Founded by
Dutch IT Channel
Datto

Tweede bijeenkomst Dutch IT Cybersecurity Assembly

Het MKB heeft, als het om security gaat, een stok en een wortel nodig

Tweede bijeenkomst Dutch IT Cybersecurity Assembly

Het MKB heeft, als het om security gaat, een stok en een wortel nodig

Na een succesvolle eerste bijeenkomst in Almere, begin juni, vond de tweede bijeenkomst van de Dutch IT Cybersecurity Assembly op 23 september in Bodegraven plaats. Met grotendeels nieuwe gezichten, want het doel om de cyber-resilience in Nederland te verhogen moet zo breed mogelijk gedragen worden. De twaalf aanwezige thought leaders vanuit IT-bedrijven, overheden, onderzoeksplatformen en brancheorganisaties, gingen het gesprek aan en deelden kennis. De focus lag dit keer op de positie van het MKB.

Vaktitel Dutch IT-channel en securityleverancier Datto namen eerder dit 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. 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. De gedachte dat er bij kleinere bedrijven niets te halen valt voor cybercriminelen is een van de grootste misverstanden rondom security. Maar die denkwijze zorgt er wel mede voor dat veel MKB'ers zich nog niet goed beschermen. 'Hoe zorgen we voor meer cyber-resilience in het MKB', was dan ook de centrale vraag van deze avond.

Positie van het MKB

Tijdens de voorstelronde, waarin moderator Danny Frietman de deelnemers ook vroeg wat ze die avond wilden halen en brengen, bleek al snel dat de keuze voor het thema een goede was. "Ik merk dat veel MKB-bedrijven het op dit vlak moeilijk hebben", zei de eerste deelnemer die zich voorstelde. "Het is heel moeilijk om dit onderwerp daar binnen te krijgen. Er moet aandacht voor komen, want het MKB is wel de plek waar innovatie ontstaat."

"Het MKB houdt zich bezig met wat hun grootste prioriteit heeft", zei een IT-diensterlener. "In de eerste plaats hun business en hun klanten, maar ook alles wat met financiën en administratie te maken heeft. We krijgen security niet op de agenda. Ze voelen de urgentie niet. Ze moeten op de één of andere manier beloond worden. Alleen een foldertje over het belang van security gaat het verschil niet maken."

Een andere dienstverlener haakte daar op in met een metafoor. “Als IT-bedrijven bieden we auto’s aan waarin qua veiligheid alles geregeld is: gordels, ABS, goede sloten. Maar het lukt ons niet om de mensen aan wie we de auto’s verkopen uit te leggen dat ze die gordels moeten gebruiken en dat ze hun auto op slot moeten zetten.”

Er is behoefte aan actie, zo werd ook duidelijk. “Het is belangrijk dat er ideeën komen die voorbij de fase van ‘plan’ gaan en die echt praktisch en concreet worden gemaakt. Veel plannen lijken daarnaast interessant, maar gaan bij nader inzien toch gepaard met veel nadelen”, schetste iemand.

“Als het om cybersecurity en cyberweerbaarheid gaat zie je dat Nederland een gefragmenteerd land is”, zei een andere deelnemer. “Als we het MKB echt cyber-weerbaarder willen maken, is er verbinding nodig.”

Keurmerk

Na de uitgebreide voorstelronde, waarin de thematiek, de uitdagingen en de urgentie werden geschetst en deelnemers soms al stelling innamen, begon de echte discussie. Er werd in eerste instantie gebrainstormd over een mogelijk verplicht keurmerk voor MKB-bedrijven waarmee ze aan kunnen tonen cyberveilig te zijn. “Dat geeft schijnveiligheid”, was de eerste reactie. “En wat is het signaal dat je afgeeft wanneer je als overheid dat soort keurmerken uitdeelt en bedrijven vervolgens toch getroffen worden?”

Daartegenover stonden ook positievere reacties. “Er bestaan natuurlijk al diverse normeringen die met security te maken hebben, zoals ISO 27001”, zo gaf iemand aan. “Zo’n keurmerk blijft altijd een momentopname, maar dat is niet anders wanneer je bij het afsluiten van een verzekering aan moet tonen aan bepaalde normen te voldoen. Het is belangrijk dat je bedrijven blijft monitoren om te kunnen controleren of ze hun niveau blijven houden.”

Ketenveiligheid

Een keurmerk kan een goed idee zijn, vonden veel deelnemers, vooral vanwege het belang van ketenveiligheid. “Als er één bedrijf omvalt, kan er een domino-effect ontstaan”, verduidelijkte iemand. “Daar kan de overheid een rol in spelen met wetgeving en een keurmerk. Net zoals je met het behalen van een rijbewijs laat zien dat je om kan gaan met wat er op een snelweg gebeurt, toon je met zo’n keurmerk aan dat je de spelregels van de digitale snelweg kent.”

Op Europees niveau zijn er initiatieven in de maak om de ketenveiligheid bij online activiteiten te vergroten, legde iemand uit. “Maar het moet wel haalbaar, laagdrempelig en betekenisvol zijn.” Ook in Nederland wordt er in samenwerking met een aantal grote bedrijven gewerkt aan dit soort certificaten, voegde iemand toe.

Om de ketenveiligheid te verbeteren moet er meer transparantie zijn, benadrukte een deelnemer. “Bijna iedere partij organiseert IT-veiligheid nu voor zichzelf en vaak zijn bedrijven daarin niet transparant. Zolang je binnen de keten niet van elkaar weet waar iemands zorgplicht begint en eindigt, is de verantwoordelijkheid niet goed georganiseerd. Je moet dat samen oppakken.”

Securityverzekering

Pratend over de rol die de overheid moet spelen, kwam al snel een ander plan op tafel. “Ik denk dat de overheid MKB-ondernemingen moet verplichten om een securityverzekering af te nemen. Zo’n verzekering moet dan een audit bevatten, die afgevinkt wordt. Dat is meer haalbaar en realistisch dan een keurmerk of certificaat en zo krijgt iedereen, ook aan de onderkant, een bepaald niveau”, motiveerde iemand.

Een deelnemer tekende aan dat dat soort verzekeringen en de bijbehorende audits sterk van elkaar zullen verschillen. Maar er was ook bijval voor het plan. “Verzekeraars willen weten welk risico ze dragen, dus hebben ze belang bij een goede audit. Zo gaat het nu op financieel gebied ook.”

“Ik zou het omdraaien”, zei iemand. “Eerst verplichte wetgeving, met bepaalde eisen, zoals we ook ARBO-eisen hebben om de gezondheid van werknemers te waarborgen. Het voldoen aan dat soort eisen op het gebied van cyber-resilience moet je niet bij verzekeraars neerleggen, dat moet een basishygiëne zijn.”

Jaarverslag

In het verlengde hiervan noemde iemand het idee van een digitaal jaarverslag. “Het zou verplicht moeten worden om ‘cyber’ in je jaarverslag op te nemen. Dus een verklaring, naast de bestaande financiële verklaring, die over IT-regie gaat. Dat kan het verschil gaan maken en de hefboom zijn waar we op zitten te wachten.” Over dat voorstel, waarbij de controle op cyber-resilience deels in handen wordt gelegd van accountants, werd nog een tijdje verder gepraat. Er waren andere voorstanders. Maar iemand zei ook: “Het is heel moeilijk om dan

vast te stellen waar je aan moet voldoen. Er is standaardisatie nodig." Een ander wees er later tijdens de bijeenkomst op dat veel MKB'ers met een boekhouder werken en niet met een accountancykantoor dat zoiets uit kan voeren.

Iemand zei ook: "De overheid moet stoppen met het ontwikkelen van allerlei verschillende normenkaders, wat nu overal in Europa steeds gebeurt. Die zijn er al genoeg. De overheid moet op een hoger abstractieniveau gaan zitten en verplichten dat er verantwoordingsrapportages komen, waarin je als bedrijf motiveert welk stelsel je hebt gekozen." Iemand viel deze deelnemer bij. "Daarmee maak je bestuurders verplicht om ermee bezig te gaan, omdat anders de toezichthouders op de deur kloppen, die dan zelf ook aansprakelijk zijn. Als je dat via de jaarrekening laat lopen, heb je geen extra toezichthouders nodig, maar valt het binnen het bestaande wettelijke kader."

Bewustwording in het MKB

Iemand was van mening dat het probleem op een andere manier aangevlogen moet worden. "Cybersecurity wordt in het MKB vaak nog gezien als een vervelende kostenpost. Niet iedereen is ervan doordrongen dat het niet hebben van cybersecurity meer kosten met zich meebrengt. Daar begint het bij. Mensen vragen toch ook niet om een auto zonder remmen, om kosten te besparen?"

Er werd door iemand anders een onderzoek aangehaald, om te benadrukken dat MKB'ers de urgentie van cybersecurity vaak niet inzien. "Van de managed service providers maakt 80 procent zich zorgen over cybersecurity, van de MKB'ers maar 20 procent. Ze denken, ten onrechte, dat ze niet interessant zijn voor cybercriminelen."

"MKB'ers zijn er gewoon helemaal niet mee bezig. Ze steken hun kop in het zand", zei iemand. Maar dat kun je ze niet kwalijk nemen, werd er ook gezegd. "De ondernemer is bezig met bijvoorbeeld kaas verkopen. Daar is ie goed in." Een ander was het daar niet mee eens. "Een ondernemer sluit ook onder andere een aansprakelijkheidsverzekering en een verzekering op het pand af. Dat vinden we heel normaal. Cybersecurity niet." Later in het gesprek opperde iemand dat er Postbus-51-spotjes zouden moeten komen om ondernemers meer inzicht te geven in mogelijke gevolgen.

Security is vaak ook te complex voor MKB'ers, zei iemand. "Zelfs ik haak op een gegeven moment bijna af door bijvoorbeeld alle verschillende lagen van mijn IT die ik moet back-uppen. De genoemde kaasboer is de draad dan al lang kwijt. Maar dat geldt ook voor het bedrijf in de maakindustrie met 500 medewerkers."

Rol van brancheorganisaties

Brancheorganisaties in allerlei verschillende sectoren zouden een rol kunnen spelen bij het geven van ondersteuning aan hun achterban en het creëren van bewustwording, gaven meerdere deelnemers aan. Een deel ervan pakt die rol te weinig, anderen hebben die potentie wel. "Als brancheverenigingen is voorlichting heel belangrijk. Je moet MKB'ers de goede kant op sturen. Ze zitten te wachten op concrete voorbeelden en hebben daar begeleiding bij nodig."

Iemand noemde de BOVAG als voorbeeld, die een pilot draait waarbij aangesloten bedrijven verplicht aan een bepaalde cyber-standaard moeten voldoen. "Alles draait om de vraag waar we de verantwoordelijkheid neerleggen. Bij de overheid? Bij de branche? Bij de ondernemer? Of ergens ertussenin?" Wat het ook wordt, er is eenduidigheid nodig, zo vond deze deelnemer. "Iedereen moet het snappen en zich eraan conformeren."

Cybersecurity wordt in het MKB vaak nog gezien als een vervelende kostenpost

Cyberscan

Het uitvoeren of uit laten voeren van bestaande cybersecurityscans is voor veel bedrijven in het MKB nog te duur. Werken met een soort vouchersysteem vanuit het ministerie van EZK, die het betaalbaar maakt om zo'n scan uit te voeren, zou volgens iemand een oplossing kunnen zijn. Een andere deelnemer gaf aan dat er bij een vergelijkbaar initiatief in het verleden, weinig vraag was naar de vouchers. Maar dergelijke vouchers kunnen de drempel wel verlagen tijdens gesprekken die dienstverleners met hun klanten voeren, zo werd ook gezegd.

Er werd gewezen op de basisscan van het Digital Trust Center die ondernemers zelf uit kunnen voeren, als een beginpunt van securitybeleid, en de vijf basisprincipes van digitaal ondernemen die dezelfde instantie ook opstelde. Eén van de aanwezige dienstverleners voert ook scans uit en wees op de complexiteit daarvan. Weer iemand anders deelde de ervaring dat securityrapporten regelmatig onderin een la belanden. "Na een scan vragen we de bedrijven of wij de security voor ze moeten doen, of dat ze het zelf willen doen. Vanwege de kosten doen ze het vaak liever zelf. Als je na een paar maanden opbelt om te vragen hoe het gaat, blijkt vaak dat ze niets met de scan hebben gedaan."

Er werd door iemand op gewezen dat zeker de wat meer oppervlakkige securityscans bij lange na geen garantie bieden op volledige bescherming. Maar er waren ook veel positieve geluiden. "Als IT-service providers samen een goede scan opstellen die ervoor zorgt dat de basis op orde is, dan kun je een groot deel van de problemen aan de onderkant van het MKB al oplossen. Bij grotere bedrijven moet je meer doen en echt dingen afdwingen. De overheid moet zijn rol pakken en zijn nek uitsteken. In combinatie met brancheverenigingen, het Digital Trust Center en andere initiatieven heb je al een mooie structuur staan."

In die structuur zou de Dutch IT Cybersecurity Assembly zelf ook een rol kunnen spelen, vooral op het gebied van securityscans, zo zei iemand. "We kunnen dit morgen al organiseren. Als je een flink aantal brancheverenigingen plus IT-dienstverleners en -leveranciers bij elkaar pakt, heb je de body om wat te kunnen betekenen. Geen duizenden verschillende scans meer, maar één scan die door een bredere groep gedragen wordt. Die scan hoeft niet perfect te zijn, dat is een APK-keuring ook niet."

Verbod op losgeldbetalingen

Korte tijd ging het erover of de overheid het bedrijven moet verbieden om cybercriminelen te betalen na een ransomware-aanval, of verzekeraars moet verbieden om die bedragen uit te keren. Daarmee zou je de noodzaak van bescherming verhogen en het verdienmodel van de aanvallers onderuit halen. De Nederlandse overheid onderzoekt momenteel die mogelijkheden. Maar weinig deelnemers waren het met die plannen eens. "Dat is ethisch onverantwoord", was iemand stellig. "Dan zeg je eigenlijk tegen een ondernemer dat hij zichzelf op moet offeren voor het grotere belang. Dat kun je niet maken."

"Een bedrijf dat wordt getroffen door ransomware kan alle voorzorgsmaatregelen hebben genomen en gewoon het slachtoffer zijn van domme pech. Die voorbeelden zijn er genoeg", voegde iemand toe. "Dan kun je het echt niet maken om ondernemers te verbieden te betalen. Dat is draconisch en ook niet haalbaar."

Wortel en stok

"Je hebt bij dit soort onderwerpen altijd een wortel en een stok nodig", vatte iemand aan het einde van de avond samen. "De stok bestaat uit mogelijke wettelijke verplichtingen. Een andere stok is de angst om getroffen te worden, maar de praktijk leert dat veel bedrijven dat gevaar niet voelen. Een beetje zoals bij de opwarming van de aarde. De wortel, de incentive, is er bijna niet. Security goed uitvoeren kost alleen maar meer geld."

"We moeten versnellen", gaf iemand als noodkreet aan, daarmee wijzend naar de overheid. "De overheid moet dingen afdwingen, bepaalde basiselementen die gewoon verplicht zouden moeten zijn. Backups maken en security als onderdeel van de jaarrekening, bijvoorbeeld. Die elementen worden dan een soort security APK. Natuurlijk is dat soms vervelend voor ondernemers en hebben ze daar hulp bij nodig. Maar dat geldt ook voor financiën. Als het moet, dan moet het. Met voorlichting en ondersteuning komen ze daar echt wel uit."

Andere plannen

Tijdens de avond kwamen ook nog een aantal andere plannen kort langs.

- De overheid die als klant meer securityeisen stelt, bij aanbestedingen met name. "Je zou er bij hen niet meer in moeten kunnen komen, als je je security niet op orde hebt", werd er gezegd.
- Incident response als basiselement van de cyber-hygiëne. Onderdeel daarvan zou kunnen zijn dat bedrijven de verplichting hebben om aangifte te doen. "Nu gebeurt dat vaak niet omdat het idee bestaat dat de politie er niets mee doet en het jezelf veel extra tijd kost", vertelde iemand.
- Een verplichting op two factor authentication. Een deelnemer: "Als je dat toepast, wordt de kans om getroffen te worden gewoon een heel stuk kleiner."
- Een focus op het creëren van businesscases rond cybersecurity voor MKB-bedrijven. "Zodat security hen uiteindelijk geld oplevert", zei iemand.

Afsluiting

De deelnemers sloten met een voldaan gevoel de bijeenkomst af, zo gaven ze stuk voor stuk aan. “Ik heb veel interessante mensen ontmoet en zie potentiële samenwerkingen”, zei iemand. “Ik popel om hiermee samen aan de slag te gaan”, gaf een ander aan. Iemand zei ook: “Er was veel energie. Heerlijk dat dit weer in fysieke vorm kan.”

“Het blijft een uitdaging om het concreet te maken, maar dit is een goed begin”, vond een deelnemer. Weer iemand anders zei: “De gereedschapskist voor oplossingen is al best wel goed gevuld. Veel dingen zijn er al. We moeten nu de puzzelstukjes samenvoegen.”

De moeilijke rol van de overheid kwam aan bod. “Van de ene kant vragen we de overheid om actie en concrete hulp. Certificeringen en wetgeving, dus. Maar bij de uitvoering kom je bezwaren tegen. Ondernemers willen geen extra regelgeving. Dat blijft een lastige balans.”

De rol van brancheverenigingen bij het ondersteunen en aanjagen van hun achterban werd tijdens de afsluiting ook nog een keer aangehaald.

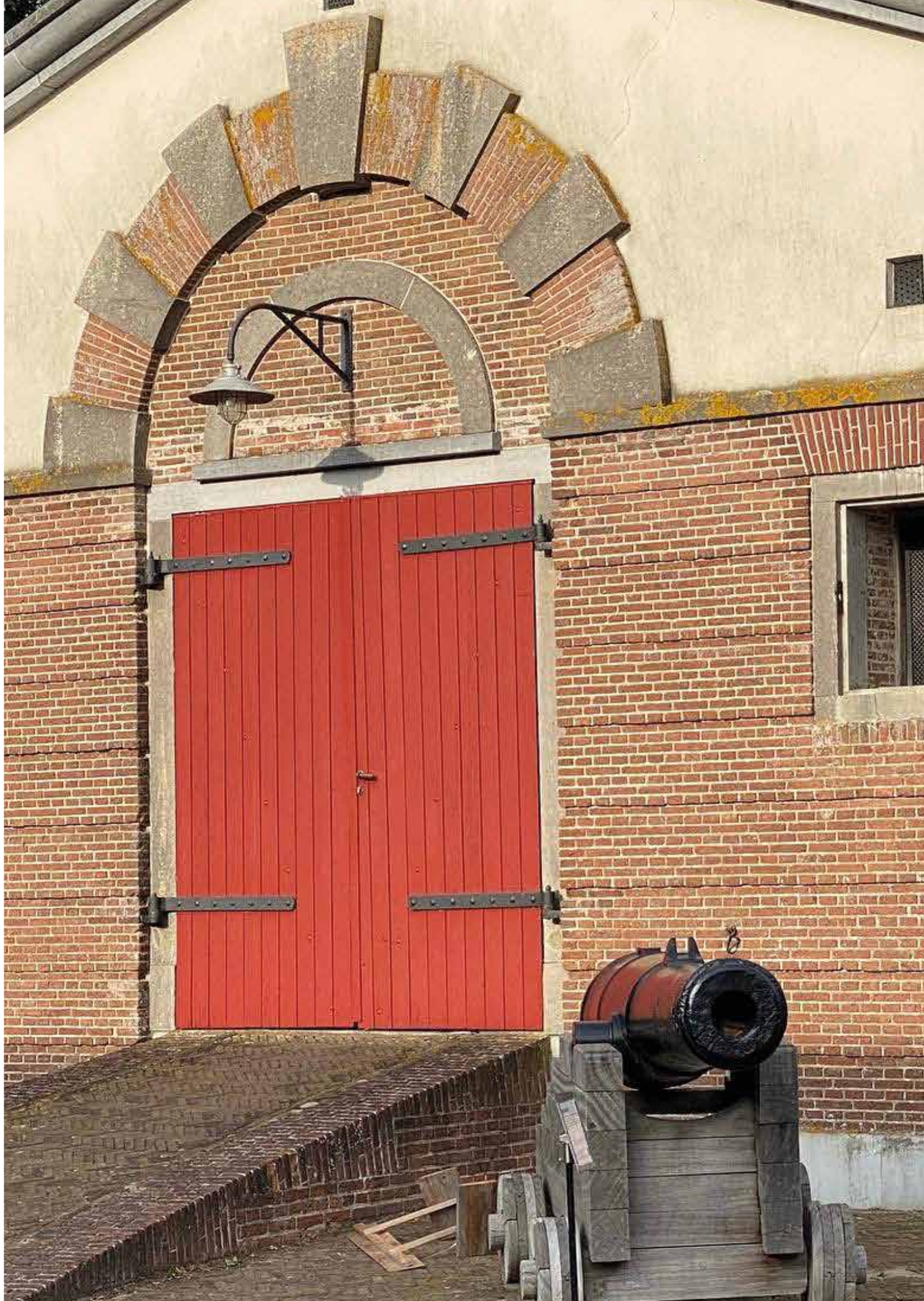
Namens initiatiefnemer Dutch IT-channel zei Witold Kepinski als afsluiting: “Er is veel bereidheid om het MKB in Nederland cyber-secure en cyber-resilient te maken. Maar er is ook een stok achter de deur nodig en daar moet de overheid voor zorgen. Er is behoefte aan een beter systeem, ook in de hulpverlening voor ondernemers die getroffen zijn. Deze twee en een half uur waren eigenlijk te kort en smaken zeker naar meer voor nieuwe bijeenkomsten, die er absoluut gaan komen.”

Ariën van Wetten gaf namens Datto, de andere initiatiefnemer, aan: “Ik merk dat er veel bereidheid is, maar ook veel onbekendheid met de mogelijkheden. Er zijn deze avond relaties gebouwd om bijvoorbeeld de scans beter te maken. Ons doel met deze Assembly is om organisaties en instanties met hetzelfde doel samen te brengen, en dat is hier goed gelukt. Maar er is zeker ook een vervolg nodig. Rome werd ook niet in één dag gebouwd.”

Belangrijkste conclusies

De belangrijkste conclusies van de avond:

- De basisscan van het Digital Trust Center biedt enorme kansen voor MKB-bedrijven
- Een security-paspoort voor het MKB kan de adoptie versnellen
- Brancheorganisaties vervullen op het gebied van cyberweerbaarheid een sleutelrol als het gaat om kennisdeling en het mobiliseren van de achterban
- De Dutch IT Cybersecurity Assembly moet zich richten op kennisdeling en het verbinden van publieke en private partners



Founded by

Dutch IT Channel

Datto