Deloitte.

Februari 2018

Rondetafelgesprek Tweede Kamer der Staten Generaal inzake Cybersecurity

Veel grote en kleine bedrijven zijn zich pijnlijk bewust geworden van hun digitale kwetsbaarheid. De grote cyberaanvallen WannaCry en notPetya zorgden vorig jaar voor nog eens een hardhandige wake-up call. Grote bedrijven investeren momenteel tot vele tientallen miljoenen in cyberveiligheid. Er zijn zelfs bedrijven die in hun eentje bijna net zoveel hierin investeren als de 95 miljoen die de Nederlandse overheid in het regeerakkoord uittrekt voor cybersecurity.

Slimme bedrijven combineren investeringen in digitale veiligheid met verbeteringen van hun producten en dienstverlening. De experts zijn niet aan te slepen; onze roosters en ook die van onze branchegenoten zitten volgeboekt tot ver in de lente.

Op uw vraag of er bij bedrijven wel voldoende aandacht is voor cybersecurity is het antwoord volmondig ja. Het besef leeft dat de continuïteit van de onderneming in het geding is. Goed nieuws is dat ook bij regering en parlement de belangstelling voor het onderwerp toeneemt. Het minder goede nieuws is dat de beperkte budgettaire middelen in het regeerakkoord (95 miljoen, versnipperd over de departementen) vrijwel geheel worden aangewend voor repressie en het bestrijden van excessen: defensie, opsporing en inlichtingen. En niet voor preventie. Ik kom dan ook tot de volgende aanbevelingen en suggesties:

1. Kies in de wet- en regelgeving voor een risicogerichte benadering; zwicht niet voor de verleiding van ad hoc-wetgeving

Vrijwel de hele cybersecuritybranche is het erover eens dat gedetailleerde wetten en richtlijnen voor digitale veiligheid en het uitdelen van boetes bij overtreding niet werken. Het leidt slechts tot een cultuur van afvinken, niet tot veiligere systemen. Het afvinken van voorschriften terwijl men weet dat het systeem niet veilig is, komen we in de praktijk helaas nog teveel tegen. Een goed voorbeeld hoe het ook kan, is het project TIBER (Threat Intelligence Based Ethical Red teaming) van De Nederlandsche Bank. Bij dat project stellen financiële instellingen zich bloot aan cyberaanvalssimulaties om de weerbaarheid van hun systemen te testen. Het project is ingericht op het belonen van goed gedrag in plaats van het bestraffen van slecht gedrag. Het toont de constructieve houding van de toezichthouder.

"Investeren in preventie, met de blik op de lange termijn, is dan ook mijn hoofdboodschap."

Inge Philips
Director Cyber Risk Services
Deloitte Nederland

Het zou goed zijn als ook de Autoriteit Persoonsgegevens voor een risicogerichte aanpak kiest en bedrijven en instellingen meer zou prikkelen om hun systemen veiliger te maken.

2. Digitale dreigingen moeten beter en breder gedeeld worden

Bij de Nederlandse opsporings- en inlichtingendiensten is veel kennis over digitale bedreigingen, maar deze wordt lang niet altijd gedeeld met het bedrijfsleven. In de cyberwereld leeft breed het idee dat er veel valt te verbeteren in de signalering over en weer. Daar waar het gaat om vertrouwelijke informatie zou de overheid kunnen werken met een vertrouwde schil van bedrijven.

Een goed initiatief is dat er 2,5 miljoen euro wordt geïnvesteerd in het Digital Trust Center door het ministerie van Economische Zaken in samenwerking met de branche om het MKB beter in staat te stellen hun cyberveiligheid te vergroten. Opgemerkt zij wel dat het bedrag van 2,5 miljoen in het niet valt bij de miljarden schade die de Nederlandse economie nu al jaarlijks lijdt door cybercriminaliteit. Daarnaast is het belangrijk om te blijven investeren in lokale CERT's (Computer Emergency Response Teams).

3. Een digitaal contract tussen overheid en bedrijfsleven

Van groot belang is dat overheid en bedrijfsleven systematisch met elkaar in gesprek gaan met als inzet te komen tot een gemeenschappelijk gedragen digitale strategie en duidelijkheid over en weer wat partijen van elkaar kunnen verwachten. Naar analogie van de deltacommissaris zou een regeringscommissaris kunnen worden benoemd die belast wordt met het formuleren van een cyberstrategie en die toeziet op uitvoering daarvan op alle beleidsterreinen. Behalve een risicogerichte strategie staat hoog op het wensenlijstje van het bedrijfsleven een fiscaal klimaat dat proactieve investering in cybersecurity stimuleert, zoals een kortere termijn van fiscale afschrijving van deze investeringen.

4. Investeer in onderzoek

De technische universiteiten luidden vorige maand de noodklok dat cyberonderzoekers worden weggetrokken uit Nederland. Wij geven slechts 2 miljoen uit aan cybersecurity gerelateerd onderzoek vergeleken met 50 miljoen door onze oosterburen. Je kunt denken aan nieuwe leerstoelen voor veelbelovende onderzoeksgebieden als 'net neutrality' en de ontwikkelingen rondom digitale identiteiten die mensen meer regie over hun eigen gegevens geven ('self sovereign identities').

Voor de duidelijkheid: meer geld voor onderzoek hoeft niet alleen van de overheid te komen. Deloitte, maar ook andere bedrijven zijn bereid onze universiteiten te steunen met geld en samenwerking. Wij hebben die handschoen al opgepakt. Hier ligt ook een kans voor de overheid.

5. Veranker cyberkennis in het curriculum van het onderwijs

Als er wordt gesproken over 'digitalisering van het onderwijs' gaat het in de praktijk om het gebruik van tablets en appjes over roosters en resultaten van leerlingen. Uitzonderingen daargelaten zit programmeren en cyberkennis niet in het curriculum. In maart begint herziening van het curriculum van het voortgezet onderwijs. Als daarin cyberkennis wordt verankerd, duurt het nog jaren voordat dit zich daadwerkelijk vertaalt in het lesprogramma. Ingrijpen is nodig om te voorkomen dat ook de huidige lichting in het voortgezet onderwijs een verloren generatie wordt. Ook hier is het bedrijfsleven bereid te helpen om het gat te dichten.