Ministerie van Economische Zaken
en Klimaat

Informatiedeling binnen de keten

Interactievormen & taken en rollen – de methode

1. Inleiding

De verregaande digitalisering van de laatste decennia heeft het dagelijks leven en de economie in hoog tempo veranderd. Naast economische kansen leiden deze ontwikkelingen ook tot nieuwe kwetsbaarheden en ruimte voor nieuwe vormen van criminaliteit, zoals digitale bedrijfsspionage of afpersing. Om de Nederlandse samenleving weerbaarder te maken tegen deze cyberdreigingen, kan het delen van cybersecurity informatie tussen organisaties helpen. Cybersecurity informatiedeling (CSID) helpt organisaties risico's beter in te kunnen schatten en passende maatregelen te treffen. De overheid heeft daarom in de Nederlandse Cyber Security Agenda de ambitie uitgesproken om een Landelijk Dekkend Stelsel (LDS) voor cybersecurity informatiedeling te willen ontwikkelen.

Er zijn meerdere initiatieven ondernomen om het LDS vorm te geven. Voor de bescherming van de vitale infrastructuur zijn een aantal jaar terug diverse Information Sharing & Analysis Centers (ISACs) opgericht om cybersecurity informatiedeling te stimuleren. Deze ISACs worden ondersteund door het Nationaal Cyber Security Centrum (NCSC). Het succes van de ISACs heeft zich vertaald in de vraag ook voor het niet-vitale bedrijfsleven een structuur op te zetten waarin cybersecurity informatie gedeeld kan worden. Hiertoe is in 2018 het Digital Trust Center (DTC) opgericht. Het DTC draagt bij aan de inrichting van het LDS door cybersecurity informatie aan te bieden en cybersecurity samenwerkingsverbanden tussen organisaties te stimuleren.

TNO innovation for life

digital trust center.

Praktische methode voor het inrichten, ontwikkelen en verbeteren van CSID

IIn het kader van de hierboven geschetste ontwikkelingen, heeft het DTC aan TNO gevraagd onderzoek te doen naar CSID voor het niet-vitale bedrijfsleven. Het doel van het onderzoek is om ondersteuning te bieden aan het DTC en de via het DTC gevormde samenwerkingsverbanden bij het inrichten, ontwikkelen en verbeteren van cybersecurity informatiedeling. In 2018 is hiertoe een viertal notities opgeleverd bij het DTC.1 In 2019 heeft het onderzoek verder vorm gekregen, waarbij drie aspecten van cybersecurity informatiedeling zijn onderzocht:

- Soorten cybersecurity informatie
- Interactievormen
- Rollen & taken

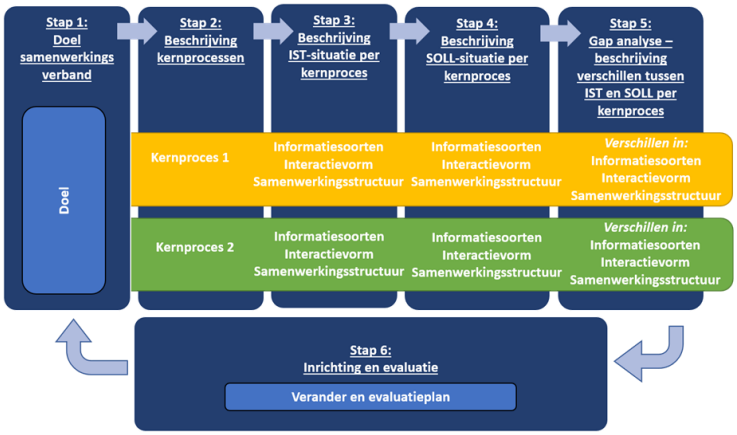
Deze aspecten zijn gekozen in samenspraak met het DTC en hebben geresulteerd in het rapport "Cybersecurity informatiedeling voor DTC Samenwerkingsverbanden". Binnen het rapport is de 'Methode voor het (door)ontwikkelen van cybersecurity informatiedeling binnen DTC samenwerkingsverbanden' opgezet. De methode kent zes stappen. Aan de hand van deze zes stappen kan cybersecurity informatiedeling worden geanalyseerd en (door)ontwikkeld. De methode is ontwikkeld gedurende een iteratief proces met vier DTC samenwerkingsverbanden. Deze vier samenwerkingsverbanden zijn als cases opgenomen in het rapport. In deze samenvatting wordt kort beschreven wat de methode is, wat de gemene deler is in de bestudeerde cases, welke rollen en taken een samenwerkingsverband kan inrichten, en worden conclusies en aanbevelingen gedaan.

2. Toelichting methode voor het (door)ontwikkelen van CSID binnen DTC samenwerkingsverbanden

De *Methode voor het (door)ontwikkelen van cybersecurity informatiedeling binnen DTC samenwerkingsverbanden* ondersteunt een stapsgewijze analyse van cybersecurity informatiedeling binnen een samenwerkingsverband:

- Zowel het DTC als de samenwerkingsverbanden kunnen de methode gebruiken om cybersecurity informatiedeling in kaart te brengen en te professionaliseren.
- Het DTC kan de methode inzetten als toetsinstrument voorafgaand aan de subsidieverstrekking en als statuscheck in de lopende subsidies.

Onderstaande figuur geeft een overzicht van de methode, bestaande uit zes stappen. Deze stappen worden vervolgens kort toegelicht. Verdere informatie om met de methode aan de slag te gaan (zoals voorbeeldvragen, tabellen, en bronnen) is beschikbaar in het rapport *Cybersecurity informatiedeling voor DTC Samenwerkingsverbanden*, dat opvraagbaar is bij het DTC.



Figuur 1: Stappen in de methode cybersecurity informatiedeling, TNO, 2020

[1] Twee van de vier notities zijn beschikbaar gesteld op de website van het DTC, URL: https://www.digitaltrustcenter.nl/factsheets-informatiedeling-binnen-de-keten. De overige documenten zijn opvraagbaar bij het DTC.

Stap 1: Wat is het doel van het samenwerkingsverband?

In de eerste stap wordt het doel van het samenwerkingsverband beschreven. In deze beschrijving wordt opgenomen wat de partijen die gaan samenwerken willen bereiken en waarom dit belangrijk is.

Stap 2: Wat zijn de kernprocessen?

In de tweede stap identificeren deelnemers van een samenwerkingsverbanden gezamenlijk de kernprocessen en de beoogde resultaten van elk kernproces. Kernprocessen zijn activiteiten die bijdragen aan de realisatie van het doel van het samenwerkingsverband. De kernprocessen zijn afgeleid van het doel. Het zijn de processen waar samenwerkingsverbanden veel capaciteiten voor vrijmaken. [2] Vanwege de scope van het onderzoek zijn kernprocessen die zich niet richten op cybersecurity informatiedeling buiten beschouwing gelaten.

Stap 3: Hoe ziet de huidige informatiedeling in het samenwerkingsverband eruit? (IST-situatie)

De derde stap brengt per kernproces in kaart wat een samenwerkingsverband op dit moment doet aan cybersecurity informatiedeling (IST-situatie). In deze stap wordt antwoord gegeven op de volgende drie vragen:

1) welke cybersecurity informatie deelt het samenwerkingsverband? (soort informatie) [3]
2) hoe deelt het samenwerkingsverband deze informatie? (interactievorm), en
3) welke samenwerkingsstructuur gebruikt het samenwerkingsverband daarbij? (bijv. een model waarbij één partij als centraal informatiepunt fungeert, of een zelfsturend model)

Stap 4: Hoe ziet de gewenste informatiedeling in het samenwerkingsverband eruit? (SOLL-situatie)

Naast het in kaart brengen van de bestaande (IST-)situatie, is het ook belangrijk de toekomstig gewenste informatiedeling in het samenwerkingsverband in kaart te brengen (SOLL-situatie). Het in kaart brengen van de SOLL-situatie is belangrijk omdat het een duidelijk punt geeft om naartoe te werken. Om de SOLL-situatie te identificeren worden dezelfde elementen beschreven als in de IST-situatie, maar dan voor de gewenste informatiedeling in het samenwerkingsverband.

Stap 5: Wat is het verschil tussen de IST- en SOLL-situatie? (gap analyse)

De volgende stap is het uitvoeren van een gap analyse per kernproces. Een gap analyse vergelijkt de bestaande situatie met de toekomstige situatie. Daarmee wordt inzichtelijk gemaakt welke stappen het samenwerkingsverband moet zetten om de SOLL-situatie te bereiken. Hiermee wordt duidelijk of er een verschil is tussen de IST en SOLL-situatie. Er zijn vervolgens twee mogelijkheden:

1. Als er inderdaad een verschil is tussen de IST- en SOLL situatie, kan het samenwerkingsverband analyseren wat er nodig is om tot de SOLL-situatie te komen. Moet het samenwerkingsverband, gelet op de gap, bijvoorbeeld andere interactievormen opzetten om de gewenste soorten informatie te kunnen delen? Het samenwerkingsverband kan dan in stap 6 een veranderplan maken om de gap te overbruggen. Vervolgens evalueert men of het doel- en de kernprocessen nog passen bij de inrichting (zie stap 6).
2. Het kan ook voorkomen dat met de gap analyse wordt vastgesteld dat de IST- en SOLL situatie niet verschillen. Er hoeft dan geen veranderplan te komen. Ook dan blijft het van belang een evaluatie te doen.

Stap 6: Inrichting en evaluatie

Als met behulp van de gap analyse is bepaald wat er nodig is om tot de SOLL-situatie te komen, is het zaak dit te gaan inrichten. Om een verandertraject in te gaan, kan gebruik worden gemaakt van een op te stellen veranderplan. Het veranderplan bevat stappen die moeten worden gezet om een verandering door te voeren, in dit geval om een bepaalde *gap* te overbruggen. Stap 1 tot en met 4 vormen de input voor dit plan. Het plan moet concreet beschrijven hoe het samenwerkingsverband van de IST-situatie naar de SOLL-situatie komt. Daarbij wordt bijvoorbeeld

[2] Zie hoofdstuk 5 van het rapport *Cybersecurity informatiedeling voor DTC samenwerkingsverbanden* voor meer informatie over de kernprocessen per samenwerkingsverband.
[3] Zie bijlage 3 van het rapport *Cybersecurity informatiedeling voor DTC samenwerkingsverbanden* voor informatie m.b.t. de verschillen tussen strategisch en operationeel.

aangegeven wie bij het proces moet worden betrokken, hoe kennis opgebouwd moet worden en op welke termijn de SOLL bereikt zou moeten zijn.
Het ontwikkelen van een samenwerkingsverband is een continu proces. Het is daarom van belang het hele proces van de doorlopen methode ook te evalueren. Is de SOLL-situatie bereikt? Moeten het doel en de kernprocessen nog worden aangepast? De eerste stappen van de methode kunnen dan daarbij weer helpen.

3. Cases

De methode is het resultaat van een iteratief onderzoeksproces met vier samenwerkingsverbanden:

- Cybersecurity Programma Noordzeekanaalgebied (NZKG) van de Port of Amsterdam (PoA),
- Cybersecurity Centrum Maakindustrie (CCM),
- Cybersecurity Synergie Schiphol Ecosysteem (CYSSEC) en
- FERM (Rotterdamse haven).

Door middel van interviews is onderzocht hoe deze vier samenwerkingsverbanden cybersecurity informatiedeling op dit moment in de praktijk hebben ingericht (doel, kernprocessen, interactievormen en samenwerkingsstructuur in de IST-situatie). De uitkomsten zijn in een empirisch (kwalitatief) onderzoek vergeleken om gemene delers te identificeren en variaties tussen cases te analyseren. Deze inzichten kunnen andere samenwerkingsverbanden helpen in hun eigen (door)ontwikkeling. De volledige casebeschrijvingen zijn te vinden in het rapport "*Cybersecurity informatiedeling voor DTC Samenwerkingsverbanden*", op te vragen bij het DTC. Hieronder zijn aspecten van samenwerkingsverbanden samengevat en gestructureerd volgens de kenmerken van de methode.

Doel van de samenwerkingsverbanden

Alle samenwerkingsverbanden hebben een doel geformuleerd. Hoewel de bewoording daarbij verschilt, zijn de genoemde elementen van de doelen vergelijkbaar. Het doel kan voor alle samenwerkingsverbanden worden samengevat als "het cyberweerbaar maken van de doelgroep".

Kernprocessen

Elk samenwerkingsverband heeft kernprocessen geïdentificeerd. Twee kernprocessen worden door alle onderzochte samenwerkingsverbanden aangeboden: 1) het organiseren van bijeenkomsten, en 2) het beschikbaar stellen van cybersecurity informatie vanuit een centraal punt. Drie kernprocessen worden slechts door één samenwerkingsverband aangeboden, namelijk 1) de cybersecurity scan van het CCM, 2) de actiecentra van FERM en 3) het onderling delen van cybersecurity informatie in de koude fase bij het NZKG.

Interactievormen

Op dit moment delen alle samenwerkingsverbanden cybersecurity informatie via mens-mens interactie. Daarbij gaat het bijvoorbeeld om informatiedeling via website, nieuwsbrief, bijeenkomst of vragenlijst. Mens-mens interactie is voor de samenwerkingsverbanden op dit moment de beste manier om organisaties te betrekken en betrokken te houden. Op termijn is het mogelijk dat ook andere interactievormen interessant worden om toe te passen. Een eerste stap daartoe is meer informatiedeling tussen samenwerkingsverbanden en deelnemers.

Soort cybersecurity informatie

Het blijkt dat de samenwerkingsverbanden zowel strategische als operationele cybersecurity informatie delen. Het valt op dat operationele cybersecurity informatie enkel wordt gedeeld in de samenwerkingsverbanden die een kernproces hebben waarin onderling informatie wordt gedeeld. Cybersecurity informatiedeling tussen organisaties komt dus niet spontaan tot stand Verwacht wordt dat het expliciet benoemen van het delen van specifieke soorten operationele cybersecurity informatie de deelnemers activeert om hier ook naar te handelen. Dit wordt gestimuleerd omdat het delen van relevante informatie waarde creëert voor de andere deelnemers in het samenwerkingsverband en daarmee tegelijkertijd het vertrouwen in elkaar en het samenwerkingsverband laat groeien.[4]

[4] Luiijf, H.A.M. & Kernkamp, A.C. (maart 2015). *Sharing Cyber Security Information, good practice stemming from the Dutch Public-Private Participation Approach*.

Samenwerkingsstructuur

Alle samenwerkingsverbanden hanteren feitelijk een 'broker' structuur. Dit wil zeggen dat alle samenwerkingsverbanden één centrale partij of speler hebben die de informatie verzamelt en verspreidt naar deelnemers. De precieze inrichting verschilt hierbij. In de praktijk komt het echter in alle gevallen neer op informatiedeling vanuit één centraal punt.

4. Rollen en taken

Rollen en taken biedt als los bouwblok van informatiedeling een aanvulling op de stappen van de methode. Het beschrijft de rollen en taken die van toepassing (kunnen) zijn om de structuur van de samenwerkingsverbanden ten behoeve van cybersecurity informatiedeling meer invulling te geven. Daarmee krijgen de samenwerkingsverbanden een handvat om te concretiseren welke taken en rollen kunnen worden verwacht bij het inrichten van een specifiek kernproces of type informatiedeling. Voorbeelden zijn opgenomen in het rapport **Cybersecurity informatiedeling voor DTC Samenwerkingsverbanden.**

Het raamwerk waarop het bouwblok rollen en taken gestoeld is, zijn gericht op cyber specifieke rollen, taken en competenties. Het bouwblok is daarom vooral interessant voor partijen die meer cybersecurity specifieke procesactiviteiten met een cybersecurity workforce binnen hun organisatie willen ontwikkelen en meer informatie willen m.b.t. wat hiertoe moet worden ingericht. TNO adviseert deze partijen om daarom eerst de methode te doorlopen, en het bouwblok m.b.t. taken en rollen te gebruiken ten behoeve van een verdere inrichting en operationalisering van het samenwerkingsverband.[5]

5. Reflectie op de methode

Dit onderzoek heeft de "Methode voor het (door)ontwikkelen van cybersecurity informatiedeling binnen DTC samenwerkingsverbanden" opgeleverd aan het DTC. Het DTC kan met behulp van de methode ondersteuning bieden aan de doorontwikkeling van samenwerkingsverbanden. Bovenal helpt de methode samenwerkingsverbanden om cybersecurity informatiedeling in kaart te brengen en waar mogelijk door te ontwikkelen. De methode maakt een stapsgewijze analyse van de informatiedeling binnen het samenwerkingsverband mogelijk. De processtappen van de methode bieden op dit moment, in combinatie met de materialen uit de verschillende bijlagen, voldoende handvatten om de methode toe te passen. Voor verdere informatie kunnen samenwerkingsverbanden het volledige rapport opvragen bij het DTC.

De methode lijkt een bruikbaar instrument voor zowel samenwerkingsverbanden als het DTC te vormen. De methode is uniek: er zijn nog geen alternatieven die een dergelijke structuur bieden. Wel is de methode nog weinig gevalideerd. Dit komt onder andere door de grote afhankelijkheid van de huidige status van cybersecurity informatiedeling binnen de samenwerkingsverbanden, die zich gedurende het onderzoek nog veelal in de beginfase bevonden. Voor het aanscherpen van de ontwikkelde methode kan daarom verdere validatie helpen, met meer verschillende soorten samenwerkingsverbanden en met samenwerkingsverbanden die in hogere mate informatie delen. Wanneer de methode meer gebruikt gaat worden voor het (door)ontwikkelen van cybersecurity informatiedeling, wordt verwacht dat er meer *good practices* beschikbaar komen die gedeeld kunnen worden onder bestaande en startende samenwerkingsverbanden.

[5] Zie hoofdstuk 6 van het rapport *Cybersecurity informatiedeling voor DTC samenwerkingsverbanden* voor meer informatie over rollen en taken.

6. Aanbevelingen

Uit het onderzoek blijkt dat de samenwerkingsverbanden zich tot op heden vooral richten op het weerbaar maken van de doelgroep via awareness en informatieverspreiding vanuit één centraal punt. Dit vormt een goed startpunt voor verdere informatiedeling, maar onderlinge cybersecurity informatiedeling tussen deelnemers van een samenwerkingsverband is cruciaal om de relevantie van het samenwerkingsverband te vergroten. Het verhoogt de weerbaarheid van niet-vitale bedrijven en geeft bedrijven een betere situational awareness. Onderlinge informatiedeling verhoogt ook de ketenweerbaarheid: het is een manier om tot verdere analyse en duiding van cyberdreigingen, kwetsbaarheden of incidentinformatie te komen. Samenwerkingsverbanden wordt daarom aanbevolen om de cybersecurity informatiedeling (ontvangen, versturen, verrijken en duiden) verder te ontwikkelen. Dit geldt voor informatiedeling binnen het samenwerkingsverband, maar zeker ook voor informatiedeling tussen organisaties uit samenwerkingsverband en daarbuiten. Zo kan het CSID-vliegwiel na het aflopen van de subsidie blijven draaien.

Het is ook aan te bevelen de positie van IT-leveranciers bij cybersecurity informatiedeling mee te nemen. Het blijkt in de praktijk nog lastig voor samenwerkingsverbanden om IT-leveranciers (zoals bijvoorbeeld managed service providers en managed security service providers) te betrekken bij informatiedeling. Het doen van kennisopbouw en het analyseren van good practices kan hierbij helpen.

Een belangrijke voorwaarde voor het delen van informatie is vertrouwen tussen deelnemers. Samenwerkingsverbanden bouwen dit vertrouwen nu op verschillende manieren op. Onderzocht kan worden of er alternatieven zijn voor de mens-mens-interactie zoals blijkt uit de huidige vormen waarbij het bouwen aan vertrouwen en CSID hand-in-hand gaan.

Gedurende het onderzoek is verder duidelijk geworden dat samenwerkingsverbanden veel behoefte hebben aan inzicht in hoe anderen de (kern)processen van het samenwerkingsverband geïmplementeerd hebben. De behoeftes en uitdagingen zijn voor samenwerkingsverbanden in hoge mate vergelijkbaar. Het DTC zou een rol kunnen spelen om deze bijeenkomsten te faciliteren, maar kan dit ook ergens anders beleggen. Tevens zou het DTC een faciliterende rol kunnen nemen door het ontwikkelen en beschikbaar stellen van een platform waarop deze good practice informatie gedeeld kan worden tussen samenwerkingsverbanden. Zo kan het maximaal rendement worden gehaald uit de samenwerkingsverbanden en hun initiatieven om de cyberweerbaarheid in Nederland te verhogen.

Contactgegevens

TNO innovation for life

Projectleider: Petra Vermeulen
E-mail: petra.vermeulen@tno.nl

digital trust center.

Projectbegeleider: Kim van der Veen
E-mail: k.m.vanderveen@minezk.nl