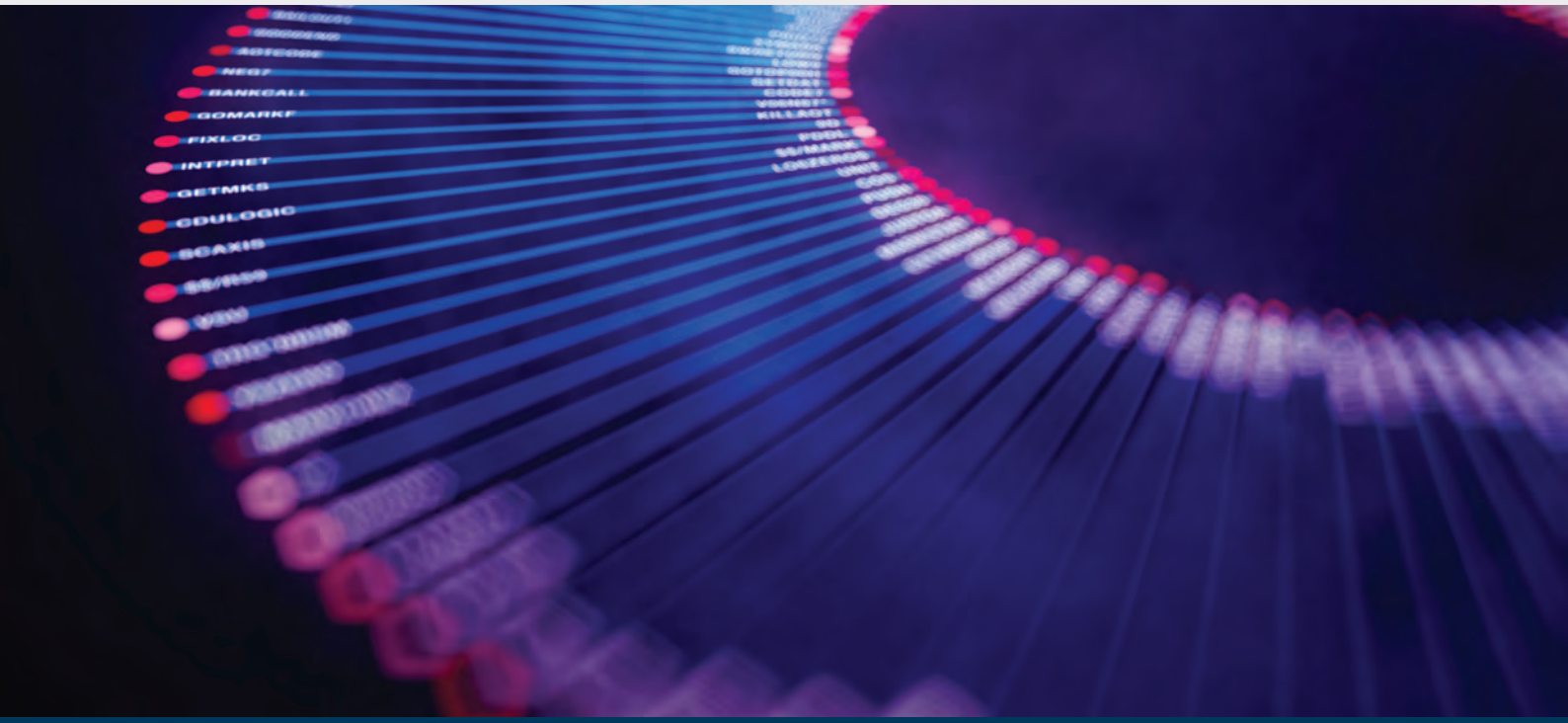
Auteurs: Luuk Bekkers is junior onderzoeker bij het Centre of Expertise Cyber Security van de Haagse Hogeschool en bereikbaar via l.m.j.bekkers@hhs.nl. Rick van der Kleij is senior onderzoeker bij het Centre of Expertise Cyber Security van de Haagse Hogeschool en TNO en is bereikbaar via r.vanderkleij@hhs.nl. Rutger Leukfeldt is senior onderzoeker bij het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving (NSCR) en directeur van het Centre of Expertise Cyber Security en is bereikbaar via e.r.leukfeldt@hhs.nl.



Succesfactoren voor het delen van cybersecurity informatie

In de afgelopen jaren zijn diverse cyberveiligheid informatiedeling-initiatieven opgericht. Dergelijke samenwerkingsverbanden zijn van groot belang om cyberdreigingen het hoofd te kunnen bieden. Maar welke factoren zorgen ervoor dat die initiatieven succesvol zijn?

Bedrijven maken tegenwoordig vaak deel uit van een keten. Een keten kan worden be¬schouwd als een verzameling organisaties waar informatie, diensten, goederen of geld doorheen stroomt (1). Hierbij staat ICT veelal centraal. Deze rol van ICT maakt dat cybergerelateerde risico's een opmars maken binnen ketens. Maar niet elke organisatie beschikt 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.

Digitale weerbaarheid

Er zijn dan ook diverse cyberveiligheid informatiedeling-initiatieven ontwikkeld. Deze samenwerkingsverbanden kunnen van grote waarde zijn voor organisaties om het risico op cyberincidenten te verkleinen. Met behulp van de informatie die wordt gedeeld zijn de deelnemende organisaties namelijk beter in staat hun eigen risicoanalyse uit te voeren en bijpassende maatregelen te treffen. Hierdoor vergroten zij de digitale weerbaarheid van de eigen organisatie en van de sector als geheel. Het is alleen nog onduidelijk welke factoren van invloed zijn op het succes van cyberveiligheid informatiedeling-initiatieven. Inzicht in dergelijke succesfactoren kan door overheidspartijen en andere belanghebbenden gebruikt worden om bedrijven te adviseren en bestaande of toekomstige samenwerkingsverbanden te ondersteunen. De Haagse Hogeschool heeft daarom in opdracht van het Nationaal Cyber Security Centrum een verkennende studie uitgevoerd naar succesfactoren van cyberveiligheid informatiedeling-initiatieven. Dit artikel bevat een overzicht van de belangrijkste resultaten. Voor een volledig overzicht van de resultaten verwijzen we naar de onderzoeksrapportage (2). Het onderzoek richtte zich op twee informatiedeling-initiatieven in de energiesector en een informatiedeling-initiatief van managed serviceproviders. Om succesfactoren te identificeren, voerden wij interviews uit met in totaal zes deelnemers. Alle respondenten zijn informatiebeveiligingsexperts die namens nationale en internationale bedrijven zijn aangesloten bij de informatiedeling-initiatieven.

Vier belangrijkste factoren voor succesvolle informatiedeling-initiatieven

In totaal zijn twintig factoren geïdentificeerd die bijdragen aan succesvolle informatiedeling-initiatieven op het gebied van cyberveiligheid. Vier factoren die door vrijwel alle respondenten zijn benoemd en daarmee worden beschouwd als de belangrijkste zijn: expertise onder de leden, vertrouwen, lidmaatschapseisen en een structurele opzet. Deze vier factoren worden nu kort toegelicht.

Vertrouwen is een thema dat bij alle respondenten aan bod komt als kritieke succesfactor: een hoge mate van vertrouwen tussen leden is vereist voor de bereidheid om informatie te delen. Met vertrouwen doelen we op de overtuiging van een lid dat andere leden de juiste bedoelingen hebben en om die reden bereid is afhankelijk te zijn van de daden van die andere leden. Ook lijkt vertrouwen gerelateerd aan veel andere factoren die zijn geïdentificeerd. Het nemen van tijd wordt door respondenten aangehaald als belangrijkste bouwsteen voor vertrouwen: er is tijd nodig om vertrouwen in de relatie te ontwikkelen. Naast het nemen van tijd, zijn andere bouwstenen voor vertrouwen volgens respondenten: er sprake is van een stabiele bezetting, de deelnemende bedrijven en diens vertegenwoordigers worden nauwkeurig in overleg gekozen, alle vertegenwoordigers zijn informatiebeveiligingsexperts en hebben overlappende vakinhoudelijke kennis (common body of knowledge). Zodra het onderlinge vertrouwen wordt geschaad, bijvoorbeeld als vertrouwelijke informatie voor commercieel gewin wordt verkocht, houdt direct alle informatiedeling op met die partij, zo stellen de respondenten.

Naast vertrouwen noemen alle respondenten expertise onder de leden als belangrijke factor voor succes. Zo zijn alle deelnemers van de onderzochte informatiedeling-initiatieven informatiebeveiligingsexperts, in tegenstelling tot sommige andere samenwerkingsverbanden waar ook beleidsmakers aansluiten. Doordat de deelnemers vakinhoudelijke kennis hebben en 'dezelfde taal spreken' wordt er relevante kennis gedeeld, weten de deelnemers hoe ze moeten handelen met die kennis en is het onderling vertrouwen hoog. Deze expertise helpt leden ook bij het maken van een afweging of bepaalde informatie toegevoegde waarde heeft en dus gedeeld zou moeten worden. De deelnemende bedrijven en diens vertegenwoordigers zijn op basis van lidmaatschapseisen gerechtigd om aan te sluiten. Zo geldt bij een van de onderzochte informatiedeling-initiatieven 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 en daar een goede informatiepositie hebben. Een dergelijke ballotage is tevens nodig voor het ontwikkelen van vertrouwen en speelt daarom een belangrijke rol bij succesvolle informatiedeling.

De informatiedeling-initiatieven zijn tevens 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 tussen leden, aldus de respondenten. Een belangrijke factor hierbij is de aanwezigheid van afspraken over hoe om te gaan met de informatie die de leden hebben, zoals het 'traffic light protocol'. Daarmee wordt voor alle deelnemers helder welke afspraken er zijn omtrent het delen van informatie en worden onnodige discussies vermeden. Verder draagt ook een jaarplan bij aan de gestructureerde opzet. Aan de hand van het jaarplan bepalen de leden welke onderwerpen op de agenda komen.

Naast de succesfactoren is er ook gevraagd naar de aanleiding en de meerwaarde voor de respondenten van de initiatieven. Zo blijkt uit de interviews dat de onderzochte informatiedeling-initiatieven 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 de initiator een belangrijke rol heeft bij het opstarten, bijvoorbeeld door organisaties en experts binnen de eigen sector te enthousiasmeren en te motiveren om deel te nemen aan een samenwerking. De meerwaarde van de initiatieven is voor alle door ons gesproken respondenten drieledig: netwerken met collegae, leren van elkaar en verbetering van de eigen bedrijfsvoering.

Vragen voor vervolgonderzoek

Het onderzoek laat zien dat er een groot aantal factoren zijn die bijdragen aan het succes van informatiedeling-initiatieven op het gebied van cyberveiligheid. Deze factoren kunnen door de overheid, maar ook door organisaties zelf, gebruikt worden om bestaande en toekomstige samenwerkingsverbanden te ondersteunen. De verkennende aard van het onderzoek maakt echter dat er nog een aantal vragen of onderwerpen zijn die nader onderzoek verdienen. Zo zou vervolgonderzoek zich kunnen richten op het identificeren van strategieën voor het opstarten van informatiedeling-initiatieven op het gebied van cyberveiligheid en hoe relevante partijen daar in eerste instantie voor bij elkaar kunnen worden gebracht. 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.

Zoals genoemd, is de factor vertrouwen cruciaal gebleken voor het succes van de door ons onderzochte samenwerkingsverbanden. Toekomstig onderzoek zou zich kunnen richten op strategieën om het onderling vertrouwen tussen deelnemers te initiëren, faciliteren en behouden over de tijd. Op basis van het huidig onderzoek kan niet (voldoende) worden geconcludeerd of en op welke manier de geïdentificeerde factoren samenhangen met elkaar. Vervolgonderzoek zou zich dus ook kunnen richten op het duiden van de onderlinge (causale) samenhang tussen succesfactoren en hoe de factoren zich ontwikkelen binnen samenwerkingsverbanden.

Een laatste mogelijkheid voor vervolgonderzoek die wij hier willen noemen is gericht op de vraag 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 van wie ICT niet de corebusiness is, aangezien dergelijke bedrijven veelal als risicovol voor cybersecurity worden beschouwd.

Referenties

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

(2) https//:www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/rapport-a4-lectoraat-cybersecurity-in-het-mkb.pdf