103E RONDETAFELBIJEENKOMST: DATASECURITYRISKS & CYBER RESILIENCE

Wisselwerking gezocht en gevonden

De discussie over cybersecurity wordt in meerdere opzichten volwassener. Waar voorheen CIO's het onderwerp nog vooral als een risicoafweging benaderden, en de technologische aspecten als een gedelegeerd onderwerp zagen, praten IT- en topbestuurder nu volop mee over aanpak en oplossingen. Bovendien wordt volop de wisselwerking gezocht, zowel met andere functionarissen, binnen industrieën als op landenniveau.

De hyperconnected wereld waarin we leven en zakendoen, biedt zowel consumenten als bedrijven ongekende economische en maatschappelijke mogelijkheden. Het feit dat alles en iedereen onderling verbonden is, maakt ons echter kwetsbaar voor identiteitsdiefstal, cyberspionage en digitale oorlogsvoering. Of zoals een kenner het tijdens de op initiatief van CGI en in samenwerking met dit blad georganiseerde rondetafelbijeenkomst verwoordde: "Je weet als drager van een intelligente bril niet wie er met je meekijkt. Of wie er meekijkt of luistert als je je mobiele telefoon gebruikt."

Digitale security laat zich als 'bewegend doelwit' verre van gemakkelijk adresseren. Samenwerking is geboden, zo bleek tijdens de rondetafelbijeenkomst. Met een vijftiental IT-beslissers, veiligheidsexperts en chief security officers werd in De Villa te Vught de verdieping gezocht. "Informatiedeling is belangrijk", stelde Dennis Pieterse, Cybersecurity Practice Leader bij CGI en medegastheer van de bijeenkomst tijdens de opening. "Onze ervaringen op securitygebied leren dat je het als organisatie of verantwoordelijke afdeling niet alleen af kunt. Het delen van *best practices* als het gaat om de inrichting van een cybersecuritybeleid met bijbehorende oplossingen is cruciaal."

Krediet

Jaap Schekkerman, global director Cybersecurity bij CGI, zoomde tijdens de bijeenkomst in op de trends en ontwikkelingen. Hij schetste daarbij cybersecurity als een veelkoppig monster. Het gaat om talloze typen aanvallen en bedreigingen, die ook nog eens uit verschillende bronnen komen. De motieven kunnen bovendien enorm verschillen. Soms gaat het om puur kwaadaardige en moedwillige acties, maar soms ook niet. Het aantal bronnen is groot: criminelen, terroristen en natiestaten. Zo hebben recentelijk ook overheden krediet verspeeld door internetverkeer te monitoren.

De specialist toonde zich bij een rondje langs alle bedreigingen een levende encyclopedie. Hij verhaalde pakkend over onder meer *advanced persistent threats*, bijvoorbeeld in het kader van cyberspionage, *enhanced attacks on mobile devices* maar ook over zogenoemde *cryptoware*. "De focus ligt in toenemende mate op zwakke plekken in software, systemen en kritische infrastructuren", aldus Schekkerman. "Kwaadwillenden proberen daar op diverse manieren misbruik van te maken."

Hoe dan ook: bedrijven, overheden en ook burgers zullen er volgens hem mee moeten leren omgaan. Gelukkig heerst aan de 'goede kant' het besef dat men samen sterker staat: individuen, organisaties, IT-afdelingen en ook het bestuur. "Al met al zien we een stijgende belangstelling voor dataprivacy en databescherming." Daarbij is het volgens Schekkerman maar de vraag wat je daar als overheid aan kunt bijdragen. "Criminelen hebben ondanks de wetgeving immers vrij spel. Daarom moeten we misschien niet investeren in wetten, maar in het voorkomen van problemen."

Door Hotze Zijlstra ✖ Fotografie Marcel Willems










Cybersecurity vanuit nationaal-
maatschappelijk en
bedrijfsperspectief
Auke Huistra

"WE MOETEN MISSCHIEN NIET INVESTEREN IN WETTEN MAAR IN HET VOORKOMEN VAN PROBLEMEN"

Discussie

De discussie spitste zich vervolgens toe op menselijk gedrag en falen, en daarmee het belang van het creëren van bewustzijn bij consumenten en medewerkers binnen een organisatie. "Mensen moeten snappen dat ze verantwoordelijk zijn voor hun data." Al te veel leunen op technische hulpmiddelen kan bovendien averechts werken, zo voegde een tafelgenoot toe: "Ze kunnen leiden tot onveiliger gebruik. Wanneer ik mijn autogordel niet om heb, rijd ik bijvoorbeeld voorzichtiger." Een IT-verantwoordelijke merkte vervolgens op dat er grenzen zijn aan wat je van mensen kunt verwachten. Wel kun je proberen de consequenties van handelingen en onoplettend gedrag duidelijk te maken.

Het is een voor de hand liggende conclusie: de integrale securityaanpak draait om mensen, processen en technologie. De IT-afdeling speelt daarbij een belangrijke rol. De bedreigingen zelf worden idealiter vertaald naar realistische, gecalculeerde bedrijfsrisico's, en oplossingen om deze het hoofd te kunnen bieden.

Wat in het speelveld van bedreigingen begint mee te spelen is het vervangen van de grens tussen traditionele informatietechnologie (IT) en operationele technologie (OT), zo bleek tijdens de discussie. Beide versmelten simpelweg tot 'technologie', waardoor de kwetsbaarheden in beide categorieën in samenhang geadresseerd dienen te worden. Dat vraagt, nogmaals, om een gezamenlijke of geïntegreerde aanpak: cross-functioneel, cross-sector, cross-nationaal en gedragen vanuit zowel de private als de publieke sector.

Scenario's

Auke Huistra, cybersecurity-expert binnen nationale en internationale overheidsprogramma's en multinationals, zocht de verdieping vanuit nationaal-maatschappelijk en bedrijfsperspectief. Hij sprak onder meer over de cybersecurityscenario's die in het kader van de Nationale Risicobeoordeling ontwikkeld zijn door de overheid, academie en het bedrijfsleven. Deze methodiek maakt het mogelijk om de impact van cyberdreigingen vergelijkbaar te maken met andersoortige dreigingen. Huistra: "Dit geeft de mogelijkheid om cybergevaren tot een onderdeel van het reguliere risicomanagement te maken. Je benadert ze precies zo als alle andere bedreigingen."

Ook Huistra hamerde tijdens de bijeenkomst in de Villa van ICT Media op het belang van samenwerking. Data-uitwisseling en leren van elkaar zijn daarbij fundamenteel. Het gaat erom risico's op wereldwijd niveau te vertalen naar onder meer economie, maatschappij en organisaties. "Cyberrisico's kunnen in die zin worden vergeleken met overstromingen of de impact van klimaatverandering. Op landelijk niveau onderzoeken analisten aan de hand van scenario's de impact van dreigingen. Daarbij worden de gevolgen voor mensen, kapitaalgoederen, omgeving en reputatie meegenomen. Zo'n assessment leidt tot een agenda met plannen en prioriteiten, en eventueel het verdelen van taken en de inzet van resources. De gevolgen en ook de maatregelen zullen per land, sector of bedrijf verschillen."

In de praktijk komt het pareren van een cyberaanval veelal neer op het op orde hebben van zogenoemde 'barriers', te vergelijken met bijvoorbeeld een serie van dijken die het land moeten behoeden voor overstromingen. Wanneer de ene barrière is doorbroken, is er een volgende te slechten. Huistra: "Je kunt als organisatie onderzoeken in hoeverre het beperken van de risico's met behulp van deze barrières de moeite van de investering waard is. De vraag is hoe ver je moet gaan om uit het kritieke risicogebied te blijven."

Resilience

Albert Markus van het Nationaal Cyber Security Centrum (NCSC) zoomde vervolgens in op het belang van publieke en private samenwerking. Hij sprak daarbij over het belang van zogenoemde 'cyber resilience' oftewel weerbaarheid in de online wereld. "Iedereen heeft daarbij gedeelde belangen", aldus Markus. "Zowel in de publieke als de private sector, maar ook nationaal en internationaal. Dat vraagt om samenwerking, onderling vertrouwen en transparantie. We moeten in vertrouwelijkheid informatie gaan uitwisselen, want ieder voor zich komen we er niet uit. Het gaat daarbij om een gezonde balans tussen vrijheid, veiligheid en maatschappelijke groei."

Markus sprak daarbij van de Cyber Security Strategie 2.0, waarbij de Cyber Security Raad gevraagd en ongevraagd advies geeft aan het kabinet en daarnaast toeziet op de uitvoering van het NCSC. Ook de sectorspecifieke Information Sharing and Analysis Centers (ISACs) spelen daarbij een rol. John Proctor, binnen CGI wereldwijd verantwoordelijk voor de cybersecuritystrategie, haalde in dat licht de samenwerking aan tussen de Canadese overheid, de private sector en andere belanghebbenden, waaronder ook bedrijven die elkaars concurrent zijn. "Het gaat om een breed gedragen overleg. Dit in tegenstelling tot de aanpak in bijvoorbeeld de VS en Groot-Brittannië, waar de nationale cybersecurity een sterk door de overheid gestuurde aangelegenheid is." Markus: "Ook hier speelt die brede samenwerking, met de overheid als een deelnemende netwerkpartner. In die zin lopen we als Nederland net als Canada redelijk voorop."

Gremia

Tijdens de rondetafelbijeenkomst werd nog wel gewaarschuwd voor al te omvangrijke overlegstructuren en gremia. "Maak het niet te breed, maar zorg dat de betrokkenen hun eigen belang blijven zien", aldus een deelnemer. Om die reden kan het goed zijn om, naast de initiatieven op internationaal en landelijk niveau, ook samenwerking binnen sectoren of industrieën te zoeken. "Daartoe is het belangrijk dat men ook aan de bestuurstafels de zaak op het netvlies krijgt", stelde moderator Rob Beijleveld, CEO van ICT Media en uitgever van dit blad, tot slot. Dat blijkt gelukkig steeds meer het geval. ✖