Founded by
Dutch IT Channel
Datto

Derde bijeenkomst Dutch IT Cybersecurity Assembly

Baseline en basisvragen kunnen cyberbewustwording in het MKB vergroten

Derde bijeenkomst Dutch IT Cybersecurity Assembly

Baseline en basisvragen kunnen cyberbewustwording in het MKB vergroten

Na twee succesvolle bijeenkomsten in 2021, gold voor de derde bijeenkomst van de Dutch IT Cybersecurity Assembly een duidelijk doel: met concrete plannen komen. Met dat streven gingen 14 thought leaders op 17 februari met elkaar in gesprek, in Kasteel De Hooge Vuursche in Baarn. De deelnemers werken bij zeer uiteenlopende organisaties waaronder IT-leveranciers, brancheorganisaties, overheidsinstellingen, IT-partners en zakelijke eindgebruikers. Prima ingrediënten voor een discussie met diepgang, zo bleek.

Vaktitel Dutch IT-channel en securityleverancier Datto namen vorig jaar 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. Dat gebeurt door de verbinding met elkaar te zoeken, onder andere tussen overheden en commerciële bedrijven. Het centrale doel is om de cyber-resilience, ofwel de cyber-weerbaarheid, van de BV Nederland te verbeteren. Want cybercriminaliteit wordt een steeds groter gevaar. Voor grote bedrijven, zelfs voor landen, maar zeker ook voor MKB'ers.

Net als bij de eerste twee bijeenkomsten, werd het gesprek ook nu tijdens de voorstelronde al inhoudelijk. Onder leiding van moderator Danny Frietman schetsen de deelnemers de stand van zaken in het MKB zoals ze hem nu zien. "De cyberweerbaarheid in het MKB is in de hele wereld alarmerend laag", gaf iemand aan. Een andere deelnemer, werkzaam bij een MSP'er, merkt dat ook onder zijn MKB-klanten. "De bewustwording is heel laag. Een verhaal zoals de huidige hack van de olieterminals is voor een kleinere MKB'er een ver-van-zijn-bed-show. Zij willen met hun business bezig zijn."

Strengere regels vanuit de overheid?

Daarna barstte de echte discussie los. Daarbij ging het in eerste instantie over de concrete stappen die de overheid kan zetten om de cybersecurity-awareness te vergroten. Iemand opende met een duidelijke stellingname. "Als je de bewustwording bij ondernemers wilt laten groeien heb je twee middelen: een stok en een wortel. Een wortel heeft de overheid eigenlijk niet, vind ik. Dus is er een stok nodig: wettelijke verplichtingen en boetes. Bedrijven moeten

verantwoordelijk of aansprakelijk worden voor schade die ontstaat omdat zij hun zaakjes niet op orde hebben." De deelnemer bedoelde niet dat je ondernemers nog eens na moet trappen nadat ze getroffen zijn, maar wel dat ze gestraft moeten worden als ze voor problemen in een keten hebben gezorgd. "Maar je kunt ook denken aan certificeringen, zoals banken ook een banklicentie nodig hebben. Hogere eisen zijn broodnodig. Dat geldt ook voor het MKB. Het MKB is niet alleen de bakker om de hoek. In deze steeds meer digitale samenleving, is het mogelijk dat een cruciaal bedrijf plat komt te liggen omdat er ergens in de keten een bedrijf van zes personen zijn zaakjes op het gebied van cybersecurity niet op orde had. Je zult daar binnen het MKB onderscheid in moeten maken."

Een andere deelnemer was het daar niet helemaal mee eens. "Als je met regelgeving komt, dan zullen MKB'ers waarschijnlijk nét over het randje lopen om binnen de regels te vallen. Op papier hebben ze hun zaken dan voor elkaar, maar in de praktijk niet. Je moet MKB'ers meenemen met subsidies en begeleiding. Vaak is het nu zo dat deze bedrijven niet weten hoe groot de impact op de keten kan zijn. Het is niet een kwestie van 'niet willen'. Soms is de stok nodig, in sommige sectoren. Maar je moet vooral nadenken hoe je ondernemers in kunt laten zien dat ze hun business beter kunnen doen en hun rol in de keten beter in kunnen vullen als ze aandacht besteden aan cybersecurity."

Er was meer scepsis over strengere regelgeving. "Ik ben bang dat we dan de AVG-kant opgaan", zei iemand. "Er werd toen gesproken over boetes. Wij zijn daar als dienstverlener op ingesprongen, maar uiteindelijk is de handhaving er niet, waardoor iedereen de teugels laat vieren."

Iemand van een overheidsorganisatie zei: "Regulering vanuit de overheid is link. Als wij als overheid gaan vertellen waar je als bedrijf allemaal aan moet voldoen, geven we dan eigenlijk niet een soort garantie dat bedrijven vervolgens niet meer getroffen kunnen worden door ransomware? Als ze dan getroffen worden, klagen ze de overheid dan aan? Ondernemers willen ook echt geen certificering. Dat zijn wel de mensen die gaan stemmen, dus politiek gezien is dat lastig om er doorheen te krijgen." Iemand anders zei: "Hoe meer regulering, hoe groter het voordeel voor de cybercriminelen. Want zij hoeven zich niet aan regels te houden."

De overheid heeft op het gebied van regelgeving meer mogelijkheden. "De BHV'er is ook in het MKB verplicht geworden en dat heeft iedereen geaccepteerd. Misschien moeten we die kant op denken", opperde iemand. Die vergelijking leverde positieve reacties op. "De acceptatie daarvan was wel een lang en ingewikkeld proces", nuanceerde iemand. "Maar safety op de werkvloer, zoals het dragen van een helm in sommige branches, wordt ook steeds meer geaccepteerd." Het kan dus wel.

Andere mogelijkheden vanuit de overheid

Strengere regelgeving, subsidies en begeleiding werden al genoemd. Maar er is meer dat de overheid kan doen. “De overheid is de grootste opdrachtgever van Nederland”, gaf iemand aan. “Als alle verschillende overheden cybersecurity-eisen gaan stellen aan de producten of diensten die ze zelf inkopen, niet alleen IT-diensten maar ook bijvoorbeeld de bouw van een sluis, dan ben je al een heel eind op weg.” Daar moeten overheden dan wel toe verplicht worden, vulde iemand anders aan.

Er kwam ook een ander voorstel. “Tijdens de bouwcrisis, tien jaar geleden, is het BTW-tarief verlaagd. Waarom zou zo’n financiële prikkel niet kunnen werken voor het investeren in opleiding of mensen op het gebied van security. Met zo’n positieve prikkel kun je meer bereiken dan met wet- en regelgeving, denk ik.”

Iemand van een leverancier zei: “We horen vaak van onze partners dat MKB’ers wel willen investeren in antivirus-producten, maar dat ze er niet over nadenken hoe ze kunnen voorkomen dat hun bedrijf naar de knoppen gaat nadat ze getroffen worden. Daar moeten ze in investeren en dat gebeurt niet. Misschien moet de overheid dát wel subsidiëren tot een bepaald bedrag.”

“De overheid moet vooral faciliteren”, zei iemand. “Er bestaan in het private domein al veel goede initiatieven, zoals bijvoorbeeld de DIVD (Dutch Institute for Vulnerability Disclosure, red). De overheid moet zich daar niet actief mee bemoeien, maar wel de krenten in de pap eruit kiezen en daarin investeren.”

Iemand, die ooit voor de overheid werkte en nu voor een private organisatie, zei: “De dialoog is cruciaal. Daarnaast is het belangrijk dat de deuren open zijn, dat je bij de overheid binnen kunt stappen voor dit soort vragen. Ook moeten ze hun verantwoordelijkheid pakken. Maar als het nodig is, moet die verantwoordelijkheid ook teruggelegd kunnen worden op ondernemers.”

Een deelnemer, werkzaam bij een MSP'er met vooral MKB-klanten, vertelde dat er veel onwetendheid is bij eindgebruikers. "Je moet het simpeler voor ze maken. De overheid moet ze bereiken. Niet met simpele SIRE-reclames, maar door ze echt mee te nemen in het verhaal."

Juiste taal vanuit de sector

Bij het vertellen van dat verhaal ligt ook een taak voor de sector, gaf iemand aan. "We moeten het verhaal niet te veel vanuit het securityperspectief vertellen. Veel MKB'ers hebben geen affiniteit met digitalisering. IT huren ze in en daarmee denken ze alles te hebben afgekocht. Pas als je ze vertelt over het gemiddelde van 21 dagen downtime na een ransomware-aanval, dan snappen ze wat de gevolgen kunnen zijn. Dan spreek je hun taal. Als we als branche alleen maar vertellen over het belang van patchen of backup, dan gaat dat het ene oor in en het andere oor uit."

Daar waren anderen het mee eens. "Ondernemers denken vaak dat hun backup op orde is. Maar als je ze vraagt hoe snel ze up-and-running kunnen zijn na een ransomware-aanval, dan wordt het stil. Dat is de relevante vraag die je moet stellen. Dan raak je de ondernemer." Iemand anders zei: "Je moet met relevante voorbeelden komen vanuit specifieke sectoren."

"Het zou fijn zijn als wij daarbij kunnen putten uit informatie van de overheid", vulde een deelnemer, een MSP'er, aan. "We kunnen wel voorbeelden of onderzoeksresultaten noemen, maar wij hebben een commercieel belang. Het zou fijn zijn als de overheid onafhankelijke marktonderzoeken kan communiceren en daarmee ook de publiciteit zoekt. Dan krijgen we rugdekking."

Een deelnemer, werkzaam bij een overheidsinstelling, gaf aan dat bedrijven en ondernemers elkaar moeten helpen. "Als overheden staan we toch ver van ondernemers af, hoe hard we ook proberen om die afstand te verkleinen. Ondernemers luisteren naar andere ondernemers, niet naar de overheid. Het is zeker zo dat de overheid als opdrachtgever aandacht kan geven aan cybersecurity, maar dat geldt ook voor andere opdrachtgevers, in hun waardeketen."

Iemand kwam met een mening die later op de avond terug zou komen. "We hebben een verantwoordelijkheid als branche om bedrijven op een bepaald niveau te krijgen. Er moet een baseline komen met wat er minimaal geregeld moet zijn."

Iemand van een grote eindgebruiker die veel in contact staat met MKB-bedrijven wilde het opnemen voor ondernemers. "Ondernemers van getroffen bedrijven hebben in de meeste gevallen echt wel maatregelen genomen. Alleen niet genoeg. Het is supermoeilijk voor ze. Wanneer moet je een CISO nemen? Wanneer heb je genoeg maatregelen getroffen? Bovendien is het heel moeilijk om aan goede mensen te komen. Er zijn op het gebied van cybersecurity heel veel openstaande vacatures."

Informatie delen door de overheid en door bedrijven

De overheid moet meer informatie delen, vond iemand. “De overheid monitort onze infrastructuur. Die infrastructuur is in Nederland heel goed en dus hebben ze veel informatie. Voor een paar belangrijke bedrijven, zoals de nucleaire kernreactor in Petten, delen ze die informatie. Maar in veel andere gevallen gebeurt dat niet. Daar is een inhaalslag te maken.” Hij noemde voorbeelden van aanvallen waar de overheid al vroegtijdig van op de hoogte was, maar waarvan het die informatie niet mocht delen.

Iemand die werkzaam is bij een overheidsinstelling was het daarmee eens, maar gaf wel aan dat dat qua wetgeving lastig is. “Daar zijn al veel stappen in gezet, en nee, we zijn er nog lang niet. Dat we niet alles mogen delen vanwege bijvoorbeeld de AVG is ook logisch. Die wetten zijn er niet voor niets, daar beschermen we mensen mee. Niemand wil een te machtige overheid.”

De overheid geeft nu vaak algemene informatie over datalekken. “Maar die informatie kan nog wel een stuk dieper gaan dan nu gebeurt, zonder op het punt te komen dat je kunt herleiden om welk bedrijf het gaat. Daar is ook nog veel te winnen”, gaf een deelnemer aan.

Niet alleen de overheid maar ook bedrijven moeten meer informatie delen, legde iemand op tafel. “Bedrijven leren ervan als ze zelf gehackt worden, maar ook als hun buurman het slachtoffer is. Zou je het niet moeten verplichten om openheid van zaken te geven als het misgaat?”

“Die informatie delen is cruciaal”, stemde iemand in. “Een ondernemer die onlangs getroffen was, vertelde daarover via een openbaar medium en daar kwamen heel veel reacties van andere ondernemers op. Nu weten ze waar ze op moeten letten. Dat zou veel meer moeten gebeuren.”

Doorbreken van het taboe

Waarom gebeurt dat dan nog maar zelden? Het antwoord ligt voor de hand: een combinatie van schaamte en angst voor reputatieschade. Iemand zei: “Een van de grootste problemen is dat er een taboe rust op het zijn van slachtoffer. Er wordt gedacht dat het jouw fout is, dat je iets doms hebt gedaan. Er is schaamte. Maar niemand kan alles voorkomen.”

“Als slachtoffers beter geholpen worden door overheden of door andere bedrijven bij het heropbouwen van hun netwerk, dan zullen ze er makkelijker over communiceren en ook minder snel bereid zijn om te betalen na een ransomware-aanval”, zo zei een deelnemer.

“Toen de gemeente Hof van Twente werd afgeperst, had iedereen het verwijt dat ze een te makkelijk wachtwoord, Welkom2020, hadden gekozen.” Maar victim-blaming is nooit de oplossing. “Hof van Twente was slachtoffer en moet zo behandeld worden. Als bedrijven niet eerlijk zijn geweest, verdienen ze reputatieschade, maar als ze slachtoffer zijn, zijn ze slachtoffer.”

“Het is moeilijk om ondernemers in het openbaar te laten vertellen over lekken en aanvallen”, voegde iemand toe. “Niet alleen vanwege schaamte, maar ook omdat ze gewoon bang zijn voor hun reputatie als naar buiten komt dat klanten zijn benaderd als gevolg van hun lek.”

Een van de grootste problemen is dat er een taboe rust op het zijn van slachtoffer.

Rol brancheorganisaties, trusted advisors en het Digital Trust Center

"Het zou helpen als de partijen waar MKB-bedrijven in vertrouwen, zoals banken, accountants, verzekeraars en IT-dienstverleners, hun rol pakken en het gesprek aangaan over bijvoorbeeld de gevolgen van downtime. Daar is veel meer uit te halen dan nu gebeurt", vond een deelnemer. "Misschien moet je je met een campagne op MKB'ers richten en hen daarin uitleggen welke drie of vier vragen ze aan die 'trusted advisor' moeten stellen over cybersecurity", gaf iemand anders aan.

Een deelnemer ging daarop door. "Een goede accountant neemt in de jaarrekening ook een risicoparagraaf op. Daar horen ook cybersecurityrisico's bij. Jammer genoeg gebeurt dat nog niet zo vaak, omdat ze er vaak weinig verstand van hebben."

Het Digital Trust Center (DTC), dat in het najaar van 2021 werd opgericht door het ministerie van Economische Zaken en Klimaat (EZK), kan een grote rol spelen bij het helpen van ondernemers, zo gaven meerdere deelnemers aan. Het DTC heeft als doel om individuele bedrijven proactief te informeren over digitale dreigingen. Maar het initiatief is bij veel bedrijven nog onbekend, zo concludeerden meerdere mensen ook.

"Het DTC zou als overheidsorganisatie het gesprek aan moeten gaan met brancheorganisaties. Want behalve de accountant of de IT-dienstverlener is ook een brancheorganisatie een partner waarop bedrijven vertrouwen", gaf iemand aan.

Volgende stap

Wat zou op dit moment een goede volgende stap zijn en wie moet die zetten? Iemand vatte een aantal eerdere conclusies samen en voegde er nog een paar aan toe. "De brancheorganisaties moeten scherp krijgen waar de grenzen van de verantwoordelijkheid van hun afnemers liggen. Accountants moeten zorgen dat het risicomanagement op orde is. Inlichtingendiensten moeten de dadernetwerken in kaart brengen en aanpakken. De overheid kan het hele stelsel dragen. Al die aspecten doen ertoe, al die stakeholders zijn belangrijk. Er is niet één maatregel om alles te regelen. De eerste stap is dus het organiseren van de stakeholders. Je moet dat publiek-privaat aanpakken."

Het creëren van awareness is de sleutel tot succes, daar was iedereen het over eens. "Dat is een gedeelde verantwoordelijkheid van de overheid en van bedrijven. Dat gaat verder dan alleen een awareness-training. Het moet onderdeel van de bedrijfsvoering worden, maar bij de bakker op de hoek is dat een uitdaging. Onderwijs is daarin een heel belangrijk aspect, daar begint het. Daar zitten de slachtoffers én de daders van morgen. Awareness moet door de hele samenleving heen lopen."

Organisaties en initiatieven op dit gebied komen als paddenstoelen uit de grond. "Daar is misschien sprake van wildgroei, maar die moet je nu niet de nek om draaien", zei iemand. "Beter wat overlap dan dat er gaten zijn."

Na een eerdere suggestie stelde iemand voor om met de Dutch IT Cybersecurity Assembly een baseline op te stellen, of een aantal vragen die elke ondernemer kan stellen aan zijn IT-dienstverlener of een andere 'trusted advisor'. De vijf basisprincipes van het Digital Trust Center (DTC) zijn daar mogelijk al heel geschikt voor, zo werd aangegeven. "Daarbij zijn brancheorganisaties, zelfs de allerkleinsten, een zeer geschikt doorgeefluik", benadrukte iemand, helemaal aan het eind van de avond.

Hans ten Hove, directeur Northern Europe van mede-initiatiefnemer Datto, was blij met de avond. "Het was een vruchtbare discussie. Het is een heel breed onderwerp, maar we hebben het terug kunnen brengen naar concrete plannen die kunnen dienen als start, zoals die vier vragen. Het gaat erom dat we een boodschap bij ondernemers krijgen en nu moeten we kijken wie daar het beste toegang tot hebben. Dat moeten we met zijn allen doen."

Na die conclusie werd er, met een kop koffie in de hand, nog een tijd nagepraat.

Belangrijkste conclusies

- Awareness creëren bij ondernemers is cruciaal.
- Brancheorganisaties, IT-dienstverleners en andere trusted advisors zoals accountants zijn allemaal belangrijk om de ondernemer te bereiken.
- Er moet een 'baseline' komen, of een aantal basisvragen of basisprincipes waarmee elke ondernemer zijn security-status kan toetsen.
- Aangevallen bedrijven moeten als slachtoffer worden gezien in plaats van als mede-schuldige, zodat de schaamte verdwijnt om daarover te spreken.


EVENT
WWW.EVENTCOMPANY.NL

Founded by

Dutch IT Channel

Datto