Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Start een ISAC: Sectoraal samenwerken

Handreiking

Stappenplan sectorale samenwerking

Om aan de slag te gaan met het versterken van de digitale weerbaarheid in je sector, heeft het NCSC samen met het DTC en de ISAC's een handreiking opgesteld. Hierin worden drie fases gepresenteerd om te komen tot een succesvolle samenwerking en deze te bestendigen.

Fase 1: Verkennen

Zoek gelijkgestemden en creëer draagvlak:

- Begin klein met enkele enthousiaste (chief) information security offers.
- Zet een informele werkgroep op en leer elkaar beter kennen.
- Ga tijdens de eerste bijeenkomst op zoek naar gezamenlijke doelen en andere overeenkomsten.

Fase 2: Opzetten

Zet een solide basis neer:

- Organiseer een kick-off meeting om de ISAC formeel te starten.
- Maak afspraken over wie de rol van voorzitter, vice-voorzitter en secretaris op zich neemt.
- Spreek af hoe vaak je bij elkaar wilt komen en hoe je onderling gaat communiceren.
- Stel richtlijnen op voor het lidmaatschap en informatie-uitwisseling.

Fase 3: Continueren

Blijf samen aan vertrouwen bouwen:

- Wees kritisch op je eigen deelname aan de ISAC.
- Maak ruimte om te evalueren.
- Blijf focussen op de meerwaarde van informatie-uitwisseling.

Start een ISAC

Wil je de digitale weerbaarheid van je sector verhogen? Start een ISAC!
Een Information Sharing and Analysis Centre (ISAC) is een uitstekend middel om met andere organisaties in jouw sector samen te werken om de digitale weerbaarheid van je organisatie te vergroten. Je kunt daarvoor gebruik maken van jarenlange ervaring van het NCSC en van organisaties die zelf een ISAC hebben opgezet.

Het starten van een ISAC met sectorale concurrenten klinkt misschien als een grote stap die veel tijd, geld en middelen kost. Gelukkig blijkt uit de praktijk dat dit niet het geval is. Door met een paar collega-informatiespecialisten uit je sector te starten met ervaringen en informatie uit te wisselen, heb je al een begin gemaakt. In deze handreiking geven we je onze 'best practices' uit al deze ervaringen.

Doelgroep

(Chief) information security officers van bedrijven en organisaties die een start willen maken met het opzetten van een ISAC.

Aan deze handreiking hebben de volgende ISAC's bijgedragen:

Airport, Chemie/Olie, Energy, Financial Institutions, Haven, Keren en Beheren, Legal, Media, Multinationals, Managed Service Providers, Nucleair, Pensioen, Rijksoverheid, Telecom, Water en Zorg.

Deze handreiking is een samenwerking tussen

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

"Door gezamenlijk incidenten te analyseren en elkaar op de hoogte te houden van (voorgenomen) maatregelen, zorgen we er als Managed Service Providers voor dat klanten van verschillende MSP's geen wezenlijk verschillende adviezen krijgen. Dit voorkomt verwarring bij onze (gezamenlijke) klanten en creëert de rust die nodig is om een incident goed aan te pakken."

MSP-ISAC

Wat is een ISAC?

Een ISAC is een sectoraal[1] overleg over cybersecurity. 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.

Er is geen 'standaardvorm' van een ISAC. Een samenwerking in een ISAC kan formeel of informeel zijn; gestructureerd of flexibel; met fysieke vergaderingen, teleconferenties, via een digitaal platform of een mix van deze drie. De deelnemers kiezen zelf de best passende vorm. In deze handreiking staan adviezen die jou en je partners in staat stellen de juiste keuzes te maken om een succesvolle samenwerking te starten. Ervaring leert dat samenwerking het beste werkt als de deelnemers zelf voor een vorm die bij hen past.

Nut en noodzaak van een ISAC

Leren van elkaar

Het doel van een ISAC is om door uitwisseling van kennis en ervaring de digitale weerbaarheid van jouw organisatie en de sector te verhogen. Door te leren van incidenten en effecten van mitigerende maatregelen bij andere organisaties kun je anticiperen om soortgelijke incidenten binnen je eigen organisatie te voorkomen of sneller te mitigeren.[2] De ene keer leer jij van anderen, de andere keer leren anderen van jou - een incident bij de een leidt tot preventie voor de ander.

Versterking kwaliteit cybersecurity

Door samenwerking binnen je sector ontvang je sneller informatie en krijg je een (beter) situationeel beeld van de potentiële dreigingen. Je kunt aanvallen detecteren die je anders niet had opgemerkt. Je leert betere risico-inschattingen te maken en effecten van mitigerende maatregelen te beoordelen.

Kostenreductie

Een verstoring van bedrijfsprocessen kost geld. Van elkaar leren kan de kans hierop verkleinen. Door samen te werken kun je ook gezamenlijk vraagstukken oppakken. Dit kost minder tijd en geld doordat je niet zelfstandig een oplossing hoeft te bedenken of het wiel opnieuw hoeft uit te vinden.

Imago

Aan (potentiële) klanten laat je via deze samenwerking zien dat je de continuïteit van dienstverlening en de bescherming van gevoelige data hoog in het vaandel hebt staan. Daarnaast kan je deelname aan een ISAC helpen potentiële reputatieschade te voorkomen.

Leading by doing

Samenwerking op het gebied van cybersecurity kan een onderdeel zijn van het Maatschappelijk Verantwoord Ondernemen-beleid van je organisatie.

Hoe ga je te werk?

Vertrouwen, gedeelde belangen en gelijkwaardigheid zijn randvoorwaarden voor succes. Als je vanaf het eerste moment inzet op bouwen van vertrouwen en zoeken naar gedeelde belangen door gelijkwaardigheid binnen je ISAC, kies je de weg naar de beste resultaten.

Vertrouwen

Vertrouwen is de sleutel tot samenwerking. Je moet ervan uit kunnen gaan dat de informatie die jij deelt niét morgen in de krant staat. Of dat informatie niet zomaar wordt doorgestuurd en de ander zich aan gemaakte afspraken houdt. Zonder vertrouwen is een ISAC gedoemd te mislukken.

Welke middelen zet je in om vertrouwen te bouwen? Bijvoorbeeld richtlijnen voor het lidmaatschap en afspraken over hoe en met wie informatie gedeeld mag worden. Voor het laatste wordt aangeraden van het Traffic Light Protocol (TLP)[3] gebruik te maken. Ook vaste vertegenwoordigers, dus steeds dezelfde gezichten, zorgen voor een snellere opbouw van vertrouwen

Ga ook eens na een overleg samen iets drinken of een hapje eten. Het helpt als je elkaar ook op een informele manier leert kennen. Kortom: investeer in de relatie, gedraag je betrouwbaar, kom je beloften na en geef het goede voorbeeld.

"Het kost echt tijd om vertrouwen te krijgen, maar laat dit geen belemmering zijn om te starten, het resultaat is de moeite waard!"

Nucleair-ISAC

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.

2 Zie ook https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models.

3 https://www.first.org/tlp

Gedeeld belang

Wat is jouw belang of dat van jouw organisatie om aan een ISAC deel te nemen en hoe zit dat met de andere deelnemers? Praat daarover met elkaar en leg eerlijk en open op tafel hoe je er in zit. Je zult dan al snel ontdekken wat het gedeeld belang is. Wanneer je aan een gezamenlijk doel werkt, krijgt de ISAC al meerwaarde. Overigens mogen verschillende belangen ook blijven bestaan, mits deze uitgesproken en niet conflicterend zijn. In dat laatste geval ga je elkaar tegenwerken en is de ISAC geen lang leven beschoren.

Gelijkwaardigheid

De beste samenwerking is die waar deelnemers gelijkwaardig zijn aan elkaar. Dat betekent dat er geen sprake is van hiërarchische verhoudingen. Als buiten de ISAC organisaties verantwoording aan elkaar moeten afleggen, zal de bereidheid tot informatiedeling binnen de ISAC waarschijnlijk beperkt zijn. Je legt niet al je gevoeligheden op tafel, als je daar later op kan worden afgerekend.

In de volgende drie fases vind je concrete stappen om een ISAC op te zetten. De volgorde waarin je de stappen neemt is je eigen keuze. Samenwerken is tenslotte maatwerk.

Fase 1: Verkennen

Zoek gelijkgestemden en creëer draagvlak

Zoek binnen jouw sector naar gelijkgestemde partijen, die willen samenwerken en actief bezig zijn om de digitale weerbaarheid binnen hun organisatie en sector te vergroten. Begin klein met enthousiaste (chief) information security officers die in hun dagelijks werk bezig zijn met cybersecurity-vraagstukken op tactisch niveau. Met deelnemers uit drie tot vijf organisaties kom je al heel ver. Zij zullen in staat zijn de informatie die in een ISAC gedeeld wordt te vertalen naar het werk van de specialisten binnen de eigen organisatie.

Klein beginnen helpt om snel van start te gaan, vertrouwen op te bouwen en om te bepalen hoe de samenwerking eruit moet zien. Ervaring leert ook dat 20 tot 25 organisaties de limiet is. Hoe groter de groep, des te lastiger om af te spreken. Men is minder bereid informatie te delen en vertrouwen te geven, en op de langere termijn wordt het moeilijker het vertrouwen te behouden.

"Als onderdeel van de aanpak van cyberdreigingen en kwetsbaarheden hebben twee security-officers het initiatief genomen om een Legal-ISAC op te richten. Wij hebben collega's van andere kantoren benaderd die meteen zeer enthousiast waren. Hierop hebben wij een eerste sessie gepland. Met hulp van het NCSC zijn de doelstellingen concreet gemaakt. Hierna zijn wij officieel gestart, onlangs is hierover ook gepubliceerd waarna wij nog meer verzoeken ontvingen voor deelname. Een groot succes!" [4]

Legal-ISAC

Een incident binnen je organisatie of een grootschalig incident dat het nieuws haalt, creëert momentum voor de start van een ISAC. Reguliere contacten met collega's binnen je sector kunnen ook een startpunt bieden. Vaak kom je dezelfde personen in verschillende situaties tegen en kom je samen tot de conclusie dat het starten van een ISAC een goed idee kan zijn.

Wanneer je enkele collega's van andere organisaties binnen je sector hebt gevonden die het belang delen en de noodzaak zien voor het starten van een samenwerking, is de tijd rijp om hen samen te brengen in een informele werkgroep.

Leer elkaar beter kennen, wees open en stel veel vragen tijdens de eerste bijeenkomst. Neem de tijd voor het beantwoorden van onderstaande vragen en ga niet verder voor je overeenstemming bereikt over de antwoorden. Zo leg je het fundament voor een succesvolle samenwerking. Voor het beantwoorden van de vragen kunnen meerdere bijeenkomsten nodig zijn.

De volgende vragen kunnen hierbij helpen:

Wie zijn wij en wat hebben we gemeen?
Denk hierbij aan processen, systemen, ketenafhankelijkheden, gezamenlijke uitdagingen, incidenten.

Wat is het gezamenlijke doel?
Voorbeelden van een gezamenlijk doel zijn uitwisseling van informatie over dreigingen en incidenten, standaardisatie binnen de sector en bespreken van nieuwe ontwikkelingen en trends.

Hebben we nog andere organisaties nodig om dit doel te bereiken?
Maak gebruik van elkaars kennis en netwerk. Een (beperkte) stakeholderanalyse kan uitkomst bieden. Natuurlijk kan een ISAC met veel leden de ambitie zijn, maar het is belangrijk eerst de basis op orde te hebben.

Wat voor informatie willen wij samen gaan delen?
Denk hierbij aan niveaus van informatie (operationeel, tactisch, strategisch), type informatie (cybersecurity, privacy, cybercrime, fraude etc.) en belangrijke thema's (cloud security, cyber threat intelligence, risico management, asset management, Internet of Things, netwerk segmentering, honeypots etc.). Bedenk aan de hand hiervan samen welke functionarissen van een organisatie in de ISAC zitting zouden moeten hebben.

Zijn wij de juiste personen die in de ISAC moeten zitten?
Bepaal samen wie de genodigden voor een eerste ISAC-bijeenkomst zijn. Het kan betekenen dat de personen die het initiatief genomen hebben en nu bij elkaar zitten, niet de juiste personen zijn om in de ISAC te zitten. Vraag jezelf dus af of jij de juiste persoon bent om deel te nemen aan de ISAC en vraag dit ook aan de anderen die aan tafel zitten.

Tip: Maak de groep voor de kick-off niet te groot. Enerzijds vanwege het opbouwen van vertrouwen en daarnaast omdat je nog moet vaststellen wat de criteria zijn voor deelname. Groei is makkelijker dan krimp.

Adviezen

- Wees transparant over je eigen organisatiedoelen en –belangen.
- Wees open over wat je wel en niet kan bieden en wat hiervoor belemmeringen zijn.
- Maak gebruik van bestaande structuren of netwerken met enthousiaste en kundige vakmensen.
- Gebruik de antwoorden op bovenstaande vragen als input voor de richtlijnen van het lidmaatschap van jullie samenwerkingsverband (zie ook fase 2).

4 http://www.advocatie.nl/grote-kantoren-binden-strijd-aan-met-cybercrime-legal-isac

Fase 2: Opzetten

Zet een solide basis neer

Organiseer een kick-off om de ISAC formeel te starten. Dit doe je nadat je de eerste (verkennende) gesprekken hebt gevoerd met enthousiaste collega's. Belangrijk is om de eerder genoemde vragen als groep te hebben beantwoord: wat maakt dat jullie bij elkaar willen komen en welk doel streven jullie gezamenlijk na?

Een kick-off is een bijeenkomst die de start van je samenwerking markeert. Voordat je de inhoud in duikt, is het van belang dat je de tijd en ruimte neemt om elkaar te leren kennen, afspraken te maken en deze te bekrachtigen.

Kennismaking

Vaak ken je een of meer deelnemers al, wat echter niet wil zeggen dat je ze écht kent of al voldoende vertrouwt. Organiseer tijdens de kick-off ruimte om hierin te investeren. Denk aan verschillende werkvormen. Je kan een 'speeddate' organiseren waarbij je werk gerelateerde en persoonlijke vragen aan elkaar kunt stellen. Ook een gezamenlijke lunch, diner of borrel is een prettige vorm.

Rollen

Nadat je uitgebreid kennis hebt gemaakt, kies je gezamenlijk vanuit de aanwezigen een voorzitter, vicevoorzitter en secretaris. Deze drie rollen zijn noodzakelijk om het overleg te structureren, het proces te bewaken en het overleg doelgericht te laten zijn. Het spreekt voor zich dat de deelnemers zelf verantwoordelijk zijn voor het succes van de samenwerking. De onderwerpen die besproken worden, de informatie die gedeeld wordt en de resultaten die uit het overleg voortvloeien, zijn het product van actieve samenwerking van iedereen.

"De belangrijkste taak als (vice-)voorzitter is om te begrijpen wat de belangrijkste informatiebeveiligingsrisico's en -incidenten zijn van de leden van de ISAC en zorgen dat we het dáár over hebben. Het is iedere keer prachtig om te zien hoeveel kennis er aanwezig is binnen de ISAC en hoe bereidwillig men is om kennis en ervaring - ook als iets verkeerd is gegaan - te delen met anderen."

Multinationals-ISAC

De voorzitter leidt niet alleen de vergadering, maar is ook de aanjager van de ISAC. De voorzitter daagt de leden uit om informatie te delen en deelnemers te motiveren een actieve rol te spelen in de samenwerking. Ook neemt de voorzitter zelf actief deel aan het overleg. Externe communicatie over de werkzaamheden van de ISAC wordt in eerste instantie gedaan door de voorzitter van de ISAC. De voorzitter acteert namens de leden van de ISAC.

"De voorzitter faciliteert het ISAC-overleg en stimuleert het netwerken waarbij cybergebeurtenissen zoveel mogelijk met elkaar worden gedeeld. Kennisverrijking en -deling is en blijft een motto om samen Nederland weerbaarder te maken."

Rijks-ISAC

De vicevoorzitter is de vervanger van de voorzitter, en wordt betrokken bij de totstandkoming van de agenda van de ISAC-bijeenkomsten. De vicevoorzitter fungeert samen met de voorzitter als eerste aanspreekpunt voor verzoeken van andere organisaties die willen toetreden tot de ISAC.

"Het (vice-) voorzitterschap van de ISAC geeft je energie om niet enkel de veiligheid en weerbaarheid van je eigen organisatie naar een next level te brengen maar tevens voor de hele sector."

Pensioen-ISAC

De secretaris heeft naast de voorzitter een belangrijke rol zowel voor, tijdens als na het overleg. De secretaris ziet erop toe dat de processen (afspraken, procedures) zoals afgesproken opgevolgd worden. Daarnaast zorgt de secretaris ervoor dat elke deelnemer de richtlijnen van het lidmaatschap kent en getekend heeft. De secretaris is de persoon die de bijeenkomsten organiseert, de uitnodigingen verstuurt en zorgt voor de agenda en een verslag van de bijeenkomsten. Ook is de secretaris verantwoordelijk voor het bijhouden van een ledenadministratie. Bovendien kan de secretaris inhoudelijk deelnemer van het overleg zijn.

"Als secretaris ben je de verbindende schakel binnen de ISAC. Samen met de VZ en VVZ geef je richting aan de ISAC en zorg je dat de ISAC optimaal kan functioneren. Een dankbare taak!"

NCSC

Frequentie

Het is goed om met elkaar af te spreken hoe vaak je bij elkaar wilt komen: vier keer per jaar, elke maand of een andere frequentie. De bestaande ISAC's vergaderen normaliter tussen de vier en acht keer per jaar. Het is ook belangrijk om af te spreken waar de bijeenkomsten gehouden worden en hoe lang deze duren. Is er overeenstemming over de frequentie, dan kunnen vergaderdata voor een heel jaar worden afgesproken. Zo'n jaarplanning helpt om de continuïteit van de onderwerpen en aanwezigheid van de leden te borgen.

Communicatie

Het is verstandig om een maillijst op te stellen. Een maillijst is een besloten lijst (aangeboden door verschillende webhosting- bedrijven), waarin je de e-mailadressen van de leden opvoert (alleen persoonlijke adressen, geen functionele mailboxen). Vergeet hierbij niet veiligheidsmaatregelen te treffen om integriteit en confidentialiteit te waarborgen[5].

Deze lijst kun je besloten maken zodat alleen de deelnemers op de lijst ernaar kunnen mailen. De beslotenheid zorgt er mede voor dat deelnemers buiten fysieke bijeenkomsten elkaar op een laagdrempelige manier weten te vinden om informatie uit te wisselen of vragen te stellen. Dit helpt bij het versterken van de vertrouwensbasis. Spreek af wie het (leden)beheer van de maillijst doet. In de meeste gevallen zal dit bij de secretaris belegd worden.

In een verder stadium is het handig om een gemeenschappelijke en vertrouwde plek in te richten om documenten te delen, zoals een teamsite. Dit komt de informatie-uitwisseling ten goede.

Richtlijnen voor het lidmaatschap

Het laatste onderwerp waar je ruim de tijd voor moet nemen tijdens de kick-off zijn de richtlijnen voor het lidmaatschap[6].

Richtlijnen voor het lidmaatschap zijn de onderliggende afspraken van de ISAC. Dit is nadrukkelijk géén juridisch document waar rechten aan ontleend kunnen worden, maar vooral een informele overeenkomst. Hierin maak je met elkaar fundamentele keuzes over de toetredingscriteria van nieuwe organisaties (scope van samenwerkingsverband) en criteria voor de persoonlijke vertegenwoordigers (niveau, rol, etc.). Daarnaast zet je in de richtlijnen procesafspraken over de toetreding van nieuwe organisaties en vertegenwoordigers en het wijzigen van de richtlijnen. Ook bevat dit document afspraken over afwezigheid van een organisatie. Aanwezigheid en de bereidheid van deelnemers om te delen is immers de sleutel tot succesvolle samenwerking – zonder dit heeft samenwerking geen zin. Ten slotte bevat dit document afspraken over hoe je omgaat met informatie die je met elkaar deelt.

Het NCSC adviseert om bij informatiedeling het Traffic Light Protocol (TLP) van FIRST te gebruiken[7]. Dit is binnen het cyberdomein een gerenommeerd en algemeen bekend protocol voor informatie-uitwisseling. Het is essentieel dat alle leden dit protocol begrijpen en hiernaar handelen, om het vertrouwen te waarborgen.

5 https://www.ncsc.nl/actueel/factsheets/factsheet-bescherm-domeinnamen-tegen-phishing.html
https://www.ncsc.nl/actueel/factsheets/factsheet-beveilig-verbindingen-van-mailservers.html
https://www.ncsc.nl/actueel/factsheets/factsheet-gebruik-tweefactorauthenticatie.html

6 Zie template lidmaatschapsrichtlijnen ISAC op http://www.ncsc.nl/samenwerking.

7 Zie gehele richtlijn op www.first.org/tlp.

Fase 3: Continueren

Blijf samen aan vertrouwen werken

Blijf aandacht besteden aan behouden en versterken van vertrouwen binnen je samenwerkingsverband. Vergeet daarnaast niet om constant zorg te hebben voor intern draagvlak binnen je organisatie, ook na de officiële kick-off. Blijf dus zowel intern als extern open communiceren over wat je wel en niet kan leveren. Bereid je voor door informatie over incidenten mee te nemen naar vergaderingen en probeer opgedane kennis te gebruiken in je eigen organisatie. Hiermee laat je je collega's en leidinggevenden de meerwaarde van de ISAC en het delen van informatie zien.

Tip: Een gezamenlijke website of nieuwsbericht kan de zichtbaarheid en draagvlak vergroten.

Na de kick-off kunnen de eerste 'echte' bijeenkomsten nog onwennig zijn. Dat verandert vanzelf. De volgende zaken kunnen helpen om er vruchtbare vergaderingen van te maken:

Agenda[8]

De (vice-)voorzitter en secretaris stellen samen de agenda op voor de eerstvolgende vergadering en versturen deze uiterlijk twee á drie weken van tevoren naar de deelnemers om zich voor te bereiden. Het is aan te raden om bepaalde onderwerpen standaard op de agenda te zetten en tegelijkertijd ruimte voor actualiteiten en vragen van deelnemers te houden. Als de tijd het toelaat, is het raadzaam om op de agenda een pauze op te nemen, om ruimte te bieden voor informeel onderling contact, wat weer bijdraagt aan onderling vertrouwen.

Jaarplanning

Tijdens de eerste bijeenkomst van het jaar is een brainstorm houden voor de jaarplanning raadzaam. Een jaarplanning bevat onderwerpen, thema's en ontwikkelingen die je graag met elkaar wilt bespreken. Koppel dan ook meteen een 'eigenaar' aan deze punten, die ervoor zorgt dat het thema wordt bijgehouden. Hiervoor kan een spreker worden gevraagd of de eigenaar houdt zelf een presentatie. Ook kunnen deze onderwerpen alvast aan specifieke bijeenkomsten in het jaar worden gekoppeld. Dat kun je op verschillende manieren doen. Je kunt de verschillende bijeenkomsten een thema meegeven, maar je kan ook onderwerpen benoemen en deze inplannen voor de vergaderingen. Vanzelfsprekend moet er voldoende flexibiliteit zijn om eventuele actuele onderwerpen te behandelen.

Jaarverslag

Sommige ISAC's kiezen ervoor om aan het eind van het jaar een kort jaarverslag op te stellen waarin staat beschreven wat er in de ISAC is behandeld en hoe de ISAC heeft bijgedragen aan de digitale weerbaarheid van (organisaties in) de sector. Zo'n jaarverslag kan de deelnemers binnen hun eigen organisatie helpen bij het aantonen van nut en noodzaak van de ISAC en de 'verantwoording' van hun tijdsbesteding hieraan.

Praktische zaken

Vergeet niet om zorg te dragen voor de praktische zaken die komen kijken bij het organiseren van een vergadering, zoals het regelen van een locatie, aanmelden van de deelnemers, presentatiefaciliteiten en eventueel een lunch of afsluitende borrel. Je kunt kiezen voor een vaste, centrale locatie of per toerbeurt op locatie bij de verschillende deelnemers. Dit laatste heeft als bijkomend voordeel dat de kosten over meerdere organisaties worden verspreid. Ook geeft dit de gastorganisatie de mogelijkheid een actueel thema binnen de organisatie te presenteren.

Tip: Als de spreker geen bezwaar heeft, kan de ISAC besluiten om bij deze presentatie een collega mee te nemen om de presentatie bij te wonen. Daarna kunnen de collega's de ruimte weer verlaten om de beslotenheid van de ISAC te handhaven.

Actieve deelname

Een succesvolle samenwerking valt of staat bij actieve deelname van en voorbereiding door de deelnemers. Zo is het belangrijk, vooral in grotere organisaties, dat je actief informatie ophaalt van gesignaleerde dreigingen, incidenten, ervaringen, geleerde lessen en andere activiteiten binnen je organisatie die van waarde kunnen zijn voor andere deelnemers in de samenwerking.

Rondje Rood

Een incident bij de een is preventie voor de ander! Gevoelige informatie over cybersecurity-incidenten kan worden gedeeld in het 'Rondje Rood' onder TLP:RED. Dit betekent dat alles wat tijdens dit rondje gezegd wordt (letterlijk!) binnenskamers blijft. Dit mag dus niet genotuleerd of opgeschreven worden. Acht je het noodzakelijk om de informatie in dit Rondje Rood te gebruiken voor bijvoorbeeld andere organisaties die niet in de ISAC zitten, dan moet je te allen tijde de bron van de informatie raadplegen of en hoe deze informatie verder gebruikt kan worden.

8 Zie template agenda op http://www.ncsc.nl/samenwerking.

Nieuwe leden

Als de ISAC eenmaal loopt, zal je merken dat meer organisaties onderdeel van dit succes willen zijn. Dit betekent dat je lidmaatschapsverzoeken binnen gaat krijgen, die je gezamenlijk moet beoordelen. Hiervoor geldt dat je het unaniem eens moet zijn of een partij en diens voorgestelde vertegenwoordiger toetreedt. Zonder unanimiteit kun je het gevoel van vertrouwen binnen de ISAC ondermijnen. Dit schaadt de wil om informatie te delen en heeft dus impact op de waarde van de ISAC. Het proces van toetreden is verschillend per ISAC en wordt vastgelegd in de richtlijnen voor het lidmaatschap.

"Doordat je collega's goed leert kennen na een aantal vergaderingen, weet je elkaar ook informeel te vinden als er dingen spelen binnen de sector. Dit versterkt de kennisdeling ten zeerste."

Energy-ISAC

Bekende gezichten

Zoals eerder gezegd, is het voor het vertrouwen essentieel om bekende gezichten aan tafel te hebben en dus te werken met één of maximaal twee vaste vertegenwoordigers per organisatie. Kiest de ISAC voor de mogelijkheid van een back-up vertegenwoordiger naast een vaste, dan is het raadzaam om af te spreken hoe vaak deze back-up vertegenwoordigers minimaal aanwezig zijn, met het oog op behoud van vertrouwen binnen de groep.

Wisseling van voorzitter, vicevoorzitter of secretaris

Maak afspraken omtrent wisseling van de vicevoorzitter of secretaris. Is er een vaste frequentie of maximale termijn? Wat is de procedure van aantreden, aftreden en overdracht? Leg dit vast in de richtlijnen voor het lidmaatschap.

"In de Haven-ISAC beseffen we, als bedrijven en organisaties in de haven, hoe afhankelijk we van elkaar en systemen zijn en hoeveel we ook kunnen leren. Daarbij kijken we niet alleen naar Nederland: als grootste Europese haven zoeken we ook de verbinding met Antwerpen, de tweede haven van Europa. Daarom zijn we drie jaar geleden voor het eerst naar Antwerpen afgereisd om daar een kijkje in de keuken te nemen. We hadden wel verwacht dat we veel uitdagingen en ambities delen, maar we waren verrast over hoeveel we van elkaar konden leren en elkaar kunnen versterken. We komen nu daarom jaarlijks bij elkaar."

Haven-ISAC

Kijkje in de keuken

Een bijeenkomst kan gecombineerd worden met een kijkje in elkaars keuken. Dit helpt om elkaar op een informele manier te leren kennen en draagt zo bij aan het onderling vertrouwen. Ook helpt het om begrip voor ieders achtergrond te krijgen. Doordat je de processen die binnen een organisatie spelen leert kennen, begrijp je waarom iemand een bepaald onderwerp belangrijk vindt.

Uitdagingen

Een ISAC opzetten en onderhouden brengt uitdagingen met zich mee. Hieronder volgt een opsomming van mogelijke uitdagingen.

Vertrouwen

Het is al veelvuldig genoemd en het kan niet vaak genoeg gezegd worden: het uitwisselen van mogelijk gevoelige informatie valt of staat met vertrouwen. Vertrouwen groeit langzaam en behoeft regelmatig onderhoud. Het beschamen van vertrouwen is funest voor het uitwisselen van informatie en daarmee voor het voortbestaan van de ISAC.

"Durf elkaar aan te spreken als iets je dwars zit, en accepteer elkaars cybersecurity-volwassenheidsniveau."

NCSC

Betrokkenheid

Een ISAC is een vrijwillige vorm van samenwerking opgezet vanuit intrinsieke motivatie. Vrijwilligheid staat echter niet gelijk aan vrijblijvendheid. Het succes van de ISAC betekent blijvend investeren vanuit alle deelnemers.

Meerwaarde en grootte van de groep

Iedereen vraagt zich wel eens af waarom bepaalde organisaties in een ISAC zitten. Vaak is dit in de loop der tijd zo gegroeid en blijkt het erg moeilijk te zijn om partijen die weinig toevoegen te verzoeken de groep te verlaten. Toch is het zaak om waakzaam te zijn op de toegevoegde waarde van deelname aan een ISAC. Wees kritisch op je eigen deelname, maar ga ook met elkaar het gesprek aan. Van belang is om elkaar scherp te houden op wat iedere deelnemer komt 'brengen' en 'halen'. Tijdens dit proces kan ook bekeken worden welke organisatie(s) je nog mist aan tafel.

Tip: Plan elke 2 jaar een evaluatie in om de ISAC kritisch tegen het licht te houden.

Concurrentie

Samenwerken in de vorm van een ISAC kan betekenen dat je gevoelige informatie met je concurrenten deelt. Indien cybersecurity niet je verdienmodel is, is het goed om naar elkaar (en wellicht ook naar buiten) uit te spreken dat jullie niet concurreren op cybersecurity.

Ook als dit wél onderdeel is van je verdienmodel en je hier dus op concurreert, zijn er mogelijkheden om informatiedeling te stimuleren. Dit zou kunnen door alleen personen in de ISAC te hebben, die een directe verantwoordelijkheid voor cybersecurity hebben en personen met een commerciële rol uit te sluiten.

"Concurreren is het nadrukkelijk benoemen van de verschillen in je uitingen. Dat doen we niet. We vinden dat we met andere banken en instellingen een gezamenlijke strijd voeren tegen cybercrime. Het gaat uiteindelijk om het vertrouwen van onze klanten in de veiligheid van hele bancaire systeem."

FI-ISAC

Gemakzucht

Dit ligt altijd op de loer. Juist omdat je elkaar goed kent, blijft het belangrijk om kritisch naar elkaar te zijn en eventuele frustraties bespreekbaar te maken. Blijf daarom vooral (nieuwe) doelen (bij)stellen, bijvoorbeeld door het opstellen van een jaarplan. Maak ruimte om te evalueren, door bijvoorbeeld te bezien of de antwoorden op de eerdere vragen over bestaansrecht van de samenwerking nog steeds gelden. Blijf altijd focussen op de meerwaarde van de informatie die gedeeld wordt.

Cross-sectorale of grensoverschrijdende informatie-uitwisseling

Naast de samenwerking binnen ISAC's kan informatie-uitwisseling en samenwerking tussen ISAC's nationaal en internationaal van grote meerwaarde zijn. Dit geldt vooral voor sectoren die vergelijkbaar zijn in volwassenheid, over onderlinge afhankelijkheden beschikken en/of over dezelfde processen en systemen beschikken. Ook zijn er steeds meer Europese ISAC's waar één van de leden aan kan deelnemen, om zo de informatie terug te kunnen brengen in de eigen ISAC.

Verder lezen

ISAC best practices

- Information Sharing and Analysis Center – Cooperative models (2018). https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

Publicaties van andere ISAC's

- European Energy ISAC [EE-ISAC]. http://www.ee-isac.eu
- Financial Services ISAC [FS-ISAC]. http:// www.fsisac.com
- National Council of ISACs [NCI]. https://www.nationalisacs.org

Informatie-uitwisseling

- Introduction to information sharing (2016). https://www.isao.org/products/isao-300-1-introduction-to-information-sharing
- Sharing cybersecurity information: Good practices stemming from the Dutch public-private approach (2015). https://www.gccs2015.com/sites/default/files/documents/Sharing%20Cyber%20Security%20Information%20GCCS%202015.pdf
- Guide to cyber threat information sharing (2016). https://www.nist.gov/publications/guide-cyber-threat-information-sharing
- Building a national cyber information – Sharing ecosystem (2017). https://www.mitre.org/publications/technical-papers/building-a-national-cyber-information-sharing-ecosystem

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