Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Haal meer uit je ISAC

Handreiking

Checklist niveau ISAC

Om te weten waar je naartoe wilt groeien met je ISAC, is het van belang om te weten waar je staat. Deze checklist helpt jou hierbij. Je kunt per capability bepalen op welk niveau jij zit met je ISAC. Het is mogelijk dat je met jouw ISAC per capability op een verschillend niveau zit. Het wordt aangeraden om deze met alle deelnemers na te lopen, zodat er een gezamenlijk beeld wordt gevormd.

Strategie en actieplan

	Capability	*Status*
Niveau 1	Is er een gemeenschappelijk geformuleerd doel van informatie-uitwisseling?	
	Zijn gemeenschappelijke kenmerken van de ISAC-deelnemers kenbaar gemaakt (denk bijvoorbeeld aan bedrijfsprocessen, systemen, ketenafhankelijkheden, gezamenlijke uitdagingen, incidenten, etc.)?	
	Stellen deelnemers tijd beschikbaar om deel te nemen aan de ISAC?	
	Hebben deelnemers steun van de eigen organisatie om deel te nemen aan de ISAC?	
	Zijn de functieprofielen en rollen van ISAC-deelnemers bekend?	
	Zijn voor de beoogde informatiedeling in de ISAC-bijeenkomst de juiste functieprofielen afgevaardigd?	
	Zijn er afspraken gemaakt die ervoor zorgen dat informatie met elkaar wordt gedeeld?	
Niveau 2	Worden jaarlijks de werkwijze en resultaten van de ISAC besproken?	
	Zijn ambities, toegevoegde waarde en activiteiten vastgelegd in een jaarplan?	
	Worden resources ad hoc beschikbaar gesteld voor ISAC-doeleinden (financiën, in-kind, personele inzet)?	
	Heeft de ISAC een afgestemde communicatiestrategie opgesteld?	
Niveau 3	Worden er gezamenlijk producten en/of processen ontwikkeld?	
	Is er een roadmap voor de middellange en lange termijn t.b.v. informatiedeling?	
	Worden resources structureel beschikbaar gesteld voor ISAC-doeleinden (financiën, in-kind, personele inzet)?	
	Is de ISAC een zelfstandige organisatie?	
	Worden er namens de ISAC PR-activiteiten ontplooid?	
	Legt de ISAC verantwoording af over de activiteiten en resultaten aan de deelnemende organisaties?	
	Hebben deelnemers mandaat om namens de eigen organisatie beslissingen te nemen en te handelen in de ISAC?	
	Is de value case van de ISAC explicit geformuleerd en vastgelegd?	

Manier van werken

	Capability	*Status*
Niveau 1	Zijn deelnemers verplicht richtlijnen en afspraken te ondertekenen alvorens deel te kunnen nemen aan informatiedeling?	
	Wordt het Traffic Light Protocol (TLP) gehanteerd?	
	Zijn de toetredingscriteria, procesafspraken en omgang met (vertrouwelijke) informatie vastgelegd in lidmaatschapsrichtlijnen?	
	Wordt er voor de bijeenkomsten een agenda opgesteld?	
	Is de rol van de voorzitter, vicevoorzitter en secretaris belegd?	
	Worden ISAC-bijeenkomsten gestructureerd (door het opstellen van agenda's en notulen)?	
Niveau 2	Komen ISAC-deelnemers in kleiner (thematisch) verband bij elkaar?	
	Vinden er activiteiten plaats buiten de ISAC-bijeenkomst?	
	Worden de werkafspraken omtrent informatiedeling nageleefd?	
	Zijn formele documenten centraal beheerd en toegankelijk voor ISAC-deelnemers (lidmaatschapsrichtlijnen, notulen, agenda's, etc.)?	
	Bereiden de voorzitter, vicevoorzitter en secretaris de ISAC-bijeenkomst voor en verdelen zij taken?	
Niveau 3	Heeft de ISAC dedicated capaciteit ter beschikking (communicatieadviseur, een analist, een projectmedewerker, technisch expert, etc.)?	
	Wordt de manier van werken systematisch verbeterd?	
	Zijn er formele afspraken en procedures opgesteld en van kracht t.b.v. het functioneren van de ISAC, de informatieuitwisseling en interne en externe samenwerking?	

Informatiestructuur en -management

	Capability	*Status*
Niveau 1	Wordt er op dit moment mondeling informatie gedeeld tussen deelnemers?	
Niveau 2	Wordt informatie volgens een methode vastgelegd en uitgewisseld?	
	Wordt er op digitale wijze informatie gedeeld (wanneer daar behoefte aan is)?	
Niveau 3	Wordt informatie ook (niet herleidbaar) buiten de ISAC gedeeld?	
	Wordt er op een online platform samengewerkt en informatie uitgewisseld?	
	Wordt informatie veilig beheerd en opgeslagen op een online platform?	
	Is er overeenstemming over de verschillen tussen operationele, tactische en strategische informatie?	
	Vindt informatiedeling (zo veel) mogelijk gestandaardiseerd plaats?	

Situational awareness en *lessons learned*

	Capability	*Status*
Niveau 1	Wordt door deelname aan de ISAC de (gemeenschappelijke) situational awareness verhoogd?	
	Vergroot deelname aan de ISAC de effectiviteit van mitigerende maatregelen in de eigen organisaties?	
Niveau 2	Wordt er (regelmatig) een sectoraal omgevingsbeeld opgesteld?	
	Wordt het omgevingsbeeld gedeeld met andere relevante organisaties?	
	Wordt informatie naar gelegenheid geduid en vertaald naar strategische en tactische informatie?	
	Wordt er bij het delen van informatie (TLP-AMBER en TLP-GROEN) bij gelegenheid handelingsperspectief toegevoegd?	
	Worden er af en toe good practices vastgesteld op basis van vorige ISAC-bijeenkomsten?	
Niveau 3	Wordt het sectorale gezamenlijk opgestelde dreigingsbeeld aan andere betrokkenen en relevante organisaties gedeeld t.b.v. collectieve situational awareness?	
	Worden er structureel analyses uitgevoerd en ontwikkelingen geduid met doorvertaling van mogelijke impact in de toekomst?	
	Wordt er structureel deelbaar handelingsperspectief toegevoegd bij informatie (TLP-AMBER en TLP-GROEN)?	
	Stellen ISAC-deelnemers structureel good practices vast op basis van inzichten uit (sectorale) trendanalyses, incidenten en informatie uit vorige ISAC-bijeenkomsten?	

Actie

	Capability	*Status*
Niveau 1	Nemen deelnemers voornamelijk deel aan de informatie-uitwisseling om goed in staat te zijn hun eigen bedrijf of organisatie veilig te houden?	
Niveau 2	Worden er activiteiten of initiatieven ontplooid die gericht zijn op het vergroten van de weerbaarheid van de sector of regio (gezamenlijk onderzoek uitvoeren, uitwisseling van medewerkers, gezamenlijke dreigingsanalyses, etc.)?	
Niveau 3	Worden er activiteiten of initiatieven ontplooid om samen de sector, regio en Nederland weerbaarder te maken?	
	Is de ISAC zichtbaar in de media, branche of regio?	

Voorwoord

Je bent met jouw organisatie gaan samenwerken binnen jouw sector en hebt een Information Sharing and Analysis Centre (ISAC) gestart. Een mooie eerste stap, maar je wilt je graag verder doorontwikkelen met jouw ISAC. In deze handreiking bieden we jou een helpende hand.

Op basis van de ervaringen van andere ISACs heeft TNO in opdracht van het NCSC een ISAC-ontwikkelmodel opgesteld. Dit model vertaalt theorie naar de praktijk. Zo kun je aan de hand van de checklist een beeld krijgen van het huidige niveau van jouw ISAC en bepalen welke ambitie je nastreeft.

De checklist vind je in de omslag van dit document of kun je online raadplegen via ncsc.nl/samenwerking. Verder vind je in deze handreiking verschillende handvatten en hulpmiddelen die je kunnen helpen om jouw ISAC verder door te ontwikkelen. Zo haal je meer uit jouw ISAC.

Toegestane verspreiding TLP: WHITE
(Traffic Light Protocol)

Deze handreiking Next Generation ISAC 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.

Haal meer uit je ISAC

Een Information Sharing and Analysis Centre (ISAC) is een uitstekend middel om met andere organisaties in je sector samen te werken om zo de digitale weerbaarheid van je organisatie te vergroten. Inmiddels zijn er in Nederland al vele ISACs opgericht. Deze ISACs verschillen op diverse vlakken van elkaar (frequentie, leden, focus, volwassenheidsniveau), wat ook past bij het ISAC-model.

Op basis van de ervaringen heeft TNO in opdracht van het NCSC een ISAC-ontwikkelmodel opgesteld. Dit ontwikkelmodel is vertaald naar een handreiking om de theorie in de praktijk te brengen. Deze handreiking helpt bestaande ISACs om de huidige werkwijze op een gestructureerde manier inzichtelijk te maken evenals de ambitie voor de samenwerking vast te stellen. Op basis van handvatten en hulpmiddelen draagt deze handreiking bij aan de verdere ontwikkeling van de ISAC.

Doelgroep

(Chief) information security officers van bedrijven en organisaties die reeds in een ISAC zitten.

Aan deze handreiking hebben bijgedragen

ISACs in de sectoren Airport, Chemie/Olie, Energy, Financial Institutions, Haven, Keren en Beheren, Nucleair, Rijk, Telecom en Water, en NZKG.

Deze handreiking is een samenwerking tussen

het Nationaal Cyber Security Centrum van het Ministerie van Justitie en Veiligheid, en TNO.

Wat is een ISAC?

Een ISAC is een sectoraal[1] overleg over met name cybersecurity-gerelateerde onderwerpen. Ook kunnen andere onderwerpen zoals cybercrime en datalekken in een ISAC besproken worden. In een ISAC creëer je een vertrouwde omgeving met organisaties uit dezelfde sector om gevoelige en vertrouwelijke informatie over incidenten, dreigingen, kwetsbaarheden, maatregelen en leerpunten op het gebied van cybersecurity te delen en indien van toepassing te analyseren.

Er is geen 'standaardvorm' van een ISAC. Een samenwerking in een ISAC kan formeel en informeel zijn; gestructureerd of flexibel; met fysieke vergaderingen, teleconferenties, via een digitaal platform of een mix hiervan. De deelnemers kiezen zelf de best passende vorm. In de handreiking 'Start een ISAC' staan adviezen die de ISAC-deelnemers in staat stellen de juiste keuzes te maken om een succesvolle samenwerking te starten.

Het ISAC-ontwikkelmodel

Ervaring leert dat samenwerking het beste werkt als de deelnemers zelf voor een vorm en werkwijze kiezen die bij hun past. Dit is ook te zien binnen het bestaande landschap van ISACs. De bestaande ISACs verschillen in frequentie, aantal deelnemende organisaties, het soort informatie dat gedeeld wordt en de mate van detail van deze informatie. Ook is de toegevoegde waarde van informatiedeling voor deelnemende organisaties verschillend. Het ontwikkelen van de manier waarop informatie wordt gedeeld vereist daarom maatwerk.

Wanneer een ISAC al langer bestaat, blijkt vaak de behoefte om meer uit de samenwerking te halen. Het ISAC-ontwikkelmodel kan de ISAC-deelnemers hierbij ondersteunen. Dit model heeft drie uitgangspunten:

1. Flexibiliteit ontwikkelmodel

Iedere ISAC bepaalt zijn eigen ambitie. Het ontwikkelmodel is flexibel te gebruiken en stuurt niet aan op een uniforme werkwijze.

2. Proportionaliteit staat centraal

De samenwerking en informatie-uitwisseling moet passen bij de sector, keten of regio. Hoe dit vormgegeven wordt hangt af van verschillende factoren zoals dreigingsniveau, type technologie, product of dienst en de risico's en effecten van de incidenten. Het ISAC-ontwikkelmodel biedt ruimte om tot de juiste verhouding te komen tussen het doel, doorontwikkeling van de ISAC, het middel en het ontwikkelmodel. Het gebruik van het ontwikkelmodel is geen doel op zich.

3. Stapsgewijs ontwikkelen

Het doorontwikkelen van de ISAC kost tijd en inspanning van de deelnemers. Je kunt met je ISAC je eigen pad uitstippelen en dit stapsgewijs vormgeven met behulp van het modulair opgebouwde ISAC-ontwikkelmodel.

1 De meest voorkomende vorm van een ISAC is sectoraal, maar het ISAC-model leent zich ook voor een samenwerking in de keten of regio. Meer specifieke adviezen voor het opzetten van een keten of regionale samenwerking kun je vinden via www.ncsc.nl/samenwerking.

Hoe ziet het model eruit?

Het model bestaat uit vijf capabilities en drie ontwikkelniveaus.

De vijf capabilities zijn: strategie en actieplan, manier van werken, informatiestructuur en informatiemanagement, situationeel beeld en geleerde lessen, en tenslotte actie.

Strategie en actieplan betreft het identificeren van de ambitie en behoefte die de sector heeft. Deze ambitie en behoefte kunnen impliciet blijven of worden vastgelegd in een gezamenlijk plan van aanpak.

De capability ***manier van werken*** richt zich op de activiteiten en afspraken die een effectieve en efficiënte interactie tussen de ISAC-deelnemers mogelijk maken.

Informatiestructuur en informatiemanagement zijn afspraken om cybersecurity-informatie efficiënt te specificeren en mogelijk te classificeren. Ook bevat deze competentie de methoden en middelen voor het delen, verzamelen, uitwisselen en opslaan van informatie.

De methoden en werkwijzen om informatie te duiden en daarmee het vermogen om inzicht op te doen en gezamenlijk te leren richt zich op de capability ***situationeel beeld en geleerde lessen***.

Samenwerking en gezamenlijk opvolging geven op basis van gedeelde informatie vindt beperkt plaats in de huidige ISACs. Dit vanwege de sterke focus op informatie-uitwisseling. Opvolging en handelingsperspectief is vervolgens een verantwoordelijkheid van de deelnemende organisaties zelf. De ***actie***-capability is bedoeld voor ISACs die de ambitie hebben daadwerkelijk samen te werken.

De hierboven beschreven capabilities zijn vervolgens opgedeeld in drie ontwikkelniveaus. Niveau 1 richt zich op de basis capability van een ISAC. Het tweede niveau bevat verder ontwikkelde capabilities die meer tijd en inspanning vragen. Het derde niveau bevat gevorderde capabilities van de ISAC.

ISAC-ontwikkelmodel	*Niveau 1*	*Niveau 2*	*Niveau 3*
Strategie en actieplan			
Manier van werken			
Informatiestructuur en -management			
Situationeel beeld en geleerde lessen			
Actie			

Hoe kan ik het model gebruiken?

De capabilities en niveaus hangen met elkaar samen omdat de ontwikkeling van veel capabilities een bepaalde basis vereist. Geadviseerd wordt om het model van boven naar beneden te gebruiken wanneer we het hebben over het opbouwen van capabilities. Voor iedere afzonderlijke capability is het raadzaam het eerdere niveau eerst ingericht te hebben alvorens een stap naar het volgende niveau te maken.

Bovenstaande is enkel een advies voor het gebruik maar geen harde eis. Maatwerk is mogelijk en blijft wenselijk.

“Om inzicht te hebben is het van belang om te weten waar je staat.”

Stap 1: Inzicht

Bepaal het huidige niveau van je ISAC

Om te weten waar je naartoe wilt groeien is het eerst van belang om te weten waar je staat als ISAC. Om je hierbij te helpen is er een checklist opgesteld waarmee je kan bepalen op welk niveau je zit per capability. Het wordt aangeraden om dit met alle deelnemers van de ISAC te doen zodat jullie een gezamenlijk beeld en daarmee uitgangspunt hebben.

Op basis van de antwoorden op de vragen uit de checklist ontstaat een beeld van het huidige niveau van de ISAC. Het kan voorkomen dat niet alle vragen met "ja" worden beantwoord. Het is aan de ISAC om te bepalen of deze voor de eigen samenwerking en verdere ontwikkeling van belang zijn. De enige die dat kan bepalen is de ISAC zelf.

Je vindt deze checklist in de binnenzijde van het omslag.

“Wanneer de gewenste situatie hoger ligt dan de bestaande situatie, is er dus een behoefte om te ontwikkelen.”

Stap 2: Groeien

Bepaal je ambitie

Om je ambitie te kunnen bepalen maak je gebruik van de checklist. Dit keer kijk je echter niet naar de bestaande situatie, maar naar de gewenste situatie.

Wanneer de gewenste situatie hoger ligt dan de bestaande situatie, is er dus een behoefte om te ontwikkelen. Door het ontwikkelen van bepaalde capabilities kan je als ISAC doorgroeien naar het gewenste niveau.

Om de ontwikkeling te ondersteunen is hieronder voor elk afzonderlijk niveau en per capability een overzicht van de kenmerken gegeven. Daarnaast worden er handvatten en hulpmiddelen aangereikt die je kunnen helpen in je ontwikkelbehoefte.

Elke ISAC bepaalt zelf tot welk niveau het zich wil ontwikkelen. Het behalen van het derde niveau niet een doel an sich. Het is belangrijker dat de ISAC zelf beziet welk niveau haalbaar is, maar belangrijker nog, benodigd is voor de eigen situatie. Het zal niet voor elke ISAC noodzakelijk zijn om op niveau drie te zitten. Kortom, bepaal binnen de ISAC de eigen ambitie.

Op de volgende pagina's worden de verschillende niveaus per capability toegelicht in een tabel.

Strategie en actieplan

Het expliciet maken van de koers en richting is een belangrijk onderdeel van de ISAC. Het wordt aangeraden om ambities en doelstellingen te beschrijven en daarover binnen de ISAC afstemming te hebben. Daarnaast is het nuttig om in een actieplan de concrete acties te benoemen om de ambities te kunnen realiseren. De verschillende ontwikkelniveaus variëren van bijeenkomsten met onderwerpen die ad hoc geagendeerd worden tot het gebruik van een roadmap voor de lange termijn. Overigens moet het expliciet maken van ambities en doelstellingen niet leiden tot een bureaucratische werkwijze. Een pragmatische aanpak welke aansluit bij de ISAC wordt hierbij aangeraden.

Aandachtspunten:

- Houd in de gaten of de ambities en het beoogde ontwikkelpad van de ISAC voor alle deelnemers duidelijk zijn.
- Maak het bespreekbaar wanneer ISAC-deelnemers onvoldoende tijd vrij (kunnen) maken voor actieve deelname.

	De capability 'Strategie en actieplan' is per niveau gekenmerkt door:	*Handvatten / hulpmiddelen*
Niveau 1	ISAC-deelnemers hebben steun van de eigen organisatie om te participeren in de ISAC. De ISAC-deelnemers hebben het gemeenschappelijke belang en doel van de samenwerking geformuleerd. Er is een gelijkwaardige relatie tussen alle ISAC-deelnemers. Oftewel, er is geen sprake van hiërarchische verhoudingen. Er is besproken welke soorten informatie wordt gedeeld. ISAC-deelnemers hebben besproken op welke manier informatie gedeeld wordt.	Het NCSC heeft een handreiking beschikbaar gesteld om een ISAC te starten, zie hiervoor: 'Start een ISAC: Sectoraal samenwerken'. De Amerikaanse Information Sharing and Analysis Organisations die opgericht is t.b.v. het cybersecurity-informatiedeling heeft een toegankelijke publicatie over de grondbeginselen van informatiedeling: 'Sharing and Analysis Organisation 100-1 Introduction to Information Sharing and Analysis Organizations' (2016)
Niveau 2	De ISAC heeft een jaarplan opgesteld waarin de ambitie, toegevoegde waarde en activiteiten van de ISAC zijn vastgelegd. Resources worden ad hoc beschikbaar gesteld voor ISAC-doeleinden (financiën, in-kind, personele inzet). Zorg voor een periodieke (jaarlijkse) evaluatie waarin de werkwijze en resultaten van de ISAC besproken worden. De ISAC stimuleert dat de business afspraken maakt op het gebied van communicatie en woordvoering in geval van incidenten zoals datalekken, trends en dreigingen, die in de sector plaatsvinden.	Door middel van een workshop kan een strategie en activiteitenplanning opgesteld worden voor het komende jaar. Leg de strategie en activiteitenplanning vast in een jaarplan. Plan aan het einde van het jaar een evaluatiemoment in waarbij het jaarplan geëvalueerd wordt en er voor het komende jaar nieuwe afspraken gemaakt wordt. Zorg dat de collega's van communicatie en/of woordvoering elkaar kennen of weten te vinden door middel van een bijeenkomst of door het hebben van een overzicht.
Niveau 3	Voor de ISAC is een langetermijnvisie en/of langetermijnroadmap opgesteld. De ISAC heeft een communicatiestrategie opgesteld. Resources worden structureel beschikbaar gesteld voor ISAC-doeleinden (financieel, in-kind, personele inzet). De value case van de ISAC is expliciet en schriftelijk geformuleerd.	Organiseer een workshop om de langetermijnvisie en communicatiestrategie op te stellen. Om de value case van de ISAC te beschrijven kan de TNO-publicatie over dit onderwerp handvatten bieden, zie: de TNO Value Case Methodology.

Manier van werken

Door het maken van afspraken wordt het delen van informatie vergemakkelijkt. De drie ontwikkelniveaus variëren van het gebruik van het Traffic Light Protocol en het opstellen van lidmaatschapsrichtlijnen tot aan het naleven van formele afspraken en procedures.

Aandachtspunten:

- Waak als groep over het aantal ISAC-deelnemers en grijp in wanneer het aantal onderling vertrouwen in de weg staat.
- Blijf aandacht schenken aan de manier van werken omdat dit grote invloed kan hebben op het efficiënt en effectief delen van informatie.
- Maak afspraken over wat te doen wanneer een ISAC-deelnemer meerdere keren niet aanwezig is bij een ISAC.

	De capability 'Manier van werken' is per niveau gekenmerkt door:	*Handvatten / hulpmiddelen*
Niveau 1	Het Traffic Light Protocol (TLP) wordt gebruikt om informatie-deling te bevorderen en de reikwijdte van de doelgroep te bepalen. De rol(len) van de voorzitter, vicevoorzitter en secretaris zijn aangewezen. De toetredingscriteria, procesafspraken en omgang met (vertrouwelijke) informatie zijn vastgelegd in lidmaatschaps-richtlijnen en zijn door iedere deelnemer ondertekend. ISAC-bijeenkomsten worden gestructureerd door een agenda te hanteren en het opstellen van notulen. Voor iedere ISAC-deelnemer is een vaste vervanger aangesteld om continuïteit te waarborgen.	Zorg dat men elkaar op de hoogte stelt van TLP-regels en het gebruik ervan. Lees hiervoor de FIRST Normdefinities en Gebruiksrichtlijnen en zie de webpagina 'Considerations on the Traffic Light Protocol' op de website van ENISA. Het NCSC heeft publicaties beschikbaar gesteld over het opzetten van een samenwerking in een regio of keten. Ook zijn hier verschillende templates te vinden die gebruikt kunnen worden als voorbeeld.
Niveau 2	De voorzitter, vicevoorzitter en secretaris bereiden de ISAC-bijeenkomst voor en verdelen taken (bijvoorbeeld het uitnodigen van gastsprekers, opstellen van een jaarplan, het ondernemen van acties gebaseerd op het jaarplan, het instellen/aanstellen van werkgroepen). Activiteiten vinden ook plaats buiten de ISAC-bijeenkomst doordat ISAC-deelnemers in kleiner (thematisch) verband bij elkaar komen om specifieke onderwerpen te bespreken en in werkgroepen onderwerpen verder uit te diepen. Formele documenten worden centraal beheerd en zijn toegankelijk voor alle ISAC-deelnemers (lidmaatschapsrichtlijnen, notulen, agenda's).	Analyseer en evalueer de taken, verantwoordelijkheden en benodigde tijd voor het houden van een ISAC. Organiseer ad hoc werkgroepen om aan thema's te werken en zorg dat de kennis weer terugvloeit naar alle ISAC-deelnemers. Organiseer kennismakingssessies of gezamenlijke bijeenkomsten met andere ISACs.
Niveau 3	De ISAC stelt dedicated capaciteit ter beschikking voor het behalen van de ISAC-doelen (zoals geformuleerd in het jaarplan). De manier van werken wordt systematisch verbeterd. Er zijn formele afspraken en procedures opgesteld t.b.v. het functioneren van de ISAC, de informatie-uitwisseling en interne en externe samenwerking.	Experimenteer met verschillende/nieuwe manieren van werken door te leren van andere nationale en internationale ISACs en samenwerkingsverbanden. Een document met best practices voor (veilig) informatie-management is beschikbaar in het ISO/IEC 27002 Best Practice for Information Management System.

Informatiestructuur en informatiemanagement

De ISAC staat of valt met de informatie die gedeeld wordt. Daarbij is het wenselijk dat de informatie ook bruikbaar is voor de eigen organisatie (achterban) of anderen in de omgeving (klanten, afnemers, leveranciers). Het maken van afspraken hierover, de wijze van het vastleggen van informatie op een uniforme manier en het centraal beheren van de informatie zijn voorbeelden die bijdragen aan de ontwikkeling van de ISAC. Dit vergroot de vindbaarheid, veiligheid en volledigheid van de informatie. Een digitaal platform waarmee op vertrouwelijke wijze informatie over incidenten, dreigingen, kwetsbaarheden, maatregelen, administratiegegevens en leerpunten verstuurd en ontvangen kan worden helpt bij de professionalisering. De drie niveaus van de capability 'Informatiestructuur en informatiemanagement' variëren van het ad hoc delen en opslaan van cybersecurity-informatie tot het gestandaardiseerd en gestructureerd opslaan en uitwisselen van informatie.

Aandachtspunten:

- Evalueer regelmatig of de juiste randvoorwaarden aanwezig zijn om informatie te delen.
- Maak afspraken over beheer en gebruik van de tooling.

	De capability 'Informatiestructuur en -management' is per niveau gekenmerkt door:	*Handvatten / hulpmiddelen*
Niveau 1	Informatie wordt mondeling gedeeld tussen ISAC-deelnemers.	Maak een lijst van soorten incidenten (Ddos, datalek, phishing, etc.) die tijdens het 'rondje rood' gehanteerd wordt ten behoeve van informatiedeling.
Niveau 2	Informatie welke gedeeld wordt in een ISAC-bijeenkomst wordt volgens een methode vastgelegd en uitgewisseld. Er wordt naar behoefte op digitale wijze informatie gedeeld.	Informatie welke gedeeld wordt in het 'rondje rood' is enkel bruikbaar voor de aanwezige ISAC-deelnemers. Om deze informatie breder te verspreiden zodat anderen binnen en buiten de organisatie hier ook baat bij hebben is het noodzakelijk om informatie te "veramberen". Hiervoor kan gebruik gemaakt worden van het Template Ambering formulier op ncsc.nl. Gebruik mailinglijsten, veilige app-groepen, conference-call software, etc. Publicatie: ENISA, Group Communications for incident response and operational communities.
Niveau 3	Informatie wordt gedeeld met partijen buiten de ISAC. Informatie wordt veilig beheerd, opgeslagen en uitgewisseld middels een online platform. ISAC-deelnemers wisselen informatie uit en werken samen op een online platform. Er wordt onderscheid gemaakt tussen operationele, tactische en strategische informatie. Informatiedeling is (zo veel) mogelijk gestandaardiseerd.	Maak afspraken over het delen van deze informatie buiten de ISAC met andere ISACs of organisaties en leg deze afspraken vast in bijvoorbeeld de lidmaatschapsrichtlijnen. Stel richtlijnen op voor het (veilig) gebruik van een platform. Bestaande gangbare normen (zoals de ISO/EC 2700:x) kunnen houvast bieden om veilig informatie te beheren, op te slaan en te delen. Informatie en best practices over informatiebeveiliging (vanuit overheidsperspectief) is beschikbaar via het Centrum Informatiebeveiliging en Privacybescherming.

Situational awareness en *lessons learned*

Het delen van informatie over ontwikkelingen in een sector of branche zorgt ervoor dat iedereen op de hoogte is van belangrijke gebeurtenissen. De capability *'Situational awareness* en *lessons learned'* draagt bij aan het vergroten van het lerend vermogen van de ISAC. Dit bevat het analyseren, duiden en verrijken van informatie (incidenten, dreigingen en mitigatie van incidenten) en het structureel uitwisselen van best practices en handelingsperspectieven. Kortweg richt deze capability zich op de 'A' van de afkorting ISAC, namelijk 'Analysis'. De ontwikkelniveaus van situational awareness en lessons learned variëren van ad hoc discussies over incidenten, ontwikkelingen en dreigingen, tot het hanteren van methoden om informatie op te stellen, te analyseren, te verspreiden en structureel van te leren.

Aandachtspunten:

- Wanneer er geen duidelijke afspraken zijn over het delen van informatie kan dit schadelijk zijn voor het onderlinge vertrouwen.
- Let erop dat er onder de ISAC-deelnemers verschillende ideeën kunnen leven over het delen en verder verspreiden van bedrijfsspecifieke situational awareness inzichten, ondanks inspanningen om de informatie te anonimiseren.

	De capability 'Situational awareness en lessons learned' is per niveau gekenmerkt door:	*Handvatten / hulpmiddelen*
Niveau 1	Deelname aan de ISAC vergroot het inzicht van organisaties over dreigingen en kwetsbaarheden en ondersteunt daarmee de effectiviteit van mitigerende maatregelen van ISAC-deelnemers op individueel niveau.	
Niveau 2	Situational awareness wordt vergroot doordat er (regelmatig) een sectoraal omgevingsbeeld wordt opgesteld. Het omgevingsbeeld wordt gedeeld met andere relevante organisaties. Informatie wordt naar gelegenheid geduid en vertaald naar strategische en tactische informatie. Bij het delen van informatie (TLP-AMBER en TLP-GROEN) wordt indien mogelijk een handelingsperspectief toegevoegd.	Stel een werkgroep in om de belangrijkste inzichten vanuit de ISAC vast te leggen in een sectorale rapportage. Leg handelingsperspectief vast en deel dit met andere ISACs.
Niveau 3	Situational awareness wordt vergroot door het intern en extern delen van sectorale dreigings- en omgevingsbeelden. Situational awareness wordt vergroot door analyses van ontwikkelingen en door deze inzichten door te vertalen naar de toekomst. Voeg structureel deelbare handelingsperspectieven toe wanneer informatie (TLP-AMBER en TLP-GROEN) gedeeld wordt. Stel structureel good practices vast op basis van inzichten uit (sectorale) trendanalyses, incidenten en informatie uit vorige ISAC-bijeenkomsten.	Vraag ondersteuning bij partners van de ISAC voor het opstellen van een sectorale rapportage. Maak gebruik van informatie van andere ISACs (binnen en buiten Nederland) en samenwerkingsverbanden. Publicatie: MS-ISAC, Water ISAC Announce Partnership to Promote Cross-Sector Security Collaboration. Er zijn verschillende toekomstgeoriënteerde methoden beschikbaar om zo eerder signalen of potentiële bedreigingen te zien aankomen. Hierbij kan gedacht worden aan horizon scanning activiteiten. Maak contact met vergelijkbare ISACs in het buitenland of Europese ISACs.

Actie

Vanuit informatie-uitwisseling en analyse in een ISAC ontstaan mogelijkheden om meer of anders samen te werken en gezamenlijk opvolging te geven aan inzichten. Voorbeelden hiervan zijn gedeelde onderzoeksprogramma's, het uitwisselen van personeel, het publiceren van rapportages en het optreden of handelen als groep namens een sector of keten. De ontwikkelniveaus van actie variëren van focus op de weerbaarheid van de eigen organisatie tot aan focus op de sector of de Nederlandse samenleving.

Aandachtspunten:

- Niet iedere deelnemer zit met hetzelfde mandaat aan tafel. Wanneer er activiteiten ontplooid worden naast informatiedeling dan dient rekening gehouden te worden met het mandaat van de deelnemers in de ISAC. Maak hier expliciete afspraken over.

	De capability 'Actie' is per niveau gekenmerkt door:	*Handvatten / hulpmiddelen*
Niveau 1	Activiteiten zijn gericht op de weerbaarheid van individuele ISAC-deelnemers.	
Niveau 2	Er worden activiteiten ontplooid gericht op het verhogen van de weerbaarheid van de sector en/of de regio.	Gezamenlijk onderzoek uitzetten of uitvoeren kan een toegevoegde waarde zijn voor de ISAC-deelnemers en de sector. Bied ruimte aan studenten, stagiaires en onderzoekers voor onderzoek gericht op de sector. Kennis delen en ervaringen opdoen kan gefaciliteerd worden door medewerkers onderling uit te wisselen. Stimuleer kennisdeling tussen ISACs door gezamenlijke bijeenkomsten te organiseren.
Niveau 3	Activiteiten zijn gericht op het vergroten van de weerbaarheid van de sector en van Nederland. De ISAC is zichtbaar in de media, branche of regio door proactieve informatiedeling.	Stel jaarlijkse informatie voor andere organisaties beschikbaar, zoals gecoördineerde deelname aan campagnes. Bij consultaties of discussies over standaardisatie en nieuwe wet- en regelgeving kan de ISAC gezamenlijk optreden.

“In de toekomst kunnen ISACs proactiever gaan functioneren, om zo meer grip te krijgen op de digitalisering, snelheid van technologische ontwikkelingen en de verschuivende dreigingen.”

Stap 3: Ontwikkelen

Aan de slag

Het ontwikkelen van capabilities kost tijd, energie en in sommige gevallen ook geld. Het is niet raadzaam om zeven capabilities gelijktijdig te ontwikkelen. Het advies is daarom om niet meer dan twee capabilities tegelijk aan te pakken. De ontwikkelambitie en bijbehorende planning wordt idealiter opgenomen in de strategie en het actieplan van de ISAC.

Het model voorbij

Er zijn meer ontwikkelactiviteiten waar een ISAC aan kan denken, welke buiten dit model vallen.

Als ISAC kan het overwogen worden de samenwerking meer te formaliseren in de vorm van een stichting om middelen te bundelen, wat kan helpen met de professionalisering en uitbouw van de capabilities van een ISAC.

Activiteiten die verder reiken dan (het ontwikkelmodel van) de ISAC zijn het formaliseren van de samenwerking door gezamenlijk te starten met een sectoraal CERT/CSIRT[2], geautomatiseerd informatie[3] met elkaar te delen, en/of dreigingsinformatie[4] in te kopen, te analyseren en (geautomatiseerd) te verwerken.

Tevens zou het er in de toekomst naartoe kunnen gaan dat ISACs proactiever functioneren door te werken op basis van cyberforecasting informatie, om zo meer grip te krijgen op de digitalisering, snelheid van technologische ontwikkelingen en de verschuivende dreigingen.

Het model is bedoeld als een opmaat naar het zetten van de volgende stappen, maar zoals gebruikelijk zijn er meerdere wegen naar Rome. Het toepassen van hetgeen bij de eigen ISAC past blijft dan ook voorop staan.

Verder lezen

- ENISA-publicatie over cybersecurity gedragsaspecten (Engels), 2019, https://www.enisa.europa.eu/news/enisa-news/behavioural-aspects-of-cybersecurity
- Samenwerking in een ISAC | Aan de slag, 2018, Nationaal Cyber Security Centrum, https://www.ncsc.nl/aan-de-slag/samenwerken/start-zelf-samenwerking/samenwerking-sector
- Lidmaatschapsrichtlijnen van de Amerikaanse Research Education Networking Information Sharing & Analysis Center (REN-ISAC), https://www.ren-isac.net/membership/MembershipDocs/REN-ISAC_Membership_Guide.pdf
- Het MaGMa Use Case Framework (UCF) helpt organisaties met het operationaliseren van hun security monitoring strategie. Management, Growth, Metrics & assessment; Use Case Framework (UCF), https://www.betaalvereniging.nl/veiligheid/publiek-private-samenwerking/magma/
- Factsheet SOC inrichten: begin klein en Measuring capability maturity in Security Operations Centers (SOC-CMM), https://www.ncsc.nl/aan-de-slag/richt-een-soc-in
- Handboek MISP en Guide to Cyber Threat Information Sharing, NIST Special Publication 800-150, https://www.circl.lu/doc/misp/book.pdf
- Cyber threat intelligence sharing through national and sector-oriented communities, Frank Fransen & Richard Kerkdijk; Collaborative Cyber Threat Intelligence, Auerbach Publications, 2017. pp. 187-224, https://www.crcpress.com/Collaborative-Cyber-Threat-Intelligence-Detecting-and-Responding-to-Advanced/Skopik/p/book/9781138031821

2 Factsheet SOC inrichten: begin klein en Measuring capability maturity in Security Operations Centers (SOC-CMM)

3 Handboek MISP en Guide to Cyber Threat Information Sharing, NIST Special Publication 800-150

4 Cyber threat intelligence sharing through national and sector-oriented communities, Frank Fransen & Richard Kerkdijk; Collaborative Cyber Threat Intelligence, Auerbach Publications, 2017.

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

Januari 2020