KETENWEERBAARHEID TEGEN CYBERDREIGINGEN

UITGANGSPUNTEN, GOOD PRACTICES EN EEN STAPPENPLAN VOOR HET VERGROTEN VAN CYBER-KETENWEERBAARHEID

WHITEPAPER
Februari 2017

TNO innovation for life

TNO.NL/cybersecurity
WE MAKE CYBER WORK FOR YOU

INLEIDING

Dit whitepaper biedt achtergrondinformatie, good practices en een stappenplan voor het vergroten van cyber-ketenweerbaarheid en is bedoeld voor organisaties die onderdeel zijn van een keten en cybersecurity willen versterken. Cyber-ketenweerbaarheid betreft het vermogen van ketens om zich te beschermen tegen cyberdreigingen, te herstellen van incidenten en zich voortdurend aan te passen aan een veranderend dreigingslandschap. Het vergroten van cyber-ketenweerbaarheid is niet eenvoudig. Het vergt investeringen, afstemming en samenwerking terwijl het ketenrisico moeilijk is te doorgronden en het lastig kan zijn om nut en noodzaak van een gezamenlijke aanpak uit te leggen. Dit whitepaper biedt praktische handvatten om deze uitdaging aan te gaan.

Cyberdreigingen hebben weinig op met organisatiegrenzen. Het op orde hebben van de eigen organisatie is niet voldoende om het cyberrisico voor een organisatie te beheersen. Denk bijvoorbeeld aan diefstal van medische gegevens, niet van een ziekenhuisserver, maar via een dienstverlener die werkt aan een nieuw patiëntenportaal of een andere zorgverlener die via een interface toegang heeft tot gegevens die door het ziekenhuis worden ingevoerd. Tegelijkertijd is het beheersen van het cyberrisico door individuele ketenorganisaties niet voldoende om het cyberrisico van de keten als geheel te beheersen. Denk bijvoorbeeld aan het gebruik van één aanbieder van communicatienetwerken door meerdere ketenorganisaties. Uitval van communicatie bij één ketenorganisatie kan door de keten worden opgevangen. Maar in geval van uitval van communicatie bij meerdere ketenorganisaties stagneert uiteindelijk de hele keten. Het beheersen van een dergelijk cyber-ketenrisico vereist afstemming en samenwerking tussen ketenorganisaties.

FOCUS OP KETENS

Samenwerking op het gebied van cybersecurity wordt in veel gevallen geïnitieerd vanuit bestaande samenwerkingsverbanden zoals brancheorganisaties, clusters van bedrijven of regio's. Vanuit zulke samenwerkingsverbanden is het vaak lastig om concreet met cybersecurity aan de slag te gaan. Bewustwording en kennisuitwisseling zijn in alle samenwerkingsverbanden relevant maar het nemen van concrete maatregelen, afstemming en samenwerking zijn pas nodig wanneer organisaties daadwerkelijk van elkaar afhankelijk zijn. En dat is het geval voor organisaties die in een keten opereren.

Veel belangrijke processen komen door middel van ketens tot stand. Denk bijvoorbeeld aan de voor Nederland gedefinieerde vitale processen[1] zoals toonbankbetalingsverkeer, vlucht- en vliegtuigafhandeling of de grootschalige productie, verwerking en opslag van (petro)chemische stoffen. Net als de rest van de samenleving raken ook ketens in steeds sterkere mate gedigitaliseerd. Hierdoor neemt het belang van cybersecurity toe, zowel voor individuele ketenorganisaties als voor de digitale ketens waar zij gebruik van maken.

TOTSTANDKOMING

Dit whitepaper is tot stand gekomen op basis van gesprekken met personen die vanuit hun organisatie betrokken zijn (geweest) bij initiatieven op het gebied van ketenweerbaarheid. Daarnaast is literatuuronderzoek gedaan naar bestaande kaders en good practices voor de bescherming van ketens (supply chain (cyber) security) en is een oefening georganiseerd met drinkwaterbedrijven. De oefening vormde een case study voor het (efficiënt) in kaart brengen van een cyber-fysieke keten en het verkennen van ketenkwetsbaarheden.

LEESWIJZER

Dit whitepaper bestaat uit drie onderdelen. Het eerste deel bestaat uit uitgangspunten en achtergrondinformatie voor ketenweerbaarheid en behandelt achtereenvolgens ketens, cyber-kwetsbaarheden in ketens, ketengovernance en cyber-ketenweerbaarheid. Deel twee beschrijft vijf good practices voor cyber-ketenweerbaarheid. Deel drie beschrijft een stappenplan dat organisaties helpt met het nemen van initiatief voor het vergroten van ketenweerbaarheid. Onderstaand figuur 1 geeft de opbouw van het whitepaper schematisch weer.

UITGANGSPUNTEN: KETENWEERBAARHEID TEGEN CYBER-DREIGINGEN

- Ketens
- (Cyber-kwetsbaarheden in ketens)
- Ketengovernance
- Cyber-keten-weerbaarheid

GOOD PRACTICES VOOR HET VERGROTEN VAN KETENWEERBAARHEID TEGEN CYBER-DREIGINGEN

- Een dialoog tussen ketenpartners
- Informatie-uitwisseling
- Ketenoefeningen
- Ketenrisicoanalyse
- Ketenrisicobeheersing

STAPPENPLAN VOOR HET VERGROTEN VAN KETENWEERBAARHEID TEGEN CYBERDREIGINGEN

- **Stap 1.** Breng ketenorganisaties bij elkaar
- **Stap 2.** Voer een dialoog over scope en basisniveau cybersecurity
- **Stap 3.** Creëer commitment
- **Stap 4.** Organiseer een ketenoefening
- **Stap 5.** Begin met informatie uitwisseling
- **Stap 6.** Voer een ketenrisicoanalyse uit
- **Stap 7.** Stel een roadmap op voor ketenrisicobeheersing
- **Stap 8.** Monitor cyberketenweerbaarheid

1 Zie voor een overzicht van de Nederlandse vitale processen: https://www.nctv.nl/organisatie/nationale_veiligheid/vitale_infrastructuur/index.aspx

KETENS

Veel producten en diensten – waaronder een aantal vitale processen voor de maatschappij – komen door ketens tot stand. Een keten is een veelzijdig begrip. Een veelgebruikte definitie van een keten is een 'network of companies involved in the upstream and downstream flows of products, services, finances, and information from the initial supplier to the ultimate customer' (Metzer et al., 2001). Volgens deze definitie zijn organisaties in een keten verbonden doordat zij deel uitmaken van een stroom van producten, diensten, geld of informatie.

Ketenkenmerken

Ketens hebben een aantal kenmerken. Ten eerste, kan in een keten onderscheid worden gemaakt tussen de grondslag – de individuele ketenorganisaties – en de keten – de ketenorganisaties tezamen. Ten tweede moet er sprake zijn van een 'dominant ketenprobleem' (Grijpink, 2010), een probleem dat de organisaties in de keten verbindt en dat geen van de organisaties op eigen kracht kan oplossen. Ten derde is er zowel sprake van afhankelijkheid als autonomie. Het gezamenlijke probleem en de samenwerking die nodig is om het probleem op te lossen, maken dat ketenorganisaties van elkaar afhankelijk zijn. Tegelijkertijd is er sprake van autonomie; ketenorganisaties hebben geen zeggenschap over elkaar maar kunnen elkaar enkel beïnvloeden. Ten vierde hebben ketens een bepaalde mate van complexiteit. De complexiteit van ketens varieert van een lineair verband tussen enkele organisaties – een directe keten – tot wederzijdse afhankelijkheden tussen een groot aantal organisaties – een complexe keten (Metzer et al., 2001). Het verschil zit naast het aantal ketenorganisaties dus ook in de manier waarop producten, diensten, geld of informatie worden uitgewisseld. Lineaire ketens waarin producten enkel worden doorgegeven zijn eenvoudiger dan ketens waarin ook terugkoppeling plaatsvindt (Grijpink, 2010). Deze ketenkenmerken bepalen tezamen de omvang en de mogelijkheden van ketenvraagstukken zoals kwaliteit, efficiëntie, betrouwbaarheid en weerbaarheid.

Soorten ketens

Ketens bestaan in allerlei samenstellingen maar een paar aspecten helpen om soorten ketens te onderscheiden. Ten eerste kan onderscheid worden gemaakt tussen ketens van bedrijfsprocessen ((vitale) toeleveringsketens) en ketens van informatie- en communicatiesystemen die bedrijfsprocessen ondersteunen (informatieketens). In toeleveringsketens worden producten, diensten of geld uitgewisseld tussen ketenorganisaties. In informatieketens wordt informatie uitgewisseld, vaak om bedrijfsprocessen die onderdeel uitmaken van een toeleveringsketen aan te sturen of te controleren. Informatieketens kunnen ook meerdere of zelfs alle organisaties in een toeleveringsketen bedienen. In dat geval is er sprake van een keteninformatiesysteem.

Een voorbeeld van een keteninformatiesysteem is Portbase, het systeem waarmee bedrijven en andere organisaties in de logistieke keten in de Rotterdamse Haven informatie uitwisselen[2].

Daarnaast wordt onderscheid gemaakt tussen ketens door hetgeen dat in de keten wordt uitgewisseld. Zo is er sprake van een productieketen wanneer een product door meerdere ketenorganisaties wordt gemaakt. In procesketens worden producten bewerkt en verrijkt totdat zij bij een uiteindelijke afnemer worden afgeleverd. En in betaalketens werken banken, betaalinstellingen, telecomproviders en winkeliers samen om te zorgen dat financiële transacties goed verlopen.

Afnemers en leveranciers

Vanuit een individuele ketenorganisatie gezien is naast het soort keten waarin de organisatie zich bevindt ook de positie in de keten van belang. Zo kan een ketenorganisatie leverancier zijn in een keten. In dat geval bedient de organisatie een keten en moet worden voldaan aan de eisen die andere ketenorganisaties aan de levering stellen. Aan de andere kant kan een ketenorganisatie afnemer zijn. Afnemers stellen doorgaans eisen aan leveranciers waardoor zijn een grote rol hebben bij het bepalen van kwaliteit, efficiëntie, betrouwbaarheid en weerbaarheid in een keten. In veel gevallen is een ketenorganisatie zowel leverancier als afnemer. Op ketenniveau kunnen organisaties actief zijn die ketens (of delen daarvan) overzien en vertegenwoordigen zoals branche- of sectororganisaties.

Ketens in ontwikkeling

Door verdergaande digitalisering raken bedrijfsprocessen en informatievoorziening zo met elkaar verweven dat het onderscheid tussen toeleveringsketens en informatieketens steeds minder betekenisvol lijkt. Er zijn vaak meerdere informatieketens nodig om een toeleveringsketen te laten functioneren. Bij sterke integratie van bedrijfsprocessen en onderliggende digitale systemen is in de praktijk sprake van een cyber-fysiek systeem. De integratie van bedrijfsprocessen en informatiesystemen maakt het overzien van een keten steeds moeilijker. Het in beeld brengen van een cyber-fysieke keten vergt immers inzicht in de keten van bedrijfsprocessen, de onderliggende informatieverwerkende systemen én de onderlinge verbanden. In de praktijk mondt dit al snel uit in een zeer complexe, tijdrovende systeemanalyse. Het onderscheid tussen de toeleveringsketen en informatieketens houdt hierbij wel analytische waarde omdat het helpt om complexe cyber-fysieke systemen in meer overzichtelijke delen te splitsen.

De verscheidenheid aan soorten ketens en verschillen in complexiteit maken dat er geen uniforme aanpak bestaat voor het borgen van kwaliteit, efficiëntie en weerbaarheid van ketens. Inzichten en ervaringen die zijn opgedaan in de ene keten kunnen niet zonder meer worden gebruikt

2 https://www.portbase.com/port-community-system/

in andere ketens. Generieke maatregelen moeten steeds weer worden vertaald naar de specifieke kenmerken en omstandigheden van een keten om effectief te worden ingezet. Dat geldt ook voor de good practices en het stappenplan in dit whitepaper. Steeds moet worden nagegaan of en hoe de inzichten toepasbaar zijn in een specifieke keten.

WAAR BEVINDT UW ORGANISATIE ZICH IN DE KETEN?
Voordat u met ketenweerbaarheid aan de slag gaat, en om te bepalen welke delen van dit whitepaper het meest relevant voor u zijn, is het nodig vast te stellen van wat voor keten uw organisatie onderdeel is en waar u zich in deze keten bevindt. Het beantwoorden van onderstaande vragen helpt u daarbij.

BENT U EEN KETENORGANISATIE OF EEN KETEN OVERKOEPELENDE ORGANISATIE?
Ketenorganisatie vormen de grondslag van een keten en leveren samen met andere ketenorganisaties een product of dienst. Ketenorganisaties zijn doorgaans gezamenlijk verantwoordelijk voor de kwaliteit van het product en de weerbaarheid van de keten. Voor ketenorganisaties is het logisch in eerste instantie naar individuele kwetsbaarheden en maatregelen te kijken. Keten overkoepelende organisaties zijn actief op het niveau van de keten waar zij coördineren of de belangen van meerdere ketenorganisaties behartigen. Voor deze organisaties zijn specifieke ketenkwetsbaarheden en ketenmaatregelen het meest relevant.

BENT U LEVERANCIER, AFNEMER OF BEIDE?
Naast de positie van uw organisatie in een keten heeft uw organisatie ook een rol. Levert u een product of dienst aan andere ketenorganisaties of neemt u producten of diensten af? Wanneer uw organisatie zich in het midden van een keten bevindt, heeft uw organisatie beide rollen. Voor leveranciers is een voldoende basisniveau van weerbaarheid belangrijk. Voor afnemers is het verzekeren van de kwaliteit en veiligheid van geleverde diensten of producten belangrijk.

IS UW ORGANISATIE ONDERDEEL VAN EEN TOELEVERINGSKETEN OF EEN INFORMATIEKETEN?
Is uw organisatie onderdeel van een toeleveringsketen waarmee een product of dienst bij een uiteindelijke afnemer, klant of burger wordt bezorgd? Of bent u onderdeel van een informatieketen die helpt om een toeleveringsketen te laten functioneren? Bij het beantwoorden van deze vragen is het belangrijk te bepalen waar uw keten begint en waar hij ophoudt en hoe de keten waar uw organisatie onderdeel van is zich verhoudt tot andere ketens.

Wat is het dominante ketenprobleem in uw keten? Samenwerking tussen ketenorganisaties en een gecoördineerde aanpak komen enkel tot stand wanneer het dominante ketenprobleem daar voldoende draagvlak voor genereert (Grijpink, 2010). Wat is het probleem waarvoor uw keten de oplossing biedt en dat geen van de ketenorganisaties zelf kan oplossen? Hoe groter (het bewustzijn van) deze gezamenlijke uitdaging, hoe meer draagvlak voor afstemming en samenwerking er doorgaans is. De mogelijkheden om aan de slag te gaan met ketenkwetsbaarheden en ketenmaatregelen hangen deels af van de omvang van het dominante ketenprobleem.

HOE COMPLEX IS DE KETEN WAAR UW ORGANISATIE ONDERDEEL VAN IS?
Voor het beantwoorden van deze vraag kunt u nagaan met hoeveel ketenorganisaties vormt u een toeleverings- of informatieketen vormt en hoe de ketenorganisaties zich tot elkaar verhouden. Een keten van enkele organisaties die een product of dienst zonder gezamenlijke afstemming doorgeven (bijvoorbeeld een distributiekanaal) kent weinig complexiteit. Een keten van veel organisaties die producten en diensten gezamenlijk afstemmen kent meer complexiteit.

(CYBER)KWETSBAARHEDEN IN KETENS

Ketenkwetsbaarheden

Om de cyber-kwetsbaarheden van ketens te begrijpen is het nodig eerst stil te staan bij algemene ketenkwetsbaarheden. We behandelen er drie: zwakke schakels, verspreiding van informatie en negatieve externe effecten (Pettit et al., 2010[3]).

Veel ketens raken verstoord bij uitval van één schakel. Denk bijvoorbeeld aan een betaalketen waarin een transactie niet kan plaatsvinden wanneer de telecomverbinding tussen een betaalinstelling en een winkelketen uitvalt. Wanneer uitval van afzonderlijke schakels tot uitval van een hele keten leidt, is de keten zo sterk als de zwakste schakel. In dit geval bepalen zwakke schakels de betrouwbaarheid en weerbaarheid van een keten als geheel. Zwakke schakels vormen daarmee een eerste ketenkwetsbaarheid. Een tweede soort ketenkwetsbaarheid komt voort uit de verspreiding van informatie over verschillende ketenorganisaties en het feit dat geen van de organisaties over een totaalbeeld beschikt. Een voorbeeld hiervan zijn inbraken in de haven voor het achterhalen van informatie over containers. Omdat elke organisatie enkel weet heeft van de inbraken die zelf zijn gesignaleerd, ziet geen van de ketenorganisaties een patroon. Pas wanneer de beschikbare informatie bij elkaar wordt gebracht, wordt zichtbaar dat criminelen systematisch op zoek zijn naar manieren om informatie te achterhalen. Verspreiding van informatie is zodoende een tweede ketenkwetsbaarheid. Negatieve externe effecten tussen ketenorganisaties vormen een derde soort ketenkwetsbaarheid. De weerbaarheid van een keten wordt niet alleen wordt bepaald door de kracht van individuele schakels maar ook door de samenhang tussen de schakels. In sommige gevallen kunnen kwetsbaarheden die voor een ketenorganisatie niet evident zijn voor een andere ketenorganisatie een aanzienlijk risico vormen. Dit kan ook opgaan voor maatregelen waardoor een ketenorganisatie weerbaarder wordt, die kunnen in sommige gevallen (aanzienlijk goedkoper) door een andere ketenorganisatie worden genomen. Een voorbeeld hiervan is controle op de juistheid van de invoer van informatie in een informatieketen. Voor de organisatie die de informatie invoert is de volledigheid of juistheid van de informatie niet altijd even belangrijk als voor andere organisaties. Voor de partij die de informatie invoert is een extra controle eenvoudig te regelen terwijl een partij verderop in de keten aanzienlijke kosten moet maken om de informatie te controleren of aan te vullen.

Cyber-ketenkwetsbaarheden

De generieke ketenkwetsbaarheden die eerder zijn beschreven, zijn ook van toepassing op het digitale domein. Ook voor ICT geldt dat de zwakke schakels de sterkte van een gehele keten bepalen, dat informatie verspreid is over meerdere ketenorganisaties en dat externe negatieve effecten voor ketenkwetsbaarheden zorgen en het nemen van maatregelen moeilijker maken. Daarnaast kan er in ketens sprake zijn van specifieke cyber-ketenkwetsbaarheden; kwetsbaarheden waardoor de beschikbaarheid, integriteit en vertrouwelijkheid van ICT in een keten gevaar komt. We beschrijven er drie: interfaces, keteninformatiesystemen en gezamenlijke ICT-diensten.

Interfaces vormen de infrastructuur waarmee ketenorganisaties informatie uitwisselen. Een interface is vaak niet meer dan een programma waarmee informatie uit een systeem van een ketenorganisatie wordt verstuurd naar een systeem van een andere ketenorganisatie en andersom. Interfaces zijn potentieel kwetsbaar omdat ze per definitie in verbinding staan met de buitenwereld. Daarmee bestaat bijvoorbeeld een mogelijkheid van ongeautoriseerde toegang. Daarnaast zijn meerdere organisaties betrokken bij het beheer en de bescherming van interfaces wat de kans op onduidelijkheden en misverstanden doet toenemen.

Keteninformatiesystemen zijn specifiek ontworpen om meerdere of zelfs alle organisaties in een keten van informatie te voorzien. Eerder is al het voorbeeld van Portbase genoemd, het informatieportaal voor de haven van Rotterdam. Keteninformatiesystemen worden ook steeds vaker gebruikt in de zorg waar meerdere behandelaars toegang krijgen tot dezelfde informatie in een digitaal patiëntendossier. Keteninformatiesystemen zijn een aantrekkelijk doelwit voor cybercriminelen omdat ze veel en belangrijke informatie bevatten. Aantasting en uitval van keteninformatiesystemen heeft vaak een grote impact op het functioneren van een keten omdat veel ketenorganisaties van het systeem afhankelijk zijn.

De kwetsbaarheid van een keten door het gezamenlijk gebruik van diensten komt voornamelijk voort uit het feit dat een individuele organisatie de uitval van een dienst kan opvangen (bijvoorbeeld door gebruik van noodvoorzieningen) terwijl dit voor meerdere of alle organisaties in een keten niet haalbaar is. Gezamenlijke diensten vormen ook buiten het digitale domein een mogelijke ketenkwetsbaarheid. Denk bijvoorbeeld aan afhankelijkheid van elektriciteit of water. Naar dergelijke afhankelijkheden is onderzoek gedaan waardoor een duidelijk beeld bestaat van de belangrijkste afhankelijkheden, met name de alom aanwezige afhankelijkheid van elektriciteit en telecommunicatie[4]. Het digitale domein kent veel diensten die gezamenlijk afgenomen kunnen worden en waarbij de gezamenlijke afhankelijkheid niet altijd duidelijk is. Het kan bijvoorbeeld gaan om gezamenlijke afhankelijkheid van dataopslag- en clouddiensten, ICT-leveranciers, vaste en mobiele communicatienetwerken of kantoorautomatisering (zie ook Luiijf en Klaver, 2015).

3 Pettit et al., 2010 presenteren een uitgebreid overzicht van supply chain vulnerability factors en capabilities.

4 Zie bijvoorbeeld de CAET studies.

Een storing bij een telecomprovider in Rotterdam biedt een voorbeeld van het effect dat uitval van gezamenlijke diensten kan hebben. Door de storing vielen delen van industriële controlesystemen uit en bleken servicemonteurs en andere belangrijke personen in crisisorganisaties niet bereikbaar[5].

Cyberdreigingen
Cyberdreigingen zijn dreigingen die hun oorsprong hebben in het digitale domein. Cyberdreigingen zijn relevant voor een keten wanner ze substantiële impact kunnen hebben op het voortbrengingsvermogen van een keten. Welke cyberdreigingen relevant zijn voor een keten hangt af van de kwetsbaarheden in een keten, zowel bij individuele ketenorganisaties als in de keten als geheel.

Digitalisering introduceert cyberkwetsbaarheden in ketens. Deze kwetsbaarheden kunnen zowel onbedoeld tot verstoringen leiden als opzettelijk worden misbruikt. Onbedoelde verstoringen volgen bijvoorbeeld uit defecten of misconfiguraties. Moedwillige verstoringen kunnen ontstaan als gevolg van cybercriminaliteit, hacktivisme of activiteiten van statelijke actoren[6].
Het cyberdreigingslandschap verandert voortdurend en welke cyberdreigingen relevant zijn voor een keten hangt af van ketenkwetsbaarheden zoals gebrekkige cybersecurity van individuele ketenorganisaties (zwakke schakels), interfaces, keteninformatiesystemen en gezamenlijke diensten. De verspreiding van informatie en negatieve externe effecten zorgen er daarbij voor dat kwetsbaarheden en cyberdreigingen onopgemerkt blijven of blijven bestaan.

WELKE CYBERKWETSBAARHEDEN ZIJN RELEVANT VOOR UW KETEN?
Om te bepalen welke cyberkwetsbaarheden relevant zijn voor uw organisatie en de keten waar uw organisatie deel van is, moet worden nagegaan hoe de keten in elkaar steekt en welke (potentiele) kwetsbaarheden in uw keten kunnen bestaan. Het beantwoorden van onderstaande vragen helpt u daarbij.

HEBBEN DE INDIVIDUELE KETENORGANISATIES IN UW KETEN CYBERSECURITY OP ORDE?
Wat voldoende cybersecurity is voor een organisatie hangt af van de specifieke bedrijfsprocessen en het risicoprofiel van een organisatie. Voor alle organisaties geldt echter dat het op orde hebben van de basis een noodzakelijke voorwaarde vormt. Denk hierbij aan elementaire bescherming- en incident response maatregelen en een information security managementsysteem. Er zijn zowel generieke en als industrie specifieke standaarden die helpen bij het bepalen wat een basisniveau voor cybersecurity is (zie ook de good practice ‘een dialoog tussen ketenpartners’). Naast een basis is het ook raadzaam na te gaan of er sprake is van mogelijke specifieke kwetsbaarheden in de keten zoals het bestaan van legacy systemen.

WISSELT U (GEAUTOMATISEERD) INFORMATIE UIT MET KETENPARTNERS?
De koppelingen tussen organisaties waarmee (geautomatiseerd) informatie wordt uitgewisseld vormen een mogelijke ketenkwetsbaarheid. Zijn de koppelingen die u gebruikt voldoende beschermd en zijn de taken en verantwoordelijkheden ten aanzien van de bescherming duidelijk belegd?

MAAKT UW KETEN GEBRUIK VAN EEN KETENINFORMATIESYSTEEM?
Een keteninformatiesysteem bevat doorgaans veel en belangrijke informatie voor een keten. Is het keteninformatiesysteem in uw keten voldoende beschermd en zijn de taken en verantwoordelijkheden ten aanzien van de bescherming duidelijk belegd?

MAAKT U GEBRUIK VAN DEZELFDE ICT-PRODUCTEN EN DIENSTEN ALS UW KETENPARTNERS?
Gezamenlijk gebruik maken van dezelfde ICT-producten en diensten betekent dat uitval van deze producten of diensten een grote impact heeft op het functioneren van de keten waar u onderdeel van bent. Denk bijvoorbeeld aan communicatienetwerken of dataopslag.

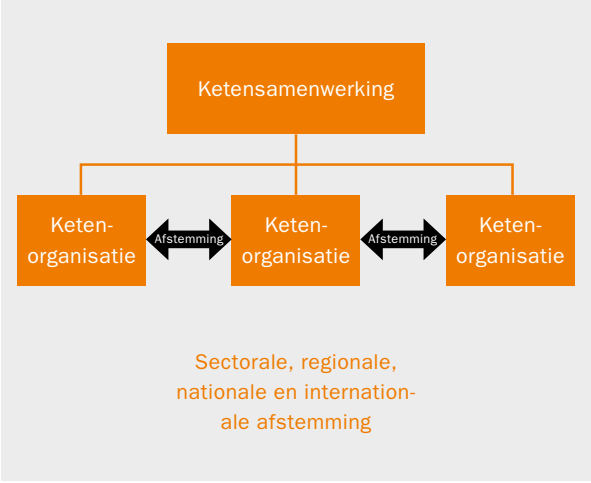
Het ligt voor de hand dat u geen volledig antwoord kunt geven op deze vragen. Het stappenplan in deel drie van die whitepaper biedt handvatten om meer inzicht in de mogelijke cyber-kwetsbaarheden van uw keten te krijgen.

5 Zie: http://webwereld.nl/it-beheer/1080-5-pijnlijke-waarheden-van-de-vodafone-storing en https://www.agentschaptelecom.nl/sites/default/files/rapport-storing-telecommunicatienetwerk-waalhaven-rotterdam.pdf

6 Zie ook NCSC (2016) voor een uitgebreide specificatie van actoren die aanvallen uitvoeren. Daar worden ook recente ontwikkelingen en activiteiten van iedere groep actoren aangehaald.

KETENGOVERNANCE

Ketengovernance omvat de mechanismes die beschikbaar zijn in een keten voor afstemming en het oplossen van gezamenlijke problemen (Ghosh & Fedorowicz, 2008). Dit zijn bijvoorbeeld overleggen en afspraken tussen ketenorganisaties, ketenbrede afspraken en samenwerkingsverbanden en coördinatie en sturing door keten overkoepelende organisaties of overheden.
De mechanismes voor ketengovernance kunnen zich op het niveau van individuele ketenorganisaties bevinden, in dat geval is er sprake van afstemming tussen ketenorganisaties. Daarnaast kunnen mechanismes zich op het ketenniveau bevinden. In dat geval is er sprake van ketensamenwerking. Ook zonder mechanismes voor afstemming, coördinatie en samenwerking kan er overigens sprake zijn van een keten (Metzer et al, 2001). In dat geval wordt vaak gesproken over distributiekanalen. Daarnaast hoeven mechanismes voor afstemming en coördinatie niet specifiek voor een keten te gelden. Ze kunnen ook breder zijn vastgelegd tussen organisaties in een netwerk, cluster of sector. Denk bijvoorbeeld aan (internationale) industriestandaarden en afspraken. Figuur 2 geeft de verhouding tussen afstemming tussen ketenorganisaties en ketensamenwerking weer in de bredere context van sectorale, regionale, nationale en internationale afspraken en samenwerkingsverbanden.



Figuur 2 - Twee niveaus voor ketengovernance

Afstemming tussen ketenorganisaties

Het is typerend voor ketens dat er geen sprake is van een hiërarchische relatie tussen ketenorganisaties en dat ketenorganisaties elkaar nergens toe kunnen dwingen. Er is enkel sprake van wederzijdse beïnvloeding. Afstemming tussen ketenorganisaties vormt daarom een groot deel van ketengovernance.

Afstemming tussen ketenorganisaties kan onder andere plaatsvinden in de vorm van informatie-uitwisseling, (contractuele) afspraken zoals Service Level Agreements (SLA's) en wederzijdse hulp bij incidenten. Vanuit onderlinge afspraken kan zogenaamde 'estafette-coördinatie' ontstaan. Dit houdt in dat ketenaspecten langs opeenvolgende schakels worden geregeld. Een voorbeeld hiervan is een afspraak over de maximale uitvalsduur van bijvoorbeeld een softwareapplicatie. De afspraak geldt in eerste instantie tussen de gebruiker en de leverancier. De leverancier maakt dezelfde afspraak vervolgens met zijn eigen leveranciers om de afspraak naar de eindgebruiker na te kunnen komen. Deze leveranciers maken op hun beurt weer soortgelijke afspraken waardoor de afspraak over de maximale uitvalsduur uiteindelijk voor de hele keten geldt.

Ketensamenwerking

Ketensamenwerking betekent dat afstemming over ketenaspecten op het niveau van de keten plaatsvindt. Dit is bijvoorbeeld het geval wanneer er sprake is van ketenoverleg en ketenafspraken of wanneer er een ketenregisseur wordt aangesteld. Deze vormen van verticale coördinatie ontstaan doorgaans pas wanneer het dominante ketenprobleem zo sterk is dat afstemming tussen ketenorganisaties geen acceptabele oplossing biedt (Grijpink, 2010). Ketensamenwerking kan variëren van ad hoc initiatieven tot meer geformaliseerde vormen van coördinatie of zelfs strategische samenwerking (van Duivenboden, 2000). Wanneer het functioneren van ketens van groot belang is voor de samenleving – zoals het geval is bij de vitale infrastructuur – kan ketensamenwerking worden gestimuleerd of zelf vereist door overheden.

WELKE VORMEN VAN KETENGOVERNANCE KENT UW KETEN?

Is er sprake van onderlinge afstemming tussen ketenorganisaties?

Onderlinge afstemming tussen ketenorganisaties kan onder andere bestaan in de vorm van regelmatige overleggen of afspraken tussen ketenorganisaties. Onderlinge afspraken kunnen zowel informeel zijn als contractueel zijn vastgelegd.

Is er sprake van ketensamenwerking?

Ketensamenwerking kan bijvoorbeeld bestaan uit een ketenoverleg of de aanwezigheid van een ketenregisseur. Ketensamenwerking kan ook zijn georganiseerd via sectororganisaties zoals VEWIN voor de drinkwatersector of de Betaalvereniging in geval van betaalketen. Ketensamenwerking hoeft niet structureel te zijn maar kan ook op ad hoc basis bestaan.

CYBER-KETENWEERBAARHEID

Cyber-ketenweerbaarheid betreft het vermogen van ketens om zich te beschermen tegen cyberdreigingen, te herstellen van incidenten en zich voortdurend aan te passen aan een veranderend dreigingslandschap. Cyber-ketenweerbaarheid komt tot stand op het niveau van individuele ketenorganisaties en op het ketenniveau. Omdat producten of diensten vaak alleen worden geleverd als een gehele keten functioneert, is de weerbaarheid van elke individuele ketenorganisatie van groot belang. Ketenorganisaties moeten daartoe voldoende beschermd zijn en hun afhankelijkheden van andere ketenorganisaties beheersen. Op het ketenniveau is het van belang dat inzicht bestaat in de kwetsbaarheden en risico's van de keten als geheel en dat bescherming wanneer nodig over de keten heen wordt afgestemd. We beschrijven drie soorten maatregelen voor cyber-ketenweerbaarheid: weerbaarheid van ketenorganisaties, afstemming voor ketenweerbaarheid en samenwerking voor ketenweerbaarheid.

Weerbare ketenorganisaties

Op het niveau van individuele organisaties wordt via interne managementsturing gewerkt aan de weerbaarheid van de organisatie tegen interne en externe dreigingen. In een ideale situatie fungeert een ketenorganisatie als een zelf beschermend systeem (een self-protecting node) met ingangscontrole op informatie, producten en diensten. Door voldoende cybersecuritymaatregelen te nemen, vormt een organisatie een sterke schakel in een keten. Ingangscontrole en de beheersing van afhankelijkheden zijn doorgaans onderdeel van risico- en Business Continuity Management (BCM).

Afstemming voor ketenweerbaarheid

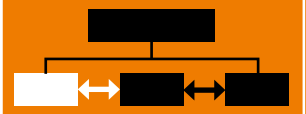
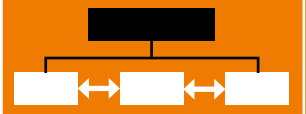
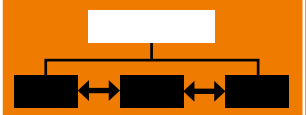
Cyber-ketenafhankelijkheden zijn inmiddels een vast onderdeel van risico- en Business Continuity Management (BCM). Wanneer er sprake is van cyberketenafhankelijkheden is het in eerste instantie aan een organisatie zelf om de nodige afspraken met ketenpartners te maken om deze afhankelijkheden te beheersen. Daarvoor wordt doorgaans gebruik gemaakt van supplier assurance, programma's en maatregelen om te controleren of een leverancier een gewenst weerbaarheidsniveau heeft en voldoende betrouwbaarheid biedt. De ISO/IEC 27000 serie is ontwikkeld met als doel een standaard te vormen waarmee organisaties er zeker van kunnen zijn dat een basisniveau van cybersecurity aanwezig is. Wanneer er sprake is van specifieke interfaces waarmee informatie tussen ketenpartners wordt uitgewisseld, is specifieke afstemming over beschermingsmaatregelen voor de interface belangrijk. Dit kan bijvoorbeeld gaan om afspraken over het gebruik van de interface en verantwoordelijkheden bij het maken van aanpassingen.

Ketenweerbaarheid door ketensamenwerking

Wanneer er sprake is van veel en sterke ketenafhankelijkheden is samenwerking ten aanzien van weerbaarheid over de gehele keten heen nodig. Ketensamenwerking kan bijvoorbeeld bestaan uit informatie-uitwisseling, het analyseren van het keten-cyberrisico en het beheersen van het ketencyberrisico door gezamenlijke maatregelen.

Informatie-uitwisseling is belangrijk voor het tegengaan van versnippering van informatie. Dreigingsinformatie in het digitale domein is doorgaans complex en alleen door het delen van informatie kan een compleet dreigingsbeeld ten aanzien van een keten worden ontwikkeld. Het analyseren van het ketencyberrisico is vooral belangrijk in relatie tot keteninformatiesystemen en gezamenlijke diensten. Keteninformatiesystemen zijn een aantrekkelijk doelwit voor cybercriminelen omdat ze waardevolle informatie bevatten. Analyse van het risico van ongeautoriseerde toegang is belangrijk, zeker wanneer het aantal aangesloten organisaties groot is. Kwetsbaarheden als gevolg van gezamenlijke diensten worden enkel zichtbaar na een risicoanalyse van een gehele keten.

Het gezamenlijk treffen van maatregelen is met name belangrijk wanneer er sprake is van negatieve externe effecten. Afstemming over wie welke maatregelen neemt en eventuele herverdeling van kosten is cruciaal voor het waarborgen van ketenweerbaarheid. Dit is zeker het geval wanneer de kosten van maatregelen door andere partijen moeten worden gedragen dan de partij die het risico draagt.

WELKE MAATREGEN VOOR CYBER-KETENWEERBAARHEID ZIJN GETROFFEN IN UW KETEN?	
Maatregen voor ketenorganisaties 	**Zijn er standaarden of andere normen gesteld waarmee een basisniveau van cybersecurity wordt gewaarborgd voor organisaties in uw keten?** De standaarden of normen kunnen bijvoorbeeld zijn gebaseerd op (industrie) standaarden zoals CobiT, PAS 555, ISA/IEC62443 of de ISO/IEC 27000 serie.
Afstemming tussen ketenorganisaties 	**Zijn er binnen uw keten afspraken gemaakt tussen ketenorganisaties over cybersecurity?** Afspraken kunnen bijvoorbeeld zijn gemaakt in het kader van leveringsovereenkomsten en Service Level Agreements. Door supplier assurance kan een standaard voor cybersecurity zoals hierboven beschreven worden 'opgelegd'. Een andere mogelijkheid zijn afspraken over wederzijdse hulp bij incidenten.
Ketensamenwerking 	**Is er sprake van informatie-uitwisseling en overleg over cyberdreigingen in uw keten?** Informatie-uitwisseling over een keten kan ook in de context van sectorale informatie-uitwisseling plaatsvinden, bijvoorbeeld binnen Information Sharing en Analysis Centers (ISACs)[7]. Hou daarbij in gedachten dat ketens de branche of sector vaak overstijgen, zeker wanneer het ICT ketens betreft. **Is er sprake van afstemming en samenwerking ten aanzien van cybersecurity in uw keten?** Afstemming en samenwerking kan bijvoorbeeld bestaan in de vorm van ketenrisico-analyse en/of ketenrisicobeheersing. Dit kan door ketenorganisaties zelf worden gedaan of door externe organisaties zoals branche- en sectororganisaties.

GOOD PRACTICES VOOR CYBER-KETENWEERBAARHEID

Op basis van gesprekken met organisaties die betrokken zijn (geweest) bij initiatieven op het gebied van cyber-ketenweerbaarheid en literatuuronderzoek zijn vijf good practices geïdentificeerd voor het versterken van cyber-ketenweerbaarheid. Dit zijn:

- Een dialoog tussen ketenorganisaties over ketenweerbaarheid
- Cybersecurity informatie-uitwisseling tussen ketenorganisaties
- Ketenoefeningen
- Ketenrisicoanalyse
- Ketenrisicobeheersing

Een dialoog tussen ketenpartners

Aandacht voor ketens is niet vanzelfsprekend en contact tussen organisaties over cybersecurity is vaak beperkt. Het opstarten van een dialoog over ketenweerbaarheid vormt in deze gevallen een eerste stap voor het vergroten van ketenweerbaarheid. Een geschikt eerste onderwerp voor deze dialoog is het basisniveau van cybersecurity binnen de keten.[8]

7 https://www.ncsc.nl/samenwerking/isacs.html

GOOD PRACTICE 1.
EEN DIALOOG OVER KETENWEERBAARHEID TEGEN CYBERDREIGINGEN

Er zijn veel kaders beschikbaar op basis waarvan een gesprek met ketenpartners over een basisniveau voor cybersecurity kan worden aangegaan. Denk bijvoorbeeld aan de ISO27000 serie en de eerdergenoemde industriestandaarden. De dialoog kan dan gaan over waarom een bepaalde standaard wel of niet ketenbreed wordt geadopteerd. Wanneer er geen voor de hand liggend kader of standaard beschikbaar is om een basisniveau voor cybersecurity te bespreken, stellen we hieronder een aantal thema's voor. Deze thema's zijn afgeleid van ISO27000 en verschillende supplier assurance kaders. Ook wanneer er wel sprake is van een gedeelde standaard is het waardevol een dialoog met ketenpartners te starten. In dit geval kan worden ingegaan op de wijze waarop standaarden zijn ingevuld. Veel standaarden zijn generiek en stellen bijvoorbeeld dat moet worden nagegaan 'welke ICT-systemen worden gebruikt' en wat een 'acceptabele uitvalduur' is. Binnen ketens is het zinvol te bespreken hoe ketenorganisaties de standaard toepassen en interpreteren en wat de consequenties van afwegingen van ketenorganisaties zijn voor ketenpartners en de keten als geheel.

Thema's voor een dialoog over een basisniveau van cybersecurity voor ketenorganisaties:
Information Security Management System (ISMS). Beschikken ketenorganisaties over een ISMS, is het systeem gedocumenteerd en zijn verantwoordelijkheden en functies ten aanzien van informatiebeveiliging en cybersecurity belegd?
Assetmanagement. Beschikken ketenorganisaties over een assetmanagement programma? Assetmanagement betekent onder andere dat belangrijke systemen, middelen en bedrijfsprocessen (schematisch) zijn vastgelegd. Een overzicht van bedrijfsprocessen is onder andere belangrijk om in een later stadium een ketenrisicoanalyse te kunnen uitvoeren.
Toegang en autorisatie. Beschikken ketenorganisaties over een gedocumenteerd systeem voor toegang en autorisatie (identity and access management) ten aanzien van locaties en ICT-systemen en wordt dit structureel bijgehouden?
Software beveiliging. Beschikken ketenorganisaties bijvoorbeeld over gescheiden omgevingen voor kantoorautomatisering en procesautomatisering? Worden beschikbare security patches direct of spoedig geïnstalleerd? En is software geïnstalleerd voor bescherming tegen malware en schadelijk inkomend internetverkeer?
Netwerkbeveiliging. Beschikken ketenorganisaties over een gedocumenteerde netwerkarchitectuur, is duidelijk wie is betrokken bij instandhouding en uitbreiding van het netwerk, is toegang tot netwerken georganiseerd en wordt toegang tot netwerken voor verschillende groepen gebruikers gescheiden, en wordt gevoelige informatie versleuteld?
Leveranciersrelaties: Beschikken ketenorganisaties over aanpak voor supplier assurance en houden leveranciers en ontwikkelaars van software-, hardware- en netwerksystemen zich aan een vergelijkbaar informatiebeveiligingsbeleid?
Testing en incident respons. Beschikken ketenorganisaties over beleid ten aanzien onafhankelijke tests op naleving van informatieveiligheid-procedures en de uitvoering van technische beschermingsmaatregelen? En zijn (beleids)verantwoordelijken, meldplichten, maatregelen en procedures gedocumenteerd voor incidentafhandeling en worden deze regelmatig geoefend?

Informatie-uitwisseling
Vanwege de complexiteit van het digitale domein is informatie-uitwisseling tussen ketenorganisaties cruciaal voor het opstellen van een dreigingsbeeld en het tegengaan van versnippering van informatie.

Cybersecurity informatie-uitwisseling kan zowel voor een sector als geheel als voor een specifieke keten worden ingericht. De afnemer – leverancier verhoudingen en de onderliggende contracten tussen ketenorganisaties maken informatie-uitwisseling in ketens doorgaans wel uitdagender. Voor cybersecurity informatie-uitwisseling zijn verschillende good practices beschreven.

8 Deze thema's zijn ook benoemd in de ISO 27000 serie en komen terug in verschillende supplier assurance frameworks zoals de Google Vendor Security Assessment Questionnaire.

GOOD PRACTICE 2.
CYBERSECURITY INFORMATIE-UITWISSELING TUSSEN KETENORGANISATIES

Luiijf & Kernkamp (2015) hebben good practices voor cybersecurityinformatie-uitwisseling opgesteld. Voor een compleet overzicht verwijzen we naar het document zelf[9]. Hieronder beschrijven we een aantal good practices die specifiek relevant zijn voor informatie-uitwisseling tussen ketenorganisaties.

'Speculate to accumulate': Informatie-uitwisseling werkt alleen wanneer meerdere organisaties bereid zijn om informatie te delen. Organisaties die beginnen met informatie-uitwisseling moeten er dus op vertrouwen dat ze ook iets terug zullen krijgen. Deze drempel zal moeten worden overwonnen voordat informatie-uitwisseling in een keten succesvol kan worden.

'Embed at the top': Informatie-uitwisseling kan alleen succesvol plaatsvinden wanneer er steun voor is bij de top van de deelnemende organisaties. Om deze steun te krijgen moet duidelijk zijn wat de meerwaarde van informatie-uitwisseling is. Voor ketenorganisaties moet duidelijk wat de toegevoegde waarde van informatie-deling is voor individuele ketenorganisaties en de keten als geheel.

'Noblesse Oblige: No Free Ride': Informatie-uitwisseling werkt alleen wanneer het tweerichtingsverkeer is. Wanneer informatie-uitwisseling binnen een keten wordt ontwikkeld is het verstandig op voorhand af te spreken dat organisaties die geen informatie inbrengen geen onderdeel van het initiatief kunnen zijn of blijven.

'Scoping is Key to Success': Het succes van informatie-uitwisseling wordt onder andere bepaald door de juiste 'scope'. Het moet duidelijk zijn welke informatie wordt uitgewisseld tussen wie en wat de meerwaarde daarvan is. Binnen ketens zal moeten worden bepaald welke informatie specifiek relevant is om binnen een keten te delen en welke informatie wellicht breder binnen de sector of zelfs daarbuiten moet worden gedeeld.

Ketenoefeningen
Ketenweerbaarheid is een complex onderwerp. Het is bij deelnemende organisaties doorgaans niet direct duidelijk wat ketenkwetsbaarheid, ketendreigingen en ketenmaatregelen zijn. Een ketenoefening helpt om ketenweerbaarheid concreet te maken. Door het ontwikkelen en uitvoeren van een ketenoefening wordt veel geleerd over de keten zelf, mogelijke kwetsbaarheden en de noodzaak (of het gebrek daarvan) voor het nemen van ketenmaatregelen.

GOOD PRACTICE 3.
ORGANISEER (RED-TEAM/BLUE-TEAM) KETENOEFENINGEN
Een manier om snel en concreet met ketenweerbaarheid aan de slag te gaan is het organiseren van oefeningen met ketenpartners. Een uitdagende vorm is de 'red-team/blue-team oefening'. Het idee van een red-team/blue-team ketenoefening is eenvoudig; één team valt een keten aan, het andere team verdedigt de keten.

TNO heeft recent een red-team/blue-team oefening georganiseerd voor de industriewatersector.
Ter voorbereiding werden drie bestaande waterzuiveringsketens in kaart gebracht. De systeembeschrijvingen van zowel de zuiveringsketen als de relevante ICT-systemen en de aanwezige beschermingsmaatregelen vormden de basis (de spelborden) van de oefening. Tijdens de oefening werden drie bestaande waterzuiveringsketens fictief aangevallen en verdedigd.
De aanvallende teams kropen om beurten in de huid van beroepscriminelen, een hackergroep of een ontevreden medewerker. De verdedigende teams kregen enkel een hint over het soort actor dat een aanval voorbereidde. Vervolgens werden opeenvolgend aanvals- en verdedigingsstappen uitgevoerd, steeds gevolgd door een discussie over de kans van slagen van de opgevoerde aanvallen en verdedigingen in de praktijk. Tijdens de evaluatie van de oefening gaven de deelnemende partijen aan dat deze vorm van oefenen zeer waardevol is. Ondanks dat de ketenpartijen in dit geval al goed bekend met elkaar waren, hielp de oefening om informatie over kwetsbaarheden en risico's te delen. Daarnaast werden medewerkers uit de informatiebeveiliging, procesautomatisering en bedrijfsvoering samengebracht – zowel vanuit de keten als intern bij de deelnemende organisaties – die doorgaans weinig samenwerken.

Vooral het kunnen combineren van cyber en fysieke dreigingen levert nieuwe inzichten en wederzijds begrip op. Dit leidt onder andere tot een toename van wederzijds begrip en vertrouwen, een beter beeld en voorbeelden van ketenkwetsbaarheden en een vervolginitiatief voor een ketenrisicoanalyse voor een keten waarvoor de oefening zorgpunten aan het licht heeft gebracht.

9 http://publications.tno.nl/publication/34616508/oLyfG9/luiijf-2015-sharing.pdf

Ketenrisicoanalyse
Een risico-gebaseerde aanpak is noodzakelijk om schaarse middelen efficiënt en effectief in te zetten voor het vergroten van ketenweerbaarheid. Hoewel het een aanzienlijke gezamenlijke inspanning kan zijn, vormt een ketenrisicoanalyse een noodzakelijk onderdeel van ketenweerbaarheid.

GOOD PRACTICE 4.
VOER EEN KETENRISICOANALYSE UIT
Ketenrisicoanalyses ten aanzien van cyberdreigingen zijn al uitgevoerd. Zo hebben vijf Nederlandse olie-, gas- en elektriciteitsbedrijven[10] in Nederland gezamenlijk een risicoanalyse uitgevoerd. Medewerkers van de deelnemende bedrijven zijn meerdere malen bij elkaar gekomen om gezamenlijk de keten in kaart te brengen en kwetsbaarheden te identificeren.
In samenwerking zijn cyberkwetsbaarheden geïdentificeerd die mogelijk misbruikt kunnen worden. Op basis van de uitkomsten van de ketenrisicoanalyse hebben ketenorganisaties op individuele basis mitigerende maatregelen uitgevoerd.

De risicoassesment en -beoordelingsmethode die is gebruikt, is vervolgens beschikbaar gemaakt in een handleiding[11]. In het algemeen biedt de gevolgde methode een geoperationaliseerd stappenplan dat uitgaat van kwantificeerbare risico's. Daarmee biedt het een leidraad voor risicoanalyses in andere ketens.

Ketenrisicobeheersing
Het vergroten van ketenweerbaarheid vergt niet alleen inzicht in ketenrisico's maar ook het treffen van mitigerende maatregelen. Dit kan aan de individuele ketenorganisaties worden gelaten of worden vastgelegd in een gezamenlijk plan. Een gezamenlijk plan of roadmap is nodig om er zeker van te zijn dat de juiste maatregelen ook daadwerkelijk en tijdig worden genomen.

GOOD PRACTICE 5.
STEL EEN GEZAMENLIJKE ROADMAP OP MET ACTIES VOOR HET VERGROTEN VAN KETENWEERBAARHEID
Een aantal organisaties op luchthaven Schiphol heeft gezamenlijk een risicoanalyse van cyberdreigingen voor de keten van vlucht- en vliegtuigafhandeling gemaakt. De deelnemende organisaties zijn verschillenden keren bij elkaar gekomen om ketenrisico's te identificeren. Op basis van de geïdentificeerde risico's zijn maatregelen benoemd die de individuele organisaties nemen om de weerbaarheid van de keten te vergroten.
De maatregelen zijn vastgelegd in een actieplan of roadmap. Na de afronding van de risicoanalyse zijn de betrokken organisaties herhaaldelijk bij elkaar gekomen om de voortgang van de uitvoering van de maatregelen in de roadmap te bespreken. Het bestaan van de roadmap zorgt voor een gestructureerde en gecontroleerde opvolging van de ketenrisicoanalyse.

STAPPENPLAN VOOR HET ONTWIKKELEN VAN CYBER-KETENWEERBAARHEID
Ketensamenwerking is niet eenvoudig en veel organisaties worstelen met de vraag hoe een concreet begin kan worden gemaakt met het vergroten van cyber-ketenweerbaarheid. Dit whitepaper biedt een aanpak in acht stappen. Welke stap als eerst kan worden gezet, hangt af van de reeds bestaande mate van samenwerking op het gebied van cybersecurity binnen een keten. Organisaties die al actief zijn op het gebied van cyber-ketenweerbaarheid kunnen enkele van de eerste stappen naar eigen inzicht overslaan. Daarnaast hoeven stappen niet alle stappen in deze volgorde worden gezet. Zo kan cybersecurity informatie-uitwisseling ook worden geïnitieerd nadat een ketenrisicoanalyse is uitgevoerd. De acht stappen zijn weergegeven in figuur 3 op de volgende pagina.

10 Koninklijke Nederlandse Shell, Nederlandse Gasunie, Nuon, TenneT, Alliander
11 Voster & de Bruijn (2016).

Figuur 3 – Stappen voor het ontwikkelen van cyber-ketenweerbaarheid

De verticale as geeft de mate van samenwerking die nodig is voor realisatie van de samenwerkingsvorm weer (zie Cyber-ketenweerbaarheid en de good practices). De horizontale as geeft de tijd aan en laat zien wat een logische volgordelijkheid is voor het ontwikkelen van ketensamenwerking.

1. Breng ketenorganisaties bij elkaar
Ketensamenwerking komt niet zomaar tot stand. De meerwaarde van samenwerking moet duidelijk zijn en er moet steun zijn vanuit de leiding van de betrokken organisaties. Ook wanneer nog niet (voor alle ketenpartners) aan deze begincondities voor samenwerking wordt voldaan, kunnen ketenorganisaties onderling in gesprek gaan over ketenweerbaarheid. Dit kan bijvoorbeeld vanuit bestaande samenwerkingsverbanden of door een ad hoc initiatief van een sectororganisatie worden gestart. Wanneer enkele ketenorganisaties succesvol samenwerken vergroot dat de kans dat andere organisaties aansluiten en uiteindelijk een samenwerking in de gehele keten ontstaat.

2. Voer een dialoog over de scope van de keten en het basisniveau van cybersecurity
In het eerste deel van dit whitepaper (zie ‘Soorten ketens’) staan we stil bij de complexiteit van ketens en de mogelijke verwevenheid tussen toeleveringsketens en informatieketens. Vanaf het begin van ketensamenwerking is het belangrijk een dialoog te voeren over de scope van de keten. Wat is de keten precies en welke organisaties maken deel uit van de keten? Wanneer overeenstemming bestaat over de scope van een keten, kan met de betreffende ketenorganisaties worden gesproken over het basisniveau van cybersecurity. De good practice en lijst met thema’s in dit whitepaper biedt handvatten voor een dialoog tussen ketenorganisaties.

3. Zorg voor commitment bij ketenorganisaties voor (de eerste stappen van) samenwerking
Ketensamenwerking kan verschillende vormen aannemen. Onderstaand figuur 3 geeft een overzicht van samenwerking ten aanzien van cyber-ketenweerbaarheid. Om commitment voor samenwerking te krijgen is het nodig te bepalen wat de huidige situatie in de keten is en expliciet te maken wat de toegevoegde waarde is van de verschillende samenwerkingsvormen. Een vuistregel daarbij is dat het geen zin heeft meer intensieve samenwerkingsvormen op te zoeken als meer eenvoudige samenwerking nog niet bestaat.

4. Organiseer een ketenoefening
Om samenwerking te starten en richting te geven aan verdere samenwerking kan een ketenoefening worden georganiseerd. De ketenoefening die is beschreven in de good practices biedt hiervoor een handvat. Door een ketenoefening raken ketenorganisaties beter met elkaar bekend en groeit het vertrouwen. Daarnaast kunnen de voorbeelden van kwetsbaarheden die in een oefening naar voren komen het commitment voor ketensamenwerking versterken. Deze voorbeelden kunnen ook als aandachtpunten voor verdere samenwerking dienen.

5. Begin met informatie-uitwisseling tussen ketenorganisaties (eventueel in aansluiting op bestaande informatie-uitwisseling)
Deze stap en de vorige kunnen ook in omgekeerde volgorde worden gezet. Informatie-uitwisseling kan parallel aan een ketenoefening worden geïnitieerd. De good practice informatie-uitwisseling en de publicatie van Luijf en Kernkamp (2015) bieden praktische handvatten voor de ontwikkeling van cybersecurityinformatie-uitwisseling binnen een keten.

6. Voer een ketenrisicoanalyse uit
Een ketenrisicoanalye vormt een noodzakelijke stap voor het efficiënt en effectief vergroten van ketenweerbaarheid. De cybersecurity supply chain risicoanalyse methode die is uitgebracht door de Cyber Security Raad en is beschreven in de good practices biedt hiervoor een praktisch handvat.

7. Stel een roadmap op met uit te voeren maatregelen voor het vergroten van cyber-ketenweerbaarheid en het regelmatige herhaling van de ketenrisicoanalyse.
Een roadmap met maatregelen voor het vergroten van ketenweerbaarheid omschrijft in ieder geval welke

maatregelen door welke organisatie op welke termijn worden getroffen. Daarnaast kan in de roadmap worden afgesproken op welke termijn of onder welke omstandigheden een nieuwe ketenrisicoanalyse wordt uitgevoerd.

8. Monitor cyber-ketenweerbaarheid
Nadat cyber-ketenweerbaarheid op basis van een ketenrisicoanalyse en met behulp van een roadmap is georganiseerd, blijft het belangrijk de cyber-ketenweerbaarheid van een keten te monitoren. Dit kan bijvoorbeeld door regelmatige herbeoordelingen of audits van de hele keten, ketenorganisaties of specifieke systemen. Penetratie testen en ketenoefeningen zorgen ook voor een beeld van de weerbaarheid van een keten.

LITERATUUR

Referenties

Computer Emergency Response Team United Kingdom (2015), Cyber-security risks in the supply chain, beschikbaar via https://www.ncsc.gov.uk/guidance/cyber-security-risks-supply-chain.

Duivenboden, H.P.M. van, M. van Twist, M. Veldhuizen en R. in 't Veld (2000), Ketenmanagement in de publieke sector, Lemma, Utrecht.

Ghosh, A., & Fedorowicz, J. (2008). The role of trust in supply chain governance. Business Process Management Journal, 14(4), 453-470.

Grijpink, J. H. A. M., & Plomp, M. G. A. (2009). Kijk op ketens: Het ketenlandschap van Nederland. Grijpink, Den Haag.

Luiijf, E., & Klaver, M. SYMPOSIUM ON CRITICAL INFRASTRUCTURES: RISK, RESPONSIBILITY AND LIABILITY. Governing Critical ICT: Elements that Require Attention, European Journal of Risk Regulation, Vol. 6, Issue 2 (2015). pp. 263 – 270.

Mentzer, J. T., DeWitt, W., Keebler, J. S., Min, S., Nix, N. W., Smith, C. D., & Zacharia, Z. G. (2001). Defining supply chain management. Journal of Business logistics, 22(2), 1-25

Nationaal Cybersecurity Centrum (2015), Zicht op risico's van legacysystemen: Een self-assessmentmethode om de risico's van (vitale) legacysystemen in kaart te brengen, Beschikbaar via https://www.ncsc.nl/actueel/whitepapers/zicht-op-risicos-van-legacysystemen.html.

Nationaal Cybersecurity Centrum (2016), Cybersecuritybeeld Nederland 2016, beschikbaar via https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2016.html.

Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: development of a conceptual framework. Journal of business logistics, 31(1), 1-21.
Voster, W., de Bruijn, J. (2016), Cyber security supply chain risicoanalyse 2015, beschikbaar via https://www.cybersecurityraad.nl/binaries/Brochure%20Cyber%20Security_NL_WEB_tcm56-79499.PDF.

Verder lezen

Joosten, R., Smulders, A. (2013), Advanced Risk Management: Succesvol risico's beheersen bij toenemende complexiteit en dynamiek. Beschikbaar via publications.tno.nl/publication /34608610/90qVeW/joosten-2013-advanced.pdf.

Luiijf, H.A.M., Kernkamp, A. (2015), Sharing Cyber Security Information: Good Practice Stemming from the Dutch Public-Private-Participation Approach, beschikbaar via https://www.gccs2015.com/nl/node/373.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001), Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE Control Systems, 21(6), pp.11-25.

Van Erp, J. (2016), New Governance of corporate cybersecurity: A case study of the petrochemical industry in the port of Rotterdam, Crime, Law and Social Change, nog te verschijnen, beschikbaar via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2807027.

Verhagen, H. (2016), De economische en maatschappelijke noodzaak van meer cybersecurity: Nederland digitaal droge voeten. Beschikbaar via https://www.cybersecurityraad.nl/binaries/CybersecurityAdviesHernaVerhagen_tcm56-122110.pdf.

COLOFON:

Auteurs
Theo van Ruijven
Bas Keijser

TNO
Lange Kleiweg 137
2288 GJ Rijswijk
tno.nl/cybersecurity

TNO CONNECTS PEOPLE AND KNOWLEDGE TO CREATE INNOVATIONS THAT SUSTAINABLY BOOST THE COMPETITIVE STRENGTH OF INDUSTRY AND WELL-BEING OF SOCIETY.

TNO.NL/cybersecurity
WE MAKE CYBER WORK FOR YOU