Ministerie van Economische Zaken
en Klimaat

Ontwikkel een cybersecurity scan

In samenwerking met onderwijsinstellingen

Inhoud

Inleiding 2
Over het Digital Trust Center 3
Voorbeelden van bestaande initiatieven 4
Werk samen met onderwijsinstellingen 4
Motiveer bedrijven om mee te doen 5
Bepaal de inhoud van de scan 6
Bespreek randvoorwaarden 6
Zorg voor een overeenkomst met duidelijke afspraken 7
Dataverzameling 7

Inleiding

Het is voor ondernemers niet eenvoudig een helder beeld te krijgen van de mate waarin hun onderneming digitaal veilig is. Sommige ondernemers geven aan dat digitale veiligheid niet het eerste is waar ze aan denken als het gaat om bedrijfsrisico's. Daarnaast zijn bedrijven ten onrechte soms in de veronderstelling dat dit 'moderne begrip' alleen van belang is voor grote ondernemingen.

Het aanbieden van een tool, zoals een cybersecurity scan, geeft ondernemers en bedrijven door middel van een relatief beperkte tijdsinvestering snel inzicht in hun huidige digitale veiligheid. Het is ook een uitstekend middel om bedrijven aan te sporen tot het nemen van concrete acties om hun digitale weerbaarheid te vergroten.

Met de invoering van de Algemene Verordening Gegevensbescherming (AVG) hebben bedrijven ook wettelijk de verantwoordelijkheid om persoonsgegevens van klanten op een goede manier te beschermen. Een onderzoek naar veel voorkomende kwetsbaarheden kan hen ondersteuning bieden bij het inzichtelijk maken van mogelijke gebreken.

Over het Digital Trust Center

Het Digital Trust Center (DTC) helpt ondernemers met veilig digitaal ondernemen. De doelgroep van het DTC bestaat uit 1,7 miljoen bedrijven: van zzp'ers tot en met het grootbedrijf. Het gaat om alle bedrijven in Nederland die niet tot de zogenaamde vitale sectoren behoren, zoals banken, telecom-, energie-, en waterbedrijven. Het DTC ondersteunt bedrijven via een digitaal platform, www.digitaltrustcenter.nl, en sociale mediakanalen met actuele informatie en betrouwbare adviezen. Daarnaast, is er een subsidieregeling beschikbaar, die bedrijven en organisaties stimuleert om te gaan samenwerken en zich te verenigen in een samenwerkingsverband om ondernemers te helpen met veilig digitaal ondernemen. Het Digital Trust Platform wordt in 2019 gelanceerd. Het platform biedt kennis en actualiteiten rondom veilig digitaal ondernemen binnen een veilige omgeving en faciliteert samenwerking tussen ondernemers, security- en IT-specialisten.

Doelgroep
Deze handreiking is bedoeld voor bestaande en toekomstige samenwerkingsverbanden, die bedrijven een tool, een cyberveiligheid scan, willen bieden, waarmee inzicht wordt gegeven in de actuele cyberweerbaarheid van een bedrijf.

Aan deze handreiking hebben bijgedragen
Stichting Cyberweerbaarheid Noord Nederland, Cyberweerbaarheid Limburg.

Deze handreiking is tot stand gekomen door
Het Digitaal Trust Center (Ministerie van Economische Zaken en Klimaat)

Voorbeelden van bestaande initiatieven

De cyberweerbaarheidsnetwerken in Noord Nederland en in Limburg zijn verschillende initiatieven gestart om bedrijven een stap op weg te helpen met het op orde krijgen van hun digitale veiligheid. In samenwerking met regionale opleidingscentra (ROC) met MBO en HBO ICT-opleidingen, bieden zij de bedrijven de mogelijkheid een scan uit te laten voeren door studenten.

In Noord Nederland gaan studenten van ROC Friese Poort in multidisciplinaire teams op bezoek bij bedrijven om ter plaatse een tweetal scans uit te voeren: De "Quick Start AVG" en "Digitaal Veilig Ondernemen". Het gaat om Mbo-studenten van de opleidingen ICT en Juridisch Administratief, en Hbo-studenten van de opleidingen Integrale Veiligheid en Recht. Na afloop maken zij een eindrapport met de status van de cyberveiligheid van het bedrijf, en doen zij tevens aanbevelingen. Voor studenten levert dit bijzonder rijke leersituaties op en bedrijven worden hiermee op een praktische manier geholpen.

In Limburg voeren de studenten van het Vista College een cyberweerbaarheidsscan bij bedrijven uit. Deze studenten gaan gedurende een paar dagen bij het bedrijf op bezoek, waarbij zij een brede risicoanalyse doen, van digitale veiligheid tot en met de bedrijfstoegang, archivering van documenten, Algemene Verordening Gegevensbescherming (AVG) toepassing, enz.

De bovengenoemde samenwerkingsverbanden hebben ieder een eigen scan ontwikkeld, met verschillende aanvliegroutes, afgestemd op de behoefte en wensen van de samenwerkingspartners. Het noordelijke initiatief richt zich met de scan op de meest voorkomende kwetsbaarheden, waar het zuidelijke initiatief een meer diepgaande scan naar alle kwetsbaarheden heeft ontwikkeld. Zij vormen daardoor een mooie aanvulling op elkaar, tegemoetkomend aan de verschillende behoeften en profielen van bedrijven.

De Stichting Cyberweerbaarheid Noord Nederland en het Expertisecentrum Cyberweerbaarheid in Limburg houden elkaar op de hoogte over de voortgang en resultaten, inspireren elkaar en wisselen *best practices* uit m.b.t. het bereiken van de ondernemer.

De lessen die voornoemde samenwerkingsverbanden hebben opgedaan tijdens het ontwikkelen van deze initiatieven zijn aanleiding geweest voor het DTC om deze handreiking te ontwikkelen, zodat ook andere samenwerkingsverbanden hiervan kunnen leren.

Werk samen met onderwijsinstellingen

Betrek het onderwijs bij het ontwikkelen van een scan. Publiek-private samenwerking is cruciaal om de digitale weerbaarheid van Nederland te verhogen. Nederland heeft een ruim aanbod aan ICT-onderwijs, waarin veiligheid een essentieel onderdeel is van het curriculum. Met behulp van gemotiveerde docenten wordt de verbinding gezocht met bedrijven. Leerlingen op zowel MBO als HBO niveau hebben veel te bieden aan nog weinig gedigitaliseerde bedrijven, of juist aan sterk gedigitaliseerde bedrijven die (te) beperkte aandacht geven aan cyberveiligheid. Met de kennis en vaardigheden uit de opleiding, kunnen studenten via een gestructureerde aanpak vaak in een kort tijdsbestek al heel veel risico's in kaart brengen voor een onderneming. Het ontwikkelen van een scan kan daarbij een uitkomst bieden, zowel voor het leerproces van toekomstig cybertalent door het ontwikkelen en/of toepassen van een methodologie en het kennismaken met de praktijk, als voor het bedrijf, dat alert wordt gemaakt op zijn digitale kwetsbaarheden.

Niet alleen voor ICT-beroepsopleidingen is het uitvoeren van een scan interessant. Ook bij andere studierichtingen, zoals bijv. MBO Juridisch Administratief, zijn er veel raakvlakken met informatiebeveiliging en kunnen kennis en kunde van studenten goed worden benut.

Bespreek met de onderwijsinstelling binnen het samenwerkingsverband de wederzijdse wensen of, indien je van plan bent een samenwerkingsverband op te zetten (raadpleeg hier[1] de handreikingen voor het opzetten van een samenwerkingsverband), betrek het onderwijs in de regio dan tijdig bij de ontwikkeling van activiteiten en ideeën.

Het nauwe contact van onderwijsinstellingen met het bedrijfsleven en diens behoeften zorgen ervoor dat het beroepsonderwijs aangesloten kan blijven op de praktijk en realiteit van het Nederlandse mkb.

[1] https://www.digitaltrustcenter.nl/netwerken-cyberweerbaarheid/handreikingen-samenwerking

Motiveer bedrijven om mee te doen

Vertrouwen is een belangrijk ingrediënt om bedrijven ertoe te bewegen zich open te stellen voor een onderzoek naar hun huidige cyberveiligheid. Dit kan vaak makkelijker worden opgebouwd en onderhouden wanneer er fysieke nabijheid is. Tegen deze achtgrond, is het aan te raden de samenwerking met lokale branche- en belangenorganisaties of ondernemersverenigingen op te zoeken. Denk hierbij aan de Gemeente, de Kamer van Koophandel (KvK), het Keurmerk Veilig Ondernemen[2], het Centrum voor Criminaliteitspreventie en Veiligheid (CCV), de Politie, etc.
Ook kan een vertrouwenspersoon van bedrijven in een bepaald gebied of bij een bedrijvenpark of een andere sleutelpersoon binnen een lokaal netwerk een stimulerende rol spelen bij het bereiken van de ondernemer.

"Samenwerking en activiteiten op elkaar afstemmen is belangrijk. Maar de ondernemer bereiken, dat moet je lokaal doen."

Expertisecentrum Cyberweerbaarheid Limburg

Benut contactmomenten en geef aandacht aan de scan-mogelijkheid tijdens bijeenkomsten, workshops, een *roadshow*, etc. Ook kan het als lokkertje werken om bedrijven juist naar een evenement toe te trekken aangezien met de scan een concreet product aan bedrijven wordt aangeboden.

Ervaringsverhalen
Het werkt heel effectief om een ondernemer een ervaringsverhaal te laten delen waarin hij/zij vertelt over de cyberrisico's en -dreigingen waar zijn/haar bedrijf mee te maken heeft gehad. Dit kan heel goed tijdens een seminar, workshop of andere bijeenkomst. De impact van een cyberincident wordt hiermee van een ontastbare zaak naar de realiteit van de werkvloer gebracht.

Het DTC zal ook testimonia via haar kanalen verspreiden. Mocht je ondernemers kennen die hun verhaal willen vertellen, laat het ons weten (www.digitaltrustcenter.nl/contact).

Algemene Verordening Gegevensbescherming (AVG)
Wijs bedrijven op deze Europese privacywetgeving. De AVG is van toepassing op alle bedrijven en organisaties die persoonsgegevens van klanten of personeel vastleggen. In de praktijk geldt dat voor vrijwel alle ondernemers. Het is voor bedrijven niet altijd helder wat de praktijkconsequenties van deze nieuwe regels inhouden en, dat om hieraan te voldoen, ook de digitale veiligheid van hun gegevensbeheer op orde moet zijn. Gebrek aan kennis t.a.v. AVG-naleving kan een stimulans voor bedrijven zijn om een weerbaarheidsscan uit te laten voeren. Breng dit daarom onder de aandacht.

Zelfevaluatie tool
Om bij te dragen aan het digitaal bewustzijn van ondernemend Nederland en de noodzaak om actie te nemen, zal het DTC ondernemers en bedrijven op korte termijn een laagdrempelige zelfevaluatietool bieden. Hiermee krijgen zij in een paar minuten tijd een eerste indicatie met betrekking tot hun basisbeveiliging. De tool is gebaseerd op de vijf basisprincipes van veilig digitaal ondernemen, die zijn opgesteld door het DTC en kunnen worden geraadpleegd op de website van het DTC[3]. De uitkomst van deze beknopte evaluatie moet een zeker gevoel van urgentie oproepen en bedrijven aanzetten om over te gaan tot het nemen van verdere acties, zoals het laten uitvoeren van een uitgebreidere cybersecurity scan bij een van de cyberweerbaarheid samenwerkingsverbanden.

[2] https://www.mkb.nl/kvob
[3] https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen/documenten/publicaties/2018/07/18/poster-5-basisprincipes-van-veilig-digitaal-ondernemen

Werk samen met andere weerbaarheidsnetwerken
Het DTC en de cyberweerbaarheidsnetwerken hebben een gezamenlijk belang. Samenwerking is cruciaal om stappen te zetten in het verhogen van de digitale weerbaarheid van regio's, sectoren en ketens.

Eén van de doelstellingen van het DTC is om tot een landelijk dekkend stelsel met aanspreekpunten voor bedrijven te komen, die onder andere tools aanbieden waarmee ondernemers in Nederland een handreiking en een impuls krijgen op weg naar het vergroten van hun digitale veiligheid.

"De grote meerwaarde van het landelijk Digital Trust Center zit in het bij elkaar brengen van partijen, elkaar verrijken en het gezamenlijk optreden in het cyberdomein."

Cybersafety Noord Nederland

Zoek je contact met andere samenwerkingsverbanden om ervaringen uit te wisselen voor het ontwikkelen van een cybersecurity scan? Laat het ons weten!

Bepaal de inhoud van de scan

Een scan die rekening houdt met alle elementen op het gebied van cyberveiligheid, analyseert zowel ICT-systemen, de hardware en software van een bedrijf, als de werkprocessen en mensen binnen de organisatie.

Er kan ook voor worden gekozen verschillende scan-varianten te ontwikkelen, met focus op een of bepaalde onderdelen op het terrein van cyberveiligheid (bijv. informatiebeveiliging, toegangsbeveiliging en autorisatie, softwarebeveiliging, netwerkbeveiliging, etc.), afhankelijk van de behoefte van het te onderzoeken bedrijf.

Voor onderwijsinstellingen is het van belang dat de uitvoering van de scan qua niveau een goede aansluiting heeft bij het curriculum van de opleiding en het leertraject van de studenten.

Daarnaast biedt het uitvoeren van scans meer dan alleen praktische ervaring met de technische kant van de opleiding. Er zijn ook sterke raakvlakken met onderwijsvakken als Burgerschap en Nederlands.

Welke methodologie voor de uitvoering van de scan wordt gebruikt, wordt in samenspraak met de betrokken partners bepaald. Er kunnen checklijsten worden gehanteerd, interviews worden afgenomen, geautomatiseerde openbare tools worden gebruikt, of zelfs 'friendly hacks' worden uitgevoerd.

Zorg ervoor dat het resultaat van de scan informatie verstrekt over digitale kwetsbaarheden van het bedrijf en daarbij (handelings)advies biedt. Op basis daarvan, kan het bedrijf zelf verdere maatregelen nemen en/of ervoor kiezen een professionele zakelijke dienstverlener in te schakelen, die oplossingen voor de geconstateerde veiligheidsgebreken implementeert.

Bespreek randvoorwaarden

Het is belangrijk dat het bedrijf waar de scan wordt uitgevoerd voldoende capaciteit beschikbaar stelt en de juiste medewerker(s). De effectiviteit van de scan is hier mede van afhankelijk. Het bedrijf zal bijv. tijd moeten besteden aan de ontvangst van de student(en), er moet gelegenheid zijn voor het afnemen interviews (bij de aangewezen persoon voor het betreffende onderwerp) en voor het in ontvangst nemen van het resultatenrapport en het geven van feedback daarop.

Daarnaast moet ook rekening worden gehouden met het gereedmaken van ICT-zaken. Zorg ervoor dat er tijdig afspraken zijn gemaakt met het bedrijf over de gewenste toegang tot systemen en netwerken, mede afhankelijk van de inhoud van de uit te voeren scan.

Zorg voor een overeenkomst met duidelijke afspraken

Het is belangrijk dat er wederzijds vertrouwen is tussen de partners die de scan aanbieden, en het bedrijf. Echter, dit is niet voldoende en zorg ervoor dat je afspraken, verantwoordelijkheden en aansprakelijkheidszaken ook schriftelijk vastlegt. Hieronder volgen een aantal aandachtspunten voor het opstellen van een overeenkomst tussen de aanbieder binnen het samenwerkingsverband, de onderwijsinstelling en het bedrijf. Let wel, de lijst is niet uitputtend en zal afhankelijk zijn van de wederzijdse en mogelijk specifieke behoeften van de betrokkenen.

- Uitleg over de werkwijze;
- Contactpersoon en ondersteuning vanuit het bedrijf aan de student(en);
- Toegang tot ICT-infrastructuur;
- Aanbrengen van wijzigingen in systemen;
- Verstrekking van informatie door het bedrijf;
- Geheimhoudingsplicht;
- Vertrouwelijke omgang met gegevens en informatie van het bedrijf;
- Opslag en beheer (of vernietiging van) bedrijfsgegevens en scan-uitkomsten;
- AVG-toepassing;
- Opvolging van of rechten ontlenen uit verstrekte adviezen;
- Etc.

Kosten

Het verdient de aanbeveling de dienst niet gratis aan te bieden maar om een eigen bijdrage van het bedrijf te vragen. Het is de bedoeling dat de ondernemer aan de slag gaat met de adviezen uit de scan en dient daarom voldoende belangstelling te hebben om bereid te zijn hier een kleine tegemoetkoming tegenover te zetten. De inkomsten hieruit kunnen aan andere activiteiten worden besteed. Zo gebruikt Stichting Cyberweerbaarheid Noord Nederland de opbrengst om de reiskosten van studenten te declareren en een afsluitende bijeenkomst voor studenten en bedrijven van te organiseren.

Dataverzameling

De uitkomsten van de scans kunnen veel waardevolle informatie bieden over de onderontwikkelde cyberveiligheidsgebieden bij bedrijven. Deze informatie kan worden benut om de informatievoorziening en adviesverlening van het weerbaarheidsnetwerk aan de regio/sector/keten op af te stemmen, of bijv. om gerichte sessies/workshops over de meest relevante onderwerpen te organiseren.

Ook kunnen mogelijk verbanden worden gelegd tussen het type bedrijf waarbij de scans worden uitgevoerd (bijv. gekeken naar bedrijfsomvang en bedrijfsactiviteit) en de digitale veiligheidsprestaties van deze deelnemers. Met het vergrote inzicht in de gemeenschappelijke kwetsbaarheden binnen de geïdentificeerde subgroepen kan gerichter aandacht worden besteed vanuit het weerbaarheidsnetwerk aan het op orde brengen van de digitale veiligheid van deze groepen.

Bepaal van tevoren met welk doel je gegevens wil verzamelen, welke gegevens je daarvoor nodig hebt (dat kunnen anonieme gegevens zijn), en hoe en waar je die gegevens gaat vastleggen voor analysedoeleinden. Houd hierbij rekening met de privacyregels van de AVG en de wensen van het deelnemende bedrijf.

Dit is een uitgave van
Digital Trust Center
Ministerie van Economische
Zaken en Klimaat Bezoekadres
Bezuidenhoutseweg 73
2594 AC Den Haag
Telefoonnummer: 070-379 8911

Postadres
Postbus 20401
2500 EK Den Haag

www.rijksoverheid.nl/ezk