

INTERVIEWS | 1 NOVEMBER 2022

MELD JE CYBERINDICENT!

Auteur: Sierd Stapersma RO EMITA

Beeld: Phil Nijhuis - Sora Shimazaki - Pexels

Leestijd: 8 min



Het cybersecuritywoordenboek definieert 'cyberweerbaarheid' als het vermogen om (relevante) digitale risico's tot een aanvaardbaar niveau te reduceren. Door middel van preventieve en detectieve maatregelen kunnen cyberincidenten worden voorkomen, kan de schade worden beperkt en/of het herstel eenvoudiger worden gemaakt. Petra Oldengarm, directeur van Cyberveilig NL, schetst haar context hierbij.

Wie is Petra Oldengarm?

"Op parttime basis leid ik het verenigingsbureau en vertegenwoordig ik de belangenvereniging Cyberveilig Nederland. Het verenigingsbureau coördineert lopende activiteiten, initieert nieuwe acties en onderhoudt de contacten met de verschillende stakeholders. Daarnaast ben ik zelfstandig adviseur voor onder andere overheidsinstellingen en doceer ik aan de Universiteit Leiden. Mijn achtergrond ligt in de technische informatica en ik ben al vele jaren actief in het cybersecuritydomein voor verschillende werkgevers waaronder de AIVD, ECN en Hoffmann."

Wat is Cyberveilig Nederland?

"Cyberveilig Nederland is de branche- en belangenorganisatie voor private ondernemingen en (semi)publieke instellingen actief in het cybersecuritydomein. Het bestuur van de vereniging bestaat uit vijf leden en bewaakt de

AUDIT

MAGAZINE

voortgang van het dagelijks bureau. De vereniging ontvangt geen overheidssubsidies, maar wordt gefinancierd door de verenigingsleden via een periodieke bijdrage. De vereniging telt nu ongeveer tachtig á negentig leden en dat is een brede vertegenwoordiging van de cybersecuritymarkt in Nederland. De leden zijn actief in het cybersecuritydomein vanuit bijvoorbeeld de technologie en/of risicobeheersing. Maar ook organisaties als KIWA, TUV Nederland en Deloitte zijn bijvoorbeeld lid.”

Hoe is de vereniging eigenlijk ontstaan?

“Enkele jaren geleden hebben acht ondernemingen het idee opgevat om een overkoepelende organisatie op te zetten om in eerste instantie de kwaliteit van cybersecuritydiensten te waarborgen. Dit leidde tot de oprichting van Cyberveilig Nederland in juni 2018. Door middel van een gezamenlijk plan wilden we de kwaliteit van het aanbod aan cybersecurityproducten en -dienstverlening verhogen. De vraag naar deze producten en diensten nam (en neemt) enorm toe als gevolg van de exponentiële groei van internet.”

“Aandacht voor cybersecurity en digitale weerbaarheid is een noodzakelijke hygiëne”

Een mooi doel

“Dit doel streven we nog steeds na. Om bovendien een goede gesprekspartner te zijn voor stakeholders in het landschap en meer transparantie te bieden in het toenemende aanbod, stellen we steeds meer kennis en informatie publiek beschikbaar. Kortom, de hoge mate van digitalisering in Nederland brengt kansen en risico's met zich mee. Om voortdurend vertrouwen te hebben in de aangeboden informatie en informatiesystemen is aandacht voor cybersecurity en digitale weerbaarheid een noodzakelijke hygiëne!”

Wie bepaalt jullie agenda?

“De verenigingsleden bepalen wat er binnen Cyberveilig Nederland gebeurt. Aan het eind van ieder jaar vindt onze algemene ledenvergadering (AL) plaats. Tijdens deze vergadering wordt de voortgang besproken en het beleid voor het volgende jaar vastgesteld. Ieder verenigingslid heeft een stem op deze vergadering. Gedurende het jaar worden de activiteiten uitgevoerd waaraan de leden actief kunnen deelnemen.”

Maar hoe doen jullie dat dan?

“Op verschillende manieren. Via een werkgroep behartigen we bijvoorbeeld de belangen van de sector binnen de overheid, wetenschap en politiek. We leveren bijdragen aan onderzoeken, rapporten en roadmaps. Cyberveilig Nederland is ook aangewezen als OKTT/schakelorganisatie waardoor een intensievere informatie-uitwisseling mogelijk wordt met het Nationaal Cyber Security Centrum (NCSC). Gevoelige informatie wordt via veilige platformen op vertrouwelijke wijze gedeeld met de leden.”



Petra Oldengarm, Cyberveilig Nederland: “Een organisatie die met een cyberincident te maken heeft, wordt vaak neergezet als een slecht beveiligde onderneming zonder verdere gedegen onderbouwing. Zij worden bijna gezien als dader”

Nog meer?

“We ontwikkelen daarnaast allerlei handige documenten, zoals ‘buyer guides’. Op 1 juli 2021 is de buyers guide Securitytesten gepubliceerd. Met dit document willen we organisaties helpen een specifiekere uitvraag te doen in de markt als zij behoefte hebben aan een securitytest. Het geeft bijvoorbeeld heldere definities van de verschillende diensten en maakt de huidige mogelijkheden op dit gebied inzichtelijk. Hierdoor zal de test beter aansluiten bij de behoefte van de organisatie en wordt het vergelijken van offertes makkelijker gemaakt. Een guide waar op dit moment aan gewerkt wordt, gaat over cyber awareness en gedrag. En volgend jaar verwachten we een guide te publiceren over monitoring.”

Wat verstaan jullie eigenlijk onder cyber resilience?

“Cyberweerbaarheid is de vertaling en kent twee belangrijke perspectieven. Het eerste perspectief is de kans op het materialiseren van cyberrisico's verminderen; preventieve maatregelen nemen om minder gevaar te lopen. Binnen dit perspectief zie ik ook een duidelijke rol voor de overheid weggelegd. Organisaties zelf moeten echter daarnaast kijken naar het perspectief van detectie. Hoe sneller cybergevaar gedetecteerd wordt, hoe sneller erop kan worden gereageerd waardoor de schade mogelijk beperkt(er) blijft. En tot slot moeten zij zorgen dat ze goed voorbereid zijn op een incident, zodat ze in geval van nood adequaat kunnen reageren, mede op basis van een goed ingerichte governancestructuur.”

“In dit verband is het interessant om te vermelden dat er een cybersecuritywoordenboek bestaat (inmiddels de 3^e druk, december 2021, ook digitaal te raadplegen via www.cybersecuritywoordenboek.nl). Cyberveilig Nederland (de werkgroep Kwaliteit & transparantie) stelde dit boek op samen met ruim zeventig organisaties en vele Nederlandse cybersecurityprofessionals en in samenwerking met de Cybersecurity Alliantie. Dit woordenboek tracht lastige termen –

die voor cyberspecialisten dagelijks jargon zijn – begrijpelijk te maken voor mensen die nog onbekend zijn met de terminologie.”

Wat zien jullie als grootste cyberrisico?

“Als we afgaan op het aantal cyberincidenten (geclassificeerd naar het type incident) dan is een ransomwareaanval het meest voorkomend. Bij zo'n aanval wordt schadelijke software gebruikt om toegang te krijgen tot een computersysteem om deze vervolgens te blokkeren totdat een geldbedrag is betaald. Het advies in zo'n geval is afhankelijk van de specifieke situatie, maar over het algemeen luidt het advies: geen geld betalen en aangifte doen. Anders houden we dit in stand. Echter, er zijn veel situaties waarin dit helaas niet mogelijk is. Dit risico wordt door de NCSC gezien als een belangrijke dreiging voor de nationale veiligheid.”

“In de private sector komt het regelmatig voor dat er pas voldoende aandacht is voor cyberrisico's nadat zich daadwerkelijk een incident heeft voorgedaan. Dan is er onmiddellijk capaciteit, tijd en budget beschikbaar”

Noem nog eens een cyberrisico

“Daarnaast komt zogenaamde CEO-fraude regelmatig voor; vanuit de naam van de CEO (of CFO, CIO, et cetera) wordt er een nepbericht gestuurd om bijvoorbeeld een urgente en bedrijfskritische betaling te doen (naar een rekening waar de criminelen over kunnen beschikken). Als gevolg van de coronacrisis en het (verplicht) thuiswerken worden veel beslissingen via e-mail gecommuniceerd (en minder telefonisch of face-to-face). Dit brengt het risico met zich mee dat nep e-mails worden gebruikt om daarvan – als crimineel – beter te worden.”

“Een type incident waar veel organisaties (nog) niet over nadenken zijn indirecte cyberaanvallen bij toeleveranciers en afnemers, maar waarvan de impact zich ook bij de organisatie zelf kan manifesteren. Het is dus goed om als organisatie na te gaan wat toeleveranciers en afnemers doen om dit te voorkomen en/of de schade te beperken, ter bescherming van de eigen organisatie.”

Wordt er wel voldoende in geïnvesteerd in preventie, detectie en respons?

“In de private sector komt het nog regelmatig voor dat er pas voldoende aandacht is voor cyberrisico's nadat zich daadwerkelijk een incident heeft voorgedaan. Het senior management is wakker geschud en stelt onmiddellijk capaciteit, tijd en budget beschikbaar om de risico's binnen de gewenste 'risk appetite' te brengen. Belangrijk is dat organisaties ieder voor zich nadenken over de vraag welke risico's zij lopen met de digitale middelen/infrastructuur die zij gebruiken. Dat kan zich vervolgens vertalen in de keuze voor passende maatregelen.”



“De overheid heeft in het jongste regeerakkoord opnieuw middelen vrijgemaakt voor cybersecurity. Hoe deze zullen worden besteed is onderwerp van de [Nederlandse Cybersecurity Strategie \(NLCS\)](#). Hierbij is inmiddels een veelheid aan ministeries betrokken die ieder een eigen verantwoordelijkheid dragen in dit domein.”

Hoe moeten kleine(re) organisaties met weinig middelen zich beschermen tegen cyberdreiging?

“Weinig cybersecuritybedrijven richten zich op het mkb en kleinere organisaties. Tegen deze organisaties wil ik zeggen dat ze goed moeten kijken naar de efficiency en effectiviteit van de voorgenomen maatregelen, aangezien ze vaak niet beschikken over veel middelen en kennis. Een aantal basismaatregelen zijn voor iedere organisatie van belang om te overwegen.”

Wat zijn die basismaatregelen?

“Het [Digital Trust Center](#) heeft een overzicht van basismaatregelen voor deze doelgroep. Dit is een overheidsorganisatie met als hoofddoel ondernemers te helpen met veilig digitaal ondernemen, mede op initiatief van het ministerie van Economische Zaken en Klimaat en wordt onder andere ondersteund door VNO-NCW en de Koninklijke Vereniging MKB-Nederland. Daarnaast beschikt het NCSC over een vergelijkbaar overzicht en heeft de AIVD-richtlijnen opgesteld om een netwerk adequaat te segmenteren.”

Op jullie website staat dat cybersecurity niet alleen een risico is, maar ook een kans.

Vertel eens

“Ondernemingen kunnen zich onderscheiden door digitale producten en diensten ‘by design’ veilig te ontwikkelen. Dit levert ze een extra waarde en dus verkoopargument op en zorgt er tevens voor dat de awareness en kennis/ervaring binnen de organisatie zelf wordt verhoogd en vergroot. Als we dit concept vervolgens op grotere schaal omarmen, dan draagt dat ook bij aan de exportwaarde van de bv Nederland, omdat Nederland dan te boek komt te staan als een land waar veilige producten en diensten worden ontwikkeld.”

“Het goed inzichtelijk maken op welke plekken de organisatie verbonden is met

internet is een belangrijk startpunt voor een gedegen risico-identificatie en het bepalen van de nodige (voorzorgs)maatregelen”

Welk cyberthema speelt er nog meer?

“Transparantie. Op dit moment rust er nog te vaak en te veel een taboe op het (publiekelijk) informeren over/melden van cyberincidenten. Een organisatie die met een materieel cyberincident te maken heeft, wordt vaak neergezet als een slecht beveiligde onderneming zonder verdere gedegen onderbouwing. Zij zijn geen slachtoffer geworden, zij worden bijna eerder nog gezien als dader. En de naming en shaming in de media draagt niet bij aan dit beeld. Om van incidenten in breder verband te kunnen leren, zou het juist goed zijn om dit taboe te doorbreken en dit met een open mind te delen. Grote ondernemingen zouden volgens ons hier het voortouw in moeten nemen. Een goed voorbeeld is de firma Hoppenbrouwers Techniek. Zij zijn recentelijk getroffen door een wereldwijde cyberaanval via hun beveiligingssoftware en zij zijn daar open over geweest naar de buitenwereld. Ze publiceren hier in september 2022 een boek over.”

Wat is de rol van de auditor in het cyberdomein?

“Naast assurance en advies verwacht ik dat de auditor een rol kan spelen in het creëren van (meer) bewustzijn voor cyberrisico's bij het senior management. Cybersecurity gaat immers veel verder dan IT en kantoorautomatisering alleen. Het goed inzichtelijk maken op welke plekken de organisatie verbonden is met internet is een belangrijk startpunt voor een gedegen risico-identificatie en het bepalen van de nodige (voorzorgs)maatregelen. Niet alleen het technische plaatje geeft dit inzicht, maar vanuit het perspectief van processen kan het ook een interessante invalshoek zijn. Een auditor levert vervolgens toegevoegde waarde als hij zijn onafhankelijke oordeel hierop geeft.”

Een verplichte/periodieke cyberaudit. Goed idee?

“Onderzoek doen naar (de beheersing) van cyberrisico's is altijd verstandig. Ik weet echter niet of je dit verplicht moet stellen. Het moet natuurlijk geen afvinklijstje of papieren tijger worden, dat werkt wellicht zelfs averechts (het wekt de indruk dat de organisatie 'klaar' is voor een cyberaanval, waar dat in werkelijkheid (nog) niet het geval is). Aan de andere kant, het kan wel mensen over de drempel helpen en aanzetten tot actie (het vliegwieleffect). Dit leidt dan meteen tot de vraag hoe je dat moet inrichten gezien de grote verschillen tussen ondernemingen en organisaties. Ik zie dan eigenlijk meer toegevoegde waarde in het mensen bewuster maken en intrinsiek motiveren hiermee aan de slag te gaan.”

Ten slotte, wat wil Cyberveilig Nederland elke auditor meegeven en waarom eigenlijk?

“Maak impact door continu de vertaalslag te maken van wat er op het gebied van cybersecurity op de werkvloer gebeurt naar adequate stuurinformatie voor het senior management. Alleen dan worden de juiste conclusies getrokken en beslissingen genomen.”

Over

De dagelijkse leiding van Cyberveilig Nederland is in handen van Petra Oldengarm. Zij heeft een achtergrond in de technische informatica en is al vele jaren actief in het cybersecuritydomein voor verschillende werkgevers en opdrachtgevers.

AUDIT

MAGAZINE

Tags: Cyber resilience, informatiebeveiliging

Bron url: <https://auditmagazine.nl/interviews/meld-je-cyberindicent/>