Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Start een ketensamenwerking

Handreiking

Stappenplan ketensamenwerking

Om aan de slag te gaan met het versterken van de digitale ketenweerbaarheid, heeft het NCSC in samenwerking met zijn partners een handreiking opgesteld. Hierin worden drie fases gepresenteerd om te komen tot een succesvolle ketensamenwerking.

Fase 1: **Verkennen**

Eerst overzicht, dan inzicht:

- Breng ketenorganisaties bij elkaar en ga op zoek naar de meerwaarde van een potentiële samenwerking.
- Voer in de verkennende fase een dialoog over de scope van de samenwerking.
- Zorg voor draagvlak en steun door op strategisch niveau ketenweerbaarheid op de agenda te zetten.

Fase 2: **Concretiseren**

Analyse en informatie-uitwisseling:

- Organiseer een verdiepende dialoog over vraagstukken in jouw keten.
- Stimuleer informatie-uitwisseling om het dreigingsbeeld in kaart te brengen en versnippering van informatie tegen te gaan.
- Organiseer oefeningen om dreigingen en bestaande weerbaarheden in de keten concreet te maken.

Fase 3: **Implementeren**

Ontwikkelen, implementeren en monitoren:

- Voer een uitgebreide risicoanalyse uit om schaarse middelen efficiënt en effectief in te zetten.
- Stel een gezamenlijke roadmap op met maatregelen voor het vergroten van ketenweerbaarheid en risicobeheersing.
- Monitor de digitale weerbaarheid van de keten door middel van herbeoordelingen, penetratietesten en ketenoefeningen.

Start een ketensamenwerking

Alle organisaties hebben in meer of mindere mate te maken met digitale dreigingen. Steeds meer organisaties zijn actief bezig hun digitale weerbaarheid te verhogen. Wordt er in ketens samengewerkt door verschillende organisaties, dan volstaat het niet als een organisatie in de keten alleen voor zichzelf risico's inschat. De organisaties in een keten zijn afhankelijk van elkaars inspanningen om risico's tot een acceptabel niveau terug te brengen. Daarvoor moeten gezamenlijke maatregelen worden genomen die voor de hele keten geschikt zijn.

In deze handreiking vind je richtlijnen om een succesvolle ketensamenwerking te realiseren en deze vast te houden. Met het stappenplan kun je aan de slag om de digitale weerbaarheid van de hele keten te versterken.

Doelgroep

Deze handreiking is bedoeld voor informatiemanagers, information security specialisten, logistieke specialisten voor een leveranciersketen en inkopers die de (contractuele) samenwerking met toeleveranciers initiëren en beheren.

Aan deze handreiking hebben bijgedragen

Alliander, Gasunie, Havenbedrijf Amsterdam, Koninklijke Luchtvaart Maatschappij (KLM), Luchtverkeersleiding Nederland (LVNL), Nuon, Portbase, Royal Schiphol Group, Tennet en Waterbedrijf Groningen.

Deze handreiking is tot stand gekomen door samenwerking tussen

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

Wat is een keten?

Veel producten en diensten komen in ketens tot stand. Organisaties in een keten maken deel uit van een stroom producten, diensten, geld en informatie, waar de organisaties individueel een deel van de stroom voor hun rekening nemen.[1] Ketens worden gekenmerkt door:[2]

- Autonome organisaties met belangen die soms tegenstrijdig of conflicterend kunnen zijn met het belang van de ketenorganisaties tezamen.
- Een dominant ketenprobleem, dus een probleem dat organisaties in een keten verbindt en dat geen van de organisaties alleen kan oplossen.
- Zowel 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.
- Een bepaalde mate van complexiteit afhankelijk van het aantal ketenorganisaties en de manier waarop producten, diensten, geld of informatie wordt uitgewisseld.[3]

Door integratie van bedrijfsprocessen en informatiesystemen is een transparant overzicht van een keten steeds moeilijker te geven. Organisaties zijn vaak onderdeel van meerdere ketens. Dit brengt verschillende ketenkwetsbaarheden met zich mee. In een zogenoemde digitale keten komen er dan ook andere uitdagingen voor de keten van organisaties bij.

Wat zijn de uitdagingen voor organisaties in digitale ketens?

Zwakke schakels

Veel ketens raken verstoord bij uitval van één schakel. Denk 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. Dan bepalen de zwakke schakels de betrouwbaarheid en weerbaarheid van de keten als geheel.

Spreiding van informatie

In een digitale keten is de spreiding van informatie ondoorzichtig wanneer geen van de organisaties over een totaalbeeld beschikt. Een voorbeeld hiervan zijn (digitale) inbraken in een organisatie in een grote haven om informatie over containers te achterhalen. Pas wanneer de beschikbare informatie bij elkaar wordt gebracht, kan een patroon zichtbaar worden dat criminelen systematisch inbraken hebben gepleegd bij meerdere organisatie in de keten.

Negatieve externe effecten

De kwetsbaarheden die voor de ene ketenorganisatie niet evident zijn, kunnen voor de andere een aanzienlijk risico vormen. Hetzelfde geldt voor maatregelen om een ketenorganisatie weerbaarder te maken. Die kunnen in sommige gevallen beter door een andere ketenorganisatie worden genomen.

Daarnaast zijn er specifieke kwetsbaarheden die de beschikbaarheid, integriteit en vertrouwelijkheid van de ICT-voorzieningen in een keten in gevaar kunnen brengen. Dit geldt bijvoorbeeld voor:

Interfaces

Interfaces zijn potentieel kwetsbaar omdat ze per definitie in verbinding staan met de buitenwereld en de infrastructuur vormen waarover ketenorganisaties informatie uitwisselen. Een interface is vaak niet meer dan een programma waarmee informatie uit een systeem van de ene organisatie in de keten wordt verstuurd naar een systeem van een andere ketenorganisatie. Vaak zijn meerdere organisaties betrokken bij beheer en de bescherming van interfaces, waardoor de kans op onduidelijkheden en misverstanden groter wordt.

Keteninformatiesystemen

Informatiesystemen in de keten zijn specifiek ontworpen om meerdere of zelfs alle geschakelde organisaties van informatie te voorzien. Deze systemen vormen een aantrekkelijk doelwit voor cybercriminelen, omdat ze vaak veel data en belangrijke informatie bevatten. Aantasting en uitval van keteninformatiesystemen hebben vaak een grote impact op het functioneren van de hele keten vanwege die afhankelijkheid bij meerdere organisaties.

Gezamenlijke ICT-diensten

Het digitale domein kent veel diensten die gezamenlijk afgenomen kunnen worden en waarbij de onderlinge afhankelijkheid niet altijd duidelijk is. Door gezamenlijk gebruik van ICT-diensten kan een keten kwetsbaar zijn. Waar een individuele organisatie de uitval van een dienst zelfstandig kan opvangen door noodvoorzieningen, is dit voor meerdere of alle organisaties in een keten niet haalbaar. Vaak is onduidelijk bij wie de verantwoordelijkheid voor afspraken voor een deel van de ICT-dienstverlening liggen. Dit geldt voor ICT-voorzieningen zoals dataopslag- en clouddiensten, ICT-leveranciers, vaste en mobiele communicatienetwerken en kantoorautomatisering.

1 Mentzer et al. (2001) *Defining supply chain management.*

2 Grijpink, J.H.A.M., (2016, 3de druk). *Keteninformatisering in kort bestek.*

3 Voor een verdere verdieping zie https://www.tno.nl/nl/aandachtsgebieden/defensie-veiligheid/roadmaps/nationale-veiligheid/whitepaper-ketenweerbaarheid-tegen-cyberdreigingen.

"Als aanbieder van een keteninformatiesysteem voor organisaties in de logistieke keten in de Rotterdamse haven zien we dat ook de informele kant van de keten zeer belangrijk is. Dus dat je weet wie waar zit en waar van is zodat je die persoon in geval van nood makkelijk kan bereiken en snel kan schakelen met mensen die je (goed) kent."

Portbase

Hoe versterk je jouw digitale weerbaarheid door ketensamenwerking?

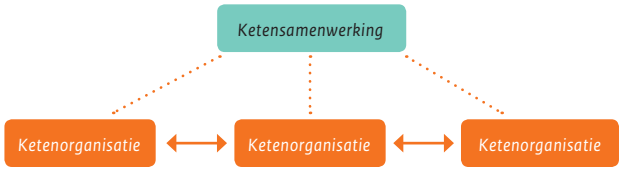
Digitale ketenweerbaarheid is het vermogen van ketens om zich te beschermen tegen cyberdreigingen, te herstellen van incidenten en mee te kunnen bewegen met de veranderingen in het dreigingslandschap. Er is van digitale ketenweerbaarheid sprake op het niveau van individuele organisaties en op ketenniveau.

Ketenorganisaties moeten voldoende beschermd zijn op ketenniveau, omdat de digitale weerbaarheid van de hele keten daarvan afhankelijk is. Op ketenniveau is het daarom van belang dat inzicht bestaat in kwetsbaarheden en risico's van de keten als geheel. Afspraken daarover moeten over de keten heen worden gemaakt.

Afhankelijk van de organisatiegraad van de keten en de behoeften van ketenpartijen kan afstemming alleen al genoeg zijn om de uitdagingen het hoofd te bieden. Wanneer het ketenprobleem zo complex is dat ketenafstemming geen acceptabele oplossing meer biedt voor het gezamenlijke probleem, kan ketensamenwerking uitkomst bieden.

Ketensamenwerking kan variëren van ad hoc initiatieven wanneer medewerkers van organisaties zich realiseren hoe afhankelijk ze zijn van andere organisaties in de keten tot geformaliseerde vormen van coördinatie en zelfs strategische samenwerking.

Figuur 1 **Twee niveaus voor versterking van de digitale ketenweerbaarheid**



Sectorale, regionale, nationale en internationale afstemming.

Wanneer er sprake is van sterke ketenafhankelijkheid is samenwerking noodzakelijk. Hoe kan ketensamenwerking eruit zien?

Informatie-uitwisseling

Informatie-uitwisseling is nodig om versnippering van informatie tegen te gaan. Dreigingsinformatie in het digitale domein is doorgaans complex en alleen door het delen van informatie kan een compleet dreigingsbeeld voor de hele keten worden ontwikkeld.

Analyseren van cyberrisico's

Een goede analyse van cyberrisico's is vooral belangrijk voor keteninformatiesystemen en gezamenlijke afname van ICT-diensten. Analyse van risico's op ongeautoriseerde toegang is zeker nodig wanneer het aantal aangesloten organisaties groot is. Ook data integriteit, beschikbaarheid van data en controleerbaarheid ervan moeten worden meegenomen. Pas wanneer de gehele keten aan gezamenlijke diensten op risico's zijn geanalyseerd, worden kwetsbaarheden zichtbaar.

Gezamenlijk treffen van maatregelen

Wanneer er sprake is van negatieve (externe) effecten door uitval van systemen, moeten er maatregelen getroffen worden in overleg met de hele keten. De ketenweerbaarheid moet worden gewaarborgd, daarvoor is afstemming over wie welke maatregelen neemt en hoe de kosten worden verdeeld cruciaal. Dit laatste is zeker het geval wanneer de kosten van maatregelen door andere partijen moeten worden gedragen dan de partij die het risico draagt.

Geen keten is hetzelfde[4], daarom zullen de richtlijnen en adviezen in deze handreiking vertaald moeten worden naar de specifieke kenmerken van jouw keten. Er is een grote verscheidenheid aan soorten ketens en complexiteit tussen de geschakelde organisaties. Maak zelf de afweging welke volgorde en handvatten nodig zijn voor jouw keten.

"Bij een recent door ons georganiseerde 'table top' met vele publieke en private partijen bleek dat een ieder voor zich wel weet wat hij of zij zou moeten doen in het geval van een cyberincident. Maar dat alleen door samenwerking de domino effecten kunnen worden verminderd van een cyberincident binnen de keten. Samen zijn we immers veel sterker dan ieder afzonderlijk. Vertrouwen, draagvlak en het bundelen en uitwisselen van kennis op het gebied van cybersecurity vanuit private en publieke partijen is daarbij essentieel. Wij zijn daar volop mee bezig."

Havenbedrijf Amsterdam

4 Zie https://www.tno.nl/nl/aandachtsgebieden/defensie-veiligheid/roadmaps/nationale-veiligheid/whitepaper-ketenweerbaarheid-tegen-cyberdreigingen voor een uitgebreider overzicht van verschillende soorten ketens.

Fase 1: Verkennen

Eerst overzicht, dan inzicht

Wil je samen met anderen een ketentraject opzetten om je digitale weerbaarheid te vergroten? Zorg dan dat je eerst een goed overzicht krijgt van het hele speelveld. In een keten zijn meerdere organisaties betrokken met deels dezelfde en deels verschillende belangen. Het is daarom zaak om te starten met het verkrijgen van een overzicht van het speelveld, het draagvlak en mogelijke gevoeligheden.

Breng ketenorganisaties bij elkaar

Ketensamenwerking komt niet zomaar tot stand. Je kunt de eerste stap zetten vanuit je eigen organisatiebelang of meteen gezamenlijk met informatiebeveiligers van ketenpartners in gesprek gaan. Zo kun je in kaart brengen welke mogelijkheden er zijn om de weerbaarheid van de keten te verhogen.

Maak gebruik van een momentum om collega's aan tafel te krijgen. Bijvoorbeeld een cybersecurityincident dat de kwetsbaarheid van een keten heeft blootgelegd, enthousiasme bij een of meerdere ketenorganisaties of sturing vanuit de bestuurskamer van je organisatie, sector of brancheorganisaties. Of creëer het momentum zelf. Misschien biedt een bestaand samenwerkingsverband tussen ketenpartners dat zich op (fysieke) veiligheid richt een aanknopingspunt.

Organiseer bijvoorbeeld van een 'table-top-oefening' waarvoor je organisaties uitnodigt met een bepaald belang bij het verhogen van de weerbaarheid van de ketenpartners. Ga vooral samen op zoek naar wat de meerwaarde van ketensamenwerking voor de individuele organisaties en de keten als geheel kan zijn. Een vuistregel daarbij is dat je vooral eenvoudig en laagdrempelig moet beginnen als er nog geen samenwerking bestaat.

Voer een dialoog over de scope en het basisniveau

Al in de verkennende gesprekken en het prille begin van de ketensamenwerking moet met elkaar overeenstemming ontstaan over de scope van de keten en de samenwerking. Je kunt de volgende vragen stellen om meer inzicht te krijgen in de rol van de andere organisaties in de keten, de onderlinge afhankelijkheden en ook het effect van deze afhankelijkheden op je eigen organisatie:

Ketens:
- Waar bevindt jouw organisatie zich in de keten?
- Ben je een leverancier, afnemer of beide?
- Is jouw organisatie onderdeel van een toeleveringsketen (waar producten, diensten of geld wordt uitgewisseld tussen ketenorganisaties) of van een informatieketen (waar informatie wordt uitgewisseld om bedrijfsprocessen die onderdeel uitmaken van een toeleveringsketen aan te sturen of te controleren)?
- Wat is het dominante probleem in jullie keten? Bijvoorbeeld een probleem of knelpunt dat de organisaties in de keten verbindt en dat geen van de organisaties op eigen kracht kan oplossen.[5]
- Hoe complex is de keten waar jullie onderdeel van zijn?

Digitale kwetsbaarheden:
- Welke digitale kwetsbaarheden zijn relevant voor jullie keten?
- Hoe hebben de individuele ketenorganisaties hun digitale weerbaarheid georganiseerd? Zijn er al maatregelen genomen om ketenrisico's te beperken (elementaire bescherming, incident response, informatiebeveiligingsmanagementsysteem)?
- Wisselen organisaties binnen de keten (geautomatiseerde) informatie uit? Zo ja, op welke manier? Zo nee, waarom niet en wat is er nodig om dit wel te gaan doen?
- Maakt de keten gebruik van een keteninformatiesysteem?
- Maken organisaties binnen jullie keten gebruik van dezelfde ICT-producten en diensten?

Vormen van overleg:
- Is er sprake van onderlinge afstemming tussen ketenorganisaties? Zo niet, zou je daar behoefte aan hebben en in welke vorm?
- Is er al sprake van bestaande ketensamenwerking, bijvoorbeeld vanuit het fysieke domein?

Digitale ketenweerbaarheid:
- Zijn er standaarden of andere normen gesteld waarmee een basisniveau van cybersecurity wordt gewaarborgd voor organisaties binnen de keten?[6]
- Zijn er binnen de keten afspraken gemaakt tussen ketenorganisaties over cybersecurity en is er al sprake van afstemming?
- Wisselen organisaties binnen deze keten informatie uit over digitale dreigingen met een deel van de keten of met organisaties uit andere ketens?

Door deze vragen te beantwoorden is een ketenpartner voorbereid op het tot stand brengen van de basis voor weerbaarheid in de keten. Iedere organisatie in de keten is uniek en moet voor zichzelf bepalen hoe deelname aan de keten het meest wenselijk is. Tijdens de bijeenkomsten kunnen de ketenpartners dit samenbrengen en vertalen naar kansen en uitdagingen voor de keten als geheel.

De antwoorden op de vragen en de eerste schets van de keten geven een goede basis voor vervolgstappen. Door het overzicht van de situatie bij alle ketenorganisaties in een eerste schets komen er details die nadere invulling behoeven naar voren. Zodra samenwerking met andere ketenorganisaties op gang komt, zal het overzicht zich stap voor stap uitbreiden en steeds volledieger worden.

5 Grijpink, J.H.A.M., (2016). *Keteninformatisering in kort bestek*.

6 Voorbeelden zijn CobiT, PAS 555, IEC62443 of ISO27000 serie, NIST 800-82 voor ICS security en overige relevante NIST normen.

Zorg voor draagvlak op strategisch niveau

Starten met een samenwerking maar vooral het in stand houden gaat niet vanzelf. Om de ketensamenwerking toekomstbestendig te maken, moet het onderwerp op strategisch niveau een blijvende plek krijgen. Dat betekent dat bij iedere organisatie in de keten iemand op dát niveau het onderwerp ketenweerbaarheid op de agenda houdt. Want je wilt dat de personen in een organisatie vrijelijk en in vertrouwen informatie met elkaar kunnen delen. Vanuit de organisatie kan dan mandaat worden gegeven om die informatie ook in de keten te delen.

Een quick-scan van de risico's bij de start van het initiatief kan helpen om dat draagvlak te creëren. De in kaart gebrachte risico's moeten met gebruik van dezelfde bedrijfseconomische begrippen gedeeld worden met het management. Dan kunnen de risico's volgens dezelfde criteria worden beschouwd als andere risico's en investeringsbesluiten.

Organisaties hebben bedrijfsdoelstellingen van uiteenlopende aard. Dat zijn financiële maar ook bijvoorbeeld veiligheidsdoelstellingen of andere bedrijfsdoelstellingen. Beslissers nemen besluiten afgezet tegen alle bedrijfsdoelstellingen. De besliscriteria moeten daarom voor alle betrokkenen in een bedrijf duidelijk zijn. Ieder bedrijf hanteert zijn eigen methodes. Besliscriteria voor het afwegen van risico's voor een organisatie in een keten hebben invloed op die van een andere ketenorganisatie.

Daarom moet je voor beslissers expliciet maken op welke wijze een risico de bedrijfsdoelstellingen of targets ondermijnt met mogelijke gevolgen voor andere organisaties in de keten. Om het onderwerp op het netvlies te houden, is het verstandig om met grote regelmaat de aanwezige risico's en ontwikkelingen in de keten aan het management te blijven rapporteren.[7]

"Voor het creëren van draagvlak voor een ketensamenwerking waren bij ons de volgende punten van belang: onze maatschappelijke verantwoordelijkheid en de kennis die we zelf zouden opdoen over de keten en de kwetsbaarheid ervan. Ik ben begonnen bij het management en toen die akkoord was, kon ik dit mandaat gebruiken bij het verkrijgen van deelnemers uit de verschillende delen van de organisatie. Voor deze mensen was met name het kennis aspect (weten hoe het nu eigenlijk echt zit) waardoor het interessant werd voor ze."

Nuon

"Naarmate de digitalisering van allerlei processen voortschrijdt, kunnen ze een aantrekkelijker doelwit worden. Om een passend antwoord te kunnen geven op deze bedreigingen hebben wij opdracht gegeven tot een inventarisatie van de risico's in het kader van cybercrime. Centraal hierbij stond de vraag 'Hoe geeft Port of Amsterdam invulling aan digitale weerbaarheid en veerkracht voor zowel het Havenbedrijf als de havengemeenschap'. Als resultaat van dit eindrapport is door de directie van het havenbedrijf opdracht gegeven tot uitvoeren van het programma cybersecurity en het aanwijzen van een programma-manager."

Havenbedrijf Amsterdam

Fase 2: Concretiseren

Ketenverkenning en vaststellen basisniveau

Na de startfase leidt de volgende stap naar gerichte acties en concretisering van de ketensamenwerking. Er is geen voorwaardelijke volgorde in handelingen. Zo kan informatie-uitwisseling ook worden geïnitieerd na een ketenrisicoanalyse. Het belangrijkste uitgangspunt is de behoefte van de ketenorganisaties om de samenwerking te intensiveren.

Verdieping van het basisniveau cybersecurity in de keten

Voer onderling uitvoerige gesprekken over het niveau waarop cybersecurity in de keten moet zijn ingericht. Wees open over motieven en wensen, ook over wat je komt halen en brengen. Maak (proces)afspraken over vertrouwelijkheid van de informatie die aan tafel gedeeld wordt. In de Handreiking sectorale samenwerking staan tips voor het creëren van de juiste randvoorwaarden voor vertrouwen en informatie-uitwisseling.[8]

Denk eraan om voor deze gesprekken niet alleen informatiespecialisten uit te nodigen. Ook collega's met zicht op de fysieke keten leveren een belangrijke bijdrage. Bespreek met elkaar vragen over hoe het werkt in de fysieke keten, wat kan daar misgaan en op welke manier. Vervolgens trek je de lijn door naar de systemen, interfaces, processen enzovoorts die een rol spelen voor de keten en hoe een digitale aanval het ketenproces zou kunnen verstoren.

Voor deze gesprekken met ketenpartners over een basisniveau voor cybersecurity zijn al veel handvatten beschikbaar. Denk bijvoorbeeld aan de ISO27000-serie. Wanneer er geen voor de hand liggend kader of standaard beschikbaar is, zijn onderstaande thema's geschikt. Deze zijn afgeleid van ISO27000 en van verschillende supplier-assurance-kaders.

7 Voor meer over het uitvoeren van keten risicoanalyses, zie pagina 9.

8 Zie www.ncsc.nl/samenwerking voor de handreiking sectorale samenwerking.

Ook wanneer er wel sprake is van een gedeelde standaard is het waardevol een dialoog met ketenpartners te voeren. Dan is de wijze waarop standaarden zijn ingevuld onderwerp van gesprek. 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 de afwegingen van ketenorganisaties zijn voor de keten als geheel.

Thema's:

Informatiebeveiligingsbeleid

- Beschikt de organisatie over een informatiebeveiligingsbeleid?
- Wordt van ieder IT-systeem een risicoanalyse uitgevoerd waarbij de afhankelijkheid en de kwetsbaarheid van het IT-systeem in brede zin wordt vastgesteld?
- Wordt er periodiek of na een grote wijziging een risicoanalyse van ieder IT-systeem uitgevoerd?
- Worden de uit de risicoanalyse resulterende maatregelen geïmplementeerd?
- Wordt de implementatie van de informatiebeveiligingsmaatregelen, voortkomend uit een risicoanalyse, periodiek ge-audit?
- Zijn de IT-systemen geaccrediteerd volgens een specifieke methodiek?
- Welke communicatiekanalen zijn ingericht bij een cybercalamiteit?

Information Security Management System (ISMS)

- Beschikken ketenorganisaties over een ISMS?
- Is het systeem gedocumenteerd?
- Zijn verantwoordelijkheden en functies voor informatiebeveiliging en cybersecurity belegd? Zo ja, op welke wijze is rapportage en verantwoording geregeld?

Assetmanagement

- Beschikken ketenorganisaties over een assetmanagementprogramma?[9]

Toegangsbeveiliging en autorisatie

- Beschikken ketenorganisaties over een gedocumenteerd systeem voor toegang en autorisatie (identiteit- en toegangsmanagement) voor locaties en ICT-systemen?
- Wordt dit structureel bijgehouden en gecontroleerd?

Softwarebeveiliging

- Beschikken ketenorganisaties bijvoorbeeld over gescheiden omgevingen voor kantoorautomatisering en procesautomatisering?
- Is patch- en kwetsbaarhedenmangement ingeregeld?
- Is software geïnstalleerd voor bescherming tegen malware en schadelijk inkomend internetverkeer?
- Op welke wijze wordt de betrouwbaarheid van de IT-diensten (onafhankelijk) getoetst?

Netwerkbeveiliging

- Beschikken ketenorganisaties over een gedocumenteerde en gesegmenteerde netwerkarchitectuur?
- Is duidelijk wie er betrokken is bij en bevoegd is voor instandhouding en uitbreiding van het netwerk?
- Is toegang tot netwerken georganiseerd en wordt toegang tot netwerken voor verschillende groepen gebruikers gescheiden?
- Wordt gevoelige informatie 'in transit en ruste' versleuteld?
- Zijn de interfases beveiligd?

Personeel

- Worden medewerkers periodiek gescreend?
- Hebben alle medewerkers een geheimhoudingsverklaring getekend?

Leveranciersrelaties

- Beschikken ketenorganisaties over een aanpak voor supplier assurance?
- Houden leveranciers en ontwikkelaars van software-, hardware- en netwerksystemen in de keten zich aan een vergelijkbaar informatiebeveiligingsbeleid?

Testen en incident response

- Beschikken ketenorganisaties over beleid voor onafhankelijke tests op naleving van informatieveiligheidsprocedures en de implementatie en uitvoering van technische beschermingsmaatregelen?
- Zijn (beleids)verantwoordelijken, meldplichten, maatregelen en procedures gedocumenteerd voor incidentafhandeling en worden deze regelmatig geoefend?

Stimuleer informatie-uitwisseling

Uitwisseling van informatie tussen ketenorganisaties leidt tot een algeheel dreigingsbeeld, kan versnippering van informatietegengaan en verhoogt de digitale weerbaarheid van je keten. Informatie-uitwisseling over cybersecurity-vraagstukken kun je voor een sector als geheel en voor een specifieke keten inrichten. De relatie tussen afnemer en leverancier en contracten over de diensten en producten maken informatie-uitwisseling in ketens doorgaans wel uitdagender. Het primaire doel voor informatie-uitwisseling moet het verhogen van de digitale ketenweerbaarheid van de deelnemende ketenorganisaties zijn. Partijen die samenwerken aan digitale weerbaarheid moeten elkaar kunnen vertrouwen. In dat vertrouwen is er geen plaats voor sentimenten over een concurrentiepositie of negatieve effecten van samenwerking.

9 Assetmanagement betekent dat belangrijke systemen, middelen en bedrijfsprocessen (schematisch) zijn vastgelegd. Overzicht van bedrijfsprocessen is belangrijk om in een later stadium een ketenrisicoanalyse te kunnen uitvoeren.

"In de meeste ketens wordt geconcurreerd op een bepaalde stap in het proces door meerdere aanbieders, maar waarschijnlijk niet in de ene proces stap met de volgende. Ondanks concurrentie zijn er genoeg opties om toch samen te werken. Wij hebben dit ondervangen door alleen naar het ketenproces te kijken en slechts één partij in elke stap van de keten te betrekken waardoor concurrentie geen belemmering vormt (in ons geval zijn dit verschillende marktrollen en één partij per marktrol)."

Nuon

Het vertrouwen tussen ketenorganisaties is gebouwd op afspraken over hoe de ketenpartners onderling omgaan met veiligheid en integriteit van gevoelige informatie. Om dit vertrouwen op te bouwen en te starten met het uitwisselen van informatie is het Information Sharing and Analysis Centre (ISAC) model zeer geschikt.[10] De kern van vertrouwen is:

- de tijd nemen elkaar te leren kennen;
- open en transparant zijn over wat je wel en niet kunt delen;
- actief zorgen voor draagvlak binnen je organisatie om bedrijfsgevoelige informatie te delen;
- actief de informatie binnen je eigen organisatie verzamelen.

Blijf ook altijd scherp op wat het gezamenlijke belang is, wat de doelen zijn van de informatie-uitwisseling en maak de toegevoegde waarde tastbaar, zowel intern als extern. Bereik ten slotte binnen je samenwerking een akkoord over de scope van informatie-uitwisseling. Ga het gesprek aan over welke informatie relevant is om in een ketensamenwerking te delen en welke informatie wellicht breder binnen de sector of daarbuiten moet worden gedeeld.

Organiseer ketenoefeningen

Een ketenoefening is een goede manier om dreigingen en bestaande weerbaarheden in de keten concreet te maken en stappen te zetten om een complex probleem beter te begrijpen. De uitkomsten kunnen ook helpen met het verder aanscherpen van de samenwerking en de toegevoegde waarde van samenwerking concreet te maken.

Door het ontwikkelen en uitvoeren van een ketenoefening leer je veel over de keten zelf en versterk je onderling vertrouwen en begrip. Ook worden mogelijke kwetsbaarheden en afhankelijkheden zichtbaar en wordt de noodzaak (of het gebrek daaraan) duidelijk om ketenmaatregelen te nemen. Verder kunnen de uitkomsten en geïdentificeerde kwetsbaarheden gebruikt worden om het draagvlak en de steun voor ketensamenwerking te versterken.

Een uitdagende vorm is de 'red-team/blue-team oefening'. Het idee hierachter is eenvoudig: één team valt een keten aan, het andere team verdedigt de keten. Ook kun je denken aan gezamenlijke bewustwordingscampagnes zoals phishing-simulaties of periodieke security-assessments.

"Wij hebben als industriewatersector samen met TNO een red-team / blue-team ketenoefening georganiseerd. Ter voorbereiding van deze oefening zijn drie bestaande waterzuiveringsketens in kaart gebracht die in de oefening fictief werden aangevallen en verdedigd. In verschillende rondes werden aanvals- en verdedigingsstappen uitgevoerd door roulerende teams, steeds gevolgd door discussie over de kans van slagen van de opgevoerde aanvallen en verdedigingen in de praktijk. De oefening hielp ons om de volgende stap te zetten in het delen van informatie over kwetsbaarheden en risico's!"

Waterbedrijf Groningen

Dergelijke oefeningen helpen om het onderlinge vertrouwen op te bouwen en elkaar en de onderlinge afhankelijkheden te leren kennen. Je hoeft niet meteen een grootschalige oefening te doen, een table-top-oefening met een scenario naspelen met andere ketenorganisaties brengt mensen ook al dichter bij elkaar.

Een ketencrisisoefening kan ook een manier zijn om medewerkers uit de informatiebeveiliging, procesautomatisering en bedrijfsvoering samen te brengen, die elkaar doorgaans weinig tegenkomen in de praktijk. Vooral combineren van digitale en fysieke dreigingen levert nieuwe inzichten en wederzijds begrip op. Ook biedt een ketenoefening handvatten voor een vervolginitiatief, bijvoorbeeld voor een ketenrisicoanalyse gebaseerd op de zorgpunten die aan het licht kwamen tijdens de oefening.

10 Zie www.ncsc.nl/samenwerking voor de handreiking sectorale samenwerking over het opzetten van een ISAC.

Fase 3: Implementeren

Ketensamenwerking ontwikkelen, uitvoeren en monitoren

In de volgende stap kunnen de ketenorganisaties daadwerkelijk de digitale weerbaarheid van de keten verhogen en borgen. De uitkomsten van de ketenoefening en de verdiepende dialoog over het basisniveau van cybersecurity komen daarbij goed van pas.

Voer een uitgebreide ketenrisicoanalyse uit

Een risico-gebaseerde aanpak is noodzakelijk om middelen efficiënt en effectief in te zetten voor het vergroten van ketenweerbaarheid. Daarvoor is een ketenrisicoanalyse een noodzakelijk onderdeel, ook al vormt het vaak een aanzienlijke inspanning van betrokkenen.

Tip: Maak gebruik van de proof of concept methodologie van een risico-analyse uitgevoerd door vijf bedrijven uit de Nederlandse energiesector.[11] *Medewerkers van deze bedrijven zijn meerdere malen bij elkaar gekomen om gezamenlijk de keten in kaart te brengen en kwetsbaarheden te identificeren. In samenwerking zijn digitale kwetsbaarheden in de keten geïdentificeerd die mogelijk misbruikt kunnen worden. Op basis van de uitkomsten van deze ketenrisicoanalyse hebben ketenorganisaties op individuele basis mitigerende maatregelen uitgevoerd.*

De methode uit het voorbeeld bevat een geoperationaliseerd stappenplan dat uitgaat van kwantificeerbare risico's. Daarmee biedt het een leidraad voor risicoanalyses in andere ketens.[12]

Stel gezamenlijk een roadmap op

Een roadmap met maatregelen om tot grotere ketenweerbaarheid en risicobeheersing te komen bevat in concrete bewoordingen welke maatregelen door welke organisatie op welke termijn worden genomen. Daarnaast kan in de roadmap worden vastgelegd hoe en wanneer een volgende ketenrisicoanalyse wordt uitgevoerd. Mitigerende maatregelen treffen kan aan de individuele ketenorganisaties worden overgelaten of worden vastgelegd in deze gezamenlijke roadmap. Het is belangrijk om dit vast te leggen om er zeker van te zijn dat de juiste maatregelen ook daadwerkelijk en tijdig worden genomen.

Monitor digitale ketenweerbaarheid

Als digitale 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 (her)beoordelingen of audits van de hele keten, ketenorganisaties of specifieke systemen binnen de keten. Penetratietesten en ketenoefeningen zorgen ook voor een beeld van de weerbaarheid van een keten.

"Royal Schiphol Group, KLM en Luchtverkeersleiding Nederland hebben het initiatief genomen om een risicoanalyse van cyberdreigingen voor de keten van vlucht- en vliegtuigafhandeling uit te voeren. De deelnemende organisaties hebben hun ketenrisico's geïdentificeerd. Op basis van de geïdentificeerde risico's zijn maatregelen benoemd die de individuele organisaties nemen om de digitale weerbaarheid in de keten te vergroten. Schiphol, KLM en LVNL monitoren gezamenlijk de voortgang van de uitvoering van de maatregelen."

KLM, Royal Schiphol Group, LVNL

11 Zie https://www.cybersecurityraad.nl/binaries/Cybersecurity_supply_chain_risico-analyse_DEF_tcm107-314472.pdf voor een gerichte *proof of concept* methodologie van een risico-analyse.

12 Voor het uitvoeren van een gedegen risicoanalyse kan men gebruik maken van diverse methodieken op dit gebied. Voor een risicoanalyse kan men bijvoorbeeld gebruik maken van de Baseline Informatiebeveiliging Overheid (BIO). Andere methodieken betreffen de OCTAVE Allegro methode van het Carnegie Mellon – Software Engineer Institute en de IRAM-methodologie van het Information Security Forum.

Verder lezen

Whitepaper ketenweerbaarheid TNO

- Ruijven, T.W.J. van, & Keijser, B. (2017), *Ketenweerbaarheid tegen cyberdreigingen: uitgangspunten, good practices, en een stappenplan voor het vergroten van cyber-ketenweerbaarheid*. Beschikbaar via https://www.tno.nl/nl/aandachtsgebieden/defensie-veiligheid/roadmaps/nationale-veiligheid/whitepaper-ketenweerbaarheid-tegen-cyberdreigingen/

Verdiepende literatuur

- Joosten, R., Smulders, A. (2013), *Advanced Risk Management: Succesvol risico's beheersen bij toenemende complexiteit en dynamiek*. Beschikbaar via http://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.
- 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
- Grijpink, J.H.A.M. (2016). *Keteninformatisering in kort bestek*. Lemma.
- 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.
- Voster, W. & de Bruijn, J. (2016). *Cyber security supply chain risico-analyse 2015*. Beschikbaar via https://www.cybersecurityraad.nl/binaries/Cybersecurity_supply_chain_risico-analyse_DEF_tcm107-314472.pdf

Colofon

De inhoud van deze handreiking is mede gebaseerd op gezamenlijk onderzoek van TNO en NCSC op het gebied van ketenweerbaarheid.

Uitgave
Nationaal Cyber
Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl/samenwerking
samenwerken@ncsc.nl
@ncsc_nl

Oktober 2018