Founded by
Dutch IT Channel
Datto

Vijfde bijeenkomst Dutch IT Cybersecurity Assembly

Dutch IT Cybersecurity Assembly wil leiding nemen bij samenstellen baseline

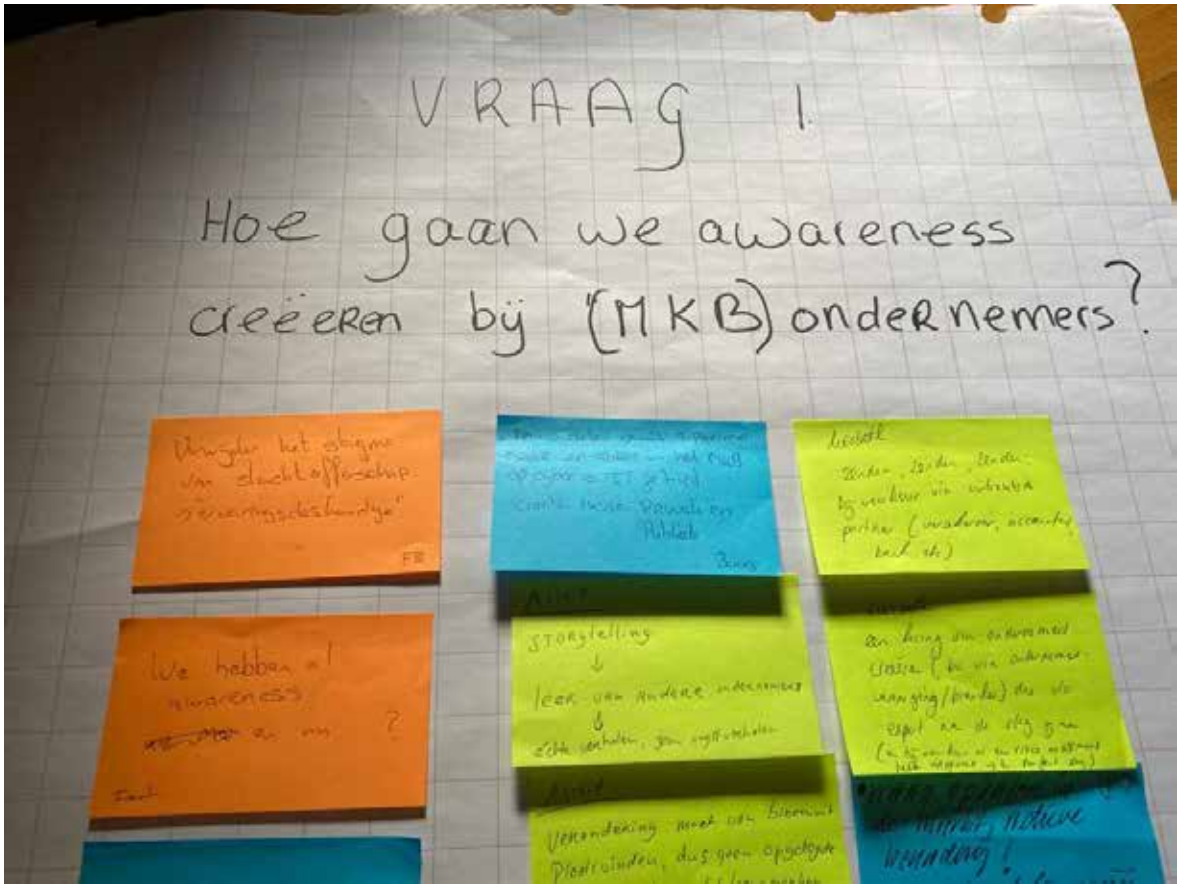
Vijfde bijeenkomst Dutch IT Cybersecurity Assembly

Dutch IT Cybersecurity Assembly wil leiding nemen bij samenstellen baseline

“We moeten vanavond aan de slag”, waren de enigszins streng klinkende openingswoorden van moderator Danny Frietman bij de vijfde bijeenkomst van de Dutch IT Cybersecurity Assembly. Hij bedoelde het uiteraard positief. De bijeenkomst op 15 juni, bij De Landgoederij in Bunnink, werd ingestoken als een verdiepende werksessie en dat werd het ook. De 14 deelnemers, allerlei verschillende stakeholders op het gebied van IT en cyberveiligheid, gaven voorzetten richting concrete acties.

Vaktitel Dutch IT Channel en securityleverancier Datto namen in 2021 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 rondom cybersecurity in Nederland. Dat gebeurt door de verbinding met elkaar te zoeken, onder andere tussen overheden, commerciële bedrijven en brancheorganisaties. 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 en het bewustzijn op dat gebied is nog laag.

De avond begon met een snelle voorstelronde en draaide vervolgens om vier centrale vragen. In tegenstelling tot bij de eerste bijeenkomsten, werd er niet vanaf nul gediscussieerd, maar vroeg moderator Danny Frietman de deelnemers om allereerst hun gedachtes over de vraag op een post-it te zetten. Dat diende steeds als startpunt voor een verder gesprek. Het leverde diepere inzichten en leuke onderlinge discussies op, maar vooral ook meer concrete voorstellen.



Vraag 1: **Hoe creëren we awareness rondom het thema cybersecurity bij MKB-ondernemers?**

Alles begint met bewustwording en vooral in het MKB is dat nog altijd een uitdaging. Die conclusie was op eerdere bijeenkomsten van de Dutch IT Cybersecurity Assembly al getrokken. Het was dan ook een logisch vertrekpunt om eerst te praten over concrete maatregelen om die awareness te vergroten.

De avond begon meteen met een gezond verschil van inzicht. De eerste deelnemer vertelde wat hij op zijn post-it had gezet: 'We hebben al awareness. En nu?'. "Zijn er namelijk nog ondernemers die denken dat ze geen risico lopen?" Daar werd door anderen op ingehaakt. "Ja, die zijn er. De meerderheid zelfs. Naarmate bedrijven groter worden, zijn ze meer met risk management bezig, maar de lokale autodealer of makelaar is dat nog niet."

De aanwezige kennis bij bijvoorbeeld de Dutch IT Cybersecurity Assembly moet worden omgezet richting het MKB met behulp van enablers, gaf iemand aan. "Om MKB'ers meer bewust te maken van de risico's, helpt het als er scans en procedures komen. Daarvoor zijn samenwerkingen nodig, bijvoorbeeld met banken, die dat kunnen koppelen aan het kredietproces. Daar kun je samen een product of dienst van maken."

Iemand anders had 'zenden, zenden, zenden!' opgeschreven. "Je moet de boodschap blijven herhalen via vertrouwenspartners zoals een verzekeraar, accountant of IT-partner. Daarnaast

is het belangrijk dat er kringen van ondernemers komen die in gezamenlijkheid cybersecurity aanpakken." Iemand haakte in op dat eerste deel. "Je moet het inderdaad overal tegenkomen, het moet niet meer iets bijzonders zijn. Cybersecurity moet worden geïntegreerd in het dagelijkse bedrijfsleven. Daarnaast moeten we zorgen dat het steeds meer standaard onderdeel wordt van producten en dienstverlening." Iemand gaf als tip mee om consultatierondes te doen en ervaringen uit te vragen. "Dan kun je ook de overheid erbij betrekken en komen tot een triple-helix-aanpak."

Een volgende deelnemer had een aantal zeer concrete tips opgeschreven. "Allereerst: ontzorg ondernemers door een pool van CISO's. Veel ondernemers willen geen eigen CISO (Chief Information Security Officer, red.) of kunnen dat niet veroorloven, maar zijn wel gebaat bij een CISO voor een paar uur. Daarnaast kun je DHV-trainingen aanbieden: digitale hulpverlening. Dat zijn simpele trainingen over de basis. Ook zie ik wel wat in een EHBDO-kaart: Eerste Hulp bij Digitale Ongelukken. Daar staat op wat je als eerste moet doen bij bijvoorbeeld een ransomware-aanval. Dat soort hulpmiddelen werken volgens mij veel beter dan opgelegde dwang, een bestraffende vinger of een keurmerk."

Er moet veel meer transparantie over cases uit het verleden komen, gaf een volgende deelnemer aan. "Vandaag gaf een gemeente volledige transparantie en ik merk aan de vragen die ik krijg, dat dat andere gemeenten echt wakker schudt."

"We moeten ons veel meer richten op onder andere investeerders, aandeelhouders, commissarissen en crowdfunders, zodat zij de juiste vragen kunnen stellen aan ondernemers", vond iemand anders. "Zij kunnen ondernemers aansporen om in actie te komen."

Een herkenbaar beeld, zoals bijvoorbeeld een logo voor ieder cyberveilig bedrijf, kan dienen als een soort kapstok waar je van alles aan op kunt hangen, gaf iemand aan. "Als wij hier allemaal besluiten om dat logo te voeren richting onze achterban, dan kun je daar campagnes en boodschappen aan ophangen."

De laatste deelnemer in het rondje kwam weer terug bij één van de eerste sprekers, degene die 'zenden, zenden, zenden!' had opgeschreven. "Het gaat om het herhalen van de boodschap. Een ongeluk blijft in een klein hoekje zitten, met mogelijk desastreuze gevolgen. We moeten het daarnaast breder trekken dan alleen IT-maatregelen. Veel ondernemers vertrouwen op hun IT'er en wanen zich onterecht veilig."

Vraag 2: Hoe activeren we private en publieke stakeholders als het om cyber security awareness richting het MKB gaat?

Er zijn verschillende belangrijke stakeholders die geactiveerd moeten worden om in het MKB voor meer awareness te zorgen, zoals partnerbedrijven, overheden en kennisinstellingen. Hoe activeer je die en krijg je ze op één lijn? Samenwerken is cruciaal, zei iemand. “Het is daarnaast belangrijk om ook het onderwijs en de wetenschap erbij te betrekken, waar heel veel kennis zit. En ook de brancheverenigingen.”

Het samenbrengen van kennis en daarover goed communiceren kwam ook nu terug. Een netwerk zoals de Dutch IT Cybersecurity Assembly zou daarin het voortouw kunnen nemen. Media spelen daar ook een rol bij, zo benadrukte een deelnemer.

Daarnaast moet je op zoek naar de belangen en de waarden voor iedereen in de keten, vond iemand. “Wat wil iedereen bereiken en hoe breng je dat samen? Als je dat bepaalt, kom je vanzelf in beweging.” Deze deelnemer kwam ook terug op het woord ‘zenden’. “Zenden is nog altijd heel belangrijk, omdat bedrijven vaak zelf nog geen idee hebben waar ze moeten beginnen.”

“Er zijn al best veel producten”, zei iemand. “Iedereen bedoelt misschien hetzelfde, maar zegt verschillende dingen. Begin met dezelfde taal te spreken en alles op dezelfde manier te uiten. Eerst moet je dus samen dingen vaststellen. Wat is essentieel voor iedere organisatie? Hoe verwoorden we het?”

Er ligt veel macht in de keten en bij overkoepelende organisaties. “Wat als dienstverleners bijvoorbeeld zeggen: we werken niet met je samen als je niet aan multi-factor-authenticatie doet? Brancheverenigingen kunnen dat misschien aansturen”, zei iemand. De volgende persoon zag haken en ogen in dat plan, maar ook positieve kanten. Daar werd op voortgeborduurd, maar dan met een focus op verzekeraars en accountants. Zij kunnen het MKB stimuleren of min of meer dwingen om hun zaken op orde te hebben voordat ze een verzekering of een lening kunnen afsluiten. “Accountants kunnen bijvoorbeeld ook forceren dat bedrijven een cybersecurity-plan afgeven in hun jaarrekening. Daar zijn meerdere partijen al heel goed mee bezig. Op lokaal niveau werkt dat goed.”

Bij het behandelen van deze vraag ging het meermaals over de wortel en de stok. Wat werkt beter: goed gedrag belonen of slecht gedrag afstraffen? De meeste mensen geloofden meer in de wortel dan in de stok. “Een keurmerk voelt voor mij een beetje als een stok, maar als je een verzekering of een lening af kunt sluiten als je je zaken op orde hebt, dan voelt dat meer als een wortel.” “Ook ik ben meer van de wortel dan van de stok”, zei iemand anders. “Tegelijkertijd moet de vrijblijvendheid er wel vanaf.”

Sommige grote organisaties dwingen hun kleinere partnerbedrijven om cyberweerbaar te worden, wist iemand te vertellen. “Grote bedrijven helpen de kleinere”, voegde een ander daaraan toe en dat gebeurt niet altijd vanuit een commerciële insteek. “Dat is goed, want op die manier sijpelt het vanzelf de keten door.”

Vraag 3: Hoe creëren we een baseline voor security die ondernemers kunnen gebruiken als toets?

Een meerderheid van de deelnemers wil dus geen harde dwang, maar is wel voorstander van een toets of een richtlijn die MKB-ondernemers duidelijkheid geeft. Hoe moet die eruit zien en hoe kan die neergezet worden?

"Er zijn online al allerlei gratis toetsen en scans beschikbaar die je kwetsbaarheden inzichtelijk maken", zei iemand. Een andere deelnemer bevestigde dat. Maar weet een MKB-ondernemer waar die toetsen te vinden zijn en hoe je ze inzet? "Het begint ook hier weer bij awareness. Als mensen googelen, dan zijn ze te vinden, maar er wordt nog weinig naar gezocht. Een groot deel van MKB-Nederland is er gewoon nog niet echt mee bezig." Iemand anders zei: "Ze vertrouwen hiervoor volledig op hun IT'er."

Misschien kan de Dutch IT Cybersecurity Assembly een stempel geven aan een goede baseline of scan, zo werd geopperd. De risicoanalyse van het Digital Trust Center zou een goede eerste stap zijn, gaf iemand aan. "Daar worden vragen gesteld waarmee ondernemers verder gaan en een volgende stap kunnen zetten. Maar het DTC is jammer genoeg ook nog niet bekend genoeg in het MKB." Ook is de vragenlijst niet voor iedere ondernemer even geschikt, zeker niet voor bedrijven die meer dynamisch zijn, zo zei iemand ook.

Een ander trok de vergelijking met brandveiligheid. "Soms moet je buiten je eigen grenzen naar andere voorbeelden kijken. Hoe ontstond er ooit een baseline voor brandveiligheid? Daar zijn veel verplichtingen die iedereen zonder problemen accepteert en dus zou dat als voorbeeld kunnen dienen."

De awareness groeit wel degelijk in hoog tempo, mede door de coronapandemie, benadrukte iemand. Er komen ook steeds meer scans. “De olievlek verspreidt zich.” Dat leverde instemmend geknik op. Iemand zei: “Er zijn inderdaad al veel scans, maar die zijn niet altijd gecombineerd. Met de groep zoals we hier zitten kunnen we kennis combineren en tot een gezamenlijk initiatief komen, met bijvoorbeeld een stuk of zes regels. Daar kunnen we gewoon mee starten.”

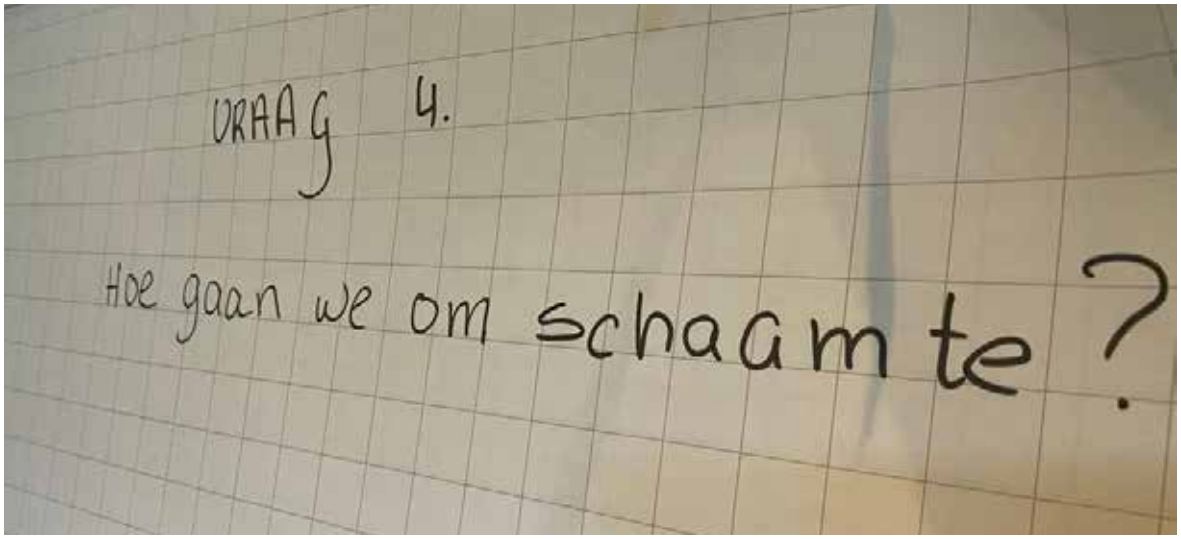
Die behoefte is er zeker, zo was duidelijk te proeven. “Nu is er nog veel onduidelijkheid. Van verschillende klanten krijgen wij verschillende eisen en van cyberverzekeraars ook. Het Agentschap Telecom komt ook weer met andere voorwaarden. Het gaat daarbij vaak om Capability Maturity, maar volwassenheid op dat gebied wil niet zeggen dat organisaties ook echt veilig zijn. En waarom accepteren we elkaars toetsen niet? Als ik mijn brandveiligheidstoets van de lokale brandwacht heb gehad, dan accepteert mijn verzekeraar die, net als de VVE en mijn pandeigenaar. Dat is in onze wereld jammer genoeg nog niet zo.” Er moet daarvoor een duidelijke standaard zijn, net als bij brandveiligheid, zo werd er later in het gesprek toegevoegd.

Maar wie neemt de regie voor zo’n baseline? De Dutch IT Cybersecurity Assembly kan daar de leiding in nemen, vonden meerdere deelnemers. “Hoe meer bedrijven dat samen doen, hoe makkelijker je het uitrolt. Als je samen een baseline opstelt en daar allemaal je naam onder zet, dan gaat dat balletje gewoon rollen.” De Assembly moet er gewoon mee beginnen, vonden meerdere deelnemers. “Er zijn heel veel partijen aanwezig. Als je de trechter aan de bovenkant vult met een toolkit, en je hebt pilotpartners die dat richting hun klanten kunnen distribueren, dan kun je van start. Je moet gewoon beginnen. Ik doe graag mee.”

Je kunt beginnen met een consultatieronde om de behoeftes van de markt in kaart te brengen, wat het draagvlak verhoogt, stelde iemand voor. Er is bij MSP’ers en bij IT-leveranciers veel data vanuit het bedrijfsleven beschikbaar, die ook benut kan worden, zo zei iemand anders. De scan moet niet alleen gaan over de vragen ‘wat?’ en ‘hoe?’, maar ook over ‘wie?’, vond een andere deelnemer. “Wie is er verantwoordelijk? Die vraag blijft bij scans vaak onbeantwoord.”

Een uitdaging zit er volgens iemand in dat, wanneer IT-dienstverleners of leveranciers bij klanten met zo’n informatie-set komen, het in de beeldvorming van die eindklant vooral als een commercieel middel wordt gezien. Dus heb je de hulp van bijvoorbeeld de overheid nodig om eerst de bewustwording te vergroten.

Sommige deelnemers plaatsen wat kanttekeningen. De baseline moet wel administratief licht zijn, zo vond iemand. Een baseline gaat nu nog een paar stappen te ver, vond iemand anders. “We moeten er eerst naartoe dat ondernemers bij noodgevallen altijd bereikbaar zijn op een bepaald mailadres. Nu bouncen er nog veel e-mails wanneer ondernemers gewaarschuwd worden. We moeten als deelnemers hier een paar stappen terug en ons verplaatsen in de beginnende MKB-ondernemer die niet technisch onderlegd is.” De baseline mag ook nooit de indruk wekken dat bedrijven daarmee veilig zijn, want dat is zeker niet het geval. “Daar moeten we waakzaam voor zijn.”



Vraag 4: "Hoe gaan we om met schaamte?"

Bedrijven die worden getroffen stoppen dat vaak in de doofpot, omdat ze zich schamen of omdat ze bang zijn voor reputatieschade. Dat zorgt ervoor dat informatie die ook nuttig kan zijn voor anderen, nu niet gedeeld wordt. Hoe kan dat veranderd worden? Dat was de laatste vraag van de avond.

"We zeggen toch te makkelijk tegen mensen die hun systeem niet op orde hebben, dat het enorme oliebollen zijn. Dat zorgt ervoor dat ze hun mond dichthouden. Maar er zijn ook goede voorbeelden. De burgemeester van Lochem staat na een aanval nu overal op het podium en ontpopt zich als digi-burgemeester om collega's te waarschuwen. Dat werkt veel beter dan wanneer experts jou iets vertellen. De verandering moet van binnenuit komen." Vooral bedrijven die wat langer geleden zijn getroffen en er weer helemaal bovenop zijn gekomen zouden hun verhaal moeten vertellen. "Dat kan enorm inspirerend werken."

"Hoezo zou je je moeten schamen als je slachtoffer bent?", stelde dezelfde persoon de vraag. "De criminelen moeten zich schamen en anderen moeten zich beschermd voelen." Dat leverde veel instemming op. "Mensen zijn bang dat het aan hun imago kleeft", zij iemand anders. "Misschien moet er een meldpunt komen, een grote pool, waar mensen anoniem hun verhalen kunnen vertellen." "Het is misschien wel meer angst op gezichtsverlies, dan schaamte", zei iemand anders.

De rol van de media werd aangehaald, die vaak voor de negatieve of smeuïge benadering kiezen. "Wij kunnen het hier allemaal wel met elkaar eens zijn, maar de MKB'ers volgen de grote landelijke media. Hoe betrekken we hen daarbij?"

Het begint met goede communicatie nadat je getroffen bent. Dat is vaak ook onderdeel van een cyberverzekering, vertelde iemand. "Als je zelf een goed persbericht naar buiten gooit, zullen media er minder snel een bepaalde negatieve draai aan geven." Daarvoor kun je ook social media inzetten, voegde iemand anders toe. Media zijn bij grensoverschrijdend gedrag zoals in het geval van The Voice of Holland van toon veranderd, zei iemand anders. Ze doen minder aan victim blaming dan vroeger. "Wij hebben hier genoeg kracht om de media te vertellen dat de schuld moet liggen bij de echte daders."

Met dat onderwerp werd de avond afgesloten. Na afloop praatten de deelnemers op informele wijze verder en werden er plannen gemaakt om samen aan de slag te gaan met een uniforme richtlijn voor MKB-bedrijven.

Ideeën en tips om MKB'ers te helpen met awareness, en met de juiste acties na een aanval:

- Ontzorg ondernemers door een pool van CISO's.
- DHV-trainingen aanbieden: digitale hulpverlening.
- Een EHBDO-kaart: Eerste Hulp bij Digitale Ongelukken.
- Een logo/keurmerk voor ieder cyberveilig bedrijf.
- Begin met dezelfde taal te spreken en alles op dezelfde manier te uiten.
- Zorg dat bedrijven een cybersecurity-plan afgeven in hun jaarrekening.

De DICA Baseline:

- Er is behoefte aan een duidelijke standaard.
- Zoek inspiratie vanuit de baseline voor brandveiligheid. Daar zijn veel verplichtingen die iedereen zonder problemen accepteert.
- De Dutch IT Cybersecurity Assembly (DICA) kan daar de leiding in nemen!
- Begin met een consultatieronde om de behoeftes van de markt in kaart te brengen.
- Gebruik de bij MSP'ers en IT-leveranciers beschikbare data vanuit het bedrijfsleven.
- Uitdaging: voorkom dat de baseline door eindklanten als een commercieel middel gezien wordt. Hulp van de overheid is nodig om de bewustwording te vergroten en de DICA als non-profit te legitimeren.

Founded by

Dutch IT Channel

Datto