Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Effectief opereren in de CERT-gemeenschap

Handreiking

Toegestane verspreiding TLP: WHITE
(Traffic Light Protocol)

Deze handreiking heeft het label TLP: WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Ligth Protocol (TLP) om eenduidig te definiëren wat er met informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard van First (www.first.org/tlp). Ontvangers mogen de informatie uit deze handreiking delen binnen en buiten hun organisatie, daarnaast mag informatie publiek gemaakt worden.

Uw reacties zijn welkom op info@ncsc.nl.

Inleiding

Een handreiking voor CERTs

In Nederland zijn binnen verschillende sectoren, regio's en grote organisaties Computer Emergency Response Teams (CERTs) actief. Zij zijn onder andere verantwoordelijk voor het voorkomen, isoleren en mitigeren van computer- en informatiebeveiligingsincidenten. Het NCSC en het DTC hebben vanuit de nationale overheid een ondersteunende en faciliterende rol richting deze CERTs, met de doelstelling om te komen tot een landelijk dekkend stelsel.

Het NCSC heeft binnen dit kader in het verleden een aantal handreikingen gepubliceerd, bijvoorbeeld over hoe men een collectief computer security incident response team (CSIRT) begint[1] en vervolgens doorontwikkelt (CSIRT Maturity Toolkit)[2]. Dit document is een aanvulling op deze eerdere handreikingen en is gebaseerd op de praktische ervaringen van bestaande regionale en sectorale CERTs.

Doelgroep

Bestaande en toekomstige CSIRTs/CERTs. De handreiking is primair tot stand gekomen voor sectorale en regionale CERTs, maar kan ook bijdragen aan het effectief opereren van andere typen CERTs en cybersecurity samenwerkingsverbanden.

Aan deze handreiking hebben bijgedragen

FERM-Rotterdam, i-CERT, Informatiebeveiligingsdienst (IBD), Z-CERT, SURFcert, Cyber Weerbaarheidscentrum Brainport en CERT-WM.

1 https://www.ncsc.nl/aan-de-slag/samenwerken/doorontwikkelen-samenwerking/start-een-collectief-csirt

2 https://www.ncsc.nl/binaries/content/documents/ncsc-nl/samenwerking/ik-werk-al-samen-en-wil-doorontwikkelen/1/CSIRT_MK_guide.pdf

De CERT-community: rijk in diversiteit

De focus van deze handreiking ligt op het effectief opereren in de CERT-community in de brede zin. De centrale vraag hierbij is hoe je als CERT van toegevoegde waarde kunt zijn voor je eigen doelgroep (constituents), maar daarnaast ook binnen de bredere CERT-community. CERTs komen tijdens hun groeipad voor meerdere dilemma's en uitdagingen te staan waar ook andere CERTs mee te maken krijgen. Er zit daarom veel toegevoegde waarde in het delen van lessen over hoe men hiermee om gaat of is gegaan. Tegelijkertijd opereren CERTs binnen een unieke context, waardoor de succesvolle aanpak van het ene CERT niet direct tot hetzelfde resultaat zal leiden bij een ander CERT. Er is een grote diversiteit aan te treffen in de doelstellingen, geschiedenis, organisatievorm en achterban/doelgroep van CERTs. Dit resulteert in grenzen aan de toepasbaarheid van een algemeen en uniform plan van aanpak om effectief te opereren. Met andere woorden: er bestaat geen '*one size fits all*'-stappenplan.

Dankzij de levendige en groeiende Nederlandse CERT-community bestaat er echter wel een grote schat aan ervaringen, opgebouwd uit de verschillende keuzes die CERTs hebben gemaakt, de motivatie die hierachter schuilging en de voor-en nadelen die zij van deze keuzes ondervonden. Het doel van dit document is om deze diversiteit te illustreren om bestaande, maar ook toekomstige CERTs te inspireren tot de beslissingen die ook in hun specifieke context tot de meeste toegevoegde waarde zullen leiden. De primaire doelgroepen waarvoor dit document tot stand is gekomen zijn sectorale en regionale CERTs, maar veel van de verzamelde lessen kunnen ook van directe meerwaarde zijn voor andere typen CERTs en samenwerkingsverbanden.

Onderzoeksaanpak

Het onderzoek is uitgevoerd in samenwerking met Capgemini en is gebaseerd op interviews met (Nederlandse) CERTs. De handreiking is op inductieve basis vormgegeven, dit wil zeggen dat diverse CERTs zijn geïnterviewd en uit deze interviews gemeenschappelijke lessons learned, best practices en uitdagingen zijn gedestilleerd.

Het onderzoek focust zich enkel op de Nederlandse CERT-gemeenschap, waarbij enkel sectorale en regionale CERTs zijn geïnterviewd. De respondenten van dit onderzoek waren SURFcert[3], CERT-WM[4], i-CERT[5], Z-CERT[6], IBD[7], FERM[8] en Cyber Weerbaarheidscentrum Brainport[9].

3 https://www.surf.nl/surfcert-247-ondersteuning-bij-beveiligingsincidenten
4 https://www.hetwaterschapshuis.nl/cert-wm
5 https://www.verzekeraars.nl/publicaties/actueel/verzekeraars-verhogen-digitale-weerbaarheid-met-i-cert
6 https://www.z-cert.nl
7 https://www.informatiebeveiligingsdienst.nl
8 https://ferm-rotterdam.nl
9 https://brainporteindhoven.com

Leeswijzer

De resultaten van dit onderzoek zijn geclusterd in een aantal thema's waar CERTs mee te maken hebben. Deze thema's betreffen aangelegenheden, uitdagingen of dilemma's waarbij CERTs voor verschillende keuzes staan, bijvoorbeeld als het gaat om de organisatievorm van het CERT, het pakket aan diensten dat het CERT haar doelgroep aanbiedt, de manier waarop zij deze doelgroep bereikt en betrekt of de externe partners waarmee zij relaties onderhoudt. Er zit een zekere volgordelijkheid in de categorisering, maar dit betekent niet dat het een chronologisch stappenplan is dat een CERT dient te doorlopen. De ontwikkeling van een CERT vindt vaak iteratief plaats, waarbij het CERT op basis van nieuwe (interne en externe) ontwikkelingen blijft evolueren om haar dienstverlening te optimaliseren. De volgende tien thema's zijn geabstraheerd uit de interviews:

1. De (interne) organisatie: **Commitment van deelnemers aan het CERT**
2. De (interne) organisatie: **Governance**
3. De (interne) organisatie: **Financieringsmodel**
4. Constituents: **Definiëren en bereiken van de doelgroep**
5. Constituents: **Betrekken van de doelgroep**
6. Constituents: **Contact met de doelgroep**
7. Dienstverlening: **Afstemmen van behoefte en aanbod**
8. Dienstverlening: **Specialisatie**
9. Dienstverlening: **Andere vormen van meerwaarde**
10. Samenwerken: **De CERT-community**

In de volgende hoofstukken worden de bovenstaande thema's behandeld, waarbij de diversiteit aan keuzes van CERTs binnen die specifieke thema's is weergegeven. Door voor- en nadelen van de verschillende aanpakken van CERTs te illustreren en concrete tips te behandelen, vormt dit document een bron van inspiratie voor bestaande en toekomstige CERTs.

“Probeer in een zo vroeg mogelijk stadium de juiste commitment en betrokkenheid op bestuurlijk niveau te regelen en te formaliseren.”

– Informatiebeveiligingsdienst (IBD)

1. De interne organisatie:

Commitment van deelnemers aan het CERT

Een CERT wordt vaak opgericht door enkele partijen in een sector/regio die besluiten dat er behoefte is aan een verhoging van de gezamenlijke slagkracht en weerbaarheid, om informatiebeveiligings-incidenten of -crises het hoofd te bieden. In zowel de vormingsfase van een collectief CERT als in latere volwassenheidsfases is commitment van de deelnemers van groot belang.

Deze deelnemers zijn de organisaties/partijen die gezamenlijk de drijvende kracht vormen achter het CERT en vaak middelen ter beschikking stellen. Het gaat hier veelal om enkele/meerdere sleutelspelers in een sector/regio die bij elkaar komen om het CERT op te zetten en zodoende deelnemen in de CERT-organisatie. Hierbij worden afspraken gemaakt om bijvoorbeeld de onderlinge rollen vast te leggen, waarbij men op elkaar wil kunnen bouwen en vertrouwen. Om vertrouwen te krijgen in deze onderlinge commitment kan ervoor worden gekozen om afspraken officieel te documenteren en vast te leggen, of juist meer te vertrouwen op informele, relationele waarborging:

Formeel vastleggen van commitment

Hierbij wordt bijvoorbeeld gebruik gemaakt van een samenwerkingsovereenkomst. Vaak wordt het aangeduid als een convenant. Het voordeel van deze aanpak is duidelijkheid voor alle betrokken partijen als het gaat om wederzijdse verwachtingen. Het kan helpen bij het vertrouwen in de gezamenlijke verantwoordelijkheid en inzet van de betrokken partijen. Voor wat betreft de formulering binnen een dergelijke overeenkomst kan men bijvoorbeeld zelfs besluiten om verplichtingen juridisch afdwingbaar te maken. Door de commitment op deze manier officieel te documenteren loop je echter wel het gevaar (potentiële) deelnemers af te schrikken. Ook kan er geruime tijd overheen gaan om een dergelijke overeenkomst juridisch vorm te geven. Dat kan ten koste gaan van andere prioriteiten en de initiële slagvaardigheid.

Semi-formeel vastleggen van commitment

Voor het CERT dat terughoudender is met harde, (juridisch) bindende documentatie is deze optie een goede uitkomst. Hierbij kan men denken aan een 'Memorandum of Understanding' of een Intentieverklaring. Dit zijn documenten waarin de wederzijdse verwachtingen worden vastgelegd en ondertekend, maar waaraan geen rechtsgevolgen kunnen worden ontleend. Hier worden de kaders vastgelegd voor samenwerking en dienstverlening. Dit om houvast te bieden. Aanspreken gebeurt pas na problemen of onduidelijkheid.

Informeel

Sommige CERTs maken geen gebruik van documentatie om commitment binnen het samenwerkingsverband te garanderen, maar vertrouwen op informele toezeggingen en onderlinge relaties. Dit kan bijvoorbeeld als er al sprake is van een intensieve onderlinge samenwerking en een basis van vertrouwen, of door hoog bestuurlijk commitment op een andere manier te regelen, bijvoorbeeld door deelname in een 'stuurgroep'. Een voordeel is de laagdrempeligheid en de (onmiddellijke) slagvaardigheid. Het gebrek aan vaststaande regels en voorschriften kan echter ook onenigheden binnen de groep versterken.

Over het algemeen geven CERTs aan dat zowel informele als formele aspecten van cruciaal belang zijn om het vertrouwen in elkaar te kunnen opbouwen. Afhankelijk van de geschiedenis tussen deelnemende partijen en de organisatiecultuur/culturen kan er worden gekozen voor varianten die meer naar het informele of formele commitment neigen. Er is een grote diversiteit aan te treffen in de manieren waarop CERTs deze balans vinden.

“Houd goed voor ogen wat je mandaat en bereik is en hoe je deze bewaakt.”

– CERT-Water Management

2. De interne organisatie:

Governance

Een andere belangrijke vraag bij de inrichting van de CERT-organisatie is hoe (aan) sturing van het CERT georganiseerd wordt. Ook wat deze inrichting betreft is er een grote diversiteit onder de CERTs waar te nemen. De wijze waarop de aansturing van een CERT is vormgegeven verschilt per CERT, waarbij er gebruik wordt gemaakt van gremia op verschillende niveaus van samenwerking:

Strategisch

Bij meerdere CERTs is er sprake van een stuurgroep of een commissie die op strategisch niveau besluiten neemt over en voor het CERT. Over het algemeen kijkt een stuurgroep naar de ontwikkeling en het functioneren van het CERT op de (semi) lange termijn, zo wordt bijvoorbeeld het mandaat in de gaten gehouden. Een stuurgroep komt vaak slechts enkele keren per jaar bijeen. Het voordeel van een dergelijke stuurgroep is dat het zorgt voor aansluiting bij de doelgroep en kan bijdragen aan de betrokkenheid en commitment van de deelnemende partijen. Een mogelijk nadeel van een dergelijke stuurgroep is dat het gevoelig kan zijn voor politieke aangelegenheden en er meer risico is op onderlinge onenigheid door het directe belang van de organisaties. In enkele gevallen is een CERT vormgegeven als een stichting, waarbij een Raad van Toezicht (RvT) toezicht houdt op het bestuur. Dit interne orgaan heeft voornamelijk als taak om toezicht te houden op de doelrealisatie van het CERT, waarbij het voordeel is dat zij deze rol juist onafhankelijk van bijkomstige belangen zullen uitoefenen. Het is daarom van belang om in de opstartfase al na te denken over besluitvormingsprocedures en te bepalen of dit bijvoorbeeld op basis van unanimiteit moet gebeuren. Bij enkele CERTs ligt de besluitvorming in handen van een overkoepelende organisatie, wat kan resulteren in slagvaardigheid maar ook in minder aansluiting van de doelgroep.

Operationeel/tactisch

Bij enkele CERTs is er ook een gremium in het leven geroepen om de deelnemers mee te laten denken en beslissen over operationele en tactische aangelegenheden. Bij een dergelijk overleg op operationeel niveau worden de praktische besluiten besproken met betrekking tot de dagelijkse bedrijfsvoering. Een dergelijke werkgroep bestaat vaak uit een groep constituents die fungeren als sparringpartner en klankbord. Een werkgroep kan erbij helpen om ook de praktische besluiten goed af te stemmen op de behoefte van de doelgroep. Een dergelijk orgaan komt vaak meerdere keren per jaar bijeen, bijvoorbeeld maandelijks. Een voordeel hiervan is dat de deelnemers aan een dergelijk gremium vaak ook tot de directe doelgroep behoren en het op die manier ook direct bijdraagt aan de betrokkenheid van de doelgroep en de aansluiting op hun directe behoeftes. Een nadeel is dat het tot vertraging van het operationele proces kan leiden en dat het niet per direct gelijk staat aan bestuurlijk commitment.

Hybride/meerdere gremia

Sommige CERTs hebben een overleg dat kan worden gezien als een combinatie van een werkgroep en stuurgroep. Aan de ene kant functioneert een dergelijk gremium als een soort klankbord en aan de andere kant worden ook strategische beslissingen binnen deze groep belegd. Tenslotte hanteren verscheidene CERTs meerdere overlegstructuren voor afstemming op verschillende niveaus, bij FERM is er bijvoorbeeld sprake van zowel een overleg op tactisch/operationeel niveau, als een stuurgroep voor strategisch overleg.

CERTs geven aan dat het goed is om na te denken over hoe de deelnemers, maar eventueel ook leden uit de doelgroep, betrokken zijn bij de aansturing van het CERT. Een dergelijke groep kan helpen bij het scherp houden van de focus van het CERT door deze specifieke taak bij hen te beleggen. De manier waarop dit wordt georganiseerd kan afhangen van wat het CERT er nog meer mee wil bereiken. Moet de nadruk bijvoorbeeld liggen op bestuurlijke of operationele betrokkenheid?

“Onderschat de bedrijfsvoering die bij een CERT komt kijken niet, zoals personeelszaken, facilitaire aangelegenheden en financiën.”

– Cyber Weerbaarheidscentrum Brainport

3. De interne organisatie:

Financieringsmodel

Een knelpunt dat men tegen kan komen, is het regelen van financiering van de capaciteit die nodig is om de dienstverlening van het CERT te kunnen (gaan) aanbieden. Vanzelfsprekend is dit ook een kwestie van het afwegen van de investeringen die nodig zijn en het effect dat daarmee bereikt wordt.

Prioriteren is voor veel CERTs een uitdaging, waarbij het van belang is om na te denken over de capaciteit die een bepaalde dienstverlening met zich meebrengt. Zo kiest een aantal CERTs, zoals het CERT-Water Management, ervoor om actief het land in te gaan om nauwe aansluiting met de doelgroep te zoeken. Op deze manier staan ze dicht bij de doelgroep. Dit vereist wel de nodige capaciteit die van tevoren moet worden begroot en waarvan het een bewuste keuze moet zijn om hierin te investeren. Het is dus van belang om een realistische blik te houden op je dienstverlening en de ambities goed af te stemmen op de volwassenheid van het CERT. Los van de diensten die een CERT haar doelgroep aanbiedt zijn er ook resources nodig voor de interne bedrijfsvoering. Vrijwel alle CERTs geven aan dat er veel bij komt kijken om een CERT *up and running* te hebben, iets wat niet moet worden onderschat. Voor wat betreft de financiering wordt er in de praktijk gebruik gemaakt van verschillende modellen:

Sponsoring/ financiering vanuit de deelnemers

Bij meerdere CERTs dragen enkele grote partijen zorg voor de financiële lasten van het samenwerkingsverband. Dit model gaat vaak uit van het principe dat de sterke schouders de zware lasten dragen en is gebaseerd op een besef van de onderlinge (keten) afhankelijkheid. Het nadeel van een dergelijk model is dat het lastig kan blijken om meerdere malen financiële toezeggingen te krijgen. Daarnaast schuilt in dit model het gevaar dat het initiatief voornamelijk in het belang van de betalende partijen zal zijn in plaats van in het algemene belang van de sector/regio.

Contributie van de leden

Een andere wijze om financiering vorm te geven, is om contributie van de leden te vragen. Gebruikers van de dienstverlening van SURFnet worden bijvoorbeeld automatisch lid van het SURFcert. Dit kan bijvoorbeeld een geschikte uitkomst zijn als het initiatief een verplicht karakter heeft of als de verwachting is dat de doelgroep hier capaciteit voor heeft. Indien het laatste niet het geval is dan blijkt in de praktijk een contributie potentiële leden toch te weerhouden van deelname. Een CERT kan hierbij een onderscheid maken tussen verschillende soorten lidmaatschap, waarbij ook de kleinere partijen deelname kunnen bekostigen.

Overheidsfinanciering

Meerdere CERTs maken gebruik van subsidies, bijvoorbeeld om de vormingsfase van een CERT te bekostigen en toe te werken naar een ander financieringsmodel. Dit heeft bijvoorbeeld bijgedragen aan de vormingsfase van het Z-CERT. Zowel op regionaal, nationaal en zelfs internationaal niveau zijn er subsidies waar CERTs aanspraak op kunnen maken. Het voordeel is dat een dergelijke financiering vaak een goede boost kan geven aan het initiatief, het nadeel is dat deze constructies vaak van tijdelijke aard zijn. Het gevaar schuilt erin dat dan niet tijdig wordt nagedacht over een ander geschikt financieringsmodel en de hiervoor benodigde stappen niet worden ondernomen.

“Probeer indien mogelijk in de beginfase van een CERT bepaalde sleutelspelers binnen de doelgroep te identificeren en deze aan te haken.”

– Z-CERT, *een CERT voor de zorg*

4. Constituents:

Definiëren en bereiken van de doelgroep

Als de organisatie is ingericht, is het taak om contact te leggen met de doelgroep: de constituents. Eén van de vragen die een CERT zichzelf allereerst moet stellen, is: hoe definieer ik mijn doelgroep? Soms ligt dit voor de hand, maar vaak ook niet. Voor je de behoeftes van de doelgroep kan achterhalen, moet je wel weten welke organisaties en personen deel uitmaken van deze doelgroep.

Het CERT heeft vaak een doelgroep die groter is dan alleen de deelnemers aan de CERT-organisatie zelf, bijvoorbeeld alle organisaties uit een sector of regio. Een uitdaging die bij veel van de CERTs dan ook speelt, is de vraag hoe het CERT deze partijen (de constituents) kan bereiken. Zelden ligt er een 'kant-en-klaar' lijstje met contactgegevens van potentiële deelnemers, en zelfs als dit wel het geval is, blijkt het in de praktijk moeilijk te zijn om deze partijen te mobiliseren. Voor wat betreft het eerste contact met de doelgroep geven meerdere CERTs aan profijt te hebben gehad van de volgende mogelijkheden:

- Onderzoek of er een **brancheorganisatie** of een andere overkoepelende organisatie actief is waarmee (een gedeelte van) de doelgroep kan worden bereikt. Door een dergelijke organisatie bij het CERT te betrekken, wordt er in de praktijk vaak directe toegang verworven tot de doelgroep. Wat communicatie betreft is dit voornamelijk grote winst. Maar dit is ook belangrijk in het kader van de legitimiteit van het CERT. Zo is een van de deelnemers aan FERM in Rotterdam de lokale ondernemersvereniging DeltaLinqs.

- Een andere mogelijkheid is om te kijken of het CERT een logisch uitvloeisel vormt van **andere initiatieven**, of met deze initiatieven kan optrekken. Wellicht zijn er in de regio of sector al andere samenwerkingsinitiatieven actief die voor ditzelfde dilemma hebben gestaan.

- Hiernaast is het nuttig om in de beginfase van het CERT bepaalde **'power players' of sleutelspelers** binnen de doelgroep te identificeren en deze aan te haken. Zij kunnen als trekker van het initiatief fungeren; zowel in de zin van financiën, als in het weghalen van koudwatervrees bij terughoudende partijen. Het zijn vaak de grotere partijen die de kleinere organisaties in hun kielzog kunnen meenemen en voor naamsbekendheid van het CERT kunnen zorgen. De positieve publiciteit die komt kijken bij deelname aan een dergelijk organisatie-overschrijdend initiatief kan voor zulke partijen als extra motivatie dienen om een trekkersrol aan te nemen binnen het CERT. Deze aanpak heeft bijvoorbeeld goed gewerkt voor het i-CERT.

- Een ander invalshoek is om vooral te kijken in hoeverre de potentiële deelnemers actiegericht (kunnen) zijn en met enkele **slagvaardige partijen** te beginnen. Zo hebben sommige CERTs de ervaring dat partijen uit het midden- en kleinbedrijf slagvaardig kunnen zijn en daardoor makkelijker in samenwerking. Het kan zijn dat grote bedrijven worden geremd in de samenwerking met lokale initiatieven zoals een CERT. Bijvoorbeeld omdat de hoofdkantoren van deze bedrijven in het buitenland liggen, en er dus internationale beperkingen gelden of afstemming moet plaatsvinden. Het overtuigen van kleinere partijen kan in eerste instantie moeilijk zijn omdat zij vaak betwijfelen of een CERT hen iets gaat opleveren en vrezen dat het veel tijd (en middelen) gaat kosten. Zij zullen over het algemeen eerder geneigd zijn om de kat uit de boom te kijken totdat er zich al een community heeft gevormd en er meer duidelijkheid bestaat omtrent de verwachtingen van het CERT naar de deelnemers en vice versa. Het kan echter lonen om juist enkele van deze partijen snel te betrekken.

“Begin met enkele essentiële partijen en breid de scope qua doelgroep pas uit op het moment dat de volwassenheid van het CERT dit toestaat.”

– i-CERT, een CERT voor de verzekeringssector

5. **Constituents:**

Betrekken van de doelgroep

Als de deelnemers aan het samenwerkingsverband zijn geïdentificeerd, is de vervolgvraag in hoeverre zij zelf ook betrokken zijn bij de uitvoering van de taken van het CERT. Er kan zelfs voor gekozen worden om leden uit de doelgroep in de CERT-organisatie werkzaamheden te laten vervullen. Opvallend is dat er een groot verschil is waar te nemen tussen de manier waarop CERTs deze operationele organisatie inrichten, variërend van CERTs waarbij de uitvoering door enkele of alle deelnemende partijen wordt verzorgd tot CERTs waar de gehele organisatie is uitbesteed.

Deelname volledig door deelnemers/constituents

Soms wordt een CERT beheerd door deelnemers uit de doelgroep die bijvoorbeeld voor een bepaalde tijd piketdienst draaien. Dit is bijvoorbeeld het geval bij de i-CERT. Een voordeel hiervan is dat de mensen uit de doelgroep reeds de benodigde kennis en ervaring hebben met de sector. Een uitdaging bij piketdiensten is dat de degene die deze dienst draait altijd het belang van het CERT voorop moet stellen, ook al vindt er bijvoorbeeld bij de eigen organisatie intern (ook) een incident plaats. Hierbij is het dus van belang om goede afspraken te maken om de kwaliteit van het CERT te garanderen en vertrouwen te waarborgen. Het is bovendien belangrijk dat deze personen een toereikend kennisniveau van informatiebeveiliging hebben, iets wat in sommige sectoren een uitdaging kan vormen. Toch zien CERTs veel voordeel in deelnemers uit de doelgroep, omdat zij de taal van de sector spreken en de kennis vanuit de doelgroep kunnen meenemen naar het CERT.

Geen deelname

De volledige organisatie is in sommige gevallen bij externen belegd, bijvoorbeeld in de vorm van commerciële inhuur. Het voordeel hiervan is de neutraliteit ten opzichte van deelnemende partijen en de kennis van informatiebeveiliging van externe experts. Wel is de concurrentie op de markt voor dergelijke experts groot en kan het kostentechnisch dus een uitdaging zijn. Ook kan het lastig zijn om professionals te vinden met een goede kennis van de specifieke sector. Toch geven CERTs aan dat het van groot belang is om juist die mensen te vinden die de taal van de constituents spreken en die de context goed kennen. Bij sommige CERTs ligt de organisatie in de handen van een overkoepelende organisatie. In deze gevallen is er dus geen directe deelname vanuit de constituents zelf, maar hierbij is het voordeel dat het CERT de kennis van de sector al in huis heeft.

Hybride vorm

Er kan voor worden gekozen om constituents in een beperkte mate onderdeel te laten uitmaken van de operationele organisatie. Bij het SURFcert leveren organisaties uit de doelgroep bijvoorbeeld de helft van de teamleden van de CERT-organisatie, die elkaar om de zoveel tijd afwisselen. Bij de IBD kunnen CISO's van deelnemende organisaties 'stage' lopen bij het CERT.

Bij de bovenstaande overwegingen kan ook het volwassenheidsniveau van zowel de doelgroep als het CERT worden meegenomen. Indien het (toegenomen) volwassenheidsniveau van de constituents het toestaat kan dit bijdragen aan de betrokkenheid van de doelgroep om hen in de CERT-organisatie zelf te betrekken. Het kan daarentegen ook helpen om juist in de beginfase van het CERT (meer) gebruik te maken van externe ondersteuning.

“Je moet mensen de tijd geven om de kat uit de boom te kijken. Dit duurt bij de een langer dan bij de ander.”

– i-CERT, een CERT voor de verzekeringssector

6. **Constituents:**

Contact met de doelgroep

Nadat er ingangen tot de doelgroep zijn geïdentificeerd en het bestaan van het CERT is gecommuniceerd, lopen CERTs vaak tegen de uitdaging aan om de doelgroep daadwerkelijk aan te sluiten op hun dienstverlening. Vaak is deelname niet verplicht en moet er worden gewerkt aan het bewustzijn van potentiële deelnemers over het belang van deelname, en vooral over de meerwaarde ervan voor de eigen bedrijfsvoering. Met name het motiveren van (kleinere) partijen blijkt lastig. Soms is het nodig om een gevoel van gemis te laten zien. Het helpt vooral om snel een aantal eerste partijen aan te haken om eventueel 'koudwatervrees' weg te halen bij de overige organisaties.

Bovenal is het belangrijk om duidelijk naar de constituents te communiceren wat je van hen nodig hebt, hoe je dit gaat gebruiken en verwerken en hoe je hen kan ontzorgen. Het kan bijvoorbeeld voorkomen dat partijen vragen stellen als 'zijn wij als partij aansprakelijk als wij kwetsbaarheidsinformatie ontvangen van het CERT maar er niets mee doen en er later (mede) daardoor een incident plaatsvindt?' Dit is het soort dilemma's waar (met name kleine) partijen mee zitten. Om de doelgroep daadwerkelijk betrokken te houden, is het handig om via de juiste communicatiekanalen contact te onderhouden. Alle CERTs onderschrijven hierbij het belang van **fysieke bijeenkomsten**: uiteindelijk is het een 'people business' en vinden mensen het prettig om een gezicht te kunnen plaatsen bij een CERT. Afhankelijk van de verdere inrichting van de dienstverlening wordt er voor meerdere communicatiekanalen gekozen, zoals bijvoorbeeld mailings, een nieuwsbrief (of 'maandmonitor'), social media (zoals Twitter of LinkedIn), WhatsApp, Signal of Skype. Enkele andere specifieke voorbeelden van hoe communicatiekanalen kunnen helpen om contact met de doelgroep te onderhouden zijn:

- Stuurgroepen van meerdere CERTs maken gebruik van een groep in een **Instant Messaging** applicatie waar zij in geval van (bijvoorbeeld) een incident elkaar snel kunnen bereiken.
- Het Z-CERT maakt gebruik van **Mattermost** (een technisch platform) om informatie-uitwisseling met en binnen de community te stimuleren. Hierdoor vindt er veel uitwisseling plaats tussen de leden zelf.
- Het i-CERT organiseert tweewekelijks een '**operational call**', waarbij de (IT-)technische professionals met elkaar kunnen overleggen en sparren over technische aangelegenheden;

Meerdere CERTs geven aan behoefte te hebben aan een 'community' platform, waarbij door de leden zelf informatie kan worden uitgewisseld, op andere manieren digitaal/virtueel actief kan worden deelgenomen aan de community en waarbij men kan aansluiten op al gebruikte communicatiemiddelen van deelnemers. In de praktijk blijkt dat CERTs moeite hebben met het vinden van een geschikte technische oplossing voor deze behoefte. Hierbij blijkt het vooral van belang om onderling lessen uit te wisselen m.b.t. dergelijke technische tools, of eventueel gezamenlijk op te trekken bij het vinden of ontwikkelen van een dergelijk platform. Al de bovenstaande communicatiekanalen hebben als doel om de doelgroep actief te betrekken bij de activiteiten van het CERT. Hierbij geven meerdere CERTs aan dat het belangrijk is om te realiseren dat er tijd overheen gaat voordat dit vruchten afwerpt. Er is een gezonde portie doorzettingsvermogen en geduld voor nodig.

"Wij evalueren onze dienstverlening zowel 'outside-in' als 'inside out': diensten moeten aansluiten op de behoefte van buitenaf, maar deze diensten moeten ook intern worden geëvalueerd op kwaliteit en toegevoegde waarde."

– Z-CERT, *een CERT voor de zorg*

7. Dienstverlening:

Afstemmen van behoefte en aanbod

De belangrijkste vraag voor een CERT is hoe zij van toegevoegde waarde kan zijn voor haar constituents. Een goede aansluiting op de behoefte van deze doelgroep is dan ook essentieel en er zijn meerdere manieren waarop dit kan worden georganiseerd. Het begint al bij de start van een CERT, waarbij men zich moet afvragen of het CERT wenselijk en haalbaar is. Men start daarom over het algemeen met een haalbaarheids-onderzoek naar de haalbaarheid en de vorm.[10]

Uit een dergelijk onderzoek kan bijvoorbeeld volgen dat een CERT wel wenselijk is, maar dat het op dit moment niet haalbaar of gewenst is om incidentafhandeling aan te bieden. Ook in de latere fases van het CERT-bestaan blijft het belangrijk om stil te staan bij de vraag of de visie van het CERT wel haalbaar en wenselijk is. Evalueer daarom periodiek de ambitie en behoefte van de constituents van het CERT. Evalueer daarom periodiek de ambitie en behoefte van de constituents van het CERT. Er zijn specifieke manieren om de behoefte van de doelgroep boven tafel te krijgen. Enkele voorbeelden die men in de praktijk tegenkomt zijn:

- Het organiseren van **bijeenkomsten** waarbij de behoeftes van de doelgroep worden geïnventariseerd, of het aanhaken bij bestaande (bijvoorbeeld regionale) bijeenkomsten met dit doel;
- Het actief betrekken van de constituents bij de **product- en dienstontwikkeling** van het CERT. Dit helpt om te waarborgen dat de producten en diensten die het CERT aanbiedt, zijn afgestemd op de behoeftes van de doelgroep;
- Het beleggen van de verantwoordelijkheid van het onderhouden van het netwerk bij een specifieke persoon. Het helpt om het CERT een gezicht te geven, men vindt het prettig om duidelijk te weten met wie zij precies te maken hebben. Zo kent het CERT-WM bijvoorbeeld een '**omgevingsmanager**' die feedback ophaalt bij de constituents en de behoeftes in kaart brengt;
- Indien het niet haalbaar is om zelf het veld in te gaan, kan er ook worden gekozen voor het uitsturen van een **enquête**, bijvoorbeeld om te achterhalen welke acties de constituents meer zouden willen zien of welke diensten meer prioriteit verdienen.

De praktijk wijst uit dat de wijze waarop een CERT van meerwaarde kan zijn voor haar constituents aanzienlijk kan veranderen na verloop van tijd. Tegelijkertijd is het belangrijk om ervoor te waken dat de aangeboden diensten van hoge kwaliteit zijn en dat ze aansluiten bij de verdere dienstverlening van het CERT, wat betekent dat je soms niet aan alle behoeftes gehoor kunt geven. Het helpt daarom om de ambitie eerst klein te houden en een risico gebaseerde fasering aan te brengen in de planning, zodat je de juiste diensten kunt blijven aanbieden aan de doelgroep.

10 https://www.ncsc.nl/aan-de-slag/samenwerken/doorontwikkelen-samenwerking/start-een-collectief-csirt

"De volwassenheid van een CERT moet zich aanpassen aan het volwassenheidsniveau van de constituents; de aangeboden CERT-diensten moeten aansluiten bij de behoefte van de doelgroep."

– Informatiebeveiligingsdienst (IBD)

8. Dienstverlening:

Specialisatie

De diensten die CERTs aanbieden en de wijze waarop zij van meerwaarde zijn voor hun doelgroep verschilt. Gebaseerd op het kader waarbinnen zij opereren kiezen CERTs vaak voor een focus op een bepaald type dienstverlening. Het traditionele beeld van een CERT die zich beperkt tot incidentafhandeling gaat daarbij in veel gevallen niet op. In de praktijk kent de dienstverlening een aantal verschijningsvormen:

Incidentafhandeling

Traditioneel gezien is dit de bestaansreden van een CERT. Maar zeker bij sectorale en regionale CERTs is dit minder vaak het geval. Er zijn wel degelijk meerdere CERTs actief op dit vlak, maar dan vaak vanuit een ondersteunende rol. Het zijn niet de *incident handlers* van de sectorale CERT die ingrijpen, maar de deelnemers zelf. Deze *incident handlers* hebben dan een adviserende, coördinerende of alarmerende rol. Het zijn veelal de beheerders van de technische infrastructuur bij de organisaties zelf die verantwoordelijk zijn voor de daadwerkelijke afhandeling van incidenten.

Informatie – en kennisdeling

Meerdere CERTs profileren zich vooral als de organisatie-overschrijdende entiteit die voor de gehele doelgroep relevante informatiebeveiligings-informatie verzamelen, verrijken en delen. Het i-CERT zet voornamelijk in op het verspreiden van relevante dreigingsinformatie onder haar leden. Dit kan gaan bijvoorbeeld om dreigingsinformatie, zoals *Indicators of Compromise*, kwetsbaarheidsadviezen (advisories) of trendanalyses. De informatie kan dus van technische of strategische aard zijn, en kan afkomstig zijn van het CERT zelf of van andere kanalen, zoals het NCSC, commerciële partijen of wellicht vanuit de doelgroep zelf.

Organiseren van activiteiten

Andere CERTs specialiseren zich vooral in het organiseren van organisatie-overschrijdende activiteiten, zoals evenementen, trainingen of oefeningen. Hierbij ligt de focus vaak op een preventieve aanpak door bewustwording te creëren bij de doelgroep en het kennisniveau over informatiebeveiliging te verhogen. Veel CERTs zetten in op het organiseren van bewustwordingscampagnes en themabijeenkomsten. Dit is met name nuttig als de volwassenheidsniveaus binnen de doelgroep sterk uiteenlopen of als deze in het algemeen aanzienlijk verbeterd kunnen worden. Trainingen worden daarbij ingezet om het kennis-en vaardigheidsniveau bij de doelgroep te verhogen. Meerdere CERTs organiseren organisatie-overschrijdende oefeningen, bijvoorbeeld door een cybercrisis te simuleren. Bij alle bovenstaande activiteiten geldt dat deze vaak resulteren in een directe impact op de doelgroep, maar op kleine schaal. Daarnaast kan het veel middelen vergen om dergelijke activiteiten te organiseren, wat dan weer vraagt om passende financiering.

Productontwikkeling

Vaak hebben organisaties zelf niet de middelen of kennis in huis om tools en hulpmiddelen te ontwikkelen. Dit is een behoefte waar sommige CERTs, zoals bijvoorbeeld de IBD, op inspelen door producten te ontwikkelen die de doelgroep binnen hun eigen organisaties kan inzetten. Het voordeel van dergelijke hulpmiddelen is dat ze vaak tegemoetkomen aan een heel directe behoefte. De meerwaarde zit vaak in het feit dat deze hulpmiddelen concrete casuïstiek omvatten en een handelingsperspectief bieden waar de partijen direct mee aan de slag kunnen. Aan de andere kant geldt ook hier weer dat er veel resources en interne kennis en vaardigheden van het CERT voor nodig zijn om tot kwalitatief goede producten te komen.

Gebaseerd op de specifieke context waarin zij actief zijn kiezen CERTs vaak voor een focus op een bepaald type dienstverlening. De bovenstaande specialisaties sluiten vanzelfsprekend niet uit dat een CERT bepaalde diensten met een andere focus zal aanbieden. Ook kan een dergelijke focus na verloop van tijd veranderen. Naarmate het CERT (en de doelgroep) groeit in volwassenheid kan het bijvoorbeeld zo zijn dat er behoefte ontstaat aan een meer ondersteunende rol bij incidentafhandeling.

“Kijk ook goed naar wat al wordt geleverd door marktpartijen. Wij springen in wanneer dat gat niet door de markt wordt beantwoord.”

– Z-CERT, *een CERT voor de zorg*

9. **Dienstverlening:**

Andere vormen van meerwaarde

De eerder benoemde specialismes ziet men vaak terugkomen in het takenpakket van CERTs. Maar daarnaast weten de CERTs ook op andere manieren van meerwaarde te zijn voor hun doelgroep.

De volgende specifieke 'diensten' zijn niet altijd toepasbaar binnen een CERT, maar kunnen dienen als mogelijke inspiratie. Dit is een korte opsomming van enkele voorbeelden uit de praktijk, variërend van concrete hulpmiddelen tot het vervullen van een specifieke rol:

Uitvoeren van cyberweerbaarheidsscans

Meerdere CERTs, zoals FERM en Cyber Weerbaarheidscentrum Brainport bieden (nieuwe) leden binnen hun doelgroep een cyberweerbaarheidsscan aan waarmee zij inzicht kunnen krijgen in hun eigen cybersecurity volwassenheid. Deze scans bieden zelfs de mogelijkheid tot het monitoren van verbetering van digitale weerbaarheid van organisaties, of binnen de gehele doelgroep.

Cyber meldpunt

Een mogelijke voorloper van echte incidentenafhandeling is het organiseren van een 'cybermeldpunt' ten behoeve van de detectie van incidenten. Dit houdt in dat organisaties in de community de mogelijkheid, of de plicht, hebben om incidenten te melden bij één centraal punt. Om een verplichte variant op te leggen aan de doelgroep kan het helpen om te onderzoeken of hier een juridische grondslag voor kan worden gevonden.

Bemiddelaar/schakelpartij

Een collectief CERT kan een functie vervullen als een partij tussen (organisaties uit) de doelgroep en andere derde partijen, zoals klanten, leveranciers, overheidspartijen of het brede publiek. Zo kan een CERT helpen bij de woordvoering ten tijde van incidenten, zeker als er gelijktijdig meerdere incidenten binnen de doelgroep plaatsvinden. Ook kan een CERT als vertegenwoordiger van haar doelgroep contact hebben met bijvoorbeeld belangrijke leveranciers van ICT-diensten om afspraken te maken in naam van haar doelgroep. Zo heeft een de IBD concrete afspraken over incidentenafhandeling met dergelijke commerciële partijen in de vorm van convenanten vormgegeven.

Advies

Meerdere CERTs geven aan dat er vaak een concrete vraag is bij organisaties binnen de doelgroep om specifiek advies te ontvangen met betrekking tot hun informatiebeveiligingsmaatregelen. Hoewel dit vaak niet de primaire insteek is van CERTs, geven zij wel aan dat ze juist hier vaak van toegevoegde waarde kunnen zijn. Dit door bijvoorbeeld goed op de hoogte te zijn van regelgeving en kennis te hebben van beveiligingsmaatregelen.

Gezamenlijk inkopen van cybersecurity-diensten

Meerdere CERTs overwegen het gezamenlijk inkopen van cybersecurity-diensten voor (een gedeelte van) de doelgroep. Door op grote schaal diensten aan te schaffen in plaats van geïsoleerd de inkoop te regelen valt er een financieel voordeel te behalen. In het kader van mededinging en eerlijke concurrentie is het mogelijkerwijs van belang om de Autoriteit Consument & Markt hierbij te betrekken.

Het scala aan mogelijkheden om van toegevoegde waarde te zijn voor de doelgroep is groot. Tegelijkertijd is het succes erg afhankelijk van de specifieke context waarbinnen een CERT opereert. Over het algemeen geven CERTs aan dat het belangrijkste is om je af te vragen in hoeverre er sprake is van een lacune waar het CERT invulling aan kan geven. Dit kan bijvoorbeeld het geval zijn als constituents zelf niet de capaciteit of kennis hebben om iets zelfstandig op te pakken, of omdat de markt niet aan een (specifieke) behoefte kan voldoen.

“Doe de Transit 1 cursus. Door deze cursus te volgen krijgt het netwerk een enorme boost, en het is leerzaam.”

– CERT-Water Management

10. **Samenwerken:**

De CERT-community

Meerdere CERTs geven aan beter te functioneren dankzij het externe netwerk: de organisaties buiten hun doelgroep waar zij directe relaties mee onderhouden. Deze toegevoegde waarde van de CERT-community is van toepassing op alle volwassenheidsfases en wederom geldt dat het niet uniform is aan welk type samenwerking een specifieke CERT het meeste profijt heeft. Er valt grofweg een onderscheid te maken tussen samenwerking met overheidsinstanties, leveranciers/commerciële partijen en andere CERTs.

Overheidsinstanties

Samenwerkingen met overheidsinstanties betreffen vaak het NCSC en andere (nationale) instanties en organisaties, zoals het Openbaar Ministerie en de Politie. Er zijn meerdere (nationale) instanties en organisaties die van meerwaarde kunnen zijn voor een CERT. De meeste toegevoegde waarde zit voor CERTs vaak in de toegang tot relevante dreigingsinformatie via dergelijke partijen. Hierbij geven CERTs aan dat het goed is om je te realiseren dat het tijd kost om een dergelijke samenwerking grondig te organiseren, gezien de juridische verplichtingen waaraan afspraken over dergelijke informatie-uitwisseling moeten voldoen. Los van informatie-uitwisseling kunnen deze partijen ook op andere manieren bijdragen, bijvoorbeeld door het aanbieden van concrete producten of ondersteuning ten behoeve van de volwassenheid van het CERT zelf.

Leveranciers/commerciële partijen

Zoals eerder besproken werken meerdere CERTs op verscheidene manieren samen met commerciële partijen. Via deze partijen verkrijgen sommige CERTs bijvoorbeeld dreigingsinformatie, eventueel door dit in te kopen. Enkele CERTs functioneren als een tussenpartij tussen leveranciers van ICT-diensten en de doelgroep, bijvoorbeeld doordat er concrete afspraken zijn gemaakt over incidentafhandeling. Voor het CERT en de doelgroep resulteert dit in meer controle over en betere invulling van de informatiebeveiliging, andersom kan dit een 'selling point' zijn voor de commerciële partij richting de doelgroep. Meerdere CERTs geven aan dat het belangrijk is om na te denken over samenwerking met deze partijen, omdat men vaak met hen te maken zal krijgen aangezien veel ICT-diensten worden uitbesteed. Enkele CERTs zoals de IBD (informatiebeveiligingsdienst) kiezen er bewust voor om deze leveranciers onderdeel te laten uitmaken van hun doelgroep en scope.

Andere CERTs

Het belang van onderlinge uitwisseling van lessons learned wordt benadrukt door alle CERTs in Nederland. Het heeft in alle volwassenheidsfases toegevoegde waarde om best practices met elkaar te delen. Daarnaast bestaan er ook op internationaal niveau initiatieven waar CERTs zich verenigen, zoals de Task Force on Computer Security Incident Response Teams (TF-CSIRT) waar leden van de CSIRT (lees: CERT) community vanuit alle hoeken van de wereld ervaringen en kennis kunnen delen in een vertrouwelijke omgeving, om samenwerking te bevorderen. Het Forum of Incident Response and Security Teams ('FIRST') is een ander vergelijkbaar initiatief. Lidmaatschap van FIRST ondersteunt CERTs met best practices, tools en vertrouwelijke communicatiemogelijkheden met andere leden, om zo een effectieve incidentafhandeling te ondersteunen. Toegevoegde waarde zit bijvoorbeeld in het bespreken hoe Europese wet- en regelgeving is geïmplementeerd. Deelname aan (internationale) cursussen, conferenties of andere (soortgelijke) activiteiten kan ten slotte helpen om contacten op te bouwen met internationale netwerkpartners.

Uitgave
Nationaal Cyber Security Centrum
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

Mei 2020