‘De vraag is niet óf u wordt gehackt, maar wanneer’

Dick Berlijn

Tijdens de Audit Committee Dialogue op 15 april in de Rotterdamse Maastoren stond het thema ‘cybersecurity’ centraal. Een actueel onderwerp, omdat Nederlandse banken en andere organisaties nog maar net daarvoor slachtoffer waren geworden van zogeheten DDoS-aanvallen. Bij zo’n Distributed Denial of Service-aanval worden de servers van een bedrijf of instelling bestookt met zo’n grote hoeveelheid aanvragen dat deze overbelast raken. “We lezen er regelmatig over in de krant”, zegt ook Dick Berlijn, voormalig Commandant der Strijdkrachten en Senior Board Advisor bij Deloitte. “Er wordt wereldwijd elke dag wel iets over cybersecurity gemeld, maar de samenhang ontbreekt. Ten aanzien van cybersecurity hebben we de verantwoordelijkheden niet goed genoeg verduidelijkt.”

Dick Berlijn begint met het uitleggen van het begrip ‘cybersecurity’: “Er is geen enkele discipline te bedenken die niets te maken heeft met cyber, met de digitale omgeving. Cyber is overal en raakt alles: energie,

‘Er is geen enkele discipline te bedenken die niets te maken heeft met cyber’

Generaal b.d. Dick Berlijn
Senior board advisor bij Deloitte, gespecialiseerd in vraagstukken rondom het thema Cyber Security.

+31 6 1312 1136
DBerlijn@deloitte.nl

transport, infrastructuur, openbare orde en veiligheid, defensie. Cybersecurity gaat over de kwetsbaarheid van en bedreigingen voor netwerken en data. Ik ben geen IT-specialist en ook geen techneut; ik wil het hebben over wat cybersecurity maatschappelijk betekent en wat we er als organisatie mee moeten. Want als we niet meer kunnen vertrouwen op netwerken, is de basis voor het functioneren van onze samenleving weg.”

De complexiteit van cybersecurity

Internet speelt een bijzondere rol, aldus de gastspreker. “Het heeft onze kennis verdiept, stelt ons in staat om kennis te verbinden en betere analyses te maken. Die innovatieve kracht hebben we nodig voor de grote uitdagingen in onze maatschappij. Maar het maakt ons ook kwetsbaar. Misbruik is geen kwestie meer van een virusje waardoor je een smiley op je beeldscherm kreeg: het is een multi million dollar industry geworden waarin op grote schaal geld wordt weggesluisd, gespioneerd en gechanteerd wordt. Het aantal incidenten groeit en de consequenties van incidenten zijn steeds heftiger. Stel: we kunnen drie dagen niet meer pinnen, we kunnen niet meer vertrouwen op de stoplichten, de berichtgeving van de overheid deugt niet en tegelijkertijd staat er ergens een sluis open, wat niet de bedoeling was. Dan krijg je situaties die de samenleving ontwrichten. Dat kennen we in ons land niet meer en dat willen we ook niet meemaken. Dus daar moeten we wat aan doen. We hebben in Nederland een cyberstrategie, een cyberraad, een cybercenter. Dat moet ook, maar als de rest van de wereld niet meedoet zitten we hier nog steeds met een cybersecurity-probleem; vergelijk het maar met de klimaatuitdaging. Wat van ons allemaal is, daar gaan we vaak slordig mee om.”

De verantwoordelijkheden voor cybersecurity zijn slecht verduidelijkt, vindt Berlijn. “Er zijn partijen die zeggen dat het met veiligheid te maken heeft en dat de nationale overheid het dus moet regelen. Er zijn anderen die zeggen dat het om een mondiaal medium gaat en dat het dus aan de VN is. Vergelijk het maar eens met dat andere belangrijke medium: de snelweg. U en ik houden ons aan de verkeersregels, de overheid zorgt voor goede wegen en autofabrikanten zorgen voor veilige auto’s. Dat totaal maakt dat we het medium veilig genoeg hebben gemaakt en het met enige zekerheid kunnen gebruiken.

Dat wil niet zeggen dat er nooit ongelukken gebeuren, maar het medium is betrouwbaar genoeg geworden. Dat idee zou model moeten staan voor de digitale omgeving. Kunnen we het eens worden over verantwoordelijkheden en hoe zorgen we ervoor dat we ernaar gaan leven? Het is niet alleen maar iets technisch, het is niet alleen aan de overheid en het is niet iets wat morgen opgelost gaat worden. Cybersecurity kent vele stakeholders en is complex."

‘Stel: we kunnen drie dagen niet meer pinnen, we kunnen niet meer vertrouwen op de stoplichten, de berichtgeving van de overheid deugt niet en tegelijkertijd staat er ergens een sluis open, wat niet de bedoeling was’

De goede vragen stellen

Vroeger beschermden we onszelf en onze kostbaarheden door een kasteel te bouwen met een slotgracht eromheen en boogschutters op de kantelen, zegt Berlijn. "Als er kapers op de kust waren vocht je de bad guys van de muren af, analyseerde wat er goed en fout ging, paste de procedures aan en wachtte op de volgende aanval. Tegenwoordig zijn ons intellectual property, onze data en onze netwerken onze kostbaarheden. Zulke zaken laten zich niet op die manier beveiligen. We moeten het kasteel uit, de slotgracht over en de dorpen in om te luisteren wat er gebeurt. Kunnen we ons eerder op de hoogte stellen van dingen die broeien? We moeten beter informatie uitwisselen, zodat we maatregelen kunnen nemen om niet in samenlevingontwrichtende situaties terecht te komen. Wat betekent dat voor bestuurders? Veel veiligheidsmaatregelen zijn al wettelijk verplicht. De eisen met betrekking tot privacy worden steeds strenger. Er komen nieuwe beveiligingsrichtsnoeren van het College Bescherming Persoonsgegevens. Er is een EU-verordening op komst; als u liable bent op dit terrein hangt u een boete van maximaal 2% van de wereldwijde omzet boven het hoofd. Ook bestaat de meldplicht bij lekken of hacks waarbij persoonsgegevens betrokken zijn. Maar daarnaast moeten mensen met een sturende rol zich op zijn minst nog een aantal vragen stellen. Weten we als organisatie wat relevante bedreigingen en kwetsbaarheden zijn? Dat moet je als organisatie tegen het licht durven houden: wat zijn onze belangrijkste datastromen, welke gegevens mogen nooit gecompromitteerd worden, hoe hebben we die beveiligd? Weten we wie in onze organisatie ultiem verantwoordelijk is? Zijn er voldoende controls die ons kunnen waarschuwen? Zo ja, waar blijkt dat dan uit? Hebben we voldoende monitoring capability en response capability die ook echt geoefend is en die



naar verschillende scenario's kijkt? Een DDoS-aanval kun je met techniek maar beperkt oplossen, dat zit hem vooral in de response capability. Hoe zorgen we ervoor dat we weten welke informatie onze organisatie zomaar verlaat? Hebben we een systeem om dat te detecteren? Hoe weten we wie op onze netwerken aan het inloggen is en waarvandaan? Is het logisch dat er midden in de nacht vanuit Peru wordt ingelogd? Hoe zorgen we dat we weten dat alle software die op onze netwerken draait ook gevalideerd is? En hoe zorgen we dat we gevoelige informatie die we vrijwillig beschikbaar stellen, bijvoorbeeld via social media, verminderen?"

In control

Vorig jaar heeft Deloitte in Davos de studie Risks & Responsibilities in the hyperconnected world gepresenteerd. Het World Economic Forum heeft Deloitte gevraagd dat gedachtegoed verder uit te dragen. Daar is het pamflet Partnering for Cyber Resilience uit voortgekomen: een initiatief waaraan bestuurders en beslissers gevraagd wordt om zich te committeren. "Als uitdrukking van het besef dat je niet moet wachten op de overheid of op de VN of op wie dan ook, maar dat je zelf je verantwoordelijkheid neemt", aldus Berlijn. "Dat geldt voor alle bestuurders. Want de vraag is niet óf u wordt gehackt, maar wanneer. En dan zult u moeten kunnen zeggen dat u op het gebied van cyber overtuigend en aantoonbaar in control bent. U moet op vragen kunnen antwoorden: Ja, ik weet wat er aan de hand is. Ja, ik was me van de risico's bewust. Ja, ik heb alle maatregelen genomen die mogelijk waren om het probleem te voorkomen. Door bijvoorbeeld praktische maatregelen als penetration testing, software patching, een cyber threat intelligence systeem en awarenessprogramma's. Elke organisatie moet weten wat de inherente risico's zijn."

Cyber Threat Risk Management: 8 vragen voor het management

1. Kennen we de relevante bedreigingen en kwetsbaarheden?
2. Weten we wie uiteindelijk verantwoordelijk is voor het mitigeren van deze cyber threats en kwetsbaarheden?
3. Zijn er maatregelen getroffen om cyber threats op te sporen en te voorkomen?
4. Zijn we voorbereid op het ergst denkbare cyber-incident?
5. Hoe gaan we na welke digitale informatie onze organisatie verlaat, en waar die informatie naartoe gaat?
6. Hoe weten we wie er inlogt op ons netwerk, en waarvandaan?
7. Hoe controleren we welke software er draait op onze apparatuur?
8. Hoe zorgen we ervoor dat we zo weinig mogelijk informatie beschikbaar stellen aan cybercriminelen?

Dialoog

Commissarissen en management onderschatten de risico's van cyber crime, is de stelling waarmee de dialoog na de pauze wordt geopend. "Het probleem is dat het management het technisch niet begrijpt", oppert iemand. "Je bent als bestuurder afhankelijk van wat anderen in je bedrijf hierover zeggen." We moeten ons realiseren dat de risico's met betrekking tot cyber te maken hebben met de continuïteit van de organisatie, is de opvatting. "Als je dit onderschat loop je het risico dat je organisatie zo hard onderuit gaat dat je niet meer overeind komt. Wanneer je straks de juiste maatregelen niet hebt genomen, loop je niet alleen risico op fysieke schade, maar ook op reputatieschade." "Zeker in de financiële sector is er steeds meer aandacht voor cybersecurity. Maar als Gasunie of Albert Heijn of de C1000 worden gehackt, heeft de samenleving ook een probleem." Er hangen vaak forse bedragen aan technologische oplossingen, wordt opgemerkt, en het kost tijd om ze te implementeren. "Maar een cyberscan is zo uitgevoerd. Er is hulp. Alleen zitten veiligheidsrisico's niet altijd alleen aan de harde kant, maar vaak ook bij mensen." Voorbeelden van USB-sticks met malware die van de parkeerplaats worden opgeraapt en de organisatie in komen of van Sinterklaas die op 5 december tijdens het personeelsfeest binnen vijf minuten in het systeem zat, onderstrepen dit.

Staat het onderwerp IT wel voldoende op de agenda van de Raad van Commissarissen, is de volgende vraag. "Voor een bank is eens per jaar niet voldoende, voor een ander soort bedrijf misschien wel." Het is in elk geval niet alleen iets voor de auditcommissie, is de heersende mening. Een echte dialoog met de CIO hebben de meeste commissarissen niet, zo blijkt. "De CIO zit vaak niet in het bestuur." De verantwoordelijkheid van de CIO blijkt met de ontwikkelingen op het gebied van cyber wel op te schuiven in de richting van de CEO. Accountants zouden een grotere rol kunnen spelen bij het informeren van de Raad van Commissarissen als het gaat om risico's op het gebied van IT, vindt men. "Voor de externe accountant liggen er kansen om dit onderwerp relevant te maken. Een accountant kent het bedrijf vaak beter dan de commissaris." "Soms krijg je opmerkingen als: 'De passwordveranderingscultuur is niet voldoende'. Ik kan me niet voorstellen dat dat de belangrijkste bevindingen zijn. Ik hoor liever antwoord op de acht vragen van Dick Berlijn." Dat er in de toekomst ondernemingen zullen zijn die ten onder gaan aan cyber crime, daarvan is iedereen overtuigd. "Dat is al gebeurd. Maar er zullen cruciale bedrijven moeten sneuvelen of majeure fysieke rampen gebeuren voor er regels en wetten komen." "Ik heb liever een commissie die in de luwte samenwerkt om de goede dingen af te spreken. Op een gegeven moment zullen er wel standaarden en regels komen: prima. Maar begin eerst eens met gegevens uitwisselen."