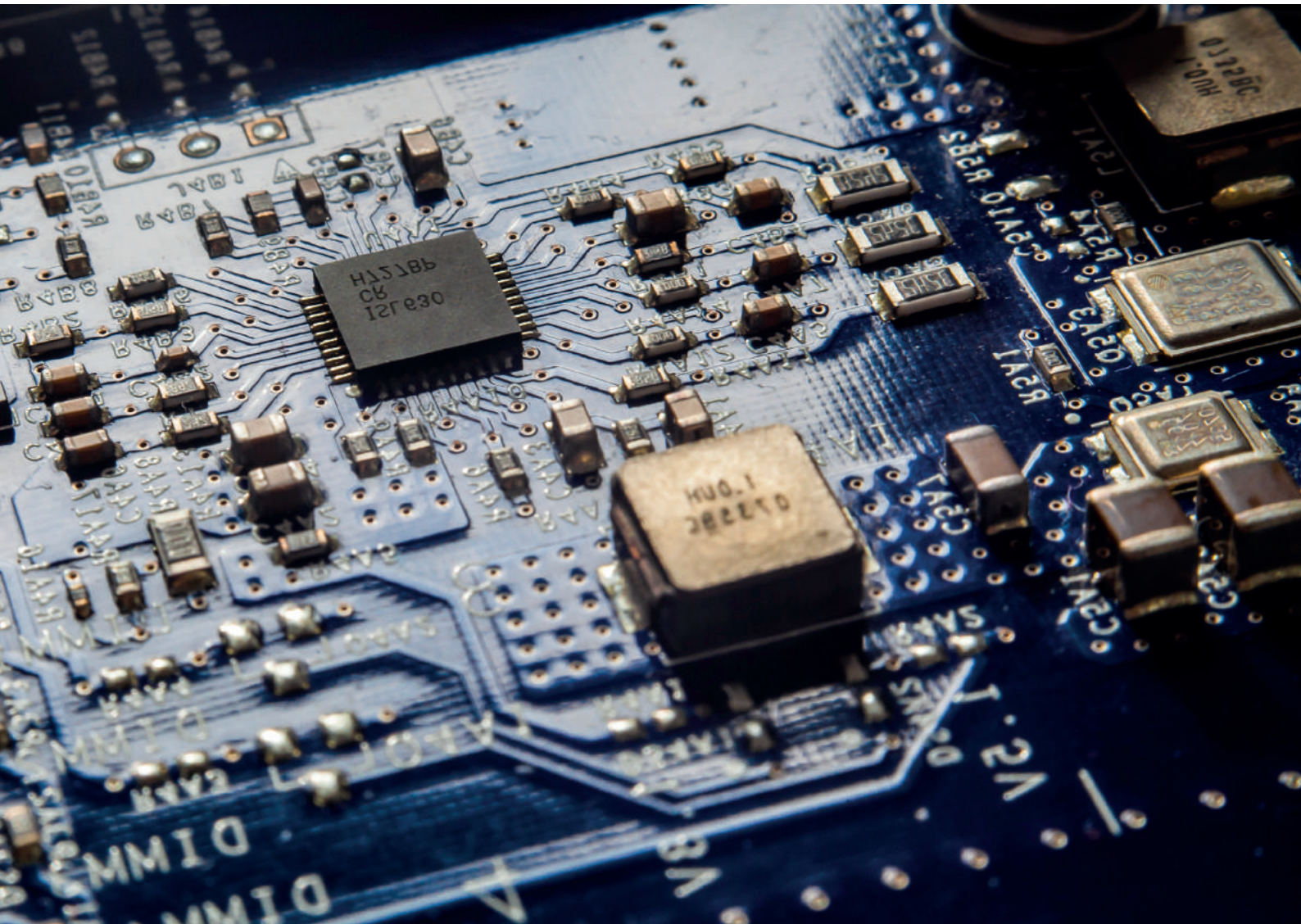
Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Start een CSIRT: Collectief samenwerken

Handreiking



Stappenplan collectief CSIRT

Om aan de slag te gaan met een collectief CSIRT, heeft het NCSC samen met zijn partners een handreiking opgesteld. In deze handreiking worden drie fases met concrete stappen genoemd om tot een succesvol collectief CSIRT te komen.

Fase 1: **Verkennen**

Bouw aan vertrouwen en maak concrete afspraken:

- Breng binnen de werkgroep de gedeelde behoeftes in beeld.
- Voer een haalbaarheidsstudie uit.
- Zorg voor voldoende kritische massa.

Fase 2: **Overeenstemmen**

Bepaal het mandaat, de diensten en activiteiten:

- Bepaal de organisatievorm.
- Breng de operationele taken onder bij de juiste partij.
- Bepaal het mandaat in zowel de koude als warme fase.
- Stel vast welke diensten en activiteiten het collectief CSIRT gaat aanbieden.

Fase 3: **Groeien**

Blijf evolueren en groei in slagkracht:

- Ga niet te snel, maar houd wel de ambitie voor ogen.
- Breid het aantal deelnemers en activiteiten uit.
- Bouw en intensiveer samenwerkingen.

Start een collectief CSIRT

Een collectief computer security incident response team (CSIRT) vergroot de slagkracht, het bewustzijn en de weerbaarheid van de deelnemende organisaties. Collectieve CSIRT's fungeren als coördinator wanneer een incident of crisis bij één of meerdere deelnemende partijen speelt. Het team is het vaste aanspreekpunt voor zowel deelnemers als niet-aangesloten organisaties. Ook kan het collectief CSIRT de functie van informatieknooppunt invullen door duiding te geven en overzicht te houden.

Het NCSC en organisaties die al eerder een (collectief) CSIRT hebben ingericht delen in deze handreiking de ervaringen over het oprichtingsproces, de toegevoegde waarde van een collectief CSIRT en welke activiteiten in een collectief CSIRT zijn ondergebracht.

Doelgroep

(Chief) information security officers van bedrijven en organisaties die met elkaar een collectief CSIRT willen oprichten.

Aan deze handreiking hebben bijgedragen

CERT-EU, CERTFin (Italie), Cyber Synergie Schiphol Ecosysteem (CYSSEC), FERM-Rotterdam, FinancialCERT, i-CERT, Informatiebeveiligingsdienst (IBD), NATO Computer Incident Response Capability (NCIRC), Nederlandse ProductiviteitsAlliantie (NPAL) en SURFcert.

Wat is een collectief CSIRT?

Een collectief CSIRT[1] is een samenwerkingsvorm waarin CSIRT-diensten voor meerdere organisaties uitgevoerd worden. Een collectief CSIRT zorgt voor coördinatie en samenwerking in geval van dreigingen of incidenten die bij één of meerdere deelnemende organisaties spelen.

Hoewel een collectief CSIRT in grote lijnen dezelfde activiteiten en verantwoordelijkheden heeft als een CSIRT van één organisatie, ligt de nadruk bij een collectief CSIRT op gecoördineerde collectieve responsecapaciteit.

In het algemeen zijn CSIRT's verantwoordelijk voor het voorkomen, isoleren en mitigeren van computer- en informatiebeveiligingsincidenten om de beschikbaarheid van diensten of informatiestromen te garanderen. Hiervoor zijn technische en niet-technische werkzaamheden nodig. Tijdens incidenten worden er handelingen verricht in systemen om het incident of voorval te isoleren of te mitigeren. In de nasleep van een incident draagt het CSIRT ook zorg voor de evaluatie om herhaling van het incident te voorkomen. Hiervoor is informatie uit systemen en personen (logbestanden, geautomatiseerde detectiemeldingen, meldinganalyse) vereist.

Bij een collectief CSIRT ligt de nadruk op de coördinatie en ondersteuning van de deelnemende organisaties om de beschikbaarheid van diensten en / of informatiestromen te garanderen. De mate waarin ook technische werkzaamheden vanuit het collectief CSIRT uitgevoerd worden, hangt af van het samenwerkingsmodel dat gebruikt wordt en de afspraken over rollen, activiteiten en mandaat

Nut en noodzaak van een collectief CSIRT

De toegevoegde waarde van een collectief CSIRT komt tot uiting als er een cybersecurity-uitdaging of -dreiging plaatsvindt. Dit zijn de voordelen van een collectief CSIRT:

Slagkracht vergroten

De slagkracht tijdens incidenten wordt vergroot, want je maakt vooraf concrete afspraken met de andere organisaties over coördinatie, informatiedeling, analyse en verantwoordelijkheden. Ook kun je met elkaar in simulaties oefenen hoe je omgaat met het afhandelen van incidenten. Of je kunt voor de leden van een CSIRT specifieke trainingen organiseren.

Bundeling krachten voor incident response

Samenvoegen van krachten tot een team voor incident response is voor veel organisaties een belangrijke reden om deel te nemen aan een CSIRT. Capaciteit wordt efficiënter benut, mede doordat informatie en duiding vanuit verschillende invalshoeken beschikbaar zijn. Voor de efficiënte en effectieve bundeling van capaciteit wordt geadviseerd om fysiek bij elkaar te zitten bij incident response.

Vergroten van weerbaarheid

Individuele bedrijven of (kleinere) organisaties zijn door gebrek aan kennis of financiële middelen vaak niet in staat (effectieve) capaciteit op te bouwen, terwijl zij wel behoefte hebben aan een adequate voorbereiding op en ondersteuning tijdens een incident. Ook voor (grotere) organisaties die wel voldoende capaciteit hebben opgebouwd is de weerbaarheid van andere (gerelateerde) organisaties belangrijk. Als alle organisaties een hogere weerbaarheid hebben, komt dit ten goede aan het totaal.

Kostenefficiëntie

De incident-response-capaciteit kan kostenefficiënt worden ingericht doordat de dienst aan meerdere deelnemers tegelijk wordt aangeboden of een gezamenlijke inkoop kan plaatsvinden.

Toegesneden informatie en duiding

De betrokken organisaties zijn aan elkaar verbonden omdat ze op hetzelfde werkterrein actief zijn (sectorale relatie), fysiek en/of digitaal met elkaar verbonden zijn (ketenafhankelijkheid), of omdat ze in de zelfde regio zijn gevestigd (geografische relatie).[2] Deelnemende organisaties ontvangen door die verbindende factor op hen toegesneden informatie en duiding over specifieke dreigingen, ontwikkelingen, nieuwe technologieën en wet- en regelgeving.

1 Zowel het begrip CSIRT als Computer Emergency Response Team (CERT) worden vaak gebruikt. In deze handreiking is gekozen voor het begrip CSIRT, omdat CERT een merknaam is van Carnegie Mellon University.

2 Zie www.ncsc.nl/samenwerking voor meer tips over het opzetten van een sectorale-, keten-, of regionale samenwerking.

Samenwerking met andere samenwerkingsverbanden en organisaties

Oprichting van collectieve CSIRT's brengt structurele en gecoördineerde informatie-uitwisseling, communicatie en samenwerking met andere relevante organisaties binnen handbereik, bijvoorbeeld met andere collectieve CSIRT's en het NCSC.

"Wij zien als IBD dat een van de grote toegevoegde waarden van de IBD is, dat we de centrale coördinatie en soms zelfs de hele taak van woordvoering op ons nemen in het geval van digitale incidenten binnen het collectief. Dit ontlast niet alleen gemeenten tijdens de crisis, maar het zorgt ook voor consistente communicatie naar buiten."

Informatiebeveiligingsdienst voor Nederlandse gemeenten (IBD)

In de volgende drie fases benoemen we concrete stappen om een CSIRT op te zetten.

Fase 1: Verkennen

Creëer draagvlak, bouw aan vertrouwen en maak concrete afspraken

Wanneer bijvoorbeeld meerdere organisaties worden geconfronteerd met een concreet incident of dreiging, ontstaat al snel het besef dat cybersecurity een onderwerp is dat aandacht verdient. Dan is de stap om te verkennen of een samenwerking op het gebied van cybersecurity incidentresponse waardevol is, niet zo groot meer.

Het initiatief om een collectief CSIRT op te richten ontstaat vaak omdat mensen met elkaar over cybersecurity in gesprek raken. Bijvoorbeeld tijdens een netwerkbijeenkomst in een sector of regio. Het initiatief schept een eerste idee van de behoeften om een collectieve samenwerking vorm te geven. Door de informele sfeer en de persoonlijke betrokkenheid van deze eerste groep ontstaat er energie. Dit enthousiasme is nodig om andere mensen en organisaties erbij te betrekken.

Wanneer de eerste ideeën concretere vormen beginnen aan te nemen, formeer je een werkgroep die de mogelijkheden voor een collectief CSIRT verder gaat onderzoeken en uitwerken. Deze werkgroep inventariseert behoeftes bij beoogde organisaties, die aan de CSIRT kunnen deelnemen.

Voer een haalbaarheidsstudie uit

Zodra de gedeelde behoeftes bij de beoogde organisaties duidelijk zijn, stel je een haalbaarheidsstudie op. Op basis van deze analyses bepaal je als groep of je verder gaat met het initiatief en in welke vorm. Dat betekent dat je een gezamenlijke visie en strategie bepaalt en een vorm vindt om de samenwerking in te richten.

Een haalbaarheidsstudie draagt bij aan:
- creëren van draagvlak bij bestuurders én deelnemers door een gestructureerde aanpak;
- verkrijgen van inzicht in verschillende modellen van samenwerking;
- inzicht verkrijgen in behoeften van initiatiefnemers.

Het haalbaarheidsonderzoek is de basis voor de initiële kosten-batenanalyse aan de hand waarvan je een businessplan inclusief groeimodel kan opstellen.

Tip: Tijdens deze eerste fase maak je dus belangrijke ontwerpkeuzes voor de verdere oprichting en uitwerking van een collectief CSIRT. Denk dan in deze fase na over groeimodellen en doorontwikkeling, zodat het model waar je nu voor kiest past bij je ambitie.

In de praktijk zal de volgende stap voor elke situatie net wat anders liggen. Belangrijke aandachtspunten zijn: beschikken over voldoende draagvlak en de inzet van de deelnemende organisaties, inzicht in de (soms verschillende) behoeften van de deelnemende organisaties en werken aan de vertrouwensbasis tussen de organisaties.

"Wij hebben in de aanloop naar de oprichting van i-CERT een uitgebreide haalbaarheidsstudie en stakeholderanalyse uitgevoerd. Tevens zijn de behoefte en het draagvlak onder verzekeraars in kaart gebracht. Een belangrijk onderdeel van de studie betrof het uitwerken en beoordelen van verschillende scenario's. Deze scenario's hadden een cumulatief karakter waarbij het ook mogelijk is om met het minst geavanceerde model te beginnen en later door te ontwikkelen.
De scenario's zijn door experts en beoogde deelnemers geanalyseerd (kosten, baten, governance, haalbaarheid van doelstellingen en risicoanalyse). Op basis van de studie is ervoor gekozen om één scenario verder uit te werken, wat uiteindelijk geleid heeft tot de oprichting van i-CERT in 2017."

i-CERT voor de verzekeringssector

Start vroegtijdig met het creëren van draagvlak

Om gezamenlijk iets van de grond te krijgen moet vroegtijdig worden gestart met het creëren van draagvlak bij de organisaties van de initiatiefnemers en bij organisaties die potentieel deelnemer kunnen worden.

Zorg ervoor dat het initiatief niet te lang bij enkele enthousiaste personen blijft liggen en stel zeker dat je binnen je eigen organisatie draagvlak en steun hebt op strategisch niveau. Zonder draagvlak en steun van de deelnemende organisaties op strategisch niveau is het oprichten van een collectief CSIRT niet mogelijk. Bij de start regelmatig met anderen van gedachten wisselen over plannen, activiteiten, capaciteiten en diensten is essentieel.

Zorg ook voor bekendheid en ondersteuning van het initiatief op andere plekken in de deelnemende organisaties. Houd er rekening mee dat het proces om voldoende draagvlak te creëren flink wat tijd in beslag kan nemen. Stuur bijvoorbeeld regelmatig een nieuwsbrief waarmee je een brede groep organisaties op de hoogte kan houden. Ook het organiseren van specifieke bijeenkomsten of sessies tijdens andere evenementen kunnen bijdragen aan een stevig draagvlak. Ook na de oprichting is het nodig om zichtbaar te zijn en blijven. Door je initiatief onder de aandacht te (blijven) brengen bij een breder publiek, zorg je dat organisaties elkaar beter leren kennen en makkelijker weten te vinden.

Tip: Met een distributiekanaal zoals e-maillijsten of een digitaal platform zorg je ervoor dat deelnemende partijen informatie op een veilige (en uniforme) manier met elkaar kunnen delen. Het Traffic Light Protocol[3] kan hierbij ondersteunen. Voor het onderlinge vertrouwen moeten alle partijen toegang hebben tot de distributiekanalen en zich houden aan de afspraken over informatiedeling.

Vertrouwen is de basis

Digitale weerbaarheid en veiligheid van de deelnemende organisaties moet het belangrijkste gezamenlijke doel zijn. Organisaties die samen werken aan de digitale weerbaarheid, moeten bereid zijn elkaar te vertrouwen en daarvoor gevoelens over hun concurrentiepositie of mogelijke negatieve aspecten van samenwerking los te laten. Om de veiligheid en integriteit van gevoelige informatie en activiteiten te waarborgen zijn (proces)afspraken vereist. Zulke afspraken kunnen in de richtlijnen voor het lidmaatschap en communicatiemiddelen worden opgenomen.

Zorg voor voldoende kritische massa

De omvang van het samenwerkingsverband is van invloed op het succes. Deelname door alle beoogde organisaties is niet vereist voordat gestart kan worden. Vaak is het zelfs doeltreffender om met een kleinere groep van drie tot vijf organisaties te starten. Uitbreiding van de groep kan dan stap voor stap plaatsvinden. Wél is het cruciaal om voldoende massa te creëren voor de volgende vervolgstappen, bijvoorbeeld om de kosten te dekken en/of werkzaamheden onderling te verdelen.

De werkgroep moet bij aanvang al nadenken over het proces voor uitbreiding en instroom. Deze vragen dienen ter voorbereiding:

- Wat is de uiteindelijke beoogde omvang van het samenwerkingsverband en waarom? Is het mogelijk of wenselijk een onder- of bovengrens vast te stellen?
- Is de scope en beschikbaarheid van de huidige dienstverlening ruim, beperkt, of precies goed voor nieuwe deelnemers?
- Kunnen nieuwe deelnemers ondergebracht worden binnen de bestaande structuur of moeten er andere samenwerkingsverbanden worden opgericht?
- Wordt de groep door uitbreiding alleen vergroot of ook verbreed? En heeft dat consequenties voor de slagkracht?
- Komt er met de uitbreiding nieuwe of aanvullende coördinatie en/of responsecapaciteit beschikbaar? Is dat wenselijk?
- Gaan alle toekomstige deelnemers op dezelfde manier participeren of zijn er verschillende 'lidmaatschapsniveaus' denkbaar?
- Hoe ziet een ideale fasering eruit (bijvoorbeeld maximale instroom per jaar)?
- Wat is het volwassenheidsniveau van de instromende organisaties?
- Hebben huidige deelnemers een vertrouwensband met de instromende organisaties en op basis waarvan?

3 Zie gehele richtlijn op: www.first.org/tlp.

Fase 2: Overeenstemmen

Bepaal het mandaat, de diensten en activiteiten

Denk samen na en bereik overeenstemming over organisatorische vraagstukken die komen kijken bij de oprichting van een collectief CSIRT.

Organisatievormen

Allereerst zijn er verschillende organisatievormen denkbaar om een collectief CSIRT in te richten:

1. Ondergebracht bij een bestaande organisatie in het samenwerkingsverband, zoals een brancheorganisatie. Met deze optie hoeft er geen nieuwe organisatie opgericht te worden, want er is al capaciteit en een relatie binnen de samenwerking. Nadelig kan zijn dat de organisatie een andere taakomschrijving heeft en misschien nog geen ervaring met een dergelijke rol in informatiebeveiliging.
2. Ondergebracht bij een nieuwe organisatie, zoals een stichting om de CSIRT-taken uit te voeren. Hiervan is het voordeel dat de nieuwe organisatie volledig is toegewijd aan de CSIRT-taken en kan worden ingericht om aan te sluiten bij de behoeften van het samenwerkingsverband. Nadelig kan zijn dat het opstarten, inrichten en beheren meer investering vereist. Denk aan tijd, geld, personeel, opbouwen en behouden van vertrouwen.
3. Ondergebracht bij een derde partij (inhuur) in dienst van het samenwerkingsverband om de taken te vervullen (uitbesteding). Daarvan is het voordeel dat de in te huren partij kan worden geselecteerd op kwaliteit en expertise. Een mogelijk nadeel is dat de in te huren partij de deelnemers in het samenwerkingsverband niet kent en misschien minder kennis van behoeftes en uitdagingen heeft. Ook moet er eerst een vertrouwensband worden opgebouwd.

Tip: Geïnteresseerde partijen kunnen soms pas later aansluiten omdat zij bijvoorbeeld lopende contracten hebben (voor incident response, dreigingsinformatie, security information and event management (SIEM). Dit hoeft geen probleem te zijn wanneer zij wel kunnen aanhaken bij andere activiteiten (informatiedeling, community-building). Na afloop van een lopend contract kunnen zij alsnog besluiten om in te stromen. Neem dit mee in je overwegingen.

Operationele uitvoering van de taken

De uitvoering van de taken moet passen bij de gekozen vorm van het samenwerkingsverband.

Mogelijkheden zijn:

1. De taken van het CSIRT worden uitgevoerd door een aantal deelnemende organisaties. Meestal zijn dit organisaties die al over een CSIRT-capaciteit beschikken.
2. Het incident-response-team wordt binnen het collectief nieuw ingericht. Hierbij wordt een team van experts aangesteld dat het CSIRT aanstuurt.
3. Het incident-response-team wordt als dienst ingekocht bij een derde partij (buiten het collectief).

Bepaal het mandaat en de rol in zowel de koude als warme fase

De bevoegdheid van het collectief CSIRT kent drie niveaus:

1. **Volledige bevoegdheid**: de leden van het team hebben de bevoegdheid om noodzakelijke acties of beslissingen te nemen namens alle deelnemende organisaties.
2. **Gedeeltelijke bevoegdheid**: de leden van het team hebben invloed op keuzeprocessen, maar kunnen niet bepalen welke acties of beslissingen genomen worden door de deelnemende organisaties.
3. **Geen bevoegdheid**: de leden van het team hebben geen formeel gezag, maar worden wel erkend als inhoudelijk expert en kunnen optreden als vertrouwd adviseur.

Het uitwisselen van informatie over (bijna-)incidenten binnen het collectief CSIRT is voor vele organisaties de motor van het collectief. Afhankelijk van het vertrouwen in en volwassenheidsniveau van een CSIRT worden bepaalde incident-response-taken en verantwoordelijkheden (gedeeltelijk) ondergebracht bij het collectief CSIRT.

Het is van belang om in de voorbereidende (koude) fase wanneer er geen incident speelt, afspraken te maken over de mate van ondersteuning tijdens de operationale (warme) fase in antwoord op een incident. De verantwoordelijkheden van het collectief CSIRT zijn per collectief anders. Een organisatie zal normaliter altijd eindverantwoordelijk zijn voor de eigen diensten en infrastructuur. Het collectief CSIRT heeft daarom een ondersteunende rol en voorziet de individuele organisatie van hulp en advies om het incident zo snel mogelijk te de-escaleren (gedeeltelijke bevoegdheid).

Personeel en rollen die van belang zijn

Ontwikkel als collectief CSIRT eerst een door iedereen gedragen visie en doelstelling(en) voordat je nadenkt over de personele invulling. Aan de hand van de met elkaar overeengekomen visie kun je kiezen hoe de personele bezetting eruit moet zien en welke opleidingen en trainingen nodig zijn om de visie te realiseren. Dit is een essentiële keuze tijdens het ontwerpen.

Voor de personele bezetting kun je experts inhuren, je kunt personeel van de deelnemende organisaties detacheren, of je kiest voor een tussenvorm die past bij visie en doelstelling(en. In ieder geval heeft het personeel van een collectief CSIRT adequate training en opleiding nodig, gericht op samenwerking. Het is wel belangrijk om ook je eigen ideeën en specialismen te behouden. Daarmee houdt je elkaar scherp

Medewerkers met uitvoerende taken moeten ervaring hebben in het vakgebied en inzicht hebben in de materie waarover zij incidenten gemeld krijgen. Daarnaast zijn er ook niet-technische rollen, zoals een relatiemanager, een juridisch adviseur, een data- privacy-officer en een communicatiespecialist voor de inrichting van interne en externe communicatie waar je over na moet denken.

Financiering

Maak aan de hand van de ontwerpkeuzes, de missie en de doelstelling(en) een inschatting van benodigde investeringen. Maak hier steeds weer de afweging tussen de functionaliteit en (verwachte) opbrengst tegenover de benodigde investering. Een kosten-batenanalyse is hier een goed uitgangspunt voor. Stel om het financieringsmodel te bepalen de volgende vragen:

Stel hierbij de volgende vragen:
- Wel of geen 24/7 beschikbaarheid?
- Samenwerken op afstand of vanuit een gedeelde fysieke locatie?
- Autonomie van medewerkers versus autonomie van deelnemende organisaties?
- Uitgebreide communicatiestrategie of op de achtergrond opereren?
- Actief monitoren en detecteren of hoofdzakelijk de focus op coördineren van response?
- Welke rol, taak en verantwoordelijkheid in de koude fase en welke in de warme?
- Personeel aanstellen of roulatiemodel voor deelnemende organisaties gebruiken?
- Lidmaatschapsgeld vs. bijdragen leveren met gesloten beurzen?
- Is er financiering vanuit bestaande middelen van het samenwerkingsverband mogelijk of is er aanvullende financiering vanuit de deelnemende organisaties nodig?
- Gelijkwaardige contributie voor iedereen of schaalbaar naar omvang van deelnemers (bijvoorbeeld een getrapt lidmaatschapsmodel)?
- Inkopen van diensten en informatie of inbreng vanuit deelnemers?

Juridische aspecten

In het ontwerp en de doorontwikkeling van het collectief CSIRT moeten op veel punten keuzes en afspraken gemaakt worden tussen de deelnemende organisaties, ook afspraken over voorwaarden voor deelname en bijbehorende verantwoordelijkheden. Vanuit juridisch oogpunt is het raadzaam deze afspraken goed vast te leggen.

Een CSIRT is een plek waar informatie met mogelijk persoonsgegevens binnen komt en waar incidenten gemeld worden.

Tip: Het vastleggen van de afspraken tussen organisaties aangesloten bij het collectief CSIRT kan bijvoorbeeld in een samenwerkingsconvenant of statuten.[4]

Daarvoor moet de relevante wet- en regelgeving[5] in de gaten worden gehouden en met elkaar afgestemd hoe het collectief daarmee omgaat.

Vaststellen van diensten en activiteiten

In de ontwerpfase moet worden bepaald welke diensten en activiteiten het collectief CSIRT gaat aanbieden en welke verantwoordelijkheden het draagt. Het pakket aan diensten kan klein beginnen en in de loop van de tijd uitgebreid worden vanuit een gezamenlijk bepaald groeimodel of roadmap. Welke taken als eerste opgepakt gaan worden is afhankelijk van de situatie.

Wat zijn die eerste taken?

Coördinatie omtrent incident response

Hiermee bepaal je de scope waarop geacteerd wordt. Ook bepaal je wie welke acties onderneemt als gevolg van een incident. Een collectief CSIRT kan fungeren als meld- en registratiepunt voor incidenten, dat alleen doorverwijst naar de juiste instanties. Natuurlijk kan het team zelf ook acties uitvoeren wanneer incidenten hebben plaatsgevonden.

Informatiedeling

Een belangrijke basis om goed te kunnen blijven functioneren, vertrouwen op te bouwen en voortdurend te professionaliseren is het stimuleren van informatie-uitwisseling. Bijvoorbeeld informatie over ontwikkelingen in cybersecurity (wetgeving, nieuwe technologieën, trends, dreigingen, aanvalstechnieken), incidenten relevant voor de doelgroep van het CSIRT en best practices.

4 Zie bijvoorbeeld https://www.verzekeraars.nl/branche/zelfregulering/overzicht/cert-verzekeringssector-convenant.

5 Sectorspecifiek (i.e. toezichthouders, inspectie, wettelijke kaders) en specifiek op onderwerp (i.e. privacy, informatiebeveiliging).

Distributiekanaal
Veilige informatiedeling tussen de deelnemende organisaties wordt mogelijk gemaakt door een beveiligd distributiekanaal, bijvoorbeeld via e-mail, een platform of een ander systeem.

Woordvoering en communicatie
Een collectief CSIRT kan woordvoering doen en communicatie over incidenten om andere organisaties te informeren. Denk aan het NCSC, klanten, stakeholders, andere overheidsorganisaties en media.

Kennis- en analysecapaciteit
De kennis- en analysecapaciteit die binnen het collectief CSIRT wordt opgebouwd komt ten goede aan het collectief. Daarvoor kan ook samenwerking worden gezocht met het NCSC, andere CSIRT's, universiteiten, kennisinstellingen of andere organisaties. Hetzelfde geldt voor de specifieke expertise van deelnemende organisaties die zo beter kan worden benut.

"Wij bieden een basispakket van diensten aan die voor alle aangesloten partijen verplicht worden afgenomen. Daarnaast zijn er aanvullende diensten die facultatief kunnen worden afgenomen. Ook hebben wij een SURFnet Community for Incident (SCIRT) Response Teams opgezet waarbinnen CSIRT's van de deelnemende organisaties onderling informatie kunnen uitwisselen. Hierdoor kunnen wij ons blijven focussen op de primaire dienstverlening en wordt tegelijkertijd de onderlinge band tussen de deelnemende organisaties bevordert.[6]"

SURFcert

De fysieke ruimte
De keuze om het collectief CSIRT ergens fysiek onder te brengen of om als virtueel team vanuit de eigen organisatie samen te werken, hangt samen met de vorm en invulling van de taken. Fysiek op één locatie samenwerken kan een opmaat zijn om de operationele samenwerking uit te bouwen, bijvoorbeeld door activiteiten zoals monitoren van systemen en netwerkverkeer op termijn bij het collectief CSIRT onder te brengen. Met een liaisonstructuur maak je een combinatie van fysiek en virtueel samenwerken.

Voor de samenwerking zij-aan-zij draagt een speciale fysieke locatie bij aan elkaar beter leren kennen en aan de groei van onderling vertrouwen. Dat maakt het als vanzelfsprekend delen van informatie eenvoudiger. Bij de inrichting van een virtueel team blijven experts in het team nauw betrokken bij de eigen organisatie, waardoor ze ook de bewustwording en het draagvlak in de eigen organisatie in stand kunnen houden. Er hoeven dan geen kosten voor een nieuwe locatie of infrastructuur te worden gemaakt.

Bij samenwerkingsverbanden met veel deelnemers kan het nuttig zijn om vanuit een centrale locatie activiteiten te coördineren. Vervolgens kunnen deelnemende organisaties een deel van de taken op afstand voor hun rekening nemen.

"Wij hebben geconstateerd dat onze organisatievorm en de capaciteiten waarover we beschikken continu aan verandering onderhevig zijn. Door jaarlijks terug- en vooruit te blikken zijn wij continu bezig met de doorontwikkeling van het team en de inbedding hiervan. Hierdoor zijn we in staat om met veranderingen mee te bewegen en ons te blijven verbeteren."

CERT-EU

Volwassenheid aangesloten organisaties
Bij oprichting kunnen (eventuele) verschillen in het volwassenheidsniveau van de individuele organisaties van invloed zijn op de taakverdeling binnen en de ambitie van het collectief. Wanneer de deelnemende organisaties deze verschillen aan elkaar kenbaar maken, geeft dat vertrouwen. Bovendien kunnen volwassenen organisaties de minder volwassen organisaties ondersteunen. Dit wordt als positief ervaren door alle organisaties.

6 Op www.surf.nl/diensten-en-producten/surfcert/index.html van SURFcert staat een uitgebreid overzicht van de diensten die zij aanbieden aan de deelnemers.

Fase 3: Groeien

Vergroot slagkracht en blijf evolueren

Ga niet te snel en houd de ambitie voor ogen

In een eerste operationele fase loopt men altijd tegen onverwachte zaken aan. Ook kunnen er externe ontwikkelingen zijn die van invloed zijn op de vervolgstappen.

Als in de ontwerpfase doorgroeimogelijkheden en ambitie wel onderwerp van gesprek zijn geweest, wordt het nu tijd om na te denken over het vervolg. Wie gaat het gesprek aan met nieuwe deelnemers? Hoe kun je meer (vertrouwelijke) informatie met elkaar delen? Is een eigen locatie of personeel nodig? Is er behoefte aan andere expertise of financiering?

"Wij, het sectorale CSIRT van de Italiaanse financiële sector (CERTFin), zijn opgericht als publiek-privaat initiatief om de samenwerking tussen banken en andere financiële instellingen te ondersteunen. Vanwege de gerelateerde werkterreinen is een volgende stap die zij beogen een uitbreiding naar de verzekeringssector."

CERTFin

Uitbreiding van deelnemers

Ga je in gesprek met een potentiële nieuwe deelnemer, kijk dan goed naar de motivatie, verwachtingen en toegevoegde waarde van deze organisatie.

Als voorbereiding moet de gemeenschappelijke visie voor het collectief CSIRT het uitgangspunt zijn, en daarnaast wat een logische en relevante uitbreiding zou zijn. Omdat collectieve CSIRT's veelal ontstaan vanuit een al bestaand verband of collectief, kunnen de gemeenschappelijke kenmerken opnieuw tegen het licht worden gehouden. Misschien zijn er andere relevante doelgroepen om mee samen te werken, vanuit een gedeeld thema of belang. Denk hierbij aan een sector of werkgebied dat ook te maken heeft met vergelijkbare dreigingen.

Uitbreiding van activiteiten

Bij oprichting kan al gekeken worden naar mogelijke uitbreiding van activiteiten. Vaak richten de initiële activiteiten zich op coördineren van gezamenlijke inspanningen en informatiedeling. De volgende stap kan zijn:

- diepgravender analyses (laten) doen;
- gezamenlijk inkopen van (dreigings)informatie of hard- en software;
- convergentie van geanonimiseerde data (netwerken en incidenten) uit de aangesloten organisaties;
- aanvragen van accreditatie;
- actief deelnemen aan de CSIRT- gemeenschap door aansluiting bij TF-CSIRT Trusted-Introducer en/of FIRST te zoeken.[7]

Welke vervolgstappen haalbaar en wenselijk zijn hangt samen met de behoeften en omstandigheden van het collectief.

Samenwerking

Ook een logische volgende stap is om een samenwerking aan te gaan met het NCSC, andere (collectieve) CSIRT's en andere relevante organisaties. Binnen deze samenwerking kan vertrouwen worden uitgebreid en aanvullende informatie worden ingewonnen. Daarvoor is actief relatiemanagement cruciaal, omdat inhoudelijke samenwerking verder kan gaan dan enkel informatieuitwisseling. Gezamenlijk optrekken in bepaalde dossiers of een gedeelde dreiging behoort dan tot de mogelijkheden. Zo'n partnerschap aangaan draagt bij aan het vergroten van de weerbaarheid.

Professionaliseren

Verder professionaliseren van een collectief CSIRT betekent dat actie wordt ondernomen op:

- De basis van het collectief – wat kan er beter?
- De organisatie van het collectief – wat moet er nog geregeld worden?
- Het personeel – voeren de medewerkers de juiste taken uit?
- Expertise – welke deskundigheid ontbreekt?
- Tooling – wat hebben we nog nodig?
- Oefenen – is er een geschikte simulatie?
- Werkprocessen – ontbreekt er een schakel in de keten?

De ambitie bij de oprichting is nu weer van belang om te weten waar naar toe gegroeid kan (of moet) worden. Daarvoor moet het huidige volwassenheidsniveau van het collectieve CSIRT worden vastgesteld. Lees daar meer over in de CSIRT Maturity Kit of doe de ENISA's CSIRT Maturity – Self-assessment Survey.[8]

7 Voor meer informatie over de accreditatievoorwaarden van internationaal gerenommeerde gemeenschappen van CSIRT's, zie TF CSIRT's Trusted Introducer (https://www.trusted-introducer.org) en het Forum of Incident Response and Security Teams (https://first.org).

8 Zie https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey om de survey te doen.

Verder lezen

Openbare informatie over bestaande collectieve CSIRT's

i-CERT

- Oprichting: https://www.verzekeraars.nl/publicaties/actueel/verzekeraars-verhogen-digitale-weerbaarheid-met-i-cert
- Convenant: https://www.verzekeraars.nl/branche/zelfregulering/overzicht/cert-verzekeringssector-convenant

SURFcert

- Service Description (RFC 2350): https://www.surf.nl/en/services-and-products/surfcert/operational-information/surfcert-service-description/index.html
- Overzicht diensten en producten en overige informatie: https://www.surf.nl/diensten-en-producten/surfcert/index.html
- SCIRT: https://www.surf.nl/diensten-en-producten/beveiligingscommunitys/scirt/index.html

IBD

- Algemeen: https://www.informatiebeveiligingsdienst.nl
- Factsheet incident coördinatie: https://www.informatiebeveiligingsdienst.nl/product/factsheet-incidentcoordinatie

Z-Cert

- Algemeen: https://www.z-cert.nl

Richtlijnen, tools en informatie over CSIRT's

- Create a CSIRT (2017): https://resources.sei.cmu.edu/asset_files/WhitePaper/2017_019_001_485695.pdf
- CSIRT Maturity Kit (2015): https://check.ncsc.nl/static/CSIRT_MK_guide.pdf
- Organizational Models for CSIRTs (2003) https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14099.pdf
- Outsourcing Managed Security Services (2003) https://resources.sei.cmu.edu/asset_files/SecurityImprovementModule/2003_006_001_14105.pdf
- Resources for Creating a CSIRT (2018) https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=485643
- The Handbook for CSIRTs (2003) https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf

Overig

- CSIRT Effectiveness and Social Maturity (2016). https://www.incidentresponse.com/wp-content/uploads/GMU-Cybersecurity-Incident-Response-Team_social_maturity_handbook-updated_10.20.16.pdf
- Cyber Security Incident Response Guide (2014). https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf
- Global Good Practices - National Computer Security Incident Response Teams (CSIRTs) (2017). https://www.thegfce.com/initiatives/c/csirt-maturity-initiative/documents/publications/2017/11/21/national-computer-security-incident-response-teams-csirts
- Guide for Alerts, Warnings and Announcements (2013). https://www.enisa.europa.eu/publications/awa/at_download/fullReport
- Incident Response Reference Guide (nd). https://info.microsoft.com/rs/157-GQE-382/images/EN-US-CNTNT-emergency-doc-digital.pdf
- Inventarisatie en classificatie van standaarden van cybersecurity (2015). https://www.wodc.nl/onderzoeksdatabase/2552-inventarisatie-van-standaarden-en-normen-voor-cyber-security.aspx
- Security Incident Management Maturity Model. https://www.terena.org/activities/tf-csirt/publications/SIM3-v15.pdf
- Study on CSIRT Maturity – Evaluation Process (2017). https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process/at_download/fullReport
- Traffic Light Protocol (TLP). https://www.first.org/tlp
- Definitions and Usage | US-CERT (nd). https://www.us-cert.gov/tlp
- CSIRT Maturity - Self-assessment Survey. https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

Colofon

Gebaseerd op onderzoek uitgevoerd door TNO.

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