Founded by
Dutch IT Channel
Datto

Eerste bijeenkomst Dutch IT Cybersecurity Assembly:

Tijd om het over cyber-resilience te gaan hebben

Eerste bijeenkomst Dutch IT Cybersecurity Assembly:

Tijd om het over cyber-resilience te gaan hebben

De Dutch IT Cybersecurity Assembly kende op 3 juni zijn aftrap. Onder zomerse omstandigheden kwamen 12 deelnemers - thought leaders met een uiteenlopende achtergrond - bij elkaar op het terras van The View in Almere. Het doel van de bijeenkomst loog er niet om: de IT-veiligheid van Nederland bespreken en kijken naar manieren om die te verbeteren.

Cybercriminaliteit heeft zich door de jaren heen ontwikkeld van kwajongenstreken tot wat het nu kan zijn: acties van misdadigers die bedrijven of zelfs landen plat kunnen leggen. Voor de complete BV Nederland is het belangrijk dat het land cyberbestendig is. Niet alleen op het niveau van individuen en bedrijven, maar zeker ook als het om de overheid gaat. Om die 'cyber-resilience' van Nederland te verbeteren namen vaktitel Dutch IT-channel en securityleverancier Datto samen het initiatief om de Dutch IT Cybersecurity Assembly op te richten. Die komt meerdere keren per jaar samen om ontwikkelingen te bespreken en plannen te agenderen.

Voorstelronde

De eerste ronde-tafel-meeting begon met een voorstelronde van de twaalf deelnemers: mensen met verschillende achtergronden, maar allemaal met een belangrijke beslissende positie op het gebied van IT of cybersecurity. Er waren CIO's en IT-managers van overheids- en semioverheidsorganisaties aanwezig, maar ook vertegenwoordigers van onder andere IT-dienstverleners, leveranciers met een specialisme in security, datacenterorganisaties, zakelijke eindgebruikers, juridische bedrijven en branche- en belangenorganisaties.

Tijdens de voorstelronde bleek al meteen het belang van het onderwerp. Eén van de deelnemers, werkzaam als CIO bij een overheidsorganisatie, gaf aan dat aanvallen steeds frequenter worden en aan de orde van de dag zijn. "We lopen steeds vaker tegen momenten van ontwrichting aan. We hebben onder meer veel met DDOS-aanvallen te maken." Andere deelnemers onderschreven dat beeld.

De deelnemers gaven aan dat ze hoopten om ideeën op te doen en geïnspireerd te raken door verrassende inzichten van anderen. Ook zochten de deelnemers verbinding met elkaar, zo zeiden ze.

Cyber-resilience

Aan de hand van stellingen startte de discussie. Dat begon met 'Er is te veel aandacht voor cybersecurity en te weinig voor cyber-resilience'. Met cyber-resilience (letterlijk: cyber-veerkracht of cyber-bestendigheid) wordt het vermogen van organisaties bedoeld om, ook als ze aangevallen worden, door te kunnen blijven gaan.

Veel deelnemers waren het met die stelling eens. "We zijn vooral bezig met het nemen van maatregelen. Normeringen zoals ISO 270001 zijn heel erg gericht op preventie", begon één van de deelnemers. "Dat is goed en dat moeten we ook blijven doen. Maar het duurt nog steeds erg lang voordat een data breach onderkend wordt. We zouden meer moeten doen aan monitoring. Alleen met preventie komen we er niet. Recente bekende voorbeelden van ransomware-aanvallen bij de Universiteit van Maastricht en het Hof van Twente laten zien dat je ook moet nadenken over goede response."

Volgens een andere deelnemer is het historisch gezien logisch dat cybersecurity meer aandacht krijgt dan cyber-resilience. "Tien jaar geleden geloofde geen enkel bedrijf dat het down zou gaan door een aanval, want dat gebeurde toen vrijwel nooit. Dus gingen de budgetten niet naar cyber-resilience. Het is nu tijd om dat te veranderen. Er is in het verleden genoeg over cybersecurity gepraat, zodat we het nu over cyber-resilience kunnen gaan hebben. Bedrijven moeten na gaan denken over wat ze doen als ze getroffen worden."

Iemand anders zei, later in het gesprek: “We zijn te veel bezig om achterdeuren te sluiten, terwijl we ervan uit moeten gaan dat er altijd wel een deur openstaat.” Weer iemand anders zei: “Je hebt eigenlijk maar twee groepen. Zij die gehackt zijn en zij die dat nog niet weten.” Cyber-resilience bestaat voor een deel uit het voorkomen dat je aangevallen wordt, inclusief awareness en risico management en daarnaast ervoor zorgen dat je snel op kan staan nadat je valt, zo vatte iemand samen.

Communicatie

Een deelnemer gaf aan hoe belangrijk communicatie is als het gaat om cyberbestendigheid. Intern bij bedrijven, maar ook naar buiten toe. “Vaak zie je dat de top van organisaties verkeerd communiceert, bijvoorbeeld met tegenstrijdigheden. Je moet, zeker als overheidsorganisatie, maatregelen nemen om ervoor te zorgen dat je de communicatie op het juiste moment en de juiste manier doet.”

Het juiste taalgebruik is belangrijk, ook intern, gaf iemand aan. “CISO’s en CIO’s willen zo intelligent mogelijk overkomen, maar veel CEO’s haken al af als het woord resilience valt. Je moet security kunnen vertalen naar een business enabler. Nu worden mensen op boardroom-niveau vaak bang als er een CISO binnenkomt.”

Security is vooral een businessvraagstuk en moet niet te veel in de hoek van de IT worden geduwd, werd tijdens de voorstelronde al door één van de deelnemers gezegd. Later in de bijeenkomst kwamen anderen daar op terug. “Cybersecurity wordt veel gelinkt aan IT. Cyber-resilience gaat veel verder, dat gaat echt om het gedrag en dus ook over de business.”

Zwakste schakel

Vaak wordt gezegd dat de mens de zwakste schakel is als het om security gaat. Daarover ging de volgende stelling. Vrijwel iedereen was het daarmee eens. “We hebben vaker te maken met knulligheid van partijen die getroffen worden, dan met hele goede inbrekers”, zei iemand.

Iemand anders nuanceerde dat beeld. Aanvallers zijn volgens deze persoon helemaal niet bezig met het bewust opzoeken van de mens als zwakste schakel. Die gebruiken gewoon alle aanwezige zwaktes, of die nu in de producten, de encryptie of op het menselijk vlak zitten. Volgens dezelfde persoon zijn security awareness-trainingen van personeel niet de oplossing. “Natuurlijk trappen bedrijven nog wel eens in een krom opgestelde mail die ze hadden moeten herkennen. Maar het beeld van de e-mail van een Nigeriaanse prins die gouden bergen beloofd is echt niet meer actueel. We zien al deep-fakes waarbij de stemmen van bestuursleden worden vervalst. Daar helpt een awareness-training niet tegen.”

Er is meer nodig, vonden ook de meeste andere deelnemers. Een cultuurverandering. Iemand gaf aan dat het belangrijk is dat kinderen van jongs af aan kennis krijgen over security-vraagstukken en mogelijke dreigingen. “Het begint met bewustwording. Ik voer daarover goede gesprekken met mijn kinderen. Waarom stelt een bedrijf privacy-voorwaarden van 20 pagina’s op voor een app? Blijkbaar hebben ze iets te verbergen. Hopelijk zorgt dat voor een basis voor de rest van hun leven.” Iemand wees op het bestaan van programma’s die kinderen op basisscholen spelenderwijs iets over dit thema leren.

Overheden en bedrijven moeten samenwerken om een cyberbestendig Nederland te creëren

Overheid

Vervolgens kwam de rol van de overheid aan bod. Hoe belangrijk is de samenwerking tussen overheden en bedrijven? Heel belangrijk, vond vrijwel iedereen. “Zonder samen te werken zullen we nooit een cyberbestendig Nederland creëren”, zei iemand. Een ander zei: “Elkaar helpen kan zeker. Dat moet het doel zijn, over je grenzen heen kijken om samen te zoeken naar waar je risico’s kunt beperken en de businesscontinuïteit kunt waarborgen.”

Toch gebeurt dat samenwerken nog veel te weinig, vonden de meeste deelnemers. “Daarin scoren we nog een onvoldoende.” Er werd gewezen op de obstakels die écht samenwerken bemoeilijken. Die zitten vooral in de regelgeving. “Nationaal is het al moeilijk, internationaal wordt het alleen maar ingewikkelder.” Een CIO van een overheidsinstelling zei: “Wij lopen tegen de aanbestedingen aan. Als ik écht wil samenwerken met bijvoorbeeld één van de hier aanwezige bedrijven, dan is er eerst een aanbestedingstraject van vele maanden nodig.”

Een ander benaderde de positieve kant. “Er zijn meerdere recente pareltjes waarbij dat samenwerken heel goed is gelukt. In de aanpak van kinderporno bijvoorbeeld. Er is door een bedrijf een toolkit ontwikkeld om dat beter op te kunnen sporen, met extreem goede resultaten. Toch gebeuren dat soort samenwerkingen nog veel te weinig. De overheden houden het bewust of onbewust nog tegen. Het is moeilijk om budget te krijgen en de regels, onder meer van aanbestedingen, zorgen inderdaad voor stroperigheid waardoor we geen stappen maken.”

Ministerie van digitalisering

Iemand gaf aan dat de overheid vaak niet efficient werkt. “Over bijvoorbeeld Artificial Intelligence zijn in Den Haag de laatste twee maanden drie verschillende kamerbrieven verstuurd, vanuit drie verschillende ministeries en naar drie verschillende commissies.” Zou een ministerie van ICT of van digitalisering daar een oplossing voor zijn? Die subvraag zorgde niet bij iedereen voor enthousiaste reacties. “Denk je dat alle neuzen met zo’n ministerie wel ineens dezelfde kant opstaan?”, zei iemand. “Alleen dat is niet voldoende.” Een ander legde dat uit: “Het is heel menselijk om weg te lopen voor verantwoordelijkheden. Als er een ministerie van digitalisering komt, dan zullen veel ministers snel en makkelijk daarnaartoe wijzen. Ik ben niet per se tegen zo’n ministerie, maar het is veel belangrijker dat er op hoog ambtelijk

niveau beter wordt samengewerkt rondom ICT dan nu het geval is. Als dat niet gebeurt, dan lost een minister niets op."

Er volgde een discussie over de positieve en minder positieve kanten van de AVG-regelgeving en de bijbehorende boetes. Daarover verschilden de meningen. Volgens sommigen is het een heel goede stok achter de deur voor bedrijven om beter na te denken over hoe ze met data omgaan. Bedrijven zijn beter naar hun privacy-voorwaarden gaan kijken. Volgens anderen zorgen die boetes er juist voor dat cybercriminelen bij bijvoorbeeld ransomware-aanvallen een betere onderhandelingspositie hebben.

Geen blame-cultuur

Gedurende de avond deden meerdere mensen een oproep om positiever te zijn. "Ik wil een bekende onderzoeker op dit gebied aanhalen", zei iemand. "Die zegt: 'Als we onze telefoon aanzetten zijn we in één klap verbonden met miljarden wereldburgers en tientallen miljarden apparaten. Als je het zo bekijkt, is het eigenlijk een wonder dat er maar zo weinig misgaat.'"

Bij de stelling over de mens als zwakste schakel ging het opnieuw over positiviteit. "Deze stelling is erg negatief", zei iemand. "In ons werkveld zijn we alleen maar bezig met bangmaken en framing. Mensen de maat nemen en wegzetten als dommeriken bij wie het mis is gegaan omdat ze 'Welkom 2020' als wachtwoord hadden gekozen, bijvoorbeeld. We moeten echt positiever zijn." De deelnemer kreeg bijval. "Door mensen belachelijk te maken bevorderen we dat er dingen onder het tapijt worden geschoven. Het is heel belangrijk dat we tolerant, begripvol en vergevingsgezind zijn."

Daar waren veel mensen het mee eens. Iemand trok de vergelijking met de luchtvaart. "Het is heel belangrijk dat er een cultuur is waar veiligheid in kan gedijen. Dat is zo in de luchtvaart. Onder andere omdat er geen blame-cultuur is, met openheid van zaken en het doel om te leren van fouten en daar de regulering op aan te passen. In de IT is die cultuur er nog niet en dat is volgens mij de heilige graal."

"Het is ook belangrijk dat we niet alleen maar over hel en verdoemenis praten om de aandacht te krijgen", zei iemand anders. Alleen maar een beroep doen op angst levert niet op, zoals dat ook het geval was toen virologen, naar nu blijkt terecht, waarschuwden voor een grote pandemie. "We moeten een andere taal gaan spreken. Ik weet niet precies welke, maar de taal van angst werkt niet. Niet bij de virologen en niet bij ons."

Blinde vlekken

Richting de volgende bijeenkomsten werd nog kort gesproken over de blinde vlekken, onderwerpen die de deelnemers nu hadden gemist en die de volgende keren op de agenda zouden moeten komen te staan. "Een belangrijke vraag die nu niet aan bod is gekomen is 'Hoe kun je informatie over aanvallen sneller en beter met elkaar delen, op een manier dat je niet meteen weet wie er slachtoffer is?'", gaf iemand aan. De olie- en gasindustrie kan daarin een voorbeeld zijn, zei een andere deelnemer.

De vraag of de overheid niet een veel grotere rol moet spelen op de digitale snelweg kan volgens een aantal deelnemers meer worden uitgediept. Educatie is volgens iemand anders ook een onderwerp dat meer aan bod moet komen. "Dat moet op de basisschool al beginnen." "Misschien moet je bekeerde cybercriminelen gaan benaderen om daar te spreken", opperde iemand.

Een deelnemer ziet de volgende keer graag wat extra focus op de eindgebruiker. Een andere suggestie was om met alle aanwezige experts een blik in de toekomst te werpen. Ook Europees of internationaal samenwerken kwam naar voren als een mogelijk toekomstig gespreksonderwerp.

Daarna werd de officiële discussie afgesloten. De deelnemers spraken over een zeer waardevolle avond, met nuttige nieuwe inzichten. Bij een volgende bijeenkomst van de Dutch IT Cybersecurity Assembly zal er onder meer worden gezocht naar praktische aanbevelingen en take aways, zo gaven de initiatiefnemers aan. De datum en locatie van die volgende bijeenkomst worden snel bekend.

De algemene take aways

- Er moet niet alleen over cybersecurity maar vooral ook over cyber-resilience worden gesproken.
- Zorg als bedrijf en overheid dat je intern en extern goed en consequent communiceert over aanvallen.
- Overheden en bedrijven moeten samenwerken om een cyberbestendig Nederland te creëren.
- De securitybranche moet leren om te praten over business-kansen in plaats van alleen over de gevaren.
- We moeten samenwerken aan een positieve cultuur waarin mensen toe durven te geven dat ze fouten hebben gemaakt, zodat iedereen ervan kan leren.

Founded by

Dutch IT Channel

Datto