VERKENNING BEST PRACTICES CYBERSECURITY INFORMATIEDELING

ONDERZOEKSRAPPORTAGE, CENTRE OF EXPERTISE CYBER SECURITY

Auteurs:

Luuk Bekkers,

Rick van der Kleij &

Rutger Leukfeldt

Datum:

24 augustus 2020

let's change
YOU. US. THE WORLD.

DE HAAGSE HOGESCHOOL

SAMENVATTING

Bedrijven bevinden zich tegenwoordig vaak in een keten. Een keten kan worden beschouwd als een verzameling organisaties die een virtueel netwerk delen waar informatie, diensten, goederen of geld doorheen stroomt. Hierbij staan ICT-systemen veelal centraal. Deze afhankelijkheid werkt in de hand dat cyber-gerelateerde risico's een opmars maken binnen ketens. Niet elke ketenorganisatie beschikt echter over de middelen en kennis om zichzelf te beschermen: om tot sterke ketens te komen is informatiedeling tussen ketenorganisaties over actuele dreigingen en incidenten van belang. Een doel van dit verkennend onderzoek, dat is uitgevoerd in opdracht van het Nationaal Cyber Security Centrum (NCSC), is om inzicht te bieden in de succesfactoren van informatiedeling-initiatieven op het gebied van cyberveiligheid. Met deze kennis kan het NCSC haar accounthouders en adviseurs helpen om de doelgroepen positief te motiveren om actie te nemen ter versterking van ketenweerbaarheid. Tevens wordt met dit onderzoek beoogd om aanknopingspunten voor vervolgonderzoek te identificeren.

Het identificeren van succesfactoren vond plaats op basis van een literatuurstudie en gestructureerde interviews met in totaal zes leden uit drie verschillende bestaande informatiedeling-initiatieven rondom cybersecurity: het Managed Service Provider (MSP) Information Sharing and Analysis Centre (ISAC), Energie ISAC en de securitycommissie van de Nederlandse Energie- Data Uitwisseling (NEDU). Alle respondenten zijn informatiebeveiligingsexperts die hun organisatie vertegenwoordigen in de samenwerkingsverbanden.

In totaal zijn 20 succesfactoren geïdentificeerd. Deze factoren zijn vervolgens gecategoriseerd tot vier thema's die bijdragen aan een succesvolle informatiedeling. De thema's zijn samen te vatten als teamfactoren, individuele factoren, managementfactoren en faciliterende factoren. De vier meest genoemde succesfactoren zijn:

- Expertise: Leden met onderscheidende en gespecialiseerde kennis bevorderen de informatiedeling en zijn ondersteunend aan het individuele leerdoel van de leden.
- Vertrouwen: Vertrouwen is een essentiële voorwaarde voor de bereidheid om samen te werken en informatie te delen. Tijd is hierin een cruciale factor: tijd is nodig voor vertrouwen om te ontstaan.
- Lidmaatschapseisen: Expliciete en impliciete lidmaatschapseisen zorgen voor een selectie op geschikte deelnemers en faciliteren daarmee het onderling vertrouwen.
- Structurele opzet: Een samenwerking dient georganiseerd te zijn volgens een structuur en met een stabiele bezetting van voldoende omvang.

Vervolgonderzoek zou zich kunnen richten op het identificeren van strategieën voor het opstarten van samenwerkingsverbanden en het over de tijd behouden van enthousiasme onder de leden in de informatiedeling-initiatieven rondom cybersecurity. Ook onderzoek naar de eigenschappen of kwaliteiten van de voorzitter en hoe deze bijdragen aan het succesvol initiëren en onderhouden van een samenwerkingsverband zijn genoemd. Ook is nog onvoldoende duidelijk hoe gedeelde of juist onderscheidende expertise van de leden bijdraagt aan succes van de informatiedeling-initiatieven. Verder is er behoefte aan kennis over hoe de samenwerking tussen ketenpartners op het gebied van cyberveiligheid buiten bestaande samenwerkingsverbanden is ingericht. Denk hierbij aan een uitbreiding van de huidige studie, maar met een focus op kleinere bedrijven die deel uitmaken van ketens, maar waarbij IT niet de corebusiness is, aangezien die volgens respondenten als risicovol worden gezien voor de keten.

INHOUDSOPGAVE

1. INLEIDING

1.1 Achtergrond

Cyber-gerelateerde risico's maken een opmars binnen ketens (Allianz Risk Barometer, 2019). Organisaties zijn voor de continuïteit en veiligheid steeds meer afhankelijk van een netwerk van aanbieders waar ze soms wel en soms niet een contract mee hebben. (Risico)management op al die afhankelijkheden in de gehele keten wordt dan ook steeds belangrijker (NCSC Onderzoeksagenda 2019-2022). Een keten, of een supply chain, is volgens Urciuoli (2015) een verzameling organisaties die een virtueel netwerk delen waar producten, diensten, informatie en geld doorheen stroomt, beweegt en wordt uitgewisseld. Deze organisaties zijn dus met elkaar verbonden door die stroming. Accenture (2019) schat dat in de komende vijf jaar ongeveer een kwart van de totale schade bij bedrijven die wordt geleden door cybercriminaliteit, veroorzaakt zal worden door ketenaanvallen (i.e. een aanval via meerdere systemen en/of organisaties; NCSC CSBN-3, 2013. p.114). Infradata (2019) noemt ketenaanvallen zelfs de grootste cyberdreiging voor 2019. Bovendien stelt Deloitte (2013) dat het risico dat komt van ketenpartners door cybersecurity professionals als grootste cyberrisico wordt gezien. Daartegenover zijn slechts 29% van de bedrijven wereldwijd voldoende geïnformeerd over de cyberbeveiligingsstrategie van hun ketenpartners (Accenture, 2019).

Om goed beschermd te zijn tegen cyberdreigingen is het belangrijk om op de hoogte te zijn van relevante ontwikkelingen op het gebied van cyberveiligheid- en criminaliteit. Informatiedeling tussen stakeholders is daarbij van cruciaal belang; niet elke organisatie heeft voldoende middelen om zich onafhankelijk goed te kunnen beschermen (Sauerwein e.a. 2017). In de afgelopen jaren zijn dan ook diverse informatiedeling-initiatieven op het gebied van cybersecurity ontstaan. Deze initiatieven zijn van grote waarde gebleken om cyberdreigingen het hoofd te kunnen bieden.

1.2 Probleemanalyse

De Kennis- en Innovatieagenda (KIA) Veiligheid (2019)[1] stelt dat effectieve informatiedeling tussen organisaties over actuele dreigingen en incidenten nodig is voor het bewerkstelligen van sterke ketens. Het NCSC wil dan ook beter inzicht in specifieke succesfactoren in informatiedeling tussen organisaties om daarmee stakeholders te adviseren en samenwerkingsverbanden te ondersteunen. Hiertoe heeft het NCSC opdracht gegeven aan de Haagse Hogeschool voor een verkennende studie op basis van casusonderzoek naar succesfactoren met betrekking tot samenwerking en informatiedeling in de cybersecurity keten.

1.3 Doelstelling

Het doel van dit verkennend onderzoek is om inzicht te bieden in de succesfactoren van informatiedeling-initiatieven op het gebied van cybersecurity. Met deze kennis kan het NCSC haar accounthouders en adviseurs helpen om de doelgroepen positief te motiveren om actie te nemen ter versterking van ketenweerbaarheid. Tevens wordt met dit onderzoek beoogd om aanknopingspunten voor vervolgonderzoek te identificeren.

1.4 Onderzoeksvragen

In navolging van de doelstelling staan de volgende twee onderzoeksvragen centraal in deze studie:

1. Hoe ontstaat succesvolle ketensamenwerking op cybersecurity gebied?

2. Welke gedrags- en organisatiefactoren zijn kenmerkend in succesvolle informatiedeling-initiatieven op het gebied van cybersecurity?

1.5 Leeswijzer

Om te beginnen wordt een theoretisch kader geschetst met betrekking tot samenwerking in ketens (hoofdstuk 2). Hierna volgt in hoofdstuk 3 een bespreking van de methode van onderzoek. In hoofdstuk 4 worden de resultaten beschreven aan de hand van de twee onderzoeksvragen, die vervolgens in de discussie zijn samengevat en vanuit een breder perspectief worden beschouwd (hoofdstuk 5). Na een conclusie volgen in het afsluitend hoofdstuk 6 concrete aanbevelingen voor vervolgonderzoek.

1 *In de KIA Veiligheid wordt in een meerjarig missie-gedreven programma beschreven welke innovaties en ontwikkelingen benodigd zijn op het gebied van veiligheid. Het plan is gezamenlijk opgesteld door vertegenwoordigers van belangrijke sectoren uit het veiligheidsdomein.*

2. THEORETISCH KADER

In het theoretisch kader worden enkele relevante thema's uitgelicht op basis van literatuur. De focus ligt hierbij op informatiedeling, communicatiestijlen en overige gedrags- en organisatiefactoren die mogelijk een rol spelen bij succesvolle samenwerkingsverbanden. Deze literatuur helpt bij het ontwikkelen van een geschikt interviewprotocol en geeft duiding aan de resultaten van het huidig casusonderzoek.

2.1 Informatiedeling

2.1.1 Behoefte aan informatievoorziening

Het opereren in een keten brengt allerlei digitale gevaren met zich mee. Ketenorganisaties hebben vaak echter niet voldoende middelen om zelfstandig kennis over dreigingen vanuit de keten op te doen en zich daar tegen te beschermen (e.g. Sauerwein e.a., 2018). Het delen van informatie over ontwikkelingen, dreigingen en *good practices* is dan ook essentieel om cyberweerbaarheid in ketens op peil te houden (Van Ruijven, 2018). Hoewel de overheid een taak heeft in de informatievoorziening, beargumenteren Boes en Leukfeldt (2017) dat informatiedeling door private partijen ook bijdraagt en zelfs nodig is voor het bereiken van digitale veiligheid. Er lopen dan ook verschillende initiatieven op het gebied van (publiek-private) samenwerking in het kader van cyberveiligheid in ketens, zoals de ISAC's (zie Boes & Leukfeldt, 2017).

2.1.2 Voordelen en barrières

De voordelen van het delen van informatie die in de literatuur worden genoemd zijn een verhoogde detectie van incidenten, verminderde schade na een incident en kostenbesparing in het algemeen (zie Zibak & Simpson, 2019). Een voorbeeld van dergelijke informatie dat gedeeld wordt zijn specifieke kenmerken waarmee een virus kan worden herkend. Succesvolle informatie-deling is echter lastig te bereiken. Zo geeft 61% van 67 ondervraagde ICT-experts uit 41 verschillende organisaties aan dat het delen van informatie vaak resulteert in irrelevante data en 43% dat het bepalen van de kwaliteit van de informatie problematisch is (Zibak & Simpson, 2019). Barrières zijn onder meer het gebrek aan standaardisatie en risico op het breken van privacyregels. Sauerwein e.a. (2018) laten bovendien zien dat informatiebeveiligingsexperts afhankelijk zijn van hun eigen informatiebronnen en dat zij informatie nauwelijks delen onder collega's, wat volgens de auteurs te wijten valt aan een gebrekkige formele informatiestroom.

2.2 Communicatiestijlen

2.2.1 Interne bedrijfscommunicatie

Interne bedrijfscommunicatie gaat over het uitwisselen van informatie tussen management en werknemers (Gardner e.a., 2001). Communicatie is essentieel voor het functioneren van bedrijven, onder meer voor het realiseren van doelen. Slechte communicatie hindert het proces van versturen, ontvangen, verwerken en ophalen van informatie tussen een leidinggevende en diens werknemers. Informatie moet op een simpele en niet-ambigue manier worden verwerkt, overgebracht en gecodeerd om de begrijpbaarheid te verhogen en de ontvangers' motivatie te verhogen om op de informatie te handelen (Den Hartog & Koopman, 2011). De toon, stijl en vorm van het 'verhaal' dat wordt gecommuniceerd moet aansluiten bij de behoeften van de organisatie. *Face-to-face* communicatie stimuleert bijvoorbeeld directe transmissie van een boodschap, waardoor de kans op miscommunicatie wordt verlaagd (Paulraj e.a., 2008).

2.2.2 Formele en informele communicatie

In het algemeen wordt een onderscheid gemaakt in formele en informele communicatie. Formele communicatie betreft instructies en informatie die door de erkende kanalen van een organisatie stroomt. Deze communicatie volgt dus de formele structuur of hiërarchie van een organisatie. Eerder onderzoek heeft formele communicatie gelinkt aan onder meer werktevredenheid (Holtzhausen, 2002) en productiviteit (Litterst & Eyo, 1982). Voorbeelden van formele kanalen zijn nieuwsbrieven, vergaderingen, e-mails en intranet (zie Gardner e.a., 2001). Hoewel formele communicatie essentieel is voor het functioneren van een organisatie, heeft het ook nadelen. Zo ervaren werknemers formele communicatie als koud of afstandelijk (Barker & Gower, 2010) en kan de informatie onvolledig zijn. *Face-to-face* communicatie tussen management en personeel is dan ook belangrijk en de meest gewenste vorm van communicatie van werknemers (Quirke, 2012). Volgens Quirke (2012) is het, naast de informatie zelf, ook van belang dat het management tijd investeert in het toetsen van de effectiviteit en wenselijkheid van communicatiestrategieën bij het personeel, bijvoorbeeld in de vorm van een *face-to-face* gesprek.

Informele communicatie is gebaseerd op sociale relaties tussen mensen. Deze vorm van communicatie volgt de doelen van werknemers, zoals het praten over problemen op het werk, terwijl formele communicatie de doelen van de organisatie dient. Het meest belangrijke doel van informele communicatie is dan ook het voldoen aan de informationele behoeftes van werknemers (Kandlousi & Abdollahi, 2010). Informele communicatie kan een oplossing bieden voor de gebreken van formele communicatie, zoals ambiguïteit en onvolledigheid (Gilsdorf, 1998). Zo kunnen werknemers

terugvallen op informele communicatie wanneer formele communicatie gebrekkig is.

2.3 Organisatie- en gedragsfactoren

Verschillende organisatie- en gedragsfactoren beïnvloeden de samenwerking tussen bedrijven. In de literatuur komen drie factoren prominent naar voren, namelijk: organisatiecultuur, vertrouwen en leiderschap.

2.3.1 Organisatiecultuur

Cultuur wordt gedefinieerd als de collectieve mentale programmering die de leden van één groep of categorie mensen onderscheidt van die van een andere (Hofstede e.a., 2016). Alvesson (2012) ziet organisatiecultuur als een systeem waarin individuen hun omgeving definiëren, overtuigingen uitdrukken en beslissingen maken. Cultuur stuurt dus gedrag. In het klassieke werk van Hofstede worden vijf culturele dimensies in organisaties beschreven (Hofstede, 1984; Hofstede, 2009): Machtsafstand (mate waarin de minder machtige werknemers in een organisatie accepteren en verwachten dat de macht ongelijk is verdeeld), individualisme (mate waarin mensen zijn geïntegreerd in groepen), masculiniteit (gaat over de verdeling van de rollen tussen mannen en vrouwen), onzekerheidsvermijding (beschrijft de mate waarin organisaties onzekerheid en ambiguïteit tolereren) en lange-termijn oriëntatie (gericht zijn op de toekomst betekent een hoog doorzettingsvermogen en gedrevenheid).

De organisatiecultuur heeft invloed op de samenwerking en informatiedeling tussen organisaties. Sterker nog, relaties, bijvoorbeeld die tussen organisaties, zijn in essentie cultureel: interacties borduren voort op culturele aannames (Ellis e.a., 2006). De voordelen van de relatie zijn afhankelijk van de mate waarin ze gewaardeerd worden op organisatieniveau en geïntegreerd zijn in de organisatiecultuur (Winkelhofer e.a., 2006). Hierbij wordt ook wel gesproken van inter-organisatie cultuur, wat door Saenz e.a. (2014) wordt gedefinieerd als een set van normen of waarden die gedeeld worden door verschillende organisaties. Cadden e.a. (2013) vonden een significante relatie tussen organisatiecultuur en prestaties in de keten. Wanneer culturen tussen ketenorganisaties verschillen, zijn succesvolle uitkomsten nog steeds mogelijk – ze moeten echter wel samen kunnen (Cadden e.a., 2013). Communicatie is een belangrijke factor bij de vorming van een inter-organisatie cultuur.

2.3.2 Vertrouwen

Een factor waar vrijwel alle studies het mee eens zijn dat het samenwerking bevordert, is vertrouwen (Smith e.a., 1995; Porta e.a., 1996). Ring en Van de Ven (1994) definiëren vertrouwen als de mate van zekerheid die een persoon heeft in de goede intentie van anderen uit een bepaalde groep en dat anderen zich consistent aan het doel van de groep gedragen. Doelconsistentie wordt zelf ook genoemd als een significante determinant van inter-organisatie samenwerking (Kim e.a., 2010). Hetzelfde geldt voor het hebben van gedeelde doelen: samenwerking wordt aannemelijk wanneer organisaties gedeelde behoeften of doelen ervaren (Schermerhorn, 1975). Het is belangrijk dat afnemers vertrouwen op leveranciers, omdat afnemers anders de samenwerking stop kunnen zetten (Kim e.a., 2010). Ook Sako (2006) onderzocht afnemer-leverancier relaties en maakt een onderscheid tussen een aantal vormen van vertrouwen, waaronder contractueel vertrouwen, wat refereert naar de verwachting dat zaken uit een contract worden nageleefd, en goodwill vertrouwen, ofwel de bereidheid van de partners om meer te doen dan is afgesproken. Een aantal factoren die een rol spelen bij het opbouwen van vertrouwen tussen organisaties zijn de inter-organisatie cultuur en rol van de leider (Tubin & Levin-Rozalis, 2008). Meer concreet, rapporteren Mattessich en Monsey (1992) zes factoren die een rol spelen bij het ontstaan van vertrouwen in de gezamenlijke sfeer, waaronder tijd nemen om elkaar en elkaars cultuur te leren kennen en intenties openlijk uitspreken.

2.3.3 Leiderschap

Ook de factor leiderschap heeft veel aandacht gekregen in de literatuur naar samenwerken. Een consistent gegeven uit de literatuur is dat leiderschap een centrale rol speelt bij het succes of falen van samenwerking tussen organisaties (Connelly, 2007). Een aantal belangrijke thema's bij leiderschap in de inter-organisatie context zijn het bewerkstelligen van open communicatie, het waarborgen van vertrouwen tussen alle partijen om de commitment te behouden en creëren van een gedeelde visie of strategie wat betreft de uitkomsten van de samenwerking (Connelly, 2007). Ook Müller-Seitz (2012) heeft een literatuurstudie verricht naar dit onderwerp. De auteur identificeert een vijftal relevante thema's die van belang zijn bij leiderschap in inter-organisatienetwerken, waaronder het ontwikkelen van een netwerkvisie, het bewerkstelligen van kennisoverdracht tussen de netwerkpartners en het faciliteren van vertrouwen tussen de participanten.

2.4 Samenvatting factoren

Op basis van de literatuurstudie zijn aantal factoren gevonden die een rol spelen bij succesvolle samenwerking. Dit betreffen: vertrouwen, leiderschap, (inter) organisatiecultuur, open en transparante communicatie, doelconsistentie, gedeelde doelen of visie, evaluatie, expertise en kennisoverdracht. Deze factoren behoren tot de meest relevante, hoewel de lijst niet uitputtend is.

3. METHODE

In deze sectie wordt de opzet van het onderzoek beschreven, bestaande uit de procedure en de participanten.

3.1 Procedure

In overleg met de opdrachtgever is gekozen voor een kwalitatief casusonderzoek, zoals ook voorgesteld door Khan en Estay (2015), waarbij door interviews en literatuurstudie de onderzoeksvragen worden beantwoord. Tevens is in overleg met de opdrachtgever bepaald het onderzoek te richten op samenwerkingsverbanden in de energiesector en een succesvol samenwerkingsverband van Managed Service Providers (MSPs)[2]: het MSP ISAC[3]. Binnen de energiesector zijn twee samenwerkingsverbanden betrokken bij het onderzoek: het Energie ISAC en de securitycommissie van de NEDU[4]. De specifieke sector is in onze ogen echter niet van belang: het onderzoek richt zich op de onderliggende processen die bijdragen aan het succes. De opdrachtgever van dit onderzoek heeft contactgegevens van vertegenwoordigers van deze samenwerkingsverbanden aangeleverd. Via deze vertegenwoordigers zijn nieuwe respondenten verkregen, waaronder zowel leden als voorzitters van deze samenwerkingsverbanden. De respondenten zijn hiermee geworven aan de hand van convenience sampling. Convenience sampling is een vorm van non-random sampling waarbij leden van een doelpopulatie worden geselecteerd op basis van bepaalde praktische eigenschappen, zoals toegankelijkheid en beschikbaarheid (Etikan e.a., 2016). Het interviewprotocol is opgesteld op basis van de onderzoeksvragen en de literatuurstudie naar factoren die de samenwerking tussen organisaties beïnvloeden (zie Bijlage I). De interviews varieerden in duur van 60 minuten tot 100 minuten. Alle interviews hebben virtueel plaatsgevonden via platforms voor videovergaderen door de eerste en tweede auteur van deze rapportage. Op basis van transcripten van interviews zijn *critical succes factors* (CSFs) voor samenwerking in ketens geïdentificeerd, volgens de methode zoals beschreven door Koutsikouri e.a. (2008). Het vaststellen van dergelijke factoren aan de hand van interviews is een gevestigde methode van organisatieanalyse (Koutsikouri e.a., 2018).

3.2 Participanten

Vanwege de verkennende aard van het project en de beperkte omvang van de opdracht is door de opdrachtgever, in samenspraak met de onderzoekers, bepaald om maximaal zes respondenten uit twee verschillende sectoren te betrekken bij dit onderzoek. Uiteindelijk zijn drie respondenten uit de energiesector (één deelnemer van de Energie ISAC en twee van de securitycommissie van de NEDU) en drie deelnemers van de MSP ISAC bevraagd voor dit onderzoek aan de hand van een semigestructureerd interview. De respondenten zijn informatiebeveiligingsexperts (CISO, CIO en cyber security officer) die namens nationale en internationale bedrijven zijn aangesloten bij de Energie ISAC, de MSP ISAC en de securitycommissie van de NEDU. Deelname aan deze samenwerkingsverbanden is een taak bovenop de reguliere functie die de respondenten bekleden bij de deelnemende bedrijven. De respondenten die de securitycommissie van de NEDU vertegenwoordigen in dit onderzoek zijn ook aangesloten bij de Energie ISAC.

2 *Managed Service Providers bieden de levering en het beheer van netwerkgebaseerde diensten, toepassingen en apparaten – in veel gevallen betreft dit informatietechnologie.*

3 *ISAC staat voor Information Sharing and Analysis Centre. Een ISAC is een samenwerkingsverband voor bedrijven uit specifieke branches uit de vitale sector, georganiseerd en geleid door het NCSC.*

4 *De NEDU is het verbindend platform van de Nederlandse Energiesector. NEDU staat voor de Nederlandse Energie Data Uitwisseling vereniging. Alle 150 marktpartijen uit de energiesector zijn daarbij aangesloten. Binnen de NEDU wordt afgesproken hoe de ketenprocessen en bijhorende datawisseling en berichtenverkeer verloopt tussen al die partijen. In de securitycommissie maakt men met name afspraken over hoe het berichtenverkeer beveiligd wordt. De leden binnen de commissie werken samen aan het opstellen van advies voor de NEDU op basis van bijvoorbeeld risicoanalyses.*

4. RESULTATEN

De resultaten worden besproken aan de hand van de twee deelvragen: (1) het ontstaan van de samenwerkingsverbanden en (2) de factoren die bijdragen aan succesvolle informatiedeling op het gebied van cybersecurity.

4.1 Hoe ontstaat succesvolle ketensamenwerking op cybersecurity gebied?

Om een oplossing te vinden voor de aanpak van cyberdreigingen en kwetsbaarheden zijn in Nederland voor de vitale sectoren de ISAC's opgericht (Huistra & Krabbendam-Hersman, 2017), waarvan de eerste in 2003 (Financial Institutes). In 2006 zijn een aantal overheidsdiensten lid geworden van deze ISAC en in hetzelfde jaar werd het publiek-private programma 'Nationale Infrastructuur tegen Cyber Crime'[5] gestart. Dit programma zorgde ervoor dat, binnen vitale sectoren in Nederland, verschillende andere ISAC's werden opgericht (Betaalvereniging, 2020). In 2014 werden de ISAC's formeel gekoppeld aan het NCSC. In de ISAC's worden - onder een strikte set van regels - informatie en ervaringen uitgewisseld over cyberveiligheid. Met behulp van deze informatie zijn de deelnemende organisaties beter in staat hun eigen risicoanalyse uit te voeren en bijpassende maatregelen te treffen, waardoor de digitale weerbaarheid van de eigen organisatie en van de gehele sector wordt vergroot (NCSC, 2020; Huistra & Krabbendam-Hersman, 2017). Het Nederlandse ISAC model is ontwikkeld op basis van ervaringen en richtlijnen van soortgelijke initiatieven in andere landen (Huistra & Krabbendam-Hersman, 2017).

Aanleiding voor het ontstaan van de ISAC's was volgens de respondenten de behoefte aan sneller en meer volledige informatie op het gebied van cyberveiligheid. Het was vóór de samenwerking lastig om goed te kunnen handelen op dergelijke informatie, aldus één van de respondenten. De oprichting van de ISAC's is (mede) vanuit initiatief van het NCSC ontstaan vanuit het idee dat Nederland veiliger wordt door een dergelijke samenwerking. Een ISAC is namelijk een netwerk dat de bundeling van expertise en het delen van kennis tussen alle relevante partijen mogelijk maakt. Er zijn ISAC's opgericht voor verschillende sectoren waar cyberveiligheid een belangrijk thema is in het kader van maatschappelijke veiligheid, zoals water, energie en telecom. Naast relevante private partijen uit de desbetreffende sector, zijn ook het NCSC, Team High Tech Crime van de Nationale Politie en de AIVD deelnemers van de ISAC-bijeenkomsten. Bij de ISAC staat publiek-private samenwerking dus centraal.

Er vinden circa zes ISAC-bijeenkomsten per jaar plaats, wat over het algemeen als voldoende wordt ervaren. De locatie van de verschillende vergaderingen wisselt tussen de bedrijven van de deelnemers. De deelnemer van het bedrijf waar de ISAC-bijeenkomst plaatsvindt, fungeert als gastheer en regelt doorgaans namens diens bedrijf een gastspreker. Verschillende respondenten beschouwen de samenwerking als succesvol en geven aan dat alle deelnemers en ook het NCSC die mening delen. De meerwaarde van de samenwerking is volgens de meeste respondenten drieledig: netwerken met collegae, leren van elkaar en verbetering van de eigen bedrijfsvoering.

De NEDU had een technische commissie, die digitale veiligheid als extra taak had. Na een incident bleek dat er beter een aparte commissie kon zijn die zich niet enkel met de technische aspecten rondom digitale veiligheid maar ook de processen bezig kon houden. Deze afzonderlijke securitycommissie functioneert nu vijf á zes jaar. Hierin maken de deelnemers afspraken over hoe het berichtenverkeer beveiligd wordt. De commissie komt eens per vier á vijf weken bijeen.

4.2 Welke gedrags- en organisatiefactoren zijn kenmerkend in succesvolle informatiedeling-initiatieven op het gebied van cybersecurity?

In totaal zijn via casusonderzoek 20 factoren geïdentificeerd die bijdragen aan succesvolle samenwerking. De belangrijkste vier factoren die door vrijwel alle respondenten zijn benoemd, zijn: expertise onder de leden, vertrouwen, lidmaatschapseisen en een structurele opzet. De factoren zijn gecategoriseerd op basis van de vier clusters zoals benoemd door Koutsikouri e.a. (2008): teamfactoren, individuele factoren, managementfactoren en (overige) faciliterende factoren. Hoewel Koutsikouri e.a. (2008) kritieke succesfactoren hebben geïdentificeerd op het gebied van projectmanagement, vertonen de factoren overlap met de factoren in dit onderzoek. De vier clusters lijken daarmee dekkend en toepasselijk voor het huidig onderzoek. Een overzicht van de vier clusters en de bijbehorende onderliggende factoren is te vinden in Tabel 2. Achter elk van de factoren staat weergegeven hoeveel van de zes respondenten deze hebben genoemd.

5 *Dit programma was ontwikkeld om vorm te geven aan de taak van de overheid op het gebied van de bestrijding van cybercriminaliteit en de niet-strafrechtelijke bestrijding ervan door informatiedeling, samenwerking en coördinatie tussen publieke en private partijen.*

Teamfactoren	Individuele factoren	Managementfactoren	(overige) Faciliterende factoren
Vertrouwen (6)	Expertise (6)	Gestructureerd leiderschap (4)	Lidmaatschapseisen (5)
Maatschappelijk/algemeen belang (4)	Persoonlijk netwerk (3)	Interpersoonlijke kwaliteiten (3)	Structurele opzet (5)
Niet-commerciële insteek (4)	Enthousiasme (3)	Rolmodel (3)	Mandaat om te handelen (3)
Feedback en evaluatie (4)			Technische infrastructuur voor communicatie (3)
Aantal leden (2)			Rol van de overheid (3)
Aantal actieve leden (2)			Verslaglegging (1)
Homogene organisatiecultuur (1)			Snelheid van informatiedeling (1)

Tabel 2. Succesfactoren informatiedeling.

4.2.1 Teamfactoren

Deze factoren hebben betrekking op de samenstelling van het team, de onderlinge relaties van diens leden en het functioneren ervan. Voorbeelden zijn onderling vertrouwen en homogeniteit.

Vertrouwen (6)

Vertrouwen is een thema dat bij alle respondenten aan bod komt als kritieke succesfactor. Een hoge mate van vertrouwen is vereist voor de bereidheid om informatie te delen. Tijd wordt aangehaald als belangrijkste bouwsteen voor vertrouwen:

> **“ Het duurde een aantal jaar voordat partijen het achterste van hun tong lieten zien. ”**

Een respondent geeft drie verklaringen voor het feit dat het vertrouwen binnen het samenwerkingsverband hoog is: (1) er sprake is van een stabiele bezetting, (2) de deelnemende bedrijven en diens vertegenwoordigers worden nauwkeurig in overleg gekozen en (3) alle vertegenwoordigers zijn informatiebeveiligingsexperts en hebben deels overlappende vakinhoudelijke kennis (*common body of knowledge*). Zodra het onderling vertrouwen wordt geschaad, bijvoorbeeld bij wisselingen van leden of als informatie wordt verkocht, houdt direct alle informatiedeling op, aldus twee respondenten.

Maatschappelijk/algemeen belang (4)

Vier respondenten geven aan dat het belangrijk is dat deelnemers gemotiveerd zijn vanuit een overkoepelend belang, bijvoorbeeld om bij te dragen aan een veilig Nederland:

> **“ Hoewel de samenwerking ook belangrijk is voor de aangesloten bedrijven, zit je daar in principe niet direct voor hen. ”**

Die overtuiging wordt breed gedragen. Een respondent doet een stap terug en stelt dat leden dienen te beseffen dat de veiligheid voor elke partij van belang is: als er bij de ene partij iets gebeurt, kan dat de deur open zetten naar een andere partij. De partijen zijn dus verbonden aan elkaar op het gebied van veiligheid.

Niet-commerciële insteek (4)

Vier respondenten geven aan dat commerciële belangen zoveel mogelijk vermeden moeten worden. De informatie binnen de initiatieven zou namelijk als concurrentievoordeel gebruikt kunnen worden door het te verkopen aan klanten. Het staat de samenwerking dan ook in de weg als deelnemers het idee hebben dat de informatie die ze delen mogelijk op een dergelijke manier gebruikt wordt door een lid.

> **“ Het ISAC is niet bedoeld als verkoopfeestje. ”**

Er worden dus geen commerciële zaken besproken en potentiële leden met mogelijke commerciële belangen worden geweerd. Dit houdt in dat mensen met bijvoorbeeld een sales- of uitsluitend compliance functie binnen hun organisatie niet worden toegelaten: enkel mensen die verantwoordelijk zijn voor cyberveiligheid in hun organisatie krijgen toegang.

Feedback en evaluatie (4)
Elkaar feedback geven op de gedeelde informatie en de evaluatie van processen en inhoud houdt de leden scherp en kritisch. Evaluatie is geen officieel onderdeel van de samenwerkingsverbanden, maar er zijn onderling wel discussies over hoe zaken zijn gelopen of zouden moeten lopen. Dit bevordert ook de band en het vertrouwen tussen de leden, aldus een van de respondenten.

Aantal leden (2)
Volgens twee respondenten is een minimum aantal leden nodig wil de samenwerking succesvol zijn. Meer leden zou niet direct beter zijn, het is met name belangrijk dat de leden voldoende tijd krijgen voor de samenwerking vanuit hun bedrijf. Een groot aantal gaat ten koste van het persoonlijk contact en dus het vertrouwen tussen de leden.

Aantal actieve leden (2)
Volgens twee respondenten zijn een minimaal aantal actieve leden nodig, omdat de samenwerking anders niet werkt. Een lid dat weinig bijdraagt (*freerider*) valt op. Dit heeft betrekking op ‘reciprociteit’:

> **“ Ik steek er tijd in en daar wordt iets voor terug verwacht. ”**

Homogene organisatiecultuur (1)
Cultuurverschillen zijn merkbaar tussen nationale en internationale organisaties. Zo is Nederland sterk gericht op samenwerking en informatiedeling, waar andere landen soms aan moeten wennen. Daarnaast hebben internationale bedrijven andere prioriteiten en belangen dan nationale organisaties. Buiten de nationaliteit spelen volgens de respondenten cultuurverschillen geen grote rol binnen het securitydomein.

4.2.2 Individuele factoren
Individuele factoren zijn factoren die betrekking hebben op persoonsgerichte kwaliteiten en eigenschappen, zoals attitudes, persoonlijkheid en competenties.

Expertise (6)
Alle respondenten halen expertise onder de leden aan als belangrijke factor voor succes. Zo zijn alle deelnemers informatiebeveiligingsexperts. Dit onderscheidt hen volgens een respondent van andere samenwerkingsverbanden, waar vaak *compliance officers* of andere beleidsmakers aansluiten. Doordat de deelnemers vakinhoudelijke kennis hebben en ‘dezelfde taal spreken’, wordt er relevante kennis gedeeld, weten de deelnemers hoe ze moeten handelen op die kennis en is het onderling vertrouwen hoog. Deze expertise helpt ook bij de afweging of bepaalde informatie toegevoegde waarde heeft en dus gedeeld zou moeten worden met het NCSC. Aangezien de samenwerkingsverbanden mede zijn bedoeld om van elkaar te leren en elkaars kennis te gebruiken, geven een aantal respondenten aan dat een diversiteit in expertise in het bijzonder van belang is (*een kijkje in de keuken van anderen*).

Persoonlijk netwerk (3)
Een goed onderhouden persoonlijk netwerk zorgt ervoor dat deelnemers elkaar weten te vinden wanneer dat nodig is. Dit bevordert het inwinnen en delen van informatie.

Enthousiasme (3)
Een samenwerkingsverband is na oprichting niet direct op het wenselijke niveau. Het kost tijd en inspanning om het verband succesvol te maken. Daarom is het, met name in het begin van een samenwerkingsverband, belangrijk dat de leider en overige leden enthousiast zijn en bereidwillig om tijd en energie te investeren.

4.2.3 Managementfactoren
Dit thema betreft het operationeel leiding- en richting geven aan het samenwerkingsverband, met een focus op zowel de leden als het verband zelf. Zo halen alle respondenten het belang van leiderschap aan als kritieke succesfactor. Binnen het thema worden een aantal concrete factoren benoemd.

Gestructureerd leiderschap (4)
De voorzitter geeft structuur aan het samenwerkingsverband en treedt op als moderator, bijvoorbeeld door ervoor te zorgen dat iedereen aan het woord komt. Dit is nodig om tot resultaat te komen.

Interpersoonlijke kwaliteiten (3)
Er zijn enthousiaste en gepassioneerde trekkers nodig voor het bewerkstelligen van een succesvolle samenwerking, aldus respondenten. Volgens een respondent moet een voorzitter belangstelling tonen, kunnen enthousiasmeren en vertrouwen uit stralen, bijvoorbeeld door voorspelbaar gedrag te vertonen. Het kost tijd, energie en doorzettingsvermogen om vertrouwen op te bouwen en de relevantie van de samenwerking aan te tonen. Geef leden bijvoorbeeld het gevoel dat ze iets toevoegen en relevant werk verrichten. Bovendien faciliteert de voorzitter een verbinding met overheidspartijen, wat de informatiedeling ten goede komt.

Rolmodel (3)
De voorzitter dient als een soort rolmodel voor de groep. Het is belangrijk dat de voorzitter uit de sector komt en het is diens taak om inactieve leden aan te spreken.

> **“ De voorzitter moet kunnen voorleven. ”**

4.2.4 Faciliterende factoren
De vierde en laatste categorie, de overige faciliterende factoren, hebben betrekking op ondersteunende factoren die de samenwerking mogelijk maken en vergemakkelijken.

Lidmaatschapseisen (5)
De deelnemende bedrijven en diens vertegenwoordigers zijn op basis van lidmaatschapseisen gerechtigd om aan te sluiten. Zo geldt bij een onderzocht samenwerkingsverband dat een bedrijf minimaal drie vitale klanten moet bedienen voordat deelname mogelijk is. De vertegenwoordiger moet tevens op senior niveau verantwoordelijk zijn voor de informatiebeveiliging binnen diens organisatie, daar een goede informatiepositie hebben en mag er geen sprake zijn van commerciële belangen die bijvoorbeeld een risico vormen dat iemand de informatie doorverkoopt aan klanten). Een dergelijke ballotage is nodig voor het ontwikkelen van vertrouwen. Een ander onderzocht samenwerkingsverband stelt minder strenge eisen aan diens leden, omdat zij minder sensitieve informatie delen. De eisen die worden gesteld lijken dus afhankelijk van het doel van het samenwerkingsverband. Naast de ‘officiële’ lidmaatschapseisen, zijn er ook impliciete gedragscodes. Zo wordt het van de leden verwacht dat ze een actieve bijdrage leveren en aanwezig zijn bij de vergaderingen.

Structurele opzet (5)
De samenwerking is mede succesvol door een gestructureerde opzet, zoals een vaste frequentie van bijeenkomsten, een stabiele bezetting en een vaste agenda. Dit is nodig om tot resultaat te komen en verhoogt het vertrouwen, aldus twee respondenten. Een andere belangrijke factor hierbij is de aanwezigheid van een protocol, zoals het ‘trafficlight-protocol’[6]. Daarmee wordt voor alle deelnemers helder welke afspraken er zijn omtrent het delen van informatie en worden onnodige discussies vermeden. Bij een hoge mate van vertrouwen en heldere afspraken zouden deelnemers in principe alles moeten kunnen delen, aldus een respondent. Verder geeft ook een jaarplan focus en structuur aan de samenwerking, waarbij op elke bijeenkomst een onderwerp uit het plan op de agenda komt. Twee respondenten noemen bovendien het belang van een duidelijke afbakening (scope) van de activiteiten van het samenwerkingsverband: niet te breed, maar ook niet te beperkt.

Mandaat om te handelen (3)
Drie respondenten geven aan dat het belangrijk is dat de deelnemende bedrijven prioriteit geven aan cyberveiligheid en de vertegenwoordigers ruimte en mandaat geven om te handelen en te investeren in het samenwerkingsverband.

Technische infrastructuur voor communicatie (3)
Volgens twee respondenten mist het samenwerkingsverband een technische infrastructuur. Het zou waardevol zijn als er een gezamenlijke cloudbased toepassing komt waarin informatie als notulen en gemaakte afspraken gedeeld kan worden. De veiligheidscommissie van de NEDU maakt hier al gebruik van. Een dergelijke infrastructuur bevordert de snelheid, effectiviteit en efficiëntie van het informatie delen, waarmee het wordt aangemerkt als succesfactor. Twee respondenten geven aan dat het wenselijk is dat de overheid hierin faciliteert om commerciële belangen te voorkomen. Volgens een van de respondenten is het tevens van belang om te investeren in het ontwikkelen van een cross-sectoraal platform waarbij informatie tussen verschillende ’samenwerkingsverbanden kan worden gedeeld, aangezien informatie uit de samenwerkingsverbanden vaak ook relevant is voor andere niet-vitale samenwerkingsverbanden. De communicatie verloopt momenteel, buiten de bijeenkomsten en directe onderlinge communicatie, primair via een gezamenlijke maillijst. Dit middel wordt door een respondent echter niet als ideaal beschouwd; mailtjes raken op den duur verloren in de mailbox. De e-mail wordt gebruikt om te communiceren over onder meer kwetsbaarheden en dreigingen, maar over het algemeen is er weinig activiteit.

Rol van de overheid (3)
Het NCSC functioneert als secretariaat voor de ISACs, wat betekent dat het NCSC een notulist aanlevert en de agenda verstuurt. Het NCSC heeft aan het begin geholpen bij het ontwikkelen en in stand houden van het samen-werkingsverband, aldus een respondent. Bovendien geeft dergelijke overheidsbelangstelling status aan de groep en de deelnemers (ook binnen de organisaties (directies) die zij vertegenwoordigen).

Verslaglegging (1)
Een respondent noemt het belang van verslaglegging van de bijeenkomsten en de daarin gemaakte afspraken. Adequate verslaglegging waarborgt de transparantie. Hierbij is het ook belangrijk dat de contactgegevens van de aanwezigen zijn opgenomen in het verslag om de bereikbaarheid te verhogen.

Snelheid van informatiedeling (1)
Een respondent is van mening dat het belangrijk is dat relevante informatie over dreigingen of kwetsbaarheden snel onder de aandacht wordt gebracht bij leden van het samenwerkingsverband, om te voorkomen dat men achter loopt op nieuwe ontwikkelingen. Deze snelheid is volgens de respondent nodig om het samenwerkingsverband ook in de toekomst relevant te houden.

6 *Het trafficlight-protocol maakt het mogelijk om op een simpele manier aan te duiden wanneer en op welke wijze informatie mag worden verspreid.*

5. DISCUSSIE EN CONCLUSIE

In deze sectie worden de resultaten van het onderzoek vanuit een breder perspectief beschouwd. Dit bestaat uit een korte samenvatting, een interpretatie van de resultaten en een vergelijking met voorgaande literatuur. Afsluitend volgt een conclusie.

5.1 Discussie

Een eerste doel van dit verkennend onderzoek is om inzicht te bieden in de succesfactoren van informatiedeling-initiatieven op het gebied van cybersecurity. Met deze kennis kan het NCSC haar accounthouders en adviseurs voorzien van topics om de doelgroepen positief te motiveren om actie te nemen ter versterking van ketenweerbaarheid.

Drie informatiedeling-initiatieven op het gebied van cybersecurity zijn hiertoe onderzocht aan de hand van semigestructureerde interviews met in totaal zes participanten (drie namens de MSP ISAC, één namens de Energie ISAC en twee namens de veiligheidscommissie van de NEDU).

Het blijkt dat de samenwerkingsverbanden zijn ontstaan vanuit het idee om Nederland veiliger te maken op het gebied van cyberveiligheid, mede op initiatief van en in samenwerking met overheidspartijen. Het valt op dat dat de initiator een belangrijke rol heeft bij het opstarten van een samenwerkingsverband, bijvoorbeeld door organisaties en cybersecurity experts binnen de eigen sector te enthousiasmeren en te motiveren om deel te nemen aan een informatiedeling-initiatief op het gebied van cybersecurity. De meerwaarde van de samenwerking is voor alle door ons gesproken respondenten drieledig: netwerken met collegae, leren van elkaar en verbetering van de eigen bedrijfsvoering.

Het zwaartepunt van deze studie lag bij het identificeren van kritieke succesfactoren wat betreft de samenwerking op gebied van gedrag en organisatie. Deze factoren zijn gecategoriseerd als vier thema's, te weten: teamfactoren, individuele factoren, managementfactoren en faciliterende factoren. In totaal zijn er 20 factoren geïdentificeerd, waarvan de meeste door meerdere respondenten zijn benoemd. De vier belangrijkste (meest genoemde) factoren uit dit onderzoek zijn:

- Expertise: Leden met onderscheidende en gespecialiseerde kennis bevorderen de informatiedeling en zijn ondersteunend aan het individuele leerdoel van de leden.
- Vertrouwen: Vertrouwen is een essentiële voorwaarde voor de bereidheid om samen te werken en informatie te delen. Tijd is hierin een cruciale factor: tijd is nodig voor vertrouwen om te ontstaan.
- Lidmaatschapseisen: Hoewel afhankelijk van het doel van de samenwerking, zorgen expliciete en impliciete lidmaatschapseisen voor een selectie op geschikte deelnemers en faciliteren daarmee het onderling vertrouwen.
- Structurele opzet: Een samenwerking dient georganiseerd te zijn volgens een structuur en met een stabiele bezetting van voldoende omvang.

Het valt op dat met name het concept vertrouwen een centrale rol lijkt te spelen in de informatiedeling-initiatieven op het gebied van cyberveiligheid. Zo hebben veel factoren een relatie met vertrouwen (lidmaatschapseisen, structurele opzet, evaluatie en feedback, aantal leden, enthousiasme en leiderschap). Deze bevinding komt overeen met literatuur, waarin vertrouwen ook naar voren komt als centraal en essentieel construct (e.g. Connelly, 2007; Müller-Seitz, 2012).

Naast vertrouwen vertonen nog een aantal andere geïdentificeerde factoren overlap met de literatuur (e.g. Connelly, 2007; Mattessich & Monsey, 1992). Zo is het belang van een agenda, gedeelde visie en leiderschap ook benoemd door Müller-Seitz (2012) en Connelly (2007). Ander onderzoek vond eveneens de factoren evaluatie en enthousiasme (Quirke, 2013; Koutsikouri e.a., 2008). Ten slotte vertonen factoren als technische infrastructuur en verslaglegging overlap met de factoren kennisoverdracht en communicatie zoals benoemd door Cadden e.a. (2013) en Müller-Seitz (2012). Daarnaast zijn er ook verschillen. De door ons geïdentificeerde succesfactoren lidmaatschapseisen en het maatschappelijk belang zijn niet gevonden in de literatuur. In de interviews is bovendien weinig evidentie gevonden voor de invloed van organisatiecultuur, zoals wel door de literatuur wordt aangehaald (e.g. Cadden e.a., 2013). Mogelijk zijn dergelijke verschillen te verklaren door de beperkte omvang van de literatuurstudie, het kleine aantal respondenten of de specifieke focus van dit onderzoek.

5.2 Conclusie

Het verkennend onderzoek laat zien dat er een groot aantal succesfactoren zijn van informatiedeling-initiatieven op het gebied van cybersecurity. De kwaliteiten van een voorzitter, enthousiasme onder de deelnemers en steun vanuit de overheid spelen een rol bij de ontwikkeling van een samenwerkingsverband. Vertrouwen en leiderschap zijn bepalende factoren voor het succes, zoals ook aangehaald in de door ons bestudeerde literatuur. Faciliterende factoren als een vaste structuur en lidmaatschapseisen zijn bovendien van invloed. Daarnaast spelen individuele factoren een rol, zoals expertise onder de deelnemers. Het NCSC kan de geïdentificeerde factoren gebruiken om binnen de doelgroep de ketenweerbaarheid te versterken door in gesprek te gaan met stakeholders en hen te adviseren op het gebied van samenwerking met branchegenoten.

6. AANBEVELINGEN VOOR VERVOLGONDERZOEK

Hoewel dit onderzoek een aantal succesfactoren heeft geïdentificeerd, maakt de verkennende aard van het onderzoek dat er nog een aantal vragen of onderwerpen zijn die nader onderzoek verdienen. Daarom doen we de volgende aanbevelingen voor vervolgonderzoek.

6.1 Initiëren en in stand houden samenwerkingsverband

Vervolgonderzoek zou zich kunnen richten op het identificeren van strategieën voor het opstarten van informatiedeling-initiatieven op het gebied van cybersecurity en hoe relevante partijen daar in eerste instantie voor bij elkaar kunnen worden gebracht. Uit dit onderzoek blijkt dat de inspanningen en kwaliteiten van een initiator bepalend zijn bij het opstarten van het verband. Advies is daarom om nader te onderzoeken wat kenmerken zijn van succesvolle voorzitters in de context van een beginnend samenwerkingsverband. Daarbij is het ook de vraag hoe een samenwerkingsverband een zelfstandig functionerende eenheid wordt over de tijd heen en minder afhankelijk kan worden gemaakt van de inspanningen van één of enkele personen, zoals de initiator of voorzitter.

6.2 Uitdiepen meest benoemde succesfactoren

Vakinhoudelijke expertise op het gebied van cybersecurity onder de deelnemers is door alle respondenten benoemd als succesfactor. Het is echter nog de vraag wat het effect is van gedeelde expertise of juist onderscheidende expertise op het succes van de samenwerking, aangezien daar geen eenduidig beeld over is ontstaan. Doe daarom nader onderzoek naar hoe expertise onder deelnemers bijdraagt aan succesvolle samenwerking. Onderzoek bovendien nader in hoeverre lidmaatschapseisen binnen een specifieke samenwerkingscontext van meerwaarde zijn, hoe deze eisen tot stand komen en hoe ze samenhangen met het doel van een samenwerkingsverband. Zoals benoemd, is de factor vertrouwen cruciaal gebleken voor het succes van de door ons onderzochte samenwerkingsverbanden. Doe daarom onderzoek naar strategieën om het onderling vertrouwen tussen deelnemers te initiëren, faciliteren en behouden over de tijd. Onderzoek ten slotte nader wat een structurele opzet inhoudt in de context van verschillende samenwerkingsverbanden en welke (f)actoren een rol spelen bij het bewerkstelligen van een dergelijke structuur.

Betrek bij het uitdiepen van deze factoren andere (internationale) samenwerkingsverbanden en methodologische technieken, zoals vragenlijsten of data-analyse op tekstuele communicatie, om het bewijs te verstevigen. Ten slotte kan op basis van het huidig onderzoek niet (voldoende) worden geconcludeerd of en op welke manier de geïdentificeerde factoren correleren met elkaar. Vervolgonderzoek zou zich dus ook kunnen richten op de onderlinge samenhang tussen succesfactoren.

6.3 Ketensamenwerking

Onderzoek hoe de samenwerking tussen ketenpartners op het gebied van cyberveiligheid buiten formele informatiedeling-initiatieven is ingericht. Focus hierbij op leveranciers, afnemers en overheidsinstanties van niet-vitale processen. Onderzoek zou zich hierbij kunnen richten op de samenwerking tussen grootbedrijven en het midden- en kleinbedrijf, waarbij IT niet de corebusiness is, aangezien die risicovol worden bevonden voor de keten.

6.4 Pas de ISAC handreiking aan

Op basis van de ervaringen van andere ISAC's is een ISAC-handreiking opgesteld. Deze handreiking is te downloaden op de website van het NCSC. De handreiking helpt ISAC's om te bepalen waar ze staan in hun ontwikkeling en om hun ambities te realiseren. Deze studie biedt nieuwe inzichten in het succes van samenwerkingsverbanden. Wij raden aan om de resultaten van deze studie te gebruiken om de ISAC-handreiking7 en bijbehorende checklist voor het faciliteren van samenwerkingsverbanden te updaten. Zorg bovendien dat deze update op een toegankelijke manier onder de aandacht wordt gebracht van stakeholders, bijvoorbeeld aan de hand van sociale media, met speciale aandacht voor partijen die zijn aangemerkt als niet-vitaal.

7 *https://www.ncsc.nl/documenten/publicaties/2020/februari/24/handreiking-haal-meer-uit-je-isac*

REFERENTIES

Accenture (2019). *Cyber Threatscape Report.* Verkregen van: https://www.accenture.com/_acnmedia/PDF-107/Accenture-securitycyber.pdf#zoom=50.

Allianz (2019). *Allianz Risk Barometer*. Verkregen van: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk Barometer-2019.pdf

Alvesson, M. (2012). *Understanding organizational culture.* Sage.

Barker, R. T., & Gower, K. (2010). Strategic application of storytelling in organizations: Toward effective communication in a diverse world. *The Journal of Business Communication*, *47*(3), 295-312.

Betaalvereniging. (2020). *Publiek-private samenwerking.* Verkregen van: https://www.betaalvereniging.nl/veiligheid/publiek-private-samenwerking/

Boes, S. & Leukfeldt, E.R. (2017). Fighting Cybercrime: a Joint Effort. In: Hakim, S. & Clark, R.M. (ed.) *Cyber-physical security at the state, provincial and local level: protecting critical infrastructure.* New York: Springer Science.

Cadden, T., Marshall, D., & Cao, G. (2013). Opposites attract: organisational culture and supply chain performance. *Supply Chain Management: an international journal.*

Connelly, D. R. (2007). Leadership in the collaborative interorganizational domain. *International Journal of Public Administration, 30*(11), 1231-1262.

Den Hartog, D., & Koopman, P. (2011). Leadership in Organizations. Handbook of Industrial, Work and Organizational Psychology. Vol. 2. *Organizational Psychology.*

Ellis, N., Lowe, S., & Purchase, S. (2006). Towards a re-interpretation of industrial networks: A discursive view of culture. *The IMP Journal, 1*(2), 20-40.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics, 5*(1), 1-4.

Gardner, M. J., Paulsen, N., Gallois, C., Callan, V. J., & Monaghan, P. (2001). Communication in organizations: An intergroup perspective. *The new handbook of language and social psychology, 2*, 561-584.

Gilsdorf, J. W. (1998). Organizational rules on communicating: How employees are-and are not learning the ropes. *The Journal of Business Communication (1973), 35*(2), 173-201.

Hofstede, G. (1984). *Culture's consequences: International differences in work-related values* (Vol. 5). Sage.

Hofstede, G. (2009). Geert Hofstede cultural dimensions. Verkregen van: http://taylortraining.com/clients/mcc/Hofstede_Cultural_Dimension_Explained(external)pdf

Hofstede, G. J., Minkov, M., & Hofstede, G. (2016). *Allemaal andersdenkenden: omgaan met cultuurverschillen.* Business Contact.

Holtzhausen, D. (2002). The effects of a divisionalised and decentralised organisational structure on a formal internal communication function in a South African organisation. *Journal of communication management, 6*(4), 323-339.

Huistra, A. W. & Krabbendam-Hersman, T. H. E. E. A. (2017). Verkenning Cybersecurity Informatiedeling binnen de Topsectoren. Verkregen van: https://zoek.officielebekendmakingen.nl/blg-808966.pdf

Infradata (2019). Global Cyber Threat Report 2019. Verkregen van: https://www.infradata.com/news-blog/global-cyber-threat-report-2019/

Kandlousi, N. S. A. E., Ali, A. J., & Abdollahi, A. (2010). Organizational citizenship behavior in concern of communication satisfaction: The role of the formal and informal communication. *International Journal of Business and Management, 5*(10), 51.

Khan, O., & Estay, D. A. S. (2015). Supply chain cyber-resilience: Creating an agenda for future research. *Technology Innovation Management Review,* (April), 6-12.

KIA Veiligheid. (2019). Verkregen van: https://www.hollandhightech.nl/kia-veiligheid

Kim, K. K., Park, S. H., Ryoo, S. Y., & Park, S. K. (2010). Inter-organizational cooperation in buyer–supplier relationships: Both perspectives. *Journal of Business Research, 63*(8), 863-869.

Krebs, B. (2014). Target Hackers Broke in via HVAC Company. *Krebs on Security*. Geraadpleegd van http://krebsonsecurity.com/2014/02/targethackers-broke-in-via-hvac comp...

Koutsikouri, D., Austin, S., & Dainty, A. (2008). Critical success factors in collaborative multidisciplinary design projects. *Journal of Engineering, Design and Technology.*

Litterst, J. K., & Eyo, B. (1982). Gauging the effectiveness of formal communication programs: A search for the communication-productivity link. *The Journal of Business Communication (1973), 19*(2), 15-26.

Mattessich, P. W., & Monsey, B. R. (1992). Collaboration: what makes it work. *A review of literature on factors influencing successful collaboration.*

Müller-Seitz, G. (2012). Leadership in interorganizational networks: a literature review and suggestions for future research. *International Journal of Management Reviews, 14*(4), 428-443.

NCSC. (2013). *Cybersecuritybeeld Nederland CSBN-3.* Verkregen van: https://www.thehaguesecuritydelta.com/media/com_hsd/report/16/document/Cybersecuritybeeld-Nederland.pdf

NCSC. (2019). *Onderzoeksagenda 2019-2022.* Verkregen van: https://www.ncsc.nl/documenten/publicaties/2019/september/26-9-2019/ncsconderzoeksagenda-2019-2020

NCSC. (2020). Handreiking: *Haal meer uit je ISAC.* Verkregen van: https://www.ncsc.nl/aan-deslag/documenten/publicaties/2020/februari/24/handreiking-haal-meer-uit-je-isac

Paulraj, A., Lado, A. A., & Chen, I. J. (2008). Inter-organizational communication as a relational competency: Antecedents and performance outcomes in collaborative buyer–supplier relationships. *Journal of operations management, 26*(1), 45-64.

Porta, R. L., Lopez-De-Silane, F., Shleifer, A., & Vishny, R. W. (1996). *Trust in large organizations* (No. w5864). National Bureau of Economic Research.

Quirke, M. B. (2012). *Making the connections: Using internal communication to turn strategy into action.* Gower Publishing, Ltd..

Ring, P. S., & Van de Ven, A. H. (1994). Developmental processes of cooperative interorganizational relationships. *Academy of management review, 19*(1), 90-118.

Saenz, M. J., Revilla, E., & Knoppen, D. (2014). Absorptive capacity in buyer–supplier relationships: Empirical evidence of its mediating role. *Journal of Supply Chain Management, 50*(2), 18-40

Sako, M. (2006). Does trust improve business performance. *Organisafional trust: A reader,* 267 294.

Sauerwein, C., Sillaber, C., Mussmann, A., & Breu, R. (2017). Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives In Leimeister, J.M.; Brenner, W. (Hrsg.): Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017), St. Gallen, S. 837-851.

Sauerwein, C., Sillaber, C., & Breu, R. (2018). Shadow cyber threat intelligence and its use in information security and risk management processes. *Multikonferenz Wirtschaftsinformatik (MKWI 2018).*

Schermerhorn Jr, J. R. (1975). Determinants of interorganizational cooperation. *Academy of management Journal, 18*(4), 846-856.

Smith, K. G., Carroll, S. J., & Ashford, S. J. (1995). Intra-and interorganizational cooperation: Toward a research agenda. *Academy of Management journal, 38*(1), 7-23.

Tubin, D., & Levin-Rozalis, M. (2008). Interorganizational cooperation: the structural aspect of nurturing trust. *International Journal of Public Sector Management.*

Urciuoli, L. (2015). Cyber-resilience: a strategic approach for supply chain management. *Technology Innovation Management Review, 5*(4).

Van der Kleij, R., & Leukfeldt, R. (2019). Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security. In *International Conference on Applied Human Factors and Ergonomics* (pp. 16-27). Springer, Cham.

Van Ruijven, T. (2018). *Ketenweerbaarheid.* TNO.

Winklhofer, H., Pressey, A., & Tzokas, N. (2006). A cultural perspective of relationship orientation: Using organizational culture to support a supply relationship orientation. *Journal of Marketing Management, 22*(1), 169-194.

Zibak, A., & Simpson, A. (2019). Cyber threat information sharing: Perceived benefits and barriers. In *Proceedings of the 14th International Conference on Availability, Reliability and Security* (pp. 1-9).

BIJLAGE I: INTERVIEWPROTOCOL

1. Hoe ontstaat succesvolle ketensamenwerking op cybersecurity gebied?

- Met welke partijen werken jullie samen op het gebied van cybersecurity? Op wat voor manier?
- Wanneer is deze samenwerking begonnen?
- Heeft dit een specifieke aanleiding? // Welke omstandigheden/ belangrijke gebeurtenissen (bv. geleden schade betrokken organisaties; onvoldoende support van overheid) hebben jullie ertoe aangezet om het samenwerkingsverband op te zetten (Environmental context and resources]?
- Waarom zijn jullie deze samenwerking aangegaan? Wat is voor jullie de meerwaarde van de samenwerking?
- In welke mate was er sprake van sociale invloeden bij het initiëren van de samenwerking, zoals voorbeeldgedrag van anderen [modelling], leiderschap (Champion)?
- Heb je het idee dat deze samenwerking nuttig is? Op welke manier?
- Wat zijn de doelen die jullie willen bereiken met de ketensamenwerking [goals]? Hebben deze aan de basis gestaan van het succes? Zo ja, in welke mate (wat maakt die doelen bijzonder)?
- Wat maakt volgens jou de samenwerking succesvol? Welke factoren zijn daarbij volgens jou van belang?

2. Welke gedrags- en organisatiefactoren zijn kenmerkend in informatiedeling-initiatieven op het gebied van cybersecurity?

- Hoe wordt informatie verspreid binnen de organisatie?
- Op welke manier communiceren jullie met ketenpartners? Met welke frequentie? Sprake van informele communicatie?
- Vind er evaluatie van interne en externe communicatiestrategieën plaats?
- In hoeverre delen jullie informatie over cyberveiligheid met ketenpartners? Op welke manier en met welke frequentie (Telefoon, e-mail, face-to-face, brief, chat, gedeelde keteninformatiesystemen)? Waar gaat die informatie over?
- In hoeverre is het delen van informatie over cyberveiligheid met partners een prioriteit?
- Verwachten jullie van ketenpartners dat zij informatie met jullie delen over cyberveiligheid? Denk je dat zij dat van jullie verwachten?
- Wat vind je van de informatie die ketenpartners met jullie delen (nuttig of niet)? Geven jullie ook feedback op elkaar?
- Wat belemmert jullie bij het delen van informatie over cyberveiligheid met ketenpartners?
- Hoe heeft het organisatieklimaat/cultuur van de betrokken organisaties bijgedragen aan het succes van de samenwerking?
- In welke mate spelen organisatieresources/ middelen / techniek een rol bij het succes van de samenwerking, zoals de beschikking over tijd van leden voor deelname en technische infrastructuur voor het delen van informatie?
- In welke mate speelt de factor mens, waaronder de kennis en competenties van de deelnemers een rol in het succes? In welke mate is er sprake van wederzijdse interesse in elkaars kundigheid en ervaring?
- Is er sprake van vrijwillige bijdragen door de leden aan het samenwerkingsverband? In welke mate draagt dit bij aan het succes van de samenwerking?
- Hoe heeft de groepsidentiteit bijgedragen aan het succes van de samenwerking?
- Wat is het belang van organisatorische inzet (commitment) van de betrokken organisaties?
- In hoeverre heeft vertrouwen in jullie eigen capaciteiten, zoals zelfvertrouwen, een rol gespeeld in het succes van de samenwerking?
- In hoeverre hebben verwachtingen over het resultaat van de samenwerking een rol gespeeld in het succes van de samenwerking?
- In hoeverre spelen emoties een rol bij het succes van de samenwerking, zoals 'fear of missing out'?
- Wat kenmerkt de betrokken organisaties?
- Hebben jullie specifieke gedragscodes voor deelnemers?
- In hoeverre hebben individuele deelnemers invloed op beleid? Besteden jullie aandacht aan evaluaties van beleid?
- Wat kenmerkt jullie organisatiecultuur?
- Welke organisatiefactoren staan het succes in de weg?
- Zijn er unieke organisatorische factoren van betrokken organisaties te benoemen die het succes versterken?
- Is er sprake van positieve uitkomsten door deelname voor de betrokken deelnemers vanuit de eigen organisatie, zoals beloning, zichtbaarheid, aanzien? Zo ja, welke?
- In welke mate zijn de rollen van organisaties duidelijk omschreven in termen van o.a. tijdsbeslag en taken? In welke mate draagt dit bij aan het succes van de samenwerking?
- In hoeverre lukt het jullie om de meerwaarde zichtbaar te maken (het meten van de effectiviteit/ ROI) en de tijdsinvesteringen te verantwoorden? Draagt dit bij aan het succes van de samenwerking?

In het algemeen:
Heeft de samenwerking met ketenpartners gezorgd voor veranderingen binnen het bedrijf? Hebben jullie bepaalde dingen geleerd van ketenpartners? Zo ja, wat dan?
Hoe bepalen de organisaties met elkaar hun risico-positie tot elkaar?

Meer informatie

www.dehaagsehogeschool.nl/onderzoek/lectoraten/details/cybersecurity-in-het-mkb#over-het-lectoraat

R.vanderKleij@hhs.nl

Johanna Westerdijkplein 75
2521 EN Den Haag

let's change
YOU. US. THE WORLD.