Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Start een regionale samenwerking

Handreiking

Stappenplan regionale samenwerking

Om aan de slag te gaan met het versterken van je regionale samenwerking, heeft het NCSC samen met zijn partners een handreiking opgesteld. In deze handreiking worden aan de hand van drie fases concrete stappen genoemd om tot een succesvolle regionale samenwerking te komen.

Fase 1: **Verkennen**

Neem de tijd voor essentiële ontwerpkeuzes:

- Ga op zoek naar enthousiaste organisaties die beweging binnen de regio kunnen aanjagen.
- Organiseer een startbijeenkomst voor de kopgroep.
- Ga het gesprek aan over doelen, ambities en behoeften.

Fase 2: **Ontwikkelen**

Toets de ideeën in een bredere groep en vergroot het draagvlak:

- Maak kennis en verdiep je in verschillende organisaties binnen het regionale ecosysteem.
- Organiseer de besluitvorming, de (mogelijke) financiering en de capaciteit.
- Verzeker het initiatief van intern en extern draagvlak.

Fase 3: **Uitbouwen**

Bouw de kopgroep uit tot een interactieve community en ga over tot actie:

- Stel een planning op met daarin de activiteiten voor het komende jaar.
- Bouw verder aan de cybersecurity community binnen het regionale ecosysteem.
- Haal inspiratie uit activiteiten van andere regionale samenwerkingen.

Start een regionale samenwerking

Samenwerken binnen een regionaal ecosysteem is een uitstekend middel om via een netwerk van relaties de digitale weerbaarheid van je organisatie te vergroten. En daarmee ook andere organisaties in je regio veiliger te maken.

Vertrouwen, het belangrijkste ingrediënt voor uitwisseling van kennis en ervaring over cybersecurity, kun je vaak snel opbouwen en onderhouden dankzij de fysieke nabijheid. Samenwerking binnen je regionale ecosysteem is daarom vaak kansrijk. In deze handreiking vind je ervaringen van verschillende regionale ecosystemen in het cybersecuritydomein in Nederland.

Doelgroep

Deze handreiking is bedoeld voor bedrijven en organisaties die binnen de regio samen willen werken aan het verbeteren van de digitale weerbaarheid.

Aan deze handreiking hebben bijgedragen

Cybersecurity Center Maakindustrie, Cybersafety Noord-Nederland, Cyber Synergie Schiphol Ecosysteem (CYSSEC), Cyber Weerbaarheidscentrum Brainport (CWCB), Eindhoven Cyber Security Group (ECSG) en FERM-Rotterdam.

Deze handreiking is tot stand gekomen door samenwerking tussen

het Nationaal Cyber Security Centrum (Ministerie van Justitie en Veiligheid) en het Digital Trust Center (Ministerie van Economische Zaken en Klimaat).

"Organisaties moeten eerst bewust worden van het feit dat ze digitaal weerbaarder moeten worden voordat ze het nut en de noodzaak van een dergelijk initiatief zullen inzien."

CYSSEC

Wat is een regionaal ecosysteem?

Een regionaal ecosysteem is afgeleid van een natuurlijk ecosysteem. Een natuurlijk ecosysteem bestaat uit een netwerk van relaties tussen levende organismen en wordt gekenmerkt door een dynamisch evenwicht, zelfherstellend vermogen en veerkracht om verstoring tot op zekere hoogte op te vangen. Vergelijkbaar daarmee is het 'cyber'-ecosysteem,[1] dat uit een groot aantal verschillende groepen bestaat – private bedrijven, overheden, individuen, processen en slimme apparaten – die met elkaar interacteren voor diverse doeleinden. Deze verschillende groepen zijn van elkaar afhankelijk door verbonden informatie-infrastructuren, processen, data en communicatietechnologieën.[2]

In een ecosysteem is het delen van informatie zowel een kans als een bedreiging. Aan de ene kant zorgt de uitwisseling van informatie en koppeling van systemen en processen voor nieuwe mogelijkheden om effectiviteit en efficiëntie te verbeteren en biedt het de mogelijkheid om nieuwe producten te ontwikkelen. Aan de andere kant zorgt deze kans voor een vergroting van het aanvalsoppervlak, meer potentiële kwetsbaarheden en andere uitdagingen om de beschikbaarheid, integriteit en vertrouwelijkheid van ICT te waarborgen.

In de sterk gedigitaliseerde samenleving is het daarom niet meer genoeg om alleen te denken aan je eigen digitale veiligheid. Je moet dus zowel investeren in het versterken van de digitale weerbaarheid van je eigen organisatie, maar ook in die van de regio waarin je opereert.

"Binnen het ecosysteem van de haven van Rotterdam zijn veel bedrijven zijn op een of andere manier verbonden met elkaar. Zowel fysiek als digitaal. Een verstoring kan grote gevolgen hebben voor het proces om vlot en veilig schepen te laten binnenkomen en uitgaan en uiteraard ook vlot en veilig te laden en lossen. Wij verbinden ons online én offline om zo samen de digitale veiligheid van onze bedrijven en onze havenstad te waarborgen. Wij zijn FERM. Geen afkorting, maar de Rotterdamse vertaling van resilience."

FERM-Rotterdam

Een regionaal ecosysteem bestaat uit organisaties die, naast het feit dat zij in een bepaalde regiozijn gevestigd, ook iets anders gemeenschappelijks hebben. Vanwege die gezamenlijke belangen in één regio is samenwerking nodig om een digitaal weerbaar ecosysteem te creëren. Dat je daarvoor verder moet kijken dan de grenzen van je eigen organisatie is essentieel. Alleen dan kun je in de regio gezamenlijk digitale dreigingen het hoofd bieden.

Waarom ga je samenwerken binnen je regionale ecosysteem?

Samenwerking binnen een regionaal ecosysteem zorgt voor:
- verbeteren van je eigen digitale weerbaarheid én die van je partners binnen de regio door te leren van elkaar;
- vergroten van het bewustzijn voor digitale dreigingen binnen het regionale ecosysteem;
- voorkomen van verstoringen van de bedrijfscontinuïteit, verlies van gevoelige data of andere (reputatie)schade door elkaar tijdig op de hoogte te brengen van mogelijke aanvallen, gebruik te maken van expertise van collega's en samen oplossingen in te kopen;
- een netwerk van specialisten nabij dat in het geval van een incident jouw situatie en type organisatie begrijpt;
- verbeteren van het vestigingsklimaat en het behouden van specialisten in de regio door een rijk scala aan uitdagende werkzaamheden te bieden in het cybersecuritydomein;
- creëren van een veilige omgeving waarin partners waardevolle informatie met elkaar kunnen delen;
- zicht hebben op de afhankelijkheden van andere organisaties en systemen binnen het ecosysteem, waardoor je maatregelen kunt nemen om risico's te verminderen.

"De wereld om ons heen is veranderd en wij hebben dat met elkaar nog lang niet genoeg in de gaten. Security moet voor iedereen begrijpbaar en toegankelijke zijn."

Cybersafety Noord-Nederland

1 https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf

2 https://www.ey.com/Publication/vwLUAssets/cyber_ecosystem/$FILE/EY-Insights_on_GRC_Cyber_ecosystem.pdf

Hoe start je een samenwerking binnen je regionale ecosysteem?

Voor goede samenwerking moeten de basismaatregelen binnen je eigen organisatie om digitale dreigingen het hoofd te bieden op orde zijn.[3]

De uitdaging bij de start van een regionaal ecosysteem in het cybersecuritydomein is om alle kennis en expertise samen te brengen. Er is vaak al meer aanwezig dan je denkt. Door de handen ineen te slaan kun je die kennis en expertise naar een hoger niveau brengen

Wil je ook de bedrijfscontinuïteit waarborgen, moet je echt verder kijken dan wat je binnen je eigen organisatie kunt realiseren. Gaat het mis omdat zich een incident voordoet met impact op meerdere organisaties binnen het regionale ecosysteem, dan wil je daarvan snel kunnen herstellen. Dit is de essentie van samenwerken in een regionaal ecosysteem.

De volgende concrete stappen kunnen helpen bij het opzetten van een samenwerking binnen je regionaal ecosysteem. De volgorde van stappen kan voor elk samenwerkingsverband anders zijn; samenwerken is tenslotte maatwerk.

"CWCB is ontstaan om ook de kleine (start-ups en MKB) toeleveranciers in hun keten te helpen meer weerbaar te worden tegen cyberaanvullen. We zijn gestart met 11 (van start-ups tot multinationals) en groeien gestaag door."

Cyber Weerbaarheidscentrum Brainport

3 https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2018.html

Fase 1: Verkennen

Neem de tijd voor essentiële ontwerpkeuzes

Een belangrijke succesfactor voor het opstarten van regionale samenwerking is de bereidheid van enkele organisaties om als 'trekker' van de samenwerking te fungeren. Bijvoorbeeld door tijd en middelen beschikbaar te stellen om de samenwerking te laten starten.

"De kunst is om je aan te passen bij het volwassenheidsniveau van de diverse organisaties en hen te overtuigen van het nut en de noodzaak van cybersecurity. CYSSEC zoekt graag persoonlijk contact met organisaties om er achter te komen waar de organisaties binnen het ecosysteem behoefte aan hebben."

CYSSEC

Ga op zoek naar enthousiaste organisaties

Vooral organisaties die een beweging kunnen veroorzaken en een breed bereik hebben binnen het regionale ecosysteem en daarbuiten zijn geschikt als trekker. Houd in deze voorbereidende fase de kopgroep klein. In een kleine kopgroep kan snel een bepaalde mate van vertrouwen worden bereikt, waarmee het vertrouwen van andere organisaties in de regio wordt gewekt. Dan zal men zich eerder geneigd voelen zich aan te sluiten dan als de kopgroep te veel verschillende branches en sectoren omvat.

Kandidaten voor de kopgroep zijn bijvoorbeeld:
- de Rijksoverheid, provincies en gemeenten;
- veiligheidsregio's;
- politieregio's;
- grote bedrijven binnen de regio;
- banken en verzekeraars;
- branche- en belangenorganisaties;
- ondernemersverenigingen;
- regionale ontwikkelmaatschappijen.

Je kunt tijdens netwerkbijeenkomsten en conferenties bij collega's van deze organisaties informeren of er interesse is voor regionale samenwerking in het cybersecuritydomein. Ook kun je gebruik maken van bestaande samenwerkingsverbanden binnen je regio, die bijvoorbeeld gericht zijn op fysieke veiligheid of innovatie. Maak hierbij dan wel duidelijk afspraken wie voor welke werkvelden verantwoordelijk is. Aansluiting bij een bestaand samenwerkingsverband kan een goede manier zijn om je ambities te realiseren.

Je kunt het idee van regionale samenwerking in een ecosysteem op kleine schaal eens bespreken met een collega. Of je houdt een presentatie over regionale samenwerking in cybersecurity binnen je eigen organisatie. Gebruik voor bewustwording van het

probleem cijfers over digitale dreigingen, economische schade van digitale aanvallen en voorbeelden van recente incidenten.[4] Je kunt ook de bestaande succesvolle samenwerkingsverbanden binnen ecosystemen in Nederland als voorbeeld gebruiken.

"Belangrijk in het begin is om alle neuzen dezelfde kant op te krijgen - dit kost tijd en heel veel uitleggen. Wat helpt is dat je aanhaakt bij bestaande samenwerkingsverbanden. Wij hebben gebruik gemaakt van het Smart Industry netwerk in Oost-Nederland (BOOST) waar bedrijven al nauw samenwerken met de (lokale) overheid, belangenorganisaties en kennisinstellingen."

Cybersecurity Center Maakindustrie

"ECSG is ontstaan door bij de bestaande Eindhovense Fabrikanten Kring (circa 70 directeuren) op te roepen om een samenwerkingsverband op het gebied van cybersecurity te starten."

Eindhoven Cyber Security Group

Organiseer een startbijeenkomst voor de kopgroep

Als je organisaties bereid hebt gevonden om aan de slag te gaan, plan je een eerste bijeenkomst in. Deze kan informeel van aard zijn. Neem tijdens deze bijeenkomst van de kersverse kopgroep de tijd om elkaar beter te leren kennen en elkaars drijfveren en belangen in kaart te brengen.

Begin in deze eerste bijeenkomst al met het inkaderen van uitdagingen. Probeer zoveel mogelijk overeenstemming te bereiken en ga het gesprek aan over:

Doelen en ambities van de samenwerking

- Wat is de reden om tot actie over te gaan?
- Wat wil je als organisatie zelf met de samenwerking bereiken en welke rol wil je hierin spelen?
- Wat wil je gezamenlijk bereiken met de samenwerking?
- Wat zijn overtuigende argumenten voor andere organisaties zich aan te sluiten?
- Wat zijn op korte termijn de doelen en volgende stappen?

Behoeften en verbindende factoren

- Waar heeft jouw eigen organisatie behoefte aan?
- Waar hebben andere organisaties in het regionale ecosysteem behoefte aan?
- Wat verbindt organisaties in het regionale ecosysteem?
- Welke gezamenlijke digitale uitdagingen spelen er binnen het regionale ecosysteem?
- Worden er veel vergelijkbare systemen gebruikt? Zijn organisaties fysiek of digitaal aan elkaar verbonden? Welke afhankelijkheden zijn bekend?
- Wat is een realistische, haalbare en logische omvang van de samenwerking?
- Hoe zit het met het volwassenheidsniveau op het gebied van cybersecurity binnen het regionale ecosysteem?

"We zijn in Oost Nederland gestart met een kleine kern en vandaar uit zijn we gaan uitbreiden en mensen gaan enthousiasmeren. Ook hebben we heel veel gewerkt met intentieverklaringen om zo veel mogelijk potentiële leden als potentiële investeerders te bereiken."

Cybersecurity Center Maakindustrie

Stakeholder- omgevingsanalyse

Voer een beknopte stakeholder- en omgevingsanalyse uit om een eerste beeld te krijgen van stakeholders en bestaande samenwerkingen binnen de regio. Gebruik hiervoor de volgende vragen:

- Wie zijn de belangrijkste stakeholders binnen het regionale ecosysteem op het gebied van cybersecurity?
- Ken je cybersecurityspecialisten bij andere organisaties die mee willen denken of zeker betrokken moeten worden?
- Zitten de juiste mensen aan tafel?
- Waar begint en eindigt het regionale ecosysteem? Hoeveel organisaties zijn dat?
- Welk type organisaties sta je in eerste instantie toe om deel te nemen? Richt het samenwerkingsverband zich op grote bedrijven, MKB, start-ups of een combinatie hiervan?
- Zijn er mogelijkheden om het regionale ecosysteem in te delen in (sub)sectoren, ketens of volwassenheidsniveaus?
- Zijn er bestaande samenwerkingsverbanden of andere regionale organisatievormen die als vehikel gebruikt kunnen worden?

Minimaliseer de ambities in het begin. Te veelomvattende ambities in de beginfase kunnen ervoor zorgen dat organisaties snel afhaken. Grote ambities zijn moeilijker en meestal pas op langere termijn te realiseren en vragen veel geld en tijd. Start door je concreet te richten op de huidige behoefte en koppel hier activiteiten aan die een tastbaar resultaat opleveren. Het vieren van successen, al zijn ze nog zo klein, draagt bij aan het groepsgevoel.

"Start met een kleine groep en geef elkaar meteen concreet advies over wat vandaag speelt. Zo heb je meteen tastbaar resultaat en toegevoegde waarde. Samen met goede spelregels en een structurele opzet volgt de rest vanzelf."

Cyber Weerbaarheidscentrum Brainport

4 Zie bijvoorbeeld het Cybersecuritybeeld Nederland 2018: https://www.ncsc.nl/csbn.

Fase 2: Ontwikkelen

Toets de ideeën in een bredere groep en vergroot het draagvlak

Ga als kopgroep van start met een kennismakingsronde op basis van de stakeholders- en omgevingsanalyse. Ga open het gesprek in en zorg ervoor dat alles wat inmiddels bekend is over ambities, doelen en behoeften bij de andere organisaties in de kopgroep wordt meegenomen.

Zorg dat meer organisaties zich aansluiten bij de samenwerking

Breid de kopgroep stap voor stap uit met enthousiaste organisaties die ook iets willen bijdragen. Maak bijvoorbeeld een flyer of een presentatie met korte uitleg over het initiatief. Presenteer dit tijdens een netwerkbijeenkomst in de regio. Daarmee kun je andere organisaties enthousiasmeren en motiveren om ook actief te gaan bijdragen aan het initiatief. Gebruik een voorbeeld van de impact van een incident op de eigen organisatie, waarin de onderlinge afhankelijkheden worden toegelicht en mogelijke gevolgen voor de regio. Daarmee geef je nieuwe organisaties een reden om te investeren in het regionale ecosysteem.

Of bedenk een fictief scenario om de impact van een cybersecurity-incident binnen het regionale ecosysteem tastbaar te maken.

Tegelijkertijd is het belangrijk om met de kopgroep stil te staan bij de sturing van de samenwerking. Er moet voldoende draagvlak zijn bij de deelnemende organisaties om het regionale ecosysteem verder uit te bouwen en te handhaven

Organiseer besluitvorming, financiering en capaciteit

Zorg ervoor dat individuele organisaties uit de kopgroep capaciteit (uren, medewerkers) vrijmaken om tijd te besteden aan het opzetten van de samenwerking en om zaken in beweging te krijgen. Met gesloten beurzen kan al veel bereikt worden in deze fase. Zodra de eerste successen zichtbaar worden en organisaties zien dat het iets oplevert, zullen ze eerder geneigd zijn bij te dragen met financiële middelen. Bespreek met de kopgroep de volgende vragen:

Taken, rollen en sturing

- Wie is of zijn de trekker(s) van de samenwerking? Zijn dit alle organisaties die nu aan tafel zitten in de kopgroep?
- Hebben alle organisaties binnen de kopgroep invloed op de koers en resultaten van het initiatief?
- Welke rollen willen de betrokken organisaties vervullen?
- Wie gaat het project trekken en wie heeft invloed op de koers?
- Aan wie moeten de trekkende partners verantwoording afleggen voor keuzes die gemaakt worden? En hoe leg je die verantwoording af?

Financiering en capaciteit

- Kunnen alle organisaties die nu aan tafel zitten een even grote bijdrage leveren en daadwerkelijk een trekkende rol op zich nemen?
- Hoe worden de werkuren geregeld die nodig zijn om over te gaan tot actie? Leg je gezamenlijk een bedrag in, is er een deelnemer die (het begin) kan en wil financieren of lever je capaciteit?
- Is de bijdrage voor elk lid van de kopgroep gelijk of zijn er enkele trekkende partners binnen de kopgroep met een flexibele schil van samenwerkingspartners?
- Is er capaciteit beschikbaar bij een of meerdere organisaties binnen de kopgroep? Of wordt de capaciteit elders ingekocht?

Sluit aan bij wat er al is, zodat onnodige overlap wordt voorkomen en afstemming beter kan verlopen. Het is gemakkelijker om op basis van een goede start tijd en geld beschikbaar te krijgen dan voor iets dat zich nog moet bewijzen.

"Zet cybersecurity ook als (potentiële) kans neer en heb het niet alleen maar over de kwetsbaarheid. Dat schrikt mensen die weinig affiniteit hebben met het onderwerp af."

Cybersecurity Center Maakindustrie

"Advies: niet zo moeilijk doen. Gewoon mensen bij elkaar roepen en elkaar laten informeren en helpen. Je creëert dan meteen enthousiasme waardoor deze mensen hun directie meekrijgen en er zelf ook tijd en andere middelen in gaan stoppen."

Cyber Weerbaarheidscentrum Brainport

Verzeker het initiatief van intern en extern draagvlak

Draagvlak en steun bij ieder van de deelnemende organisaties op verschillende niveaus is belangrijk. Uit ervaring blijkt dat dit het samenwerkingsverband een extra zet in de goede richting geeft. Daarvoor is nodig om inzicht te krijgen in hoe de samenwerking bijdraagt aan het verhogen van de digitale weerbaarheid van je eigen organisatie en van het regionale ecosysteem als geheel. Maak concreet en zichtbaar welke meerwaarde je kunt betekenen voor de desbetreffende organisaties. Idee, doel en ambitie moeten gedragen worden door het management, zodat tijd, geld en middelen daadwerkelijk kunnen worden ingezet.

Als draagvlak op verschillende niveaus is gerealiseerd, moet het worden geformaliseerd door gezamenlijke start- of intentieverklaring te tekenen. Ook een startevenement of op een andere manier de publiciteit zoeken is een goede gelegenheid om de samenwerking zichtbaar te maken. Openbare ondertekening van de intentieverklaring tijdens zo'n startevenement helpt om organisaties te enthousiasmeren zich ook aan te sluiten.

"Om het bereik te vergroten hebben we een aantal bijeenkomsten georganiseerd voor bedrijven, lokale media benaderd en een aantal belangrijke 'voortrekkersbedrijven' in de regio benaderd om het belang van het initiatief binnen hun netwerk te delen. Daarnaast heeft de gedeputeerde van de provincie Overijssel zich hard gemaakt om bij (grote) investeerders binnen te komen t.b.v. private financiering."

Cybersecurity Center Maakindustrie

Zorg dus voor aandacht in de regio. Denk aan:

- Benoem iemand tot 'gezicht' en aanspreekpunt binnen en buiten het regionale ecosysteem, zoals de Port Cyber Resilience Officer voor FERM-Rotterdam door de Havenmeester vervuld.
- Maak een website en zorg voor actuele informatie en regelmatige updates over het samenwerkingsverband en de voortgang in de uitbreiding (zie ook fase 3).
- Sluit je aan bij landelijke bewustwordingscampagnes op het gebied van cybersecurity om meer zichtbaarheid te realiseren, bijvoorbeeld via Alert Online.[5]
- Organiseer een eigen evenement rondom een actueel thema dat de aandacht trekt in de regio, bijvoorbeeld een hackathon voor kinderen.
- Leg contact met ecosystemen die al verder gevorderd zijn en wissel daarmee ervaringen uit over het op de kaart zetten van een regionaal ecosysteem.

"Houd de start van de samenwerking vooral zo praktisch mogelijk. Tuig niet een heel sturingsmodel op, maar maak wel duidelijk wie je waarop kan aanspreken zodat er wel voortgang in de samenwerking zit. Denk daarbij ook aan het organiseren van een verantwoordelijke die de aanjagende en faciliterende rol op zich neemt."

NCSC

Fase 3: Uitbouwen

Bouw de kopgroep uit tot een interactieve community

In de vorige fase heb je met de kopgroep de eerste contouren van het initiatief bepaald en trekkende partners gevonden die tijd, geld en/of middelen beschikbaar stellen om aan de slag te gaan. Nu is het tijd om over te gaan tot actie. Leg de lat niet meteen te hoog, durf nieuwe ideeën te testen, blijf openstaan voor feedback en pas je plannen aan waar nodig.

Ervaring leert dat het eerste jaar vooral draait om het opbouwen van het netwerk binnen het regionale ecosysteem. De deelnemende organisaties willen elkaar en elkaars behoeften beter leren kennen en stap voor stap het cybersecuritybewustzijn bij de eigen organisatie verhogen. Hoe het initiatief verder gestructureerd kan worden en hoe je een community bouwt vormen de aandachtspunten in fase 3.

Stel samen een roadmap op voor het regionale ecosysteem

Ga op zoek naar een gezamenlijke visie. Start met het opstellen van een roadmap met een schets van de activiteiten die je in het eerste jaar wilt uitvoeren. Deze schets moet steeds weer worden getoetst bij de organisaties in het regionale ecosysteem en aangescherpt en bijgesteld. Een samenwerking gaat gepaard met vallen en opstaan. Dat hoort er bij. Wees je ervan bewust dat niet elke activiteit meteen aanslaat. Sta daarom open om te leren van feedback van andere organisaties binnen het samenwerkingsverband. Plannen kunnen veranderen door omstandigheden, wees dus flexibel om mee te bewegen.

De roadmap kun je indelen volgens de incident response cirkel (prevent, detect, respond, recovery), maar ook op basis van de verschillende niveaus van kennis en ervaring die tijdens de verkenning naar voren kwamen. Bedenk ook dat niet iedereen overal aan mee hoeft te werken. Beter is om gebruik te maken van de energie van organisaties rond thema's waar ze het meeste belang bij hebben.

Voer activiteiten uit die passen bij het niveau en de fase waar de regio en het samenwerkingsverband zich in bevindt. Stel dat een ambitie is geformuleerd om een CSIRT[6] op te richten. Dit vraagt echter een hoog volwassenheidsniveau en onderling vertrouwen van deelnemende organisaties. Over het algemeen is dit niet realistisch in het eerste jaar.

5 Zie https://www.alertonline.nl voor meer informatie.

6 Zie www.ncsc.nl/samenwerking voor meer tips over het opzetten van een collectief CSIRT.

Neem de tijd om goed overzicht en inzicht te krijgen in wat er speelt de regio, zodat activiteiten daadwerkelijk aanslaan en resultaten opleveren. Presenteer de voortgang periodiek aan de kopgroep, zodat deze de grote lijnen kan bewaken en overzicht kan houden over de activiteiten.

Bouw verder aan de cybersecurity community binnen je regionale ecosysteem

Vier je successen, hoe klein ook, met de organisaties binnen het samenwerkingsverband. Zichtbare successen en tastbare resultaten helpen om intern draagvlak te creëren, zodat stakeholders gemobiliseerd worden en de ontwikkeling van het regionale ecosysteem op gang te houden.

"Betrek vooral ook het onderwijs bij je activiteiten. Zowel MBO als HBO. Zorg ervoor dat je binnen het onderwijs een vast aanspreekpunt hebt die meedenkt en mee ontwikkelt. Een win-win voor onderwijs en bedrijfsleven."

Cybersafety Noord Nederland

Om het bouwen van de community en verdere samenwerking te versterken is een website een goed middel.[7] Op een website kun je verschillende soorten informatie presenteren, zoals:

- grote en kleine successen;
- agenda met bijeenkomsten en events;
- tips & trucs voor cybersecurity;
- tools en scans;
- cybersecuritynieuws;
- openbare kennisproducten.

"Uit onze praktijk blijkt dat voor een website en platform het belangrijk is dat het gebruiksgemak hoog is en het praktische en pragmatische informatie moet bieden. Het kan lonen om aan te sluiten bij bestaande platformen of gebruik te maken van bestaande informatie."

CYSSEC

Zo'n platform kan uitgroeien tot een beveiligde omgeving voor het uitwisselen van (vertrouwelijke) informatie tussen organisaties onderling. Men kan informatie halen en brengen en het vormt een communicatiekanaal voor alle deelnemende organisaties.

Haal inspiratie uit activiteiten van anderen

De volgende activiteiten zijn voorbeelden uit bestaande regionale ecosystemen. Deze suggesties zijn ter inspiratie om je eigen initiatief kleur en invulling te geven. Je kunt ze ook gebruiken als kapstok om de samenhang binnen je eigen initiatief in te richten.

Organiseer bijeenkomsten over cybersecurity

Organiseer regelmatig bijeenkomsten voor het netwerk. Nodig een of meer aansprekende sprekers uit (specialisten in cybersecurity, trekkers van andere regionale ecosystemen) en kies een thema uit dat past en leeft bij de deelnemers. Deze bijeenkomsten helpen om bewustwording en draagvlak te creëren en een community te realiseren rond cybersecurity.

"Wat hebben wij geleerd van het organiseren van de Cyber roadshow: sluit vooral aan bij bestaande bijeenkomsten. Vooral de MKB-er komt niet 'speciaal' voor cyber security - tenminste het overgrote deel niet."

Cybersafety Noord-Nederland

"De meest succesvolle sessies organiseren wij met partijen uit het ecosysteem zelf. Zo krijgen zij de kans om hún ideeën, problemen of kennis te delen. Bovendien krijg je zo inzicht in wat er speelt en creëer je echte, waardevolle samenwerking."

CYSSEC

"De Port Cybercafe's zijn een knooppunt voor de ondernemers in de haven. Samen het glas heffen en ook nog een interessant, inhoudelijk programma meemaken over praktische cyberonderwerpen die spelen in het Havengebied zoals storagespoofing. Zo versterken we niet alleen het digitale netwerk, maar ook het sociale netwerk."

FERM-Rotterdam

7 Zie https://ferm-rotterdam.nl, https://cyssec.nl en www.digitaltrustcenter.nl voor meer informatie.

Organiseer een gezamenlijke oefening met het regionale ecosysteem

Het kan lonen om gezamenlijk te oefenen met ketens of andere groepen die digitaal of fysiek van elkaar afhankelijk zijn binnen de regio.[8] Dit hoeft geen grootschalige ICT-crisisoefening te zijn; een table-top-oefening waarin een scenario wordt nagespeeld is ook een krachtig instrument.

"De oefening Cybernautics wordt in 2018 voor de tweede keer georganiseerd. Hierin werken partners uit het nautische proces nauw met elkaar samen om een cybercrisis het hoofd te bieden. Deze oefening wordt binnen het ecosysteem zeer gewaardeerd."[9]

FERM-Rotterdam

In geval van een incident moet je snel kunnen handelen. Dat kan alleen als je er vooraf over nagedacht hebt, elkaar kent en directe toegang tot elkaar hebt. Ook helpt het als je eerder samen geoefend hebt, zodat je bekend bent met de crisisaanpak. Idealiter vindt een dergelijke cyberoefening periodiek plaats. Zodat er routine in ontstaat bij de betrokkenen. Op termijn vormt oefenen met de crisisaanpak een geschikte basis om heldere afspraken te maken over samenwerking tijdens een ICT-incident.

Stimuleer informatie-uitwisseling binnen het regionale ecosysteem

Het Information Sharing and Analysis Centre (ISAC) model[10] is geschikt om onderling informatie uit te wisselen op basis van vertrouwen, gedeelde belangen en gelijkwaardigheid. Deze drie waarden zijn de basis voor uitwisseling van bedrijfsgevoelige informatie.

Scan

Maak een scan van de ICT-systemen, hardware en software en neem daar de werkprocessen en de mensen in mee. Organiseer de scan bij zoveel mogelijk deelnemers. Waar zitten de zwakke plekken? Of schaf gezamenlijk een laagdrempelig self-assessment-tool of -scan aan, zodat deelnemende organisaties zelf kunnen zien of ze hun basis op orde hebben en hoe digitaal veilig ze zijn.

Organiseer de uitvoering van 'friendly hacks' bij de deelnemers

Met een zogenoemde 'friendly hack' krijg je een goed beeld van de status van de beveiliging van een bedrijf. Daarbij kan, gratis of tegen gereduceerd tarief, een betrouwbare en deskundige organisatie onderzoek doen naar de website en de ICT-omgeving van de partner in het ecosysteem.

De lessen uit deze friendly hack kan het bedrijf gebruiken om de eigen veiligheid te vergroten. Immers, als een deelnemende organisatie in het regionale ecosysteem zelf veiliger wordt, heeft dat een positief effect op de andere organisatie.

Op de website van het Digital Trust Center[11] staan voorbeelden van samenwerkingsverbanden in regionale ecosystemen en hun planning voor de komende jaren.

8 Zie www.ncsc.nl/samenwerking voor een handreiking over ketensamenwerking met meer suggesties over oefenen binnen de keten.

9 https://ferm-rotterdam.nl/nl/nieuws/cybernautics2017-rotterdamse-haven-oefent-cyberweerbaarheid

10 Zie www.ncsc.nl/samenwerking voor een handreiking over het opzetten van een ISAC voor meer informatie.

11 Kijk op www.digitaltrustcenter.nl/netwerken-cyberweerbaarheid.

Uitgave
Nationaal Cyber
Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl/samenwerking
samenwerken@ncsc.nl
@ncsc_nl

Oktober 2018