief als offensief. Onlangs kondigde Defensie aan dat het cybercommando dat voor 2015 gepland stond, versneld wordt opgericht. Begin volgend jaar moeten de eerste cybersoldaten aan de slag zijn. Daarmee wil Defensie net zo krachtig en wendbaar zijn in de virtuele als in de fysieke wereld.

iBestuur Congres 2014

Wilt u weten hoe u de achterdeuren van uw organisatie kunt sluiten?
En hoe accuraat te reageren nu dreigingen zich verplaatsen van de fysieke naar de virtuele wereld? Jaap Schekkerman zet het op een rijtje met een ‘publiek bestuurder’. (meer info via iBestuur.nl)
Kavel 7: iBestuur, zaal Dexter 25-26, 15.30 uur tot 16.00 uur. (zaal en tijden o.v.b.)