Defensie & Veiligheid
Oude Waalsdorperweg 63
2597 AK Den Haag
Postbus 96864
2509 JG Den Haag

www.tno.nl

T +31 88 866 10 00
F +31 70 328 09 61

TNO-rapport

TNO 2019 R11304

Succesfactoren voor digitaal veilige Operationele Technologie

Datum	november 2019
Auteur(s)	J. Vos P. Van den Brink MSc T. van Schie MA
Aantal pagina's	46 (incl. bijlagen)
Aantal bijlagen	3
Opdrachtgever	Nationaal Cybersecurity Centrum
Projectnaam	ICS/SCADA Security / [CY] NCSC Kennisopbouw 2019 - P105
Projectnummer	060.38869/01.04

Managementsamenvatting

Ondanks de toenemende aandacht, kennis en initiatieven is er behoefte om beter te begrijpen wat de bepalende factoren zijn bij het inbedden van Operationele Technologie (OT) op het gebied van cybersecurity in de operationele processen. Inzicht in deze bepalende factoren draagt bij aan het duurzaam inbedden van OT-security. Het doel van dit onderzoek is om factoren te bepalen voor een succesvolle OT-security invoering. Het juiste gebruik van deze factoren bieden OT-security uitdagingen, obstakels en valkuilen het hoofd en dragen daarmee bij aan een succesvolle bredere invoering van OT-security in organisaties. De onderzoeksvraag luidt:

Wat zijn organisatorische succesfactoren voor het succesvol inbedden van OT-cybersecurity in de bedrijfsvoering?

Voor het beantwoorden van deze vraag zijn vijf thema's geïdentificeerd die de uitdagingen van OT-security weergeven. Zo behandelt het eerste thema de uitdaging om het belang van cybersecurity voor OT bij het management onder de aandacht te brengen en OT-risicobeheersing in het bestaande risicomanagement in te bedden. Het tweede thema laat zien dat er al veel (basis)maatregelen beschikbaar zijn voor digitaal veilige OT en schetst de uitdagingen om deze ook in de eigen organisatie in te voeren. Het derde thema gaat in op de uitdagingen die zich voor doen voor het beheer en onderhoud van OT en de risico's die dit met zich meebrengt. De historisch ontstane kloof tussen het Informatie Technologie (IT) en OT-domein is het vierde thema, waarin de behoefte voor het dichten van deze kloof en de uitdagingen om hier te komen duidelijk worden. Het vijfde thema wijst tot slot op de uitdagingen om de juiste kennis en kunde te ontwikkelen en in de eigen organisatie te krijgen en houden.

Om met deze uitdagingen om te gaan en OT-security (verder) in te bedden in organisaties, zijn bepalende succesfactoren naar boven gekomen. Deze zijn verzameld door het afnemen van interviews met vitale- en niet vitale organisaties in Nederland. Hiermee kunnen organisaties van elkaar leren en zelf bepalen welke stappen te zetten om OT-security in te regelen. Hieronder worden een aantal succesfactoren beschreven (een volledig overzicht is opgenomen in bijlage C) die duidelijk en praktisch van aard zijn en in meerdere interviews zijn benadrukt als factoren die belangrijk zijn.

- Succesfactor. Stel een cybersecuritystrategie op waar ook structurele inbedding van OT-security in risicomanagement wordt opgenomen. Deze strategie moet ingaan op kansen en dreigingen, vertaald naar organisatiedoelen. Tevens is het van belang de doelstellingen, maatregelen en KPI's te vertalen naar individueel niveau, omdat dit kan bijdragen aan het cybersecurity bewustzijn en handelen in de hele organisatie.

- Succesfactor. Communiceer altijd de context van OT-security in het grote geheel. Besef dat OT-security een deel is van de puzzel om organisatiedoelstellingen te bereiken.

- Succesfactor. Kies de relevante standaard(en) en vertaal deze op basis van de wensen en eisen van medewerkers naar de eigen organisatie. Dit vergt kennis, tijd en geld maar het belang om dit zorgvuldig te doen wordt door de respondenten benadrukt.

- Succesfactor. Management erkent de noodzaak voor het combineren van IT- en OT- kennis en kunde en zorgt ervoor dat IT en OT in dezelfde afdeling werken.

- Succesfactor. Kennisdeling onderdeel maken van de functioneringsgesprekken. Hierdoor worden individuele medewerkers gestimuleerd en uitgedaagd om hierin uit te blinken.

- Succesfactor. Het streven naar standaardisatie van softwareprogramma's en apparatuur kan het beste worden vormgegeven in de life cycle managementprocessen.

- Succesfactor. Ontwikkel een ingrijpend en realistisch scenario, oefen het reactieplan en evalueer hoeveel tijd, personeel, geld er nodig is om de procesautomatisering weer volledig te herbouwen. Dit gezamenlijk doen zorgt voor het vergaren en versterken van kennis en kunde.

- Succesfactor. Borg OT-security als een jaarlijkse bedrijfsdoelstelling.

- Succesfactor. Het management faciliteert het delen van ervaring en kennis op dit onderwerp met andere bedrijven.

- Succesfactor. Gebruik audits om de mogelijke kwetsbaarheden als startpunt te gebruiken om OT-security onder de aandacht te brengen bij het management.

- Succesfactor. Een organisatie beschikt te allen tijde over een basis aan kennis over OT(-security) om met externen samen te werken. Dit betekent dat er meegekeken en gedacht kan worden als bijvoorbeeld leveranciers op systemen of software komen installeren.

- Succesfactor. Aan het management open en helder communiceren wat er in huis is aan OT systemen en wanneer dit (op de lange termijn) aan vervanging (of updates) toe is. Het management zorgt voor de juiste investeringsbesluiten en waarborgt daardoor het veiligstellen van OT-systemen.

Als ondersteuning voor een organisatie om (verder) aan de slag te gaan met OT-security hebben we de uitdagingen en succesfactoren uitgewerkt tot basisaspecten en vragen voor verdere invulling. De basisaspecten stellen organisaties in staat om te kijken op welke manier men nu met OT-security bezig is en hoe aan de slag te gaan. De vragen stellen organisaties in staat bij zichzelf na te gaan hoe dingen ingeregeld zijn en verdere invulling te geven aan OT-security.

Tot slot blijkt uit de interviews dat een groot aantal organisaties serieus aan de slag is met OT-security. Dit is te zien in het grote aantal succesfactoren dat uit de organisaties naar voren is gekomen.

Inhoudsopgave

1 Inleiding

1.1 Achtergrond

Operationele Technologie (OT) is een overkoepelende term voor de hardware en software die industriële processen uitvoeren, controleren en aansturen. OT wordt ook wel aangeduid als Industrial Control Systems (ICS) . De veiligheid van deze systemen is van belang voor de organisatie en medewerkers die OT gebruiken, en heeft potentieel een grote impact voor de samenleving wanneer processen verstoord raken. Denk aan processen die bijvoorbeeld voor de beschikbaarheid van energie en drinkwater zorgen.

Informatie en Communicatie Technologieën (ICT) en Operationele Technologie (OT) hebben bedrijven mogelijkheden geboden om de efficiëntie en schaalgrootte te verbeteren. Operators uit onder andere de watersector, energiesector, chemiesector en transportsector hebben operationele processen in toenemende mate geautomatiseerd en met elkaar verbonden. Ook zijn er verbindingen gemaakt tussen de interne OT en IT. Onderhoud en monitoring van processen kan nu deels op afstand plaatsvinden, bruggen en sluizen worden centraal aangestuurd, verkeerssystemen detecteren automatisch verkeersopstoppingen, het spoornetwerk wordt centraal gemonitord en fabrieksautomatisering wordt steeds verder geoptimaliseerd en geïntegreerd met andere interne en externe omgevingen.

1.2 Aanleiding

Met name de afgelopen decennia is gebleken dat het toenemend gebruik van digitale systemen in industriële processen naast positieve aspecten ook een keerzijde heeft. In nationale en internationale media is er veel berichtgeving over aanvallen op en incidenten in OT-omgevingen. Denk aan BlackEnergy, Stuxnet, NotPetya, LockerGoga en Havex waarbij malware zorgde voor gedigitaliseerde sabotage of criminaliteit. De connectiviteit van OT met IT creëert ook ongekende mogelijkheden om schade te berokkenen door eigen medewerkers (bedoeld of onbedoeld). Het bewustzijn hierover groeit en men is al jaren met maatregelen, maar de dreigingen zijn niet voor alle organisaties geïdentificeerd als risico’s of zijn pas recentelijk als zodanig geïdentificeerd (Colbert en Cott, 2016, pp. 69-64).

Door de afhankelijkheid van OT-systemen en door de toenemende risico’s die digitalisering met zich meebrengt is er toenemende aandacht voor de veiligheid en onveiligheid van systemen waarop de samenleving vertrouwt, zowel vanuit de overheid als de organisaties zelf (CSBN, 2019, p.16). Er zijn al veel instrumenten beschikbaar om de weerbaarheid te verhogen, denk aan normen en standaarden en overzichten van good practices. Toch blijkt dat in Nederland het duurzaam inbedden van OT-cybersecurity in de (vitale) sectoren nog geen vanzelfsprekendheid is . Wat zijn de succesfactoren die maken dat een deel van de organisaties met succes aan de slag is gegaan met OT security en wat waren de obstakels?

Het Nationaal Cyber Security Centrum heeft behoefte om beter te begrijpen wat de bepalende factoren zijn bij het succesvol inbedden van OT-cybersecurity in

organisaties. Inzicht in deze bepalende (succes)factoren kan bijdragen aan het duurzaam inbedden van OT-cybersecurity.

1.3 Doel en scope onderzoek

Het doel van dit onderzoek is om factoren te bepalen voor een succesvolle invoering van OT-cybersecurity . De resultaten van dit onderzoek kunnen gebruikt worden in de ondersteuning bij werkzaamheden om OT-security obstakels te overwinnen, en daardoor valkuilen en uitdagingen het hoofd te bieden. Het inzicht in en overzicht van actuele succesfactoren kan bijdragen aan een succesvollere en bredere invoering van OT-cybersecurity in organisaties. De onderzoeksvraag luidt:

Wat zijn organisatorische succesfactoren voor het succesvol inbedden van OT-cybersecurity in de bedrijfsvoering?

Dit rapport presenteert succesfactoren en praktijkvoorbeelden voor OT-cybersecurity en focust op de positieve ontwikkelingen waar sectoren met OT zich door kunnen laten inspireren. Het geeft zowel inzichten voor bedrijven die nog zoekende zijn om OT-cybersecurity in te regelen, als voor bedrijven die al veel stappen hebben gezet.

1.4 Onderzoeksmethode

We hebben diverse onderzoeksactiviteiten uitgevoerd om factoren voor het succesvol inbedden van OT-cybersecurity in de bedrijfsvoering te bepalen. We hebben een literatuurverkenning gedaan, interviews afgenomen, een analyse-raamwerk ontwikkeld en deze rapportage opgesteld.

De literatuurverkenning is gebruikt als start van het onderzoek. Hiermee zijn de kernonderwerpen en uitdagingen voor inbedding van OT-security in kaart gebracht. Met die informatie is het interviewprotocol (zie bijlage A) opgesteld. Het interviewprotocol bestaat uit hoofdvragen, onderbouwd met achtergrondinformatie, checkvragen en de doelstelling van de vraag. Daarnaast heeft de literatuurverkenning het analyse-raamwerk vormgegeven.

Het grootste onderdeel van het onderzoek besloeg de verdiepende interviews met twaalf Nederlandse vitale en niet vitale bedrijven. De interviews zijn gehouden met zowel de verantwoordelijke voor de OT-security, dus een productiemanager of IT/cybersecurity manager, als met een aantal managementleden om ook deze kant te belichten en de relatie inzichtelijk te maken.

De onderzoeksresultaten (een geanonimiseerde en geaggregeerde weerspiegeling van deze interviews) zijn aan de hand van een analyse-raamwerk geduid.
Het raamwerk bestaat uit een vijftal thema's die de uitdagingen voor het inbedden van veilige OT aan het licht brengen. Per thema's zijn bepalende succesfactoren, basisaspecten en vragen voor inbedding van OT-security beschreven.

- Een succesfactor is: informatie die in de beleving van de respondenten heeft geleid tot een wezenlijke bijdrage aan het inrichten van OT-security en waaraan ook een praktische uitvoering kan worden gegeven.

- Een basisaspect is: een aspect dat bijdraagt aan het veilig inrichten van Operational Technology. Basisaspecten komen voort uit de succesfactoren. Het zijn aspecten waar elke organisatie mee kan beginnen en zelf overwegingen in kan maken.
- Een vraag is: een specifieke vraag die organisaties zichzelf kunnen stellen om richting te geven aan de verdere invulling van OT-security in de eigen organisatie. Deze vragen helpen om organisaties na te gaan hoe er met de gevonden uitdagingen wordt omgegaan.

In sommige gevallen hebben de respondenten geen succesfactor(en) genoemd. In deze gevallen worden enkel de uitdagingen en behoeften weergegeven in het rapport.

Onder ieder thema zijn de uitdagingen gekoppeld aan succesfactoren. Organisaties kunnen intern ten rade gaan op welke manier de succesfactor wel of niet van toepassing is of kan zijn voor de eigen organisatie. Belangrijk is dat de succesfactoren noch de basisaspecten en vragen uitputtend zijn omdat dit slechts een weergave is van het aantal gehouden interviews.

1.5 Leeswijzer

Hoofdstuk 2 toont het analyse-raamwerk. Hoofdstuk 3 beschrijft de onderzoeksresultaten van de succesfactoren voor veilige OT en geeft daarbij praktijkvoorbeelden. Hoofdstuk 4 bevat een overzicht van basisaspecten en vragen voor de inbedding van OT-security die gebaseerd zijn op de succesfactoren. Hoofdstuk 5 beschrijft de bevindingen en kijkt naar mogelijke vervolgstappen.

2 Analyse-raamwerk

In dit hoofdstuk wordt het analyse-raamwerk uiteengezet. Aan de hand van de literatuurverkenning zijn vijf thema's geïdentificeerd die de historische en actuele uitdagingen rondom OT-cybersecurity aangeven. De thema's komen opeenvolgend aan bod in de paragrafen 2.1 tot en met 2.5.

De thema's zijn:
- Bewustzijn van OT-gerelateerde risico's;
- Toepassen beschikbare basismaatregelen OT-security;
- Beheer en onderhoud;
- Kloof tussen IT- en OT-domeinen;
- Kennis en kunde van OT-security.

De thema's zijn gebruikt om veel genoemde succesfactoren, uitdagingen, adviezen en opvattingen over de huidige status van OT-security te structureren en analyseren. De thema's zijn daarnaast ook gebruikt om het interviewprotocol (zie bijlage A) te ontwikkelen en de interviews te voeren.

In de volgende paragrafen worden de thema's besproken en uiteengezet voor welke uitdagingen organisaties komen te staan bij de inbedding van OT-security.

2.1 Bewustzijn van OT-gerelateerde risico's

Het eerste thema gaat in op een van de grootste uitdagingen; het bewustzijn creëren bij zowel het management als de medewerkers van een organisatie voor de risico's die digitaal onveilig OT teweeg kan brengen (SANS Institute, 2019). Dit bewustzijn is nodig om de noodzaak en het beheer te vertalen naar kansen en bedreigingen voor de eigen organisatie. Dit draagt bij aan het nemen van geïnformeerde en afgewogen (investerings-)besluiten die noodzakelijk zijn voor een veilige bedrijfsvoering.

Het OT-domein is vaak opgebouwd uit veel specifieke (unieke) systemen met specifieke functies. Het zijn systemen die bijvoorbeeld voor algemene regelingen zorgen, voor elektrische aansturingen (elektronische schakelborden), compressoren, generatoren, brandbestrijding, koeling/ventilatie (HVAC), veiligheid, afvalwater, et cetera. De eigenschappen van deze OT systemen spelen een belangrijke rol voor het in kaart brengen en bewust zijn van de cybersecurity risico's. Zo is de levensduur van een SCADA/PLC/DCS omgeving gemiddeld zo'n 15 tot 20 (plus) jaar, wat haaks staat op IT systemen die een veel kortere levensduur hebben (NIST SP.800-82 r2, 2015). Daarnaast is upgraden en patchen moeilijk in een operationele omgeving, omdat deze niet zomaar uitgezet kan worden. Tot slot hebben incidenten in potentie een hoge impact op het primaire proces (NIST SP.800-82 r2, 2015). Deze lappendeken aan systemen met verschillende operating systems, waarover soms weinig kennis beschikbaar is, zorgt voor complexiteit en creëert (digitale) risico's.

Om de OT veilig te houden is het nodig om upgrades en updates te doen van de systemen en apparatuur in de productieomgeving. Het upgraden en up-to-date houden van OT-systemen is complex, soms onmogelijk en/of te kostbaar. Het kan

processen onverwacht verstoren of het risico op een mogelijk verstoring wordt te hoog ingeschat door de kans op een productiestop. End-of-life (besturing)systemen zijn nog alom vertegenwoordigd in productieprocessen, zoals Windows XP, NT, Windows 7, Windows CE, Windows 2003 et cetera die digitaal onveilige OT veroorzaken. Verouderde en niet bijgewerkte software en hardware is niet per definitie onveilig, mits hier maatregelen voor genomen zijn (bijvoorbeeld het fysiek en digitaal isoleren) en dergelijke risico's opgenomen zijn (geweest) tijdens risicobeoordelingen.

De verwevenheid van IT- en OT-systemen, de diversiteit in levensduur en de ontbrekende kennis vraagt om goed geïnformeerd risicomanagement. Hier is het belangrijk dat het management dit inziet en hierop besluiten neemt geënt op de eigen organisatie. Aandacht en kennis over cybersecurity bij managementlagen is veelvuldig onder de aandacht gebracht door kennisinstituten, de Cybersecurity Raad en brancheverenigingen (GCCS 2015, Macaulay en Singer 2012, NIST, 2015, CSR 2018). Dit is belangrijk omdat er keuzes gemaakt moeten worden over hoe om te gaan met OT-security en vooral over de stappen die gezet moeten worden om OT-security in te bedden. Door gebrek aan ervaring met en aandacht voor OT-security hebben bedrijven veelal moeite met bijvoorbeeld het:

- Duiden van technische en organisatorische OT-security uitdagingen die benodigd zijn voor het productieproces;
- Opstellen van een risicobeoordeling die OT-security realistisch opneemt als kans en bedreiging;
- Reserveren en besteden van financiële middelen voor OT-security;
- Nemen van de juiste beslissingen tijdens incidenten (Macaulay en Singer, 2012);
- Opnemen van OT-security in offertes, aanbestedingen en werk dat leveranciers uitvoeren (Ponemon, 2019).

Bewustzijn bij het management is de eerste en een belangrijke stap om OT-security niet slechts als kostenpost, maar als kans te bestempelen voor de business continuïteit. Door een goed doordachte OT-security kan er een voordeel ontstaan ten opzichte van concurrentie. Risico's nemen af en de kosten van uitval door security-incidenten worden minder.

2.2 Toepassen beschikbare basismaatregelen OT-security

Het tweede thema gaat in op de diverse beschikbare OT-security basismaatregelen. De behoefte aan OT-security is gedurende de afgelopen jaren enorm gegroeid en er is veel ontwikkeld voor het omgaan met de risico's. Zo beschrijft een recent rapport van MITRE dat voor veel van de gangbare IT- en OT- kwetsbaarheden al bekende beveiligingsmaatregelen beschikbaar zijn (MITRE, 2018). Veel gebruikte standaarden en good practices zijn bijvoorbeeld de NIST SP 800, IEC 62443 of de ISO27001 (zie in bijlage B een overzicht van verschillende basismaatregelen).

Verstoringen en uitval van primaire processen bij bedrijven met OT zijn terugkerende nieuwsberichten in de media. Daarnaast schrijven adviesbureaus, overheden, hardware producenten en bedrijven in de informatiebeveiliging maandelijks en jaarlijks adviezen om OT veiliger te maken. Adviezen die

grotendeels teruggrijpen op bestaande basismaatregelen zoals uiteengezet in literatuur, practices en normen[1].

Het toepassen en daarmee het internaliseren van deze bestaande literatuur, practices en normen blijkt voor organisaties niet zo eenvoudig. Allereerst is er een dermate grote hoeveelheid aan maatregelen beschikbaar, dat daardoor soms niet meer duidelijk is welke het beste zijn voor het eigen proces. Daarnaast is er nog een andere reden, namelijk dat de maatregelen nog wel op de eigen organisatie geplot moeten worden om deze bruikbaar te maken. Dit vergt tijd, kennis en kunde. Eerst moet een standaard of methodologie gekozen worden en vervolgens moet deze standaard of methodologie vertaald worden naar de eigen organisatie.

Het is belangrijk om inzicht te krijgen in hoe organisaties omgaan met de huidige set van beschikbare maatregelen en de obstakels om deze in de eigen organisatie toe te passen.

2.3 Beheer en onderhoud

Het derde thema gaat in op het belang van het inregelen van beheer en onderhoud. In ononderbroken productieprocessen en aanleveringslijnen is de mogelijkheid om tussentijds onderhoud te plegen beperkt. Er moet een productiestop ingepland worden of een vooraf gepland onderhoudsmoment gebruikt worden om systeemonderhoud te doen. Productiestoppen zijn duur en vaak contractueel lastig, en ingeplande onderhoudsmomenten kunnen in tijd ver uit elkaar liggen. Het is dus een uitdaging om beheer en onderhoud in te regelen.

De beheer- en onderhoudsprocessen voor OT hebben de doelstelling om de beschikbaarheid, integriteit, vertrouwelijkheid en veiligheid van de processen te garanderen. Dat bij beheer- en onderhoudsprocessen ook rekening moet worden gehouden met digitale dreigingen op OT is een relatief nieuw inzicht (Colbert en Cott, 2016). Met de komst van IT-systemen die verweven zijn in OT-systemen, wordt de uitdaging om onderhoud tijdig te plegen groter. Dit heeft met name te maken met de verschillende levensduur van IT en OT. Daarnaast zijn er maatregelen beschikbaar in de vorm van bijvoorbeeld patches, maar het bewustzijn om deze door te voeren is in sommige gevallen niet altijd aanwezig. Zo zijn sommige patches zeven jaar geleden beschikbaar gesteld, maar nog niet toegepast op kwetsbare OT (Universiteit Twente. 2019). Hieronder volgen drie perspectieven op beheer en onderhoud vanuit verschillende partijen.

Bezien vanuit een OT-producent en leverancier
Vanuit OT-producenten en leveranciers bestaat er een uitdaging om updates en upgrades beschikbaar te stellen. Soms gebeurt dat niet. Hier zijn diverse redenen voor. Een (niet uitputtend) overzicht ter illustratie:

- De benodigde tijd om een upgrade te ontwikkelen en te testen is te lang.
- Klanten vragen niet altijd om updates en upgrades.
- Leveranciers slaan een versie van een besturingssysteem geheel over omdat de versie niet de vereiste stabiliteit blijkt te hebben in de praktijk.

[1] Een greep van deze literatuur is terug te vinden in hoofdstuk 6 ‘Referenties’ en ‘Bijlage B. Overzicht basismaatregelen’.

- Ontwikkelingen en trends op het gebied van cybersecurity worden door leveranciers en producenten niet vertaald naar risico's die van toepassing zijn op al geleverde of operationele producten.
- Accreditaties en zorgplicht van leveranciers is niet expliciet gemaakt of aanwezig.
- Cybersecurity wordt door sommige leveranciers gebruikt als een middel om extra geld te kunnen verdienen. Er is dan dus een commercieel belang om het niet standaard (by design) toe te passen in producten.

Bezien vanuit een externe beheer en onderhoudspartij
Vanuit externe partijen die beheer- en onderhoudsprocessen voor hun rekening nemen, spelen er drie uitdagingen:

- Klanten vragen niet om cybersecurity.
- Producenten en leveranciers voelen zich niet verantwoordelijk voor (OT-) cybersecurity. Een reden hiervoor is dat klanten niet de verantwoordelijkheden en verplichtingen opnemen in de contractuele afspraken die zij aangaan.
- Externe partijen bieden (vaak) geen mechanisme aan om bijvoorbeeld security patches te testen. Zeker niet als men klant-specifieke softwaresystemen levert. Een reden hiervoor is dat een onderhoudscontract voor patchonderhoud heel erg kostbaar kan zijn en sommige externe partijen het nog steeds niet kunnen aanbieden omdat ze de kennis en kunde niet in huis hebben.

Bezien vanuit de eigen processen en medewerkers
Vanuit de eigen processen en medewerkers zijn diverse uitdagingen geïdentificeerd om het beheer en onderhoud van OT-security in te bedden:

- Beschikbare (aanbevolen) updates en upgrades worden niet doorgevoerd door onwetendheid.
- Er is een gebrek aan inzicht over wijzigingen in de eigen productieprocessen als gevolg van een update.
- Bepaalde managementlagen houden beheer en onderhoud tegen, of ze worden pas lang na het publiceren ervan doorgevoerd en toegepast. Een mogelijke reden om pas later een update of upgrade te doen, is dat het soms onduidelijk is of een patch noodzakelijk is voor het veilig functioneren van OT-onderdelen. Vanuit het management zijn redenen om niet of later te upgraden onder andere hoge kosten van een productiestop of hoge kosten door nieuwe software licenties van leveranciers en de inhuur van specialistische engineers.

2.4 Kloof tussen IT- en OT-domeinen

Het vierde thema schetst de kloof tussen de IT- en OT-domeinen en de behoefte die er nu bestaat om deze samen te brengen om OT zo veel mogelijk digitaal veilig te maken. Door de digitalisering zijn IT en OT steeds meer vervlochten en afhankelijk van elkaar. Uit de literatuur komt echter naar voren dat er een in de organisatie kloof bestaat tussen deze twee domeinen en dat samenwerking niet altijd vanzelfsprekend is.

Dit is historisch zo ontstaan, omdat men voor de procesautomatisering weinig met elkaar van doen had. De toenemende verwevenheid van IT- en OT-omgevingen wil niet zeggen dat dit de verschillen tussen IT- en OT-medewerkers verkleind heeft

(Kaspersky, 2019)[2]. Daarnaast beheren en ontwikkelen medewerkers in de IT- en OT-omgevingen met verschillende doelstellingen. Bijvoorbeeld als het gaat om de beschikbaarheid, veiligheid en vertrouwelijkheid van hardware, software en informatiestromen. Een IT-afdeling kan omwille van life cycle management de IT apparatuur willen vervangen voor de hele organisatie. Een OT-manager wil een dergelijk systeem eerst in een vergelijkbare omgeving uitgebreid testen alvorens de nieuwe apparatuur te installeren, omdat het anders mogelijk een ontoelaatbare productiestop oplevert. Men spreekt in deze situaties soms over silo's binnen de organisatie omdat er op basis van andere belangen en ervaringen gewerkt wordt.

Daarnaast gebruikt men andere middelen, kennis en een andere manier van werken. Zo zijn de gangbare IT-security standaarden anders dan de gangbare OT-security standaarden. Sommige standaarden worden vanuit het IT-domein ook gehanteerd in het OT-domein, wat uitdagingen met zich meebrengt. Een voorbeeld is de ISO27001 norm die in IT-security veelal toegepast wordt, maar geen aanbevelingen over het opzetten van een netwerk architectuur bevat; belangrijk voor zowel IT- als OT-security. Ook het verschil in standaarden benadrukt de kloof, bijvoorbeeld het COBIT raamwerk dat veel in kantooromgevingen wordt toegepast als een raamwerk van beheersmaatregelen, terwijl in de OT het IEC 62443 (*Cybersecurity voor Industrial Automation and Control Systems*) raamwerk gehanteerd wordt.

Door de complexiteit en de vereiste beschikbaarheid van systemen heerst er veelal een mentaliteit van 'niet aankomen als het niet nodig', wat de kloof in stand houdt of zelfs versterkt. Hierbij komt dat men dus van oudsher anders werkt en elkaar niet dagelijks tegenkomt, waardoor samenwerking niet vanzelfsprekend is.

De digitalisering die voor vervlechting van IT en OT systemen zorgt vraagt om samenwerking tussen deze twee domeinen. Met name omdat zij elkaar kunnen versterken en men juist geen kennis wil verliezen. Dit is belangrijk voor OT die nu wordt geïntroduceerd, maar ook voor OT die al jaren in gebruik is (legacy OT) en waar cybersecurity met terugwerkende kracht zijn intrede doet. De behoefte om de kennis en kunde van IT en OT vanuit het beheerdersperspectief samen te brengen is noodzakelijk om de OT van een organisatie digitaal veilig te maken en houden.

2.5 Kennis en kunde van OT-security

Het vijfde en laatste thema is de niet altijd (voldoende) aanwezige kennis en kunde om OT-security in te voeren en in te regelen. Aan de ene kant zorgt dit ervoor dat de noodzaak van OT-security soms niet voldoende wordt onderkend. Aan de andere kant zorgt het ervoor dat zodra men de stap neemt, het veel tijd en kosten met zich mee brengt om de juiste kennis en kunde in huis te halen en in te bedden in de organisatie.

De benodigde kennis is tweeledig: technische kennis van OT is nodig om veilig te kunnen opereren en generieke cybersecurity kennis is nodig om het bewustzijn van en noodzaak voor digitaal veilige IT en OT te creëren.

[2] Kaspersky's 2019 'State of industrial cybersecurity' uitgave geeft weer dat voor 39% van de respondenten de *interconnectedness* van IT en OT een 'major challenge' voor het managen van OT-security. 38% bestempeld dit als een 'minor challenge'.

Dat er in het beginsel niet altijd voldoende technische kennis aanwezig is komt omdat voor sommige bedrijven OT-security geen kennisgebied is dat traditioneel aanwezig was, of doordat kennis wegvloeit vanwege personeelsverloop. Hoog over cybersecuritykennis is van belang voor de raad van bestuur, de directeur, managers en alle overige medewerkers die niet dagdagelijks verantwoordelijk zijn voor digitaal veilige OT. Beide soorten kennis creëren bewustzijn en zorgen voor aandacht voor het onderwerp en daadkracht in het invoeren en inregelen van digitaal veilige OT.

De benodigde kennis en kunde kunnen op twee manieren worden verworven, namelijk door uit te besteden (inkopen) of door zelf te verwerven (personeel opleiden of personeel met de juiste kennis en kunde aannemen). Een combinatie van in-house kennis en kunde uitbesteden is uiteraard ook een mogelijkheid.

Het aannemen van kundig OT-security personeel wordt echter als een grote uitdaging gezien. Er is een groot tekort aan beschikbaar geschoold personeel (Kaspersky, 2018). Dezelfde studie toont aan dat het tekort er toe leidt dat *dedicated* IT-security teams naast hun primaire verantwoordelijkheid ook zorg moeten dragen voor OT-security (ibid, p. 23), wat als negatief bestempeld wordt vanwege een te groot en te divers takenpakket van deze medewerkers.

Het inbedden van OT-security is dus enorm afhankelijk van het tijdig ontwikkelen van algemene kennis van cybersecurity. Het is ook een uitdaging om over voldoende en specialistische kennis te beschikken. Daarnaast blijft cybersecurity een veld van rappe ontwikkelingen en moet het kennispeil ook continu hoog worden gehouden.

3 Succesfactoren voor digitaal veilige OT

Uit de in hoofdstuk 2 beschreven analyse blijkt dat er enorme ontwikkelingen hebben plaatsgevonden die vragen om een digitaal veilige OT-omgeving. Om hiertoe te komen zijn al veel stappen gezet, maar er is ook een aantal uitdagingen. Om inzicht te krijgen in de succesfactoren om OT-security (verder) in te bedden zijn aan de hand van het analyse-raamwerk interviews uitgevoerd om succesfactoren en praktijkvoorbeelden te identificeren.

Dit hoofdstuk beschrijft de geïdentificeerde succesfactoren en praktijkvoorbeelden uit de interviews. De succesfactoren zijn gebaseerd op ervaringen die respondenten hebben geuit over het succesvol inrichten van hun OT-security. Het gaat specifiek om factoren die in de beleving van de respondenten hebben geleid tot een wezenlijke bijdrage aan het inrichten van OT-security en waaraan ook een praktische uitvoering kan worden gegeven. De thema's van het analyse-raamwerk worden als kapstok gebruik om de succesfactoren te duiden[3].

De succesfactoren kunnen inspireren door ze te bespreken in de eigen organisatie. Ze stellen individuen in staat om de aanpak en manier van werken in de eigen organisatie te evalueren. Waarschijnlijk leggen enkele succesfactoren blinde vlekken bloot, terwijl andere een bevestiging zijn van de bestaande manier van werken (die wellicht nog verder verbeterd kan worden).

3.1 Bewustzijn van OT-gerelateerde risico's

Om draagvlak te creëren bij management en medewerkers voor het belang van OT-security is inzicht nodig in de aan OT gerelateerde risico's. Inzicht krijgen in de kans op en impact van verstoringen op het primaire proces is mogelijk met adequaat risicomanagement. Ontwikkelingen en trends op het gebied van cybersecurity worden nog niet altijd vertaald naar risico's die van toepassing zijn op operationele processen. Dat dit niet altijd gebeurt kan komen door onvoldoende of onjuiste aandacht van het management. Het kan ook zijn dat IT- en OT-medewerkers nog niet voldoende met elkaar optrekken om de verwevenheid goed aan te pakken[4].

3.1.1 Belang aansluiten bij bestaand risicomanagement

Het is van belang om ontwikkelingen en trends op het gebied van OT-security te integreren in bestaande risicomanagementmethodieken. Dit vereist een kritische en dynamische blik op het risicomanagementproces.

Cybersecurity onderdeel van bestaand risicomanagement. Het management draagt verantwoordelijkheid voor de continuering van de primaire processen en houdt daarvoor rekening met verscheidene risico's (zowel die in de huidige risicomanagementprocessen als die in de bredere Business Continuity Management (BCM) processen van de organisatie). Het is van groot belang dat

[3] Voor de uitdagingen zijn diverse thema's naar voren gekomen uit de interviews. Niet elk thema heeft specifiek geleidt tot succesfactoren, maar schetsen wel de context van de uitdagingen. Daarnaast zijn dit thema's waar wel in de interviews het belang van is geuit.

[4] Het gaat binnen dit thema en de gevonden succesfactoren om het meenemen van OT-security. Echter zijn deze uitdagingen en de gevonden succesfactoren breder te trekken als het gaat om bewustzijn en duiden van cybersecurity risico's.

cybersecuritydreigingen hier onderdeel van zijn en dat aan de hand daarvan risico's inzichtelijk worden gemaakt. Belangrijk is dat dit besef er is bij zowel het management als het operationele niveau.
Het management moet de ernst van OT-security dreigingen begrijpen (bijvoorbeeld door uit te kunnen leggen wat de impact van OT-security verstoring is op het primaire proces). Operationele OT-medewerkers moeten risico's afstemmen op de verschillende medewerkers en juist verwoorden.
Uit meerdere interviews is namelijk naar voren gekomen dat OT-security vertaald moet worden naar risico's die voor iedereen begrepen moet worden. Dit kan ook betekenen dat risico's verschillend worden gepresenteerd. Soms is het bijvoorbeeld wel nodig extra technische informatie te geven en soms is dit juist iets dat weggelaten moet worden om aandacht op andere onderwerpen te vestigen.

Succesfactor. Zet cyberdreigingen om in realistische risico's en kansen voor de eigen organisatie. Gebruik voorbeelden van incidenten in positieve of negatieve zin (van binnen of van buiten de organisatie) voor verdere bewustwording.

Succesfactor. Sluit aan bij bestaande risicomanagement processen om geïnformeerde investeringsbesluiten te nemen.

Succesfactor. Stel een cybersecuritystrategie op waar ook structurele inbedding van OT-security in risicomanagement wordt opgenomen. Deze strategie moet ingaan op kansen en dreigingen, vertaald naar organisatiedoelen. Tevens is het van belang de doelstellingen, maatregelen en KPI's te vertalen naar individueel niveau, dit kan bijdragen aan cybersecurity bewustzijn en handelen in de hele organisatie.

Praktijkvoorbeeld. Een van de respondenten gaf aan bestaande *business continuity management* activiteiten zo in te richten dat OT-security hiervan een vast onderdeel werd.

Praktijkvoorbeeld. Een van de organisaties is aan de slag gegaan om cybersecurity mee te nemen in de *Failure Mode and Effect Analysis* methodiek die zij al hanteerden in de eigen organisatie. Immers cyber security incidenten zijn een reële mogelijkheid geworden voor het falen van apparatuur.

Uitvragen van zorgen aan management. Het is van belang om het management uit te vragen wat voor zorgen er bestaan. Het gaat hier om de zorgen in algemene zin, maar ook of zij OT gerelateerde zorgen hebben. Dit is een eerste stap om OT-security mee te nemen in risicomanagement, namelijk welke risico's on '*top of mind*' zijn bij het management. Deze zorgen geven inzicht in de aspecten waarop gestuurd kan worden door het management en de verantwoordelijke voor OT-security. OT-security kan op deze wijze als kans en bedreiging integraal opgenomen worden. Uit interviews komt naar voren dat men zich de meeste zorgen maakt over verstoringen van het primaire proces en de materiële en financiële nadelige gevolgen die hieruit voortvloeien[5]. Bedrijven over de hele wereld hebben een vergelijkbare prioritering van deze zorgen kenbaar gemaakt (Kaspersky, 2019).

[5] Door diverse respondenten is geuit dat inzicht in de zorgen van het management waardevol is. Er zijn echter geen concrete succesfactoren naar voren gekomen hoe deze zorgen uit te vragen en hiervan op de hoogte te zijn en blijven.

Safety en security dichter bij elkaar. Het kan helpen om de safety en security domeinen dichter bij elkaar te brengen. Maatregelen die genomen worden door safety en security afdelingen onderscheiden zich van elkaar. De safety afdeling wil de organisatie beschermen tegen veelal niet-moedwillige of ondoordachte handelingen. De security afdeling treft maatregelen om zich te beschermen tegen veelal moedwillige of onvoorzichtige handelingen. OT-security valt met name onder de rationale van security. Voorbeelden van cybersecurity dreigingen en cyberveilig handelen blijken beter aan te spreken bij medewerkers wanneer de consequenties gekoppeld worden aan safety voorbeelden. OT kan bijvoorbeeld onveilig zijn door slechte (digitale) toegangscontrole en als een gevolg daarvan potentieel letselschade veroorzaken.

Succesfactor. Het is van toegevoegde waarde om OT-security te koppelen aan de organisatiedoelen, omdat er anders mogelijk veiligheidsrisico's ontstaan. Dit wordt door organisaties verschillend vormgegeven.

Praktijkvoorbeeld. OT-cybersecuritymaatregelen en audits worden bij sommige organisaties gekoppeld aan handelingen, gebruiken en maatregelen die vastgesteld zijn door de Health Safety Environment (HSE) Directive. Hierdoor werd OT-security onlosmakelijk verbonden en geïntegreerd in de bedrijfsvoerings- en beheersprocessen.

Praktijkvoorbeeld. Een organisatie gaf aan dat zij medewerkers actief betrekken bij de totstandkoming van de risicobeoordelingen uit de safety en security afdelingen. Ze gebruikten hiervoor onder andere de maandelijkse HSE briefings.

Investeringsbesluiten vanuit integraal risicomanagement. De juiste investeringsbesluiten moeten worden afgezet tegen de doelen van een organisatie, bezien vanuit risicomanagement en BCM. Daarom is het belangrijk om cybersecurity in de huidige risicomanagementstructuren mee te nemen (integraal). Het gaat vaak om een afweging, een keuze, waar een investering te doen of te besluiten dit juist niet te doen. De noodzaak voor genoeg middelen om mensen op te leiden, expertise binnen te halen, de juiste systemen in te kopen, op tijd te kunnen onderhouden of vervangen en om continu de risico's in kaart te kunnen brengen, is groot. Uit de interviews komt naar voren dat er een diversiteit bestaat in het niveau van bewustzijn en het beschikbaar maken van budget voor cybersecurity. Soms is de noodzaak geprioriteerd en speelt budget geen rol. In andere gevallen moeten de risico's van cybersecurity tot in detail uitgewerkt worden om een deel van het al beperkte budget te ontvangen.

Succesfactor. Bewustwording van het belang en toegevoegde waarde van OT-security draagt bij aan investeringsbesluiten. Incidenten kunnen hiervoor in de communicatie en onderbouwing worden benut.

Succesfactor. Investeringsbehoeften uitvragen bij verschillende organisatielagen, bijvoorbeeld aan de operationele managers. Deze managementlaag is namelijk verantwoordelijk voor productie en staat dicht genoeg bij de werkzaamheden. Zo worden kosten beter ingeraamd en leidt dit tot afgewogen keuzes.

3.1.2 Communicatie over kansen en bedreigingen

Om cybersecurity mee te nemen in het risicomanagement van de organisatie, gaat het om de juiste communicatie van de OT-security kansen en bedreigingen. Steeds gedetailleerde of technische informatie communiceren draagt niet bij aan de bewustwording van het belang en mondt niet uit in investeringsbesluiten. Het is nodig om uitdagingen die gerelateerd zijn aan (OT-) security van context te voorzien, te duiden en vervolgens mogelijke oplossingen benoemen.

Context van cybersecurity kansen en bedreigingen. Het is nodig om voor uitdagingen, oplossingen en maatregelen context te schetsen, deze te duiden en te plaatsten in lijn van de organisatiedoelen. Het is hier van belang het nut en de noodzaak in begrijpelijke taal te communiceren. Context is de context vanuit de organisatie, denk aan de organisatiedoelen en de interne processen. Context gaat daarnaast ook verder dan de eigen organisatie, denk aan de ontwikkelingen in de sector en de veranderende dreigingen.

Succesfactor. Communiceer altijd de context van OT-security in het grote geheel. Besef dat OT-security een deel is van de puzzel om de organisatiedoeleinden te verwezenlijken.

Succesfactor. OT(-security) lead moet *zelf* het belang en de toegevoegde waarde van OT-security bij het management op het netvlies zetten.

Uitval primaire proces inzichtelijk maken. Het is belangrijk om de kans op een verstoring of uitval van het primaire proces door een cyberdreiging inzichtelijk maken aan het management. Zo kan een CISO bijvoorbeeld de rol duiden die OT-security kan spelen bij het voorkomen van aantasting of bij onderhoud van de kroonjuwelen of het primaire proces bij een betreffende C-level bestuurder. Als dit eenmaal bij het management bekend is, zorgt dit voor de omslag om OT-security mee te nemen in de (investerings)besluiten.

Succesfactor. OT-security dreigingen vertalen naar risico's die het primaire proces (gedeeltelijk) verstoren, idealiter gebaseerd op kwantitatieve data (die niet altijd beschikbaar is).

Praktijkvoorbeeld. Een van de ondervraagde organisaties hanteerde een methode waarbij 'kroonjuwelen' werden geïdentificeerd. Deze werden vervolgens gecommuniceerd aan de verschillende C-level verantwoordelijken. Hiermee maakten zij de kwetsbaarheid en afhankelijkheden van deze 'kroonjuwelen' duidelijk voor de betreffende directieleden. De organisatie nam OT-security op in de analyse om daarmee te zorgen dat OT-security opgenomen werd in het pakket aan verantwoordelijkheden en beheersmaatregelen om de kroonjuwelen van het bedrijf te beschermen.

Continu risico's monitoren en communiceren. Het is belangrijk om na het identificeren van de risico's voor OT, deze ook continu te monitoren en hierover te communiceren. Dit draagt bij aan het bewustzijn en kennisniveau van het management en zorgt ervoor dat zij beter op de hoogte is van de actuele OT-security risico's. Zo blijven de geïdentificeerde kritieke (aandacht)punten onder de

aandacht[6]. Hierbij is het ook waardevol om dit breder in de organisatie te communiceren, zodat elke medewerker zich steeds bewuster wordt van de risico's en van wat ze kunnen doen.

Praktijkvoorbeeld. Een van de respondenten heeft een visueel aantrekkelijk, toegankelijk en up-to-date maturity dashboard per asset uit het primaire proces (compliance, patches, back-up, downtime, uptime, aantal verouderde of niet bijgewerkte systemen) opgezet. Deze is voor de organisatie (onboarding en formalisatie van nieuwe medewerkers, rollen, aanwezige managers en specialisten) ontwikkeld. Hiermee is de organisatie in controle over de OT-security en kan hier binnen de hele organisatie over gecommuniceerd worden.

3.2 Beschikbare basismaatregelen OT-security

Er bestaan basismaatregelen voor veilige OT en deze zijn bij velen bekend. De uitdaging is om vast te stellen wat er nodig is voor de eigen organisatie. Idealiter vloeit dit voort uit informatie vanuit risicomanagement en het doel om het primaire proces draaiende te houden. Hiermee kan bewust gekeken worden naar hoe standaarden of andere maatregelen in te regelen en wat hiervoor nodig is.

3.2.1 Gebruik bestaande maatregelen voor eigen organisatie

Het is van belang om kennis te nemen en gebruik te maken van bestaande maatregelen, om deze makkelijk aan te sluiten bij de organisatie en de mensen die er mee werken.

Standaarden omzetten naar eigen organisatie. Uit alle interviews komt naar voren dat de standaarden de juiste onderwerpen beslaan, maar dat standaarden niet altijd direct te gebruiken zijn. Elke organisatie heeft de keuze welke standaarden te gebruiken en moet daarna zelf uitpluizen hoe deze standaarden helpen bij het veilig maken en houden van de eigen OT. Het is nodig om de bestaande standaarden naar de wensen en eisen van de eigen organisatie te vertalen. Dit vergt tijd, kennis en kunde. De ervaring is dat als dit de eerste keer zorgvuldig wordt gedaan en hieruit voor de organisatie zelf stappen en activiteiten worden geformuleerd, men hier jaren profijt van heeft. Belangrijk om hierin mee te nemen is dat er een keuze gemaakt moet worden aan welke normen men wil voldoen.[7]

Succesfactor. Kies de relevante standaard(en) en vertaal deze op basis van de wensen en eisen naar de eigen organisatie. Dit vergt kennis, tijd en geld maar het belang om dit zorgvuldig te doen wordt door de respondenten benadrukt.

Praktijkvoorbeeld. Een OT-security manager gaf aan het Capability Maturity Model Integration (CMMI) te hanteren. Ondanks dat het CMMI voornamelijk in de IT gebruik wordt zag hij/zij meerwaarde in de toepassing ervan op de OT. De respondent heeft niet verteld op welke manier het model toegepast is. De

[6] Door diverse respondenten is geuit dat het van belang is om een proces in te richten waarmee risico's met gepaste regelmaat gemonitord kunnen worden. Deze stap kan pas gemaakt worden op het moment dat OT-security al onderdeel is van risicomanagementprocessen. Er zijn echter geen concrete succesfactoren naar voren gekomen hoe dit proces in te richten en monitoring een vast onderdeel te maken.

[7] Standaarden en practices die gebruikt worden: ITIL, ISM, VSP, VSE, ISO27001, ISO27002, IEC62443, NIST 800, WEF Maturity model, COBIT, Capability Maturity Model Integration en Management of Change.

toegevoegde waarde voor hem/haar was dat middels het model de organisatie beter in staat was om het actuele en toekomstige OT-security maturiteitsniveau te bepalen.

Praktijkvoorbeeld. Uit standaarden zijn doelstellingen afgeleid voor de organisatie waarvoor het management verantwoordelijkheid moet afleggen. Bijvoorbeeld het behalen van het WEF maturity model niveau 3 (WEF, 2012). Hierdoor kreeg het management een gemeenschappelijk referentiekader om de organisatiedoelstellingen en OT(-security) doelstellingen met elkaar te verbinden.

Werk met bestaande frameworks en standaarden. Aangezien er al veel frameworks en standaarden beschikbaar zijn, wordt herhaaldelijk benadrukt dat organisaties met deze bekende frameworks of standaarden moeten werken. Dit geldt ook voor de eigen bedrijfsprocessen en procedures. Dit betekent dat men ook intern moet kijken welke processen en procedures al lopen om nieuwe maatregelen of standaarden hier op aan te laten sluiten. Dit zorgt dat er aansluiting is bij de medewerkers die er mee moeten werken en dat het gemakkelijker is om het in te bedden in de organisatie.

Succesfactor. Kies bestaande frameworks/standaarden en leer gezamenlijk tijdens het toepassen ervan op de eigen organisatie.

Praktijkvoorbeeld. Om bestaande frameworks en standaarden te hanteren hebben enkele bedrijven de brancheorganisaties aangesproken. Door in dergelijke verbanden bij elkaar te komen wordt kennis uitgewisseld. Dit leverde ook toegevoegde waarde op in de contracten met leveranciers. Men kon gezamenlijk bepalen en beoordelen welke frameworks en standaarden verplicht gesteld zouden moeten worden, waardoor er tussen de opdrachtgever en leverancier *supplier assurance* optrad. Door bundeling van krachten in een branche of sector ontstaan meer mogelijkheden om leveranciers aan te sporen tot meer focus op cybersecurity verbeteringen. Daarnaast bezitten bedrijven in een branche of sector vergelijkbare apparatuur en zijn de frameworks en standaarden direct voor vele bedrijven van toepassing.

Security-by-design. Er is een trend gaande om bij het ontwikkelen of vervangen van OT security-by-design na te streven. Hiermee worden de eigen organisatie, leveranciers en fabrikanten gemotiveerd (vrijblijvend en niet vrijblijvend) om bijvoorbeeld bestaande normen als basis of leidraad te gebruiken en in samenwerking met de opdrachtgever in gesprek te gaan over aanvullende functionele-, beheers- en veiligheidseisen. Het gesprek kan bijvoorbeeld vormgegeven worden door security-by-design principes (OWASP, 2016)[8].

Succesfactor. Medewerkers en management zijn op de hoogte van de kansen die ontstaan wanneer OT vervangen of ontwikkeld wordt. Dit is het moment in de life cycle van OT om security-by-design te implementeren.

[8] Minimize attack surface area, Establish secure defaults, Principle of Least privilege, Principle of Defense in depth, Fail securely, Don't trust services, Separation of duties, Avoid security by obscurity, Keep security simple, Fix security issues correctly.

3.2.2 Inbedding in de organisatie

Het belang van security kan afgelezen worden uit de manier waarop het geborgd is in een organisatie. OT-security kan als project of programma opgepakt worden, terwijl andere organisaties er een aangewezen persoon of afdeling voor hebben.

Van stapsgewijs naar structureel. Het is van belang om stapsgewijs te komen tot OT-security, bijvoorbeeld door te voldoen aan normen uit standaarden of bewustzijn te creëren. Het beperkt houden van de omvang van implementatie-projecten helpt om stapsgewijs uit te breiden en stagnatie in de ontwikkeling of uitbouw van OT-security te voorkomen. Hierbij is het heel belangrijk dat voor verdere ontwikkeling en professionalisering van OT-security, er een moment moet zijn dat OT-security structureel ingebed wordt in plaats van op projectbasis uitgevoerd blijft.[9] Door sommige respondenten is geuit dat OT-security nu in een project opgepakt is, terwijl anderen een OT-security *afdeling* bezitten. Beide organisaties uitten nadrukkelijk de behoefte om het onderwerp structureel te borgen in de organisatie.

3.3 Beheer en onderhoud

De beheer- en onderhoudsprocessen hebben de doelstelling om de betrouwbaarheid, beschikbaarheid, integriteit en veiligheid van de processen te garanderen. Dat beheer- en onderhoudsprocessen ook rekening moeten houden met digitale dreigingen op OT is een relatief nieuw inzicht, zoals in hoofdstuk 2 beschreven. Het belang hiervan en hoe dit het beste in te regelen wordt in de interviews bevestigd.

Assetmanagement op orde. Als randvoorwaarde voor het beschikbaar en veilig houden van het primaire proces, is het van belang om assetmanagement op orde te hebben. Weet wat je in huis hebt en wanneer vervanging nodig is. Als dit op orde is, dan zijn zowel taken als rollen duidelijk, maar kan er ook helder gecommuniceerd worden over wat er nodig is aan beheer en onderhoud. Wanneer het onduidelijk is wat de status is van systemen die een primair proces laten functioneren, is risicobeheersing onmogelijk.

Communicatie over onderhoud en vervanging is cruciaal voor goed assetmanagement om op de lange termijn rekening te houden met kosten en (mogelijke) aanpassingen aan het primaire proces. Daarnaast is goede communicatie van belang om de risico's van onvoldoende overzicht van assetmanagement uit te dragen en de mogelijke consequenties daarvan op het primaire proces. Uit de interviews komt naar voren dat dit besef, dat cyberdreigingen dit effect kunnen hebben, er langzaam komt. Het presenteren van een heldere lange termijn planning voor beheer en onderhoud draagt bij aan het bewust worden en stimuleert om hier ook rekening mee houden.

Succesfactor. Zorg dat je weet wat je in huis hebt en wanneer iets aan vervanging toe is. In de praktijk wordt dit op verschillende manieren vormgegeven.

[9] In veel gesprekken is naar voren gekomen dat het van belang is om stapsgewijs te beginnen en op een gegeven moment OT-security structureel in te bedden. Er zijn echter geen concrete succesfactoren naar voren gekomen hoe van ad-hoc projecten naar structurele inbedding te komen.

Succesfactor. Assetmanagement op orde hebben en hierover communiceren draagt bij aan de bewustwording en daadkracht om veilige OT te bewerkstelligen.

Succesfactor. Aan het management open en helder communiceren wat er in huis is en wanneer dit (op de lange termijn) aan vervanging (of updates) toe is, zorgt voor de juiste investeringsbesluiten en daardoor voor het veiligstellen van OT-systemen.

Praktijkvoorbeeld. Een dashboard beschikbaar maken waarin de volledige en up-to-date Configuration Management Database (CMDB) inzichtelijk is. Men streefde ernaar het dashboard te vullen met zo veel mogelijk informatie, bijvoorbeeld versiegegevens, fabrikant, reparatiegeschiedenis, leverancier, patchinformatie, afhankelijkheden, redundantie, enzovoort. Organisaties kunnen hiermee ruim van tevoren plannen voor een productiestop, vroegtijdig financiële consequenties identificeren, nieuwe functionele eisen opstellen en verantwoordelijke personen en afdelingen aanhaken.

Diversiteit van leveranciers. De afweging of het voordeel van diverse systeemleveranciers opweegt tegen de toenemende complexiteit moet zorgvuldig worden gemaakt. In de industriële automatisering is '*common mode failure'* een bekend en belangrijk begrip. Systemen en processen kunnen door een enkele fout gelijktijdig falen. Diversifiëring kan daarop een antwoord zijn. Het kan echter ook handig zijn om wel eenzelfde leverancier te hebben, zodat systemen goed op elkaar aan kunnen sluiten, en om een goede relatie op te bouwen met de leverancier. Tegelijkertijd kan diversifiëring uitdagingen met zich meebrengen op het gebied van beheer en onderhoud[10].

***In-house*-kennis om mee te kijken.** Het is noodzakelijk om over de schouder mee te kijken bij leveranciers en externe systeembeheerders om de kwaliteit van security te beoordelen. Uiteindelijk kennen de organisatiemedewerkers de eigen processen het beste en kunnen daarom het beste inschatten wanneer een dreiging reëel is. Een randvoorwaarde is wel dat er *inhouse*-kennis is op het onderwerp en om dan ook daadwerkelijk mee te kijken. Het heeft meerwaarde om hierover afspraken te maken in contracten met leveranciers.

Succesfactor. Een organisatie beschikt ten alle tijden over een basis aan kennis over OT(-security) om met externen samen te werken. Dit betekent dat er meegekeken en gedacht kan worden als bijvoorbeeld leveranciers op locatie systemen komen installeren.

Praktijkvoorbeeld. Een van de bedrijven voert aan dat zij in geval van een landelijke crisis zelfstandig willen opereren mocht een leverancier te weinig capaciteit beschikbaar hebben voor al haar klanten. Er bestaat een reële kans dat men in een crisissituatie niet de ondersteuning krijgt die men behoeft. Daarom werd aangegeven dat kennis van systemen zelf opgebouwd moet worden om zelf te kunnen handelen in noodsituaties.

[10] Door diverse respondenten is geuit dat leveranciersmanagement een blijvend punt van aandacht is. De respondenten wegen ieder voor zich af wat de veilige en werkbare balans is tussen interoperabiliteit, security, kosten van OT. Echter, er zijn geen succesfactoren of praktijkvoorbeelden naar voren gekomen voor de praktische uitvoering hiervan.

3.4 Kloof tussen IT- en OT-domeinen

Tijdens een groot deel van de interviews is bevestigd dat er historisch een kloof bestaat tussen het IT- en OT-domein. De kloof uit zich in het verschil in doelstellingen, opvattingen en manieren van werken. Tegelijkertijd is aangegeven dat dit enorm veranderd is en hier hard aan wordt gewerkt. Om stappen te zetten op het gebied van OT-security is goede samenwerking tussen de twee domeinen noodzakelijk en zijn er verschillende succesfactoren naar boven gekomen om dit te kunnen bewerkstelligen. Het gaat aan de ene kant om samenwerking en aan de andere kant om kennisdeling. Deze twee kunnen niet zonder elkaar, maar worden hieronder wel separaat beschreven.

3.4.1 Versterken van de samenwerking

Een van de belangrijkste redenen om IT en OT dichter bij elkaar te brengen, is de noodzaak voor samenwerking omdat de twee werelden steeds meer met elkaar verstrengeld raken. Om het continueren van het primaire proces te waarborgen is het noodzakelijk om de krachten te bundelen. De capaciteit moet goed benut worden en de kennis en kunde ligt in beide domeinen. Er zijn een aantal succesfactoren geïdentificeerd die bijdragen aan het versterken van de samenwerking tussen het IT- en OT-domein.

Verantwoordelijken IT en OT. Het is van belang dat er nauwe samenwerking is tussen de verantwoordelijken voor IT en OT(-security). Als de verantwoordelijken een goed voorbeeld kunnen geven en elkaar vinden, zal dit zich ook vertalen naar de werkvloer. Daarnaast creëert dit bewustzijn dat het belangrijk is om samen te werken. Dit geldt ook voor lijnverantwoordelijken, managers en directeurs. Wanneer dergelijke rollen niet belegd zijn in de organisatie is het een succesfactor om het eigenaarschap wel te de (ver)delen. Uit de interviews komt naar voren dat dit vaak succesvol is als de personen die deze functies bekleden goed met elkaar kunnen samenwerken.

Succesfactor. Zorg dat de IT- en OT-verantwoordelijken samen optrekken. Zo zetten zij een voorbeeld voor het dichter bij elkaar brengen van de domeinen en een eerste stap in die richting.[11]

Praktijkvoorbeeld. Een OT-medewerker met kennis en belangstelling voor kantoorautomatisering is de leidinggevende geworden van een team met daarin IT- en OT-medewerkers. De leidinggevende rapporteert de status van IT en OT-security aan het management. Hierdoor worden specifieke OT werkzaamheden, uitdagingen en oplossingen samen met IT op een gelijkwaardige wijze geadresseerd.

OT en IT in één team. Het is belangrijk om verschillende disciplines in teams samen te brengen, bijvoorbeeld IT, OT en bedrijfskundigen. Dit gaat verder dan hen vragen samen te werken. Het gaat erom dat men bij elkaar zit als één team en op deze wijze samen activiteiten oppakt. Mensen op dezelfde locatie onderbrengen draagt hieraan bij. Dit creëert kruisbestuiving tussen de twee vakgebieden en een menselijke band die de samenwerking ten goede komt. Zo kunnen OT-

[11] Voor het zorgen dat de IT en OT-verantwoordelijken samen optrekken zijn geen specifieke succesfactoren voor naar voren gekomen. Vaak zit het in de soort mensen, een initiatief van de een of juist de noodzaak vanuit het management.

medewerkers bijvoorbeeld leren van gebruikelijke IT-processen (zoals Information Technology Infrastructure Library (ITIL) proces) en kunnen IT-medewerkers leren van de manier waarop OT-medewerkers nadenken over risico's.

Succesfactor. Management erkent de noodzaak voor het combineren van IT-OT kennis en kunde en zorgt ervoor dat IT en OT in dezelfde afdeling werken.

Succesfactor. Een medewerker die ervaring heeft in het IT- en OT-domein ziet de toegevoegde waarde van samensmelting en geeft hier vorm aan.

Succesfactor. Het initiëren van gezamenlijk overleg tussen het IT-en OT-team kan een eerste stap in de vorming van een team zijn en kan bijdragen aan de vorming van de integrale aanpak van cyber security.

Praktijkvoorbeeld. De Chief Information Security Officer (CISO) geeft leiding aan een team waarin IT- en OT-medewerkers samenwerken.

Roulatiemodel van medewerkers. In het verlengde van een gezamenlijk team opstellen, draagt een roulatiemodel van medewerkers bij aan de kruisbestuiving van kennis en kunde. Hierbij is het waardevol goed te kijken naar de verschillende disciplines en competenties van medewerkers om tot een goede mix van mensen te komen die complementair aan elkaar zijn.

Succesfactor. Zet een pool op van mensen die elkaar kunnen vervangen. Zorg dat IT- en OT-kennis door meerdere mensen in deze pool toegepast kan worden.

Dezelfde functiewaardering. Het is aanbevolen om IT- en OT-medewerkers in dezelfde functiewaardering (salaris) te plaatsen. Dit komt de samenwerking én de waardering voor elkaar ten goede. De reden die gegeven is voor de onbalans tussen functiewaarderingen stamt uit het verleden. Toen IT zijn opmars maakte in bedrijven zijn er veel IT-medewerkers aangenomen. Zij hebben destijds betere voorwaarden kunnen bedingen en hebben door kunnen groeien in de loop der jaren. Voor OT-medewerkers is deze groei soms achtergebleven. Deze ongelijkheid zorgt dan voor frictie. Dit bewust rechttrekken heeft positieve effecten op hoe men met elkaar omgaat en zorgt voor betere samenwerking.

Succesfactor. Het management is uiteindelijk de factor die besluit om verandering teweeg te brengen. Het is daarom nodig dat het management zich realiseert dat het verschil in functiewaarderingen de samenwerking niet ten goede komt en besluit dit aan te passen.

Praktijkvoorbeeld. De discrepantie tussen IT- en OT-functiewaarderingen is bij een van de organisaties direct opgeheven nadat dit bekend werd. De organisatie merkte dat de waardering tussen IT- en OT-medewerkers verbeterd is.

3.4.2 Bevorderen van kennisdeling

Het dichter bij elkaar brengen van IT- en OT-domeinen is om kennisdeling te bevorderen. Aangezien steeds meer processen in de organisaties worden geautomatiseerd, er steeds meer gebruik wordt gemaakt van slimme apparaten en steeds meer data met elkaar wordt gekoppeld, is kennis van het IT-domein nodig. Daarnaast is er kennis van de operationele techniek nodig om de automatisering

goed in te regelen en te duiden wanneer processen risico lopen. Het is belangrijk om aandacht te besteden aan het samenbrengen van IT- en OT-medewerkers om zo expertise te delen. Mensen zijn immers de spil in kennisdeling. De tijd en het geld dat hiervoor nodig is moet ook gegund worden.

Ruimte voor persoonlijkheden die graag kennis uitdragen. Er zijn altijd mensen die de eigen kennis graag willen uitdragen. Het meemaken van het enthousiasme, de kennis en ervaring van collega's zorgt voor ontwikkeling. Laat zo verhalen door de organisatie gaan. Dit kunnen succesverhalen zijn of juist het tegenovergestelde, zo blijft men leren. Het is hier van belang dat er echt de tijd voor gegeven wordt en dat er vanuit het management wordt gestuurd op deze kennisdeling. Het blijven zitten op kennis (kennis is macht) moet positief ontmoedigd worden.

Succesfactor. Geef collega's die graag kennis uitdragen de ruimte en gelegenheid daarvoor.

Succesfactor. Door kennisdeling onderdeel te maken van de functioneringsgesprekken worden individuele medewerkers gestimuleerd en uitgedaagd om hierin uit te blinken.

Praktijkvoorbeeld. Een van de organisaties heeft een parttime docent in het gezamenlijke team. Dit teamlid heeft van nature de behoefte om kennis te delen en is daarmee zeer waardevol voor het hele team.

Praktijkvoorbeeld. Kennisdeling vindt actief (rondgang in de organisatie) en passief plaats (artikelen, rapporten, elektronisch (via een bedrijfs-wiki)).

Kennisdeling en informatie-uitwisseling buiten de organisatie om.
Cybersecurity is een allesbehalve statisch onderdeel van de bedrijfsvoering. Ontwikkelingen die vandaag niet van toepassing lijken op het eigen bedrijf kunnen morgen wel relevant zijn. Daarom is het leren van anderen zo belangrijk. Alle organisaties geven aan dat het vergaren van kennis buiten de deur cruciaal is om bij te blijven en tijdig aanpassingen te kunnen doen. Elkaar opzoeken zorgt voor kruisbestuiving tussen de medewerkers van verschillende (concurrerende) organisaties. Dit gebeurt zowel informeel als formeel en wordt door individuen zelf ingericht.

Succesfactor. Het face-to-face deelnemen aan (nationale en internationale) bijeenkomsten zorgt voor kennisdeling buiten de eigen praktijken om.

Succesfactor. Een informeel netwerk met gelijkgestemden (binnen en buiten de eigen sector) draagt bij aan het delen van kennis en het up-to date houden ervan.

Praktijkvoorbeeld. Bedrijven nemen veelal actief deel aan (nationale en internationale) werkgroepen en *information sharing and analysis centers* (ISAC).

Zelfde soort programma's en apparatuur gebruiken. Het is nuttig wanneer medewerkers zo veel mogelijk met elkaars technieken, interfaces, apparatuur en tooling in aanraking komen. Zo kunnen monteurs uit de OT kennis nemen van deze IT programma's en apparatuur en komen de verschillende medewerkers hierover

met elkaar in gesprek. Dit werkt beide kanten op. Dit draagt bij aan kennisdeling en een betere verstandhouding tussen IT- en OT-medewerkers.

Succesfactor. Het is van toegevoegde waarde om door het management het gebruik van homogene programma's en apparatuur te laten ondersteunen en hier een doelstelling van te maken.

Succesfactor. Het streven naar standaardisatie van programma's en apparatuur kan het beste worden vormgegeven in de life cycle management processen.

Succesfactor. Uit de resultaten komt geen succesfactor naar voren hoe de keuze gemaakt wordt voor dezelfde soort programma's en apparatuur. Wel kan life cycle management in combinatie met wat er aangeboden wordt in de markt invloed uitoefenen op deze keuze en is het van belang om de functionele eisen vanuit IT en OT op te stellen en uit te zetten.

Praktijkvoorbeeld. Een van de respondenten gaf aan actief te streven naar programma's en apparatuur die door zowel IT- en OT-medewerkers gebruikt kan worden. Dit heeft zich geuit in bijvoorbeeld statische netwerk monitoring. Deze dienst is gebruikt in de gehele organisatie om vreemde netwerkcommunicatie patronen van alle aangesloten apparaten te herkennen. Netwerk monitoring informatie gaat bijvoorbeeld naar het interne SOC. Bijvangst hiervan was dat deze informatie ook programmeerfouten in een SCADA systeem blootlegde. Het oplossen ervan verhoogde uiteindelijk de robuustheid van het primaire proces.

Streven naar begrijpelijke taal voor iedereen. Taalgebruik, terminologie en vakgebieden verschillen binnen een organisatie en een veelvoorkomende consequentie is dat men elkaar minder goed begrijpt. Dit komt de kennisdeling niet ten goede. Hier moet rekening mee gehouden worden in de (onderlinge) communicatie. Het is belangrijk jargon te vermijden en te streven naar het aan elkaar uitleggen van procedures, producten en werkwijzen[12].

Praktijkvoorbeeld. Een bedrijf met vestigingen wereldwijd gaf aan de awareness trainingen in de lokale taal te geven en in persoon. Het gebruik van (Engelse) *e-learning* bleek op den duur namelijk niet effectief. Daarnaast bleek het organiseren van een cybersecurity dag met niet-technische onderwerpen die op een interactieve manier werden gepresenteerd zeer waardevol. Het doel was om medewerkers op een positieve manier kennis te laten maken met het onderwerp door praktische (quiz en uitnodigen van hackers) en aansprekende (crisissimulatie) voorbeelden uit de eigen organisatie.

3.5 Kennis en kunde van OT-security

Kennis en kunde is nodig om OT-security in de organisatie op te nemen, zowel het volledig oprichten als het doorontwikkelen. Dit is van belang omdat het institutioneel geheugen van organisaties vaak tekort schiet en kennis die beschikbaar was op den duur vervaagt. Daarnaast is het van belang omdat bepaalde kennis niet

[12] Door diverse respondenten is geuit dat men elkaar soms niet begrijpt en dat het van belang is om rekening te houden met de ontvanger, bijvoorbeeld de functie, afdelingen, kennisdomein en cultuur. Er zijn echter geen concrete succesfactoren naar voren gekomen die hier praktische uitvoering voor kunnen bieden.

(voldoende) aanwezig is binnen organisaties. Kennisvergaring gebeurt zowel door eigen mensen op te leiden als door kennis in te kopen. Dat dit cruciaal is wordt in de interviews beaamd.

3.5.1 Vergaren en versterken van kennis en kunde

Zowel technische kennis en kunde van OT als cybersecurity kennis in zijn algemeenheid is cruciaal om digitaal veilige OT in te regelen. Deze kennis en kunde is er niet altijd voldoende en er zijn verschillende manieren naar voren gekomen om deze kennis en kunde te vergaren.

Eigen mensen binnenhalen en opleiden. Een belangrijke reden om eigen mensen op te leiden (in-house expertise) is om niet afhankelijk te zijn van externe expertise en leveranciers. Zeker niet op het moment van een incident waarbij externen waarschijnlijk overvraagd of niet op de hoogte zijn van de bijzonderheden in het productieproces. Daarnaast gaan ontwikkelingen snel door het dynamische karakter van cybersecurity en is er behoefte om continu kennis en kunde te vergaren. Er moet ruimte zijn voor medewerkers die uit eigen interesse hun kennis willen vergroten. Daarnaast is actief beleid nodig om ontbrekende kennis aan huidige medewerkers bij te brengen.

Succesfactor. Weet welke kennis benodigd is voor veilige OT en werf hier actief op.

Succesfactor. Geef ruimte aan medewerkers die uit eigen interesse willen groeien en die vooroplopen in de benodigde kennis.

Succesfactor. Reserveer middelen om medewerkers voortdurend bij te scholen.

IT-en OT-security deskundigheid. Het is van meerwaarde om medewerkers die de organisatie door en door kennen en die deskundigheid met leiderschap samen brengen met elkaar te verbinden. Dit is cruciaal omdat op deze wijze jarenlange operationele ervaring, eigen interesse en gevoel voor leiderschap bij elkaar worden gebracht. Het is lastig balans te vinden tussen het management en de operatie, maar dit is precies het vlak waar duiding, bewustzijn en keuzes gemaakt kunnen worden. Als een CISO ‘nieuw’ in de organisatie is en dus nog geen natuurlijke autoriteit is, is het van belang een team samen te stellen waarin de verschillende expertises bijeenkomen om deze deskundigheid toch te hebben.

Succesfactor. Maak gebruik van medewerkers die de organisatie door en door kennen en zet hen voorop in het verspreiden van de benodigde deskundigheid.

Succesfactor. De diversiteit van de competenties en deskundigheid van de medewerkers moet inzichtelijk en beschikbaar zijn voor een CISO. Organiseer de (face-to-face) interactie die hiervoor benodigd is en kennis en kunde kan versterken.

Praktijkvoorbeeld. De CISO-functie bevatte niet alle benodigde IT-en OT-expertise en ervaring. Er is doelbewust gekozen in plaats van één person een team samen te stellen waardoor de diverse disciplines in een klap vertegenwoordigd waren.

Gezamenlijk oefenen. Om kennis en kunde bij te brengen zijn oefeningen cruciaal. Hierbij is het van belang om meerdere medewerkers uit verschillende disciplines te betrekken. Zo kan er kruisbestuiving plaatsvinden en kan eenieder leren. Laat bijvoorbeeld een OT-security medewerker deelnemen aan een algemene crisisoefening, om specifieke OT risico's en consequenties van het falen van systemen mee te nemen. Binnen het cybersecurity-domein is het soms lastig te komen tot realistische dreigingen en wordt het nog moeilijker om hier dan op te acteren. Betrek daarom al tijdens het formuleren van scenario's deze OT-security specialisten, om tot realistische scenario's te komen.

Succesfactor. Ontwikkel een *ingrijpend* en *realistisch* scenario, oefen het reactieplan en evalueer hoeveel tijd er nodig is om de procesautomatisering weer volledig te herbouwen. Dit gezamenlijk doen zorgt voor het vergaren en versterken van kennis en kunde.

Praktijkvoorbeeld. Een van de respondenten waarbij het IT- en OT-team al samengevoegd is gaf aan dat daardoor de Ontwikkel-Test-Acceptatie (OTA)-omgeving een gezamenlijke activiteit geworden is. Dit droeg onder andere bij aan het implementeren van meer security-by design principes, en het uitvoeren van oefeningen en audits werd erdoor vergemakkelijkt.

Assessments met expertise. Assessments zijn van grote toegevoegde waarde omdat er met een 'blik' van buiten naar de organisatie gekeken wordt en hiermee blinde vlekken inzichtelijk worden gemaakt. Het is van belang om assessments uit te voeren met deskundigen die zowel de OT-problematiek beheersen als medewerkers erbij te betrekken die de installatie door en door kennen. Het is van toegevoegde waarde om deze assessments niet slechts als een check te zien, maar als een kans om de eigen organisatie veilig te stellen. Hierin kan een organisatie ook zelf een eerste stap nemen en bepalen waarop de assessments geënt moeten worden om een veilige OT te garanderen.

Succesfactor. Betrek OT-specialisten bij assessments.

Praktijkvoorbeeld. Een van de organisaties gaf aan dat de assessments vaak een papieren exercitie zijn, waarbij dit vaak door mensen wordt gedaan die niet zelf uit de OT komen, of er geen diepgaande kennis van hebben. Door niet naar de installaties zelf te gaan en de actuele situatie te bekijken, blijven assessments in algemeenheden hangen. Om dit te realiseren is het van groot belang dat de personen die assessments uitvoeren inhoudelijke kennis van zaken hebben.

3.5.2 Versterken aandacht van management

Om kennis en kunde te ontwikkelen, is het van belang dat de noodzaak hiervan ook bij het management bekend is. Het kost tijd en geld om mensen op te leiden, naar bepaalde conferenties te laten gaan en hun netwerk op peil te houden.

Het belang en toegevoegde waarde van OT-security wordt door het management uitgedragen[13]. Het management moet OT-security begrijpen en uitdragen in de organisatie. Dit is van belang omdat het management kan sturen op hoe OT-security in de organisatie in te regelen. Wordt er besloten om IT en OT

[13] Het kan ook van toegevoegde waarde zijn als aandeelhouders, in algemene cybersecurity zin, het belang en de toegevoegde waarde van digitaal veilige OT uitdragen en ondersteunen.

samen te zetten? Hoeveel tijd en geld wordt er vrij gemaakt voor opleidingen? En het aannemen van nieuwe mensen met bepaalde expertise?

Succesfactor. Borg OT-security als een jaarlijkse bedrijfsdoelstelling.

Succesfactor. Het management faciliteert het delen van ervaring en kennis op dit onderwerp met andere bedrijven.

Praktijkvoorbeeld. Het onderbrengen van OT-cybersecurity in een van de jaarlijkse bedrijfsdoelstellingen is bij een van de deelnemende organisaties zeer effectief gebleken. De COO was hierbij degene die OT-cybersecurity-doelstellingen verplicht liet opnemen. Deze centrale aanpak is interessant aangezien in operationele organisaties cybersecurity vaak als kostenpost (bedreiging) wordt gezien, terwijl aandacht voor het onderwerp bij het management ook besproken kan worden in termen van kansen.

Praktijkvoorbeeld. De OT(-security) lead legt *zelf* belangrijke informatie uit aan het management. Hiermee wordt het management beter in staat gesteld om het belang van OT-security in te zien. Respondenten gaven aan dat een randvoorwaarde is dat deze persoon gezaghebbend is op het onderwerp en door het management ook als zodanig wordt erkend.

Audits creëren aandacht. Het is van belang om audits te zien als een hulpmiddel om de eigen organisatie volwassener te krijgen in OT-security. Audits brengen mogelijke kwetsbaarheden naar voren. Dit is het startpunt geweest voor velen om aandacht te besteden aan OT-security. Daarnaast kunnen de resultaten van audits goed gebruikt worden om aandacht van het management voor OT-security onderwerpen te krijgen en hierin ook een overwogen keuze te nemen over wat wanneer wordt opgepakt. Audits worden meestal door externe partijen uitgevoerd. Daarbij worden gangbare technieken, zoals penetratietesten, gebruikt om de werkelijke weerbaarheid te toetsen. Natuurlijk worden ook de processen en mensen onder de loep genomen. Goede auditeurs gebruiken een set met actuele en relevante audit *controls* waarop getoetst wordt. In het algemeen eindigen de rapporten op de bureaus van het hoogste management en dat creëert aandacht.

Succesfactor. Gebruik audits om de mogelijke kwetsbaarheden als startpunt te gebruiken om OT-security onder de aandacht te brengen bij het management.

Praktijkvoorbeeld. Een van de respondenten gaf aan dat de uitkomsten van deze succesfactor ervoor zorgden dat de manager van een productieomgeving de risico’s niet meer begreep; ze bleken namelijk te technisch waardoor de resultaten van de audit nooit uitgevoerd zijn. Dit probleem is verholpen door de lokale teams verantwoordelijkheid te geven. Bijvoorbeeld voor het opvolgen van de bevindingen in de audits.

Praktijkvoorbeeld. Een ander voorbeeld uit de praktijk is het bepalen van de audit *controls* waarop getoetst wordt. Bedrijven uit een bepaalde sector hebben gezamenlijk bepaald welke van de regels uit relevante standaarden voor deze bedrijven als minimale vereiste opgenomen moesten worden. Iedere sector of verzameling van bedrijven zou dezelfde actie kunnen ondernemen om hun eigen set aan regels te definiëren.

4 Aan de slag met OT-security

In hoofdstuk 3 zijn diverse succesfactoren en praktijkvoorbeelden geïdentificeerd om bepaalde OT-security uitdagingen aan te pakken. Hiermee kunnen organisaties zelf kijken welke succesfactoren bijdragen aan de eigen OT-security inbedding. Ook kan men inspiratie opdoen door de voorbeelden. Om de succesfactoren in praktijk te kunnen brengen, zijn er in dit hoofdstuk basisaspecten geformuleerd voor de eerste stappen om OT-security in te richten (4.1). Daarnaast zijn er vragen geformuleerd die organisaties zichzelf kunnen stellen voor verdere invulling van OT-security (4.2).

Een organisatie kan met de basisaspecten en vragen voor verdere invulling inzicht krijgen in hoe men met OT-security bezig is. Deze basisaspecten en vragen gaan in op thema's[14] die naar voren zijn gekomen uit de analyse en geven inzicht in waar men mee kan starten, of er onderwerpen zijn voor verbetering en hoe men van anderen kan leren. Er wordt dus onderscheid gemaakt tussen basisaspecten waar iedere organisatie mee aan de slag kan en vragen waar organisaties mee aan de slag kunnen als men al het een en ander aan OT-security heeft ingeregeld en zoekt naar verdere invulling.

4.1 Aan de slag met OT-security aan de hand van basisaspecten

Om OT-security in te bedden in een organisatie, zijn er aspecten (niet uitputtend) naar voren gekomen die bijdragen aan de basisinrichting van OT-security. Niet alle basisaspecten zijn essentieel. Het zijn aspecten die door andere organisaties zijn genoemd die bijdragen aan OT-security en waar elke organisatie een eigen afweging in kan maken. In tabel 1 volgt een opsomming (niet volgordelijk) van deze basisaspecten naar thema.

Tabel 1 Basisaspecten voor het inrichten van OT-security.

Thema's	Basisaspecten
Basismaatregelen	
	• Werk met bestaande frameworks en standaarden. • Vertaal standaarden naar de wensen en eisen van de organisatie. • Maak zo ver als mogelijk gebruik van maatregelen die bekend zijn bij medewerkers.

[14] Er is één extra thema – communicatie – dat apart wordt uitgelicht, naast de thema's die in hoofdstuk twee zijn geïdentificeerd. De reden hiervoor is dat voor meerdere van de thema's succesfactoren naar boven zijn gekomen over communicatie.

Thema's	Basisaspecten
OT-security risico's	
	• Cybersecurity voor je OT is een vast onderdeel van je risicomanagement. • Weet waar je management van wakker ligt. • Gebruik incident voorbeelden om risico's voor je OT inzichtelijk te maken. • Creëer en gebruik ingrijpende en realistische scenario's. • Gebruik audits om OT-security onder de aandacht te brengen en te verbeteren.
Kloof IT en OT	
	• De IT- en OT-verantwoordelijken werken samen (als zij niet dezelfde persoon zijn). • De IT- en OT-medewerkers werken samen aan primaire processen. • De IT- en OT-medewerkers werken en/of overleggen geregeld op dezelfde fysieke locatie.
Kennis en kunde	
	• Ruimte en tijd worden geboden om kennis te delen met collega's om te weten wat er speelt. • Ruimte en tijd worden geboden om ontwikkelingen, incidenten en andere informatie bij te houden. • De medewerkers weten dat OT-security het primaire proces ondersteunt. • De organisatie weet welke mensen welke OT-security deskundigheid bezitten. • De organisatie weet welke kennis er wel en niet in huis is en heeft handelingsperspectief om hier mee om te gaan.
Communicatie	
	• Plaats OT-security kansen en bedreigingen in context van de organisatie en in de taal van de ontvanger(s). • Communicatie over OT-security onderwerpen wordt aangepast op basis van verschillende doelgroepen zodat de informatie aansluit. • Deel de actuele security (risico) status met het management.
Beheer en onderhoud	
	• Creëer bewustzijn van de levensduur van OT en de (mogelijke) consequenties die dit met zich meebrengt. • Breng de eventuele afhankelijkheden van leveranciers in kaart. • Creëer de capaciteit in de eigen organisatie om de kwaliteit van OT-security te beoordelen. • Breng alle OT-systemen in kaart.

4.2 Verdere invulling van OT-security

Naast de basisaspecten zijn er een aantal vragen geformuleerd die elke organisatie zichzelf kan stellen. Deze vragen geven richting aan de verdere invulling van OT-security in de eigen organisatie. Deze vragen gaan dieper in op de thema's en kunnen dienen als reflectie voor organisaties die al aan de slag zijn met de basisaspecten uit tabel 1. In tabel 2 volgt een niet volgordelijke opsomming.

Tabel 2 Vragen voor verdere invulling van OT-security.

Thema's	Stel jezelf de volgende vragen
Basismaatregelen 	• Trek je op met branchegenoten in de keuze en toepassing van frameworks, best practices en standaarden? • Zijn er standaarden omgezet naar de wensen en eisen voor je eigen organisatie?
OT-security risico's 	• Ben je er bij gebaat als OT-security structureel ingebed wordt in je organisatie? • Is OT-security aangesloten bij het BCM? En bij huidige safety processen? • Zijn de OT-security risico's gerelateerd aan de organisatiedoelen? • Neem je de risico's van cybersecurity mee in (investerings)besluiten? • Worden alle organisatielagen betrokken wanneer investeringen beraamd worden? • Ben je tevreden met de aandacht voor de audits voor OT-security?
Kloof IT en OT 	• Werken IT- en OT-medewerkers wel eens met elkaar op dezelfde fysieke locatie? • Is IT en OT bij jouw organisatie in één team belegd? • Worden IT- en OT-medewerkers op dezelfde manier beoordeeld en ingeschaald? • Wordt er in je organisatie gezamenlijk geoefend met IT en OT?
Kennis en kunde 	• Is je organisatie deelnemer aan relevante werkgroepen en overleggen om op de hoogte te zijn van dreigingsinformatie en lessen van anderen? • Weet je of de essentiële deskundigheid voor veilige OT redundant aanwezig is? • Werf en selecteer je bewust op kennis die de organisatie nodig heeft? • Is er in jouw organisatie ruimte voor OT-opleidingen?

Thema's	Stel jezelf de volgende vragen
Communicatie 	• Worden OT-security bedreigingen, maatregelen en risico's door iedereen begrepen? • Lever je oplossingen die door niet technische medewerkers begrepen kunnen worden? • Heeft ooit een communicatiemedewerker meegekeken met interne berichtgeving? • Is je communicatie over cybersecurity risico's voor OT gestructureerd of ad hoc?
Beheer en onderhoud 	• Heb je de mogelijkheid om informatie over je assets op te roepen in een overzicht? • Ben je voorbereid op het toepassen van security-by-design principes op het moment dat OT vervangen wordt? • Houd je de status van je OT-systemen bij (betrouwbaarheid, beschikbaarheid, integriteit en veiligheid)? • Communiceer en acteer je op de kennis die je hebt over je assets, kansen en bedreigingen? • Gebruik je een assetoverzicht om investeringsbesluiten te ondersteunen?

5 Conclusie

Het belang van OT-security neemt toe gezien de groeiende OT-automatisering en gezien het toenemende bewustzijn van de risico's hiervan voor het continueren van het primaire proces.

De belangrijkste uitdagingen voor het inbedden van OT-security zijn:

- De uitdaging om het management het belang van cybersecurity voor OT te laten onderkennen en hiermee de obstakels om OT-risico's in huidig risicomanagement te duiden.
- De uitdaging om de bestaande (basis)maatregelen voor digitaal veilige OT ook echt in de eigen organisatie in te bedden.
- De historisch ontstane kloof tussen IT- en OT-domein onderkennen als uitdaging, waardoor de behoefte voor het dichten van deze kloof om digitaal veilige OT te borgen duidelijk wordt.
- De veelvoorkomende uitdaging dat de juiste kennis en kunde ontbreken of niet voldoende aanwezig zijn. Deze kennis en kunde in de eigen organisatie is wel nodig om het bewustzijn van de risico's van onveilige OT te vergroten en hierin ook stappen te kunnen zetten.
- Praktische uitdagingen in het beheer en onderhoud van OT die het mitigeren van OT-cybersecurity risico's belemmeren.

Uit de interviews blijkt dat een groot aantal organisaties serieus aan de slag is met OT-security. Dit is te zien in het grote aantal succesfactoren die door organisaties naar voren is gebracht (zie bijlage C voor het overzicht). Deze succesfactoren kunnen gebruikt worden door organisaties om hun OT-security verder vorm te geven. Daarnaast geven de basisaspecten en vragen deze organisaties de gelegenheid om bij zichzelf na te gaan hoe zij OT-security in hun eigen organisatie verder kunnen verbeteren.

Met de geïdentificeerde uitdagingen en gevonden succesfactoren kunnen organisaties en het NCSC aan de slag om deze verder te toetsen, aan te vullen en te prioriteren.
`

6 Referenties

ANSSI, Agence nationale de la sécurité des systèmes d'information, Managing Cybersecurity for Industrial Control Systems; Cybersecurity for Industrial Control Systems, 2012.

Applied Risk, The State of Industrial Cybersecurity, 2019.

Colbert and Kott, Cyber-security of SCADA and Other Industrial Control Systems, 2016.

CSBN, Cybersecuritybeeld Nederland, Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), 2019.

Cybersecurity Raad CSR, Handreiking Cybersecurity voor de bestuurder, 2018.

GE Electric, An Executive Guide to Cybersecurity for Operational Technology, 2017.

Kaspersky, The State of Industrial Cybersecurity, 2018.

Kaspersky, The State of Industrial Cybersecurity, 2019.

Luiijf en te Paske, Cybersecurity of Industrial Control Systems, TNO, Global Conference on Cyberspace, 2015. URL: http://publications.tno.nl/publication/34616507/KkrxeU/luiijf-2015-cyber.pdf

Macaulay and Singer, Cybersecurity for Industrial Control Systems, 2012.

MITRE Corporation, Assessment of Operational Energy System Cybersecurity Vulnerabilities, 2018.

National Institute of Standards and Technology NIST, Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, 2015.

OWASP, Security by Design Principles, Open Web Application Security Project, 2016. URL: https://www.owasp.org/index.php/Security_by_Design_Principles

Ponemon Institute (sponsored by TÜV Rheinland Opensky Inc.), Safety, Security & Privacy in the Interconnected World of IT, OT & IIoT, febuari 2019.

SANS Institute, Secure Architecture for Industrial Control Systems, 2014.

SANS Institute, SANS 2019 State of OT/ICS Cybersecurity Survey, 2019.

Swedish Civil Contingencies Agency MSB, Guide to Increased Security in Industrial Information and Control Systems, 2014.

Trend Micro, New Critical Infrastructure Facility Hit by Group Behind TRITON, 2019.

TU Delft, Building Cybersecurity Awareness: The need for evidence-based framing strategies, 2017.

Universiteit Twente, Online Discoverability and Vulnerabilities of ICS/SCADA Systems in the Netherlands, 2019. URL: https://ris.utwente.nl/ws/portalfiles/portal/124347608/wodc_report_scada_final.pdf

World Economic Forum, WEF, Partnering for Cyber Resilience, Risk and Responsibility in a Hyperconnected World - Principles and Guidelines (2012). URL: http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf

7 Ondertekening

Den Haag, november 2019

Drs. K.Y. de Jong
Research Manager

TNO
Networked Organisations

P. van den Brink MSc
Auteur

A Interview protocol

Interviewprotocol

#	Onderzoeksvraag	Achtergrond	Checkvragen	Doel van de vraag	OT	Mngt
1	Wanneer, waardoor en hoe bent u gestart met OT-cybersecurity in uw onderneming?	Triggers kunnen bijvoorbeeld incidenten, regelgeving, nieuwsberichten, seminars, gesprekken met anderen (bv binnen de sector) of verstrekte sectorale dreigingsinfo zijn geweest. Het kan ook zijn dat intern, bottom-up, vanuit de OT of IT de interesse is ontstaan. Het antwoord op de 'hoe vraag' geeft inzicht in de initiële (uitdagende) inbedding van het onderwerp in de organisatie.	Werd het onderwerp OT-security direct als relevant gezien of is er eerst gekeken of het relevant was voor uw organisatie? Indien het laatste, hoe hebt u dan de relevantie bepaald?	Begrijpen welke triggers zo significant waren om met OT-cybersecurity te starten	√	√
	OT en cybersecurity in uw organisatie					
2	Hoe omschrijft u het OT in uw organisatie?	OT zou het geheel van alle systemen moeten zijn die tezamen zorg dragen voor aansturing, monitoring en communicatie van productie installaties. Dus naast typische instrumentatie automatisering (bv ICS-SCADA) zouden bijvoorbeeld ook elektrische installaties (switchboards), draaiende units (compressoren en generatoren) en koelsystemen er onder moeten vallen. Kortom alles dat het primaire productieproces kan verstoren.	Kunt u vertellen welke processen binnen uw bedrijf door OT aangestuurd worden? (Voorbeelden: primaire productie, utilities, elektra voorziening, interface met andere domeinen)	Wordt er wel altijd hetzelfde verstaan onder OT en is daarmee de omvang van al dan niet een succesvolle invoering van OT security vergelijkbaar tussen organisaties?	√	
3	Waar bent u bang voor? Wat zijn de effecten als uw OT geraakt wordt?	Dreigingen zouden kunnen zijn: Effecten kunnen betrekking hebben op financiële, veiligheid, milieu, ontwrichting en evt. reputatie consequenties.	Is de vereiste beschikbaarheid van uw dienst formeel vastgelegd en zo ja hoe heeft dit de invulling van OT-cybersecurity maatregelen beïnvloed?	Is het dreigingsbeeld binnen verschillende lagen in de organisaties gelijk? Wat zegt, in relatie tot de andere antwoorden, een verschil in dreigingsbeeld over de mate van volwassenheid in een organisatie.	√	√
4	Welke thema's zijn naar uw oordeel het meest relevant voor een beheersbare OT-omgeving in het algemeen en waarom vindt u dat? Komen deze thema's voldoende terug in de gangbare OT-cybersecurity standaarden?	Zijn de gebruikelijke thema's als risico management, incident management, training van personeel etc. de bepalende thema's of zien we iets over het hoofd? Insteek van de vraag is om met een open vizier naar bepalende thema's te vragen	Welke aspecten rondom OT-cybersecurity mist u in hedendaagse discussies en publicaties?	Zijn de bekende thema's inderdaad de alles bepalende thema's voor een beheersbare OT?	√	

#	Onderzoeksvraag	Achtergrond	Checkvragen	Doel van de vraag	OT	Mngt
	Risico management					
5	Hoe heeft uw organisatie risico management geformaliseerd?	Worden cybersecurity risico's gelinkt aan de organisatiedoelen? Zijn deze risico's uitgedrukt in effecten en impact of anders? Hoe houdt uw organisaties zich steeds geïnformeerd over (nieuwe) dreigingen die relevant voor uw bedrijfsvoering of sector zijn?	Welke risico analyse methodiek gebruikt u en hoe bepaalt u wat acceptabele risico's zijn?	Alle standaarden zijn gericht op risico gebaseerde besluitvorming. Is dit ook de implementatienorm, is deze norm ook implementeerbaar en welke implementatievorm is werkbaar?	√	
6	Hoe meet uw organisatie OT-cybersecurity risico's en welke interne disciplines zijn daarbij betrokken?		Doet u een analyse op het niveau van object , installatie, alle installaties ineens?	Nagaan welke risico meet methodiek werkt en op welke manier.	√	
7	Hoe worden gevonden risico's binnen de organisatie naar de diverse doelgroepen gecommuniceerd en hoe vindt risico gebaseerde besluitvorming (investering-planning-kennis) plaats?		• Hoe zorgt uw organisatie er voor dat OT-cybersecurity risico's onder de aandacht blijven van het management en de medewerkers? • Hoe frequent communiceert u risico's aan de directie?	Welke factoren bepalen dat geïdentificeerde risico's ook daadwerkelijk leiden tot passende maatregelen	√	√
	Organisatie					
8	Hoe heeft u de benodigde kennis verworven om beleidsmatige keuzes te kunnen maken om aan OT-cybersecurity te doen?	Cursussen, kennisdeling met andere bedrijven, externe dienstverleners, zelfstudie	Wie beheert het juiste kennisniveau voor de verschillende rollen in uw organisatie?	Nagaan welke methode van kennisvergaring effectief is gebleken.	√	
9	Hoe werken de IT security afdeling en OT-engineering samen? Welke aanpak hebt u gebruikt om de samenwerking, indien aanwezig, succesvol te laten zijn?	Beheer in een continue (heterogeen) proces is wezenlijk anders dan in een discontinue (homogene) omgeving. Dat vereist begrip voor en kennis van de andere discipline.	Hoe hebben de verschillende disciplines kennis over elkaars vakgebied verkregen? Welke uitdagingen bent u in de samenwerking tussen disciplines tegengekomen en hoe bent u hiermee omgegaan?	Samenwerking blijkt heel uitdagend door het verschil in cultuur. Nagaan welke hordes geslecht moeten worden en hoe dit effectief kan worden aangepakt.	√	√

#	Onderzoeksvraag	Achtergrond	Checkvragen	Doel van de vraag	OT	Mngt
	Standaarden					
10	Van welke OT CS standaarden maakt uw organisatie gebruik? Wat waren de afwegingen om juist voor deze standaard(en) te kiezen? Hoe bruikbaar zijn de standaarden gebleken?	IEC 62443 ISO 27000 serie NIST 800 …. Eigen standaard samengesteld uit ……. Welke onderdelen uit bovengenoemde standaarden waren relevant?	Wat voor kennis en kunde was er nodig om afwegingen te maken om een bepaalde standaard te kiezen? En ook, wat voor kennis en kunde was of is er nodig om een bepaalde standaard te implementeren en te vertalen naar de eigen organisatie doelen (bruikbaarheid).	Wat is de bepalende factor in het zinvol kunnen toepassen van lijvige implementatiestandaarden .	√	
11	Welke stappen in OT-cybersecurity volwassenheid onderkent u en hoe bepaalt u het gewenste volwassenheidsniveau voor uw organisatie?		Als er gevraagd wordt naar uw OT-cybersecurity , welke volwassenheidscriteria zouden dan bekeken moeten worden?	Hoe bepaald een organisatie, als onderdeel van een risico management framework, wat een acceptabel risiconiveau is.	√	√
12	Welke succesfactoren voor een volwassen OT (dus niet alleen m.b.t. cybersecurity) kunt u vanuit uw eigen ervaring benoemen?	Cybersecurity is één van de vele beheers onderwerpen in de OT. Succesfactoren voor de andere OT-aspecten kunnen ook van toepassing zijn op cybersecurity	Hoe zorg u ervoor dat het OT de gewenste functionaliteit, beschikbaarheid en kosteneffectiviteit behoudt?	Wat zijn succesfactoren in de volle OT breedte die mogelijk onderbelicht zijn voor cybersecurity, maar uiteindelijk wel heel bepalend kunnen zijn.	√	
13	Is OT-cybersecurity opgenomen in de lange termijn planning (5 jaar en meer) van uw organisatie? Op welke manier?	OT-security zal als onderdeel van goed risico management ‘ever green’ gehouden moeten worden. Dus steeds aanpassen aan nieuwe dreigingen en risico’s.	Hoe houdt u rekening met vervanging van OT-systemen?	Hoe gaat de organisatie om met het besef dat cybersecurity aanpassingen en investeringen blijvend zijn. Hoe is het besef verankerd in de organisatie.	√	√
	Incidenten					
14	Hoe reageert uw organisatie op cybersecurity incidenten in uw organisatie, sector of in de industrie in algemene zin en hoe blijft u steeds op de hoogte van de meest recente dreigingen en kwetsbaarheden?	Is de organisatie steeds op de hoogte van (recente) incidenten en hoe worden de incidenten gewogen op relevantie? Hoe leren organisaties van elkaar?	Kunt u specifieke incidenten noemen die tot verandering van inzichten hebben geleid? Hoe betrekt uw organisatie incidenten in het risico management proces?	Wat heeft een organisatie nodig om altijd alle relevante OT-dreigingen en kwetsbaarheden te kennen om het risico blijvend goed in te kunnen schatten.	√	√

B Overzicht basismaatregelen en practices

Applied Risk

De jaarlijkse overzichtsrapportage van een cybersecurity bedrijf werkzaam in de industriële sectoren onderschrijft dat door de toepassing van bestaande tegenmaatregelen vele gangbare en veelvoorkomende dreigingen snel gemitigeerd en voorkomen kunnen worden (Applied Risk, 2019). De maatregelen zijn onderverdeeld in technische en organisatorische perspectieven:

- Technisch:
  - Gedateerde en kwetsbare software;
  - Inadequate netwerksegmentering;
  - Gebrek aan hardening;
  - Zwakke toegangsbeveiliging;
  - Onvoldoende logging en monitoring.
- Organisatorisch:
  - Governance;
  - Training en awareness;
  - Business continuity management;
  - Leveranciersmanagement;
  - Incident response planning.

Gartner (to be published)

“Uit literatuurstudie en op basis van gehouden interviews blijkt niet dat er grote beleidsaanpassingen nodig zijn om de vitale sectoren veilig te houden” (Gartner, 2019). Voorbeelden van basismaatregelen volgens het onderzoek:

- Met betere monitoring en security awareness zou aanval waarschijnlijk niet hebben kunnen plaatsvinden.
- Door gebruik te maken van versleutelde communicatie en SCADA-autorisatie had de aanval voorkomen kunnen worden.
- Worm krijgt toegang tot veiligheidssystemen kerncentrale via laptop aannemer; [maatregelen voor veilig beheer en onderhoud (op afstand)].
- Maak standaard contractclausules die organisaties kunnen gebruiken bij aanbestedingen om de (IACS) beveiliging te waarborgen.
- Zorg voor gestandaardiseerde, sectorspecifieke aanvalsscenario’s.

Agence nationale de la sécurité des systèmes d'information (ANSSI, 2012).

Het Franse nationale instituut voor informatiebeveiliging heeft in 2012 een aantal good practices opgesteld voor industriële controlesystemen. Alle maatregelen zijn als basismaatregelen te bestempelen:

- Control physical access to devices and to the fieldbus;
- Network segregation;
- Management of portable devices and media;
- Account management (logical access);
- Configuration hardening;
- Management of event logs and alarm;
- Configuration management;
- Back-up and restore;
- Documentation;

- Malicious code detection;
- Upgrade and Patch management (planning);
- Protection of Controllers (PLC);
- Engineering and development stations.

National Institute of Standards and Technology (NIST)
Hanteer Security Controls and Assessment Procedures (uit, NIST 800-53 (Rev. 4) en volg zes stappen aan de hand van een lijst aan security controls, zogenaamde 'families':

- AC - Access Control
- AU - Audit and Accountability
- AT - Awareness and Training
- CM - Configuration Management
- CP - Contingency Planning
- IA - Identification and Authentication
- IR - Incident Response
- MA - Maintenance
- MP - Media Protection
- PS - Personnel Security
- PE - Physical and Environmental Protection
- PL - Planning
- PM - Program Management
- RA - Risk Assessment
- CA - Security Assessment and Authorization
- SC - System and Communications Protection
- SI - System and Information Integrity
- SA - System and Services Acquisition.

International Society for Automation (ISA) / International Electrotechnical Commission (IEC).

ISA/IEC 62443 C*yber security voor Industrial Automation and Control Systems* is de wereldwijde norm met methoden, maatregelen en technieken om OT te beveiligen.

Trend Micro best practices for organizations (Trend Micro, 2019):

- Apply network segmentation using the Purdue Model for Control Hierarchy.[15]
- Assess ICS systems to thoroughly identify the different kinds and levels of risk, and then install the corresponding safeguards.
- Evaluate external partnerships and shared resources, making sure to involve the IT team in the initial planning and development stages of designing collaborative network environments.
- Implement safeguards against insider threats with both technical and non-technical steps.
- Get network and device security solutions specifically for ICS and SCADA.
- Center for Internet Security (CIS) Controls.

[15] Het Purdue Model beschrijft een methodiek en aanpak om een logische onderverdeling te maken van een bedrijfsnetwerk en OT-omgeving. Een voorwaarde om onder te verdelen is dat de geclusterde systemen en processen functies en *requirements* hebben die met elkaar overeenkomen (SANS Institute, 2014).

Stouffer
Major security objectives for an ICS implementation should include the following (Stouffer et al., 2015):

- Restricting logical access to the ICS network and network activity;
- Restricting physical access to the ICS network and devices;
- Protecting individual ICS components from exploitation;
- Restricting unauthorized modification of data;
- Detecting security events and incidents;
- Maintaining functionality during adverse conditions;
- Restoring the system after an incident.

Universiteit Twente Online Discoverability and Vulnerabilities of ICS/SCADA Devices in the Netherlands (in opdracht van het Wetenschappelijk Onderzoek en Documentatiecentrum (WODC), 2019.

"[…] several well-known and relatively easy to deploy measures exist that help to improve the security of these ICS/SCADA device:

- Limit the access of ICS/SCADA devices from the Internet. This can be accomplished by, for example the use of firewalls, Virtual Private Networks (VPNs) or Virtual Local Area Networks (VLANs). Only devices that must have external communication may have a direct connection to the Internet.
- Install software updates in a timely manner. When it is not feasible to update the software, make sure the device can't be accessed via the Internet.
- To avoid that ICS/SCADA devices can be found too easily, change the default TCP/UDP port numbers of such devices and change the banners that identify the devices. This ensures that no unnecessary information about the device (such as product version and available modules) is revealed. Although this recommendation does not prevent discoverability of a device, it does make it harder.
- Use techniques to restrict network traffic on ports and protocols associated with ICS/SCADA services. Examples of such techniques are rate-limiting and the whitelisting of legitimate users. Restriction not only provides protection against potential hacking attempts, but also against Denial-of-Service (DoS)and/or brute force attacks.
- Harden the device configuration by disabling functionalities and services that are not used by the man-agers and operators. This process also includes removing unnecessary usernames or logins, changing default passwords and uninstalling unnecessary software and hardware modules. The goal is to reduce the potential attack surface by exposing only the necessary services.
- Maintain an up-to-date list of software and hardware that is running in your infrastructure. In this way it becomes easy to identify if newly discovered vulnerabilities may become a threat to your system.
- Monitor the manufacturer vulnerabilities. The manufacturers often directly contact their customers when a patch is available for their devices. However, subscribing to some known vulnerability databases, such as ICS-CERT and NVD is also recommended.
- Keep other systems that interact with the ICS/SCADA devices secure and ensure that they run the latest software version. Some attacks exploit weaknesses in adjacent systems, in order to bypass the imposed access restrictions.

- Monitor and assess the online discoverability and vulnerability of your ICS/SCADA devices. This report only provides a snapshot of the situation in 2018. Therefore, we suggest organizations to follow the methodology described in this report and periodically check if (parts of) their infrastructure is found to be discoverability and even vulnerable. Organizations concerned about their security should consider the regular use of professional “security red-teams” that try to explore the vulnerabilities of devices within an ICS/SCADA infrastructure
- Set-up a measurement and logging infrastructure, to detect possible scanning and attacking attempts in stage as early as possible. Examples include Intrusion Detection Systems (IDSs) and flow-measurement systems.
- Ensure that the default passwords of ICS/SCADA devices are changed, since default passwords can be easily found on the Internet.
- In addition to their SCADA protocols, ICS/SCADA devices may have built-in web services for configuration and management purposes. Be aware of such services, and take appropriate actions to protect such services.

DNS logs can be used to detect potentially unauthorized access. In the Netherlands we might consider whether organizations like SIDN, who maintains the DNS within the Netherlands, should play a role in such detection.

C Overzicht succesfactoren

Overzicht succesfactoren (1)

Thema	Uitdaging	Succesfactoren
OT-gerelateerde risico's: Belang aansluiten bij bestaand risicomanagement	Cybersecurity onderdeel van risicomanagement	Zet cyberdreigingen om in realistische risico's en kansen voor de eigen organisatie. Gebruik voorbeelden van incidenten in positieve of negatieve zin (van binnen of van buiten de organisatie) voor verdere bewustwording. Sluit aan bij bestaande risicomanagement processen om geïnformeerde investeringsbesluiten te nemen. Stel een cybersecuritystrategie op waar ook structurele inbedding van OT-security in risicomanagement wordt opgenomen. Deze strategie moet ingaan op kansen en dreigingen, vertaald naar organisatiedoelen. Tevens is het van belang de doelstellingen, maatregelen en KPI's te vertalen naar individueel niveau, dit kan bijdragen aan cybersecurity bewustzijn en handelen in de hele organisatie.
	Safety en security dichter bij elkaar	Het is van toegevoegde waarde om OT-security te koppelen aan de organisatiedoelen, omdat er anders mogelijk veiligheidsrisico's ontstaan. Dit wordt door organisaties verschillend vormgegeven.
	Investeringsbesluiten vanuit integraal risicomanagement	Bewustwording van het belang en toegevoegde waarde van OT-security draagt bij aan investeringsbesluiten. Incidenten kunnen hiervoor in de communicatie en onderbouwing worden benut.
		Investeringsbehoeften uitvragen bij verschillende organisatielagen, bijvoorbeeld aan de operationele managers. Deze managementlaag is namelijk verantwoordelijk voor productie en staat dicht genoeg bij de werkzaamheden. Zo worden kosten beter ingeraamd en leidt dit tot afgewogen keuzes.
OT-gerelateerde risico's: communicatie kansen en bedreigingen	Context van cybersecurity kansen en bedreigingen	Communiceer altijd de context van OT-security in het grote geheel. Besef dat OT-security een deel is van de puzzel om de organisatiedoeleinden te verwezenlijken.
		OT(-security) lead moet *zelf* het belang en de toegevoegde waarde van OT-security bij het management op het netvlies zetten.
	Uitval primaire proces inzichtelijk maken	OT-security dreigingen vertalen naar risico's die het primaire proces (gedeeltelijk) verstoren, idealiter gebaseerd op kwantitatieve data (die niet altijd beschikbaar is).

Overzicht succesfactoren (2)		
Thema	**Uitdaging**	**Succesfactoren**
Basismaatregelen: gebruik bestaande maatregelen naar eigen organisatie	Standaarden omzetten naar eigen organisatie	Kies de relevante standaard(en) en vertaal deze op basis van de wensen en eisen naar de eigen organisatie. Dit vergt kennis, tijd en geld maar het belang om dit zorgvuldig te doen wordt door de respondenten benadrukt.
	Werk met bestaande frameworks / standaarden	Kies bestaande frameworks/standaarden en leer gezamenlijk tijdens het toepassen ervan op de eigen organisatie.
	Security-by-design	Medewerkers en management zijn op de hoogte van de kansen die ontstaan wanneer OT vervangen of ontwikkeld wordt. Dit is het moment in de life cycle van OT om security-by-design te implementeren.
Kloof IT en OT: versterken van de samenwerking	Verantwoordelijken IT en OT	Zorg dat de IT- en OT-verantwoordelijken samen optrekken. Zo zetten zij een voorbeeld voor het dichter bij elkaar brengen van de domeinen en een eerste stap in die richting
	OT en IT in één team	Management erkent de noodzaak voor het combineren van IT-OT kennis en kunde en zorgt ervoor dat IT en OT in dezelfde afdeling werken.
		Een medewerker die ervaring heeft in het IT- en OT-domein ziet de toegevoegde waarde van samensmelting en geeft hier vorm aan.
		Het initiëren van gezamenlijk overleg tussen het IT-en OT-team kan een eerste stap in de vorming van een team zijn en kan bijdragen aan de vorming van de integrale aanpak van cyber security.
	Roulatiemodel van medewerkers	Zet een pool op van mensen die elkaar kunnen vervangen. Zorg dat IT- en OT-kennis door meerdere mensen in deze pool toegepast kan worden.
	Dezelfde functiewaardering	Het management is uiteindelijk de factor die besluit om verandering teweeg te brengen. Het is daarom nodig dat het management zich realiseert dat het verschil in functiewaarderingen de samenwerking niet ten goede komt en besluit dit aan te passen.
Beheer en onderhoud	Assetmanagement op orde	Zorg dat je weet wat je in huis hebt en wanneer iets aan vervanging toe is. In de praktijk wordt dit op verschillende manieren vormgegeven.
		Assetmanagement op orde hebben en hierover communiceren draagt bij aan de bewustwording en daadkracht om veilige OT te bewerkstelligen.
		Aan het management open en helder communiceren wat er in huis is en wanneer dit (op de lange termijn) aan vervanging (of updates) toe is, zorgt voor de juiste investeringsbesluiten en daardoor voor het veiligstellen van OT-systemen.
	Inhouse-kennis om mee te kijken	Een organisatie beschikt ten alle tijden over een basis aan kennis over OT(-security) om met externen samen te werken. Dit betekent dat er meegekeken en gedacht kan worden als bijvoorbeeld leveranciers op locatie systemen komen installeren.

Overzicht succesfactoren (3)		
Thema	**Uitdaging**	**Succesfactoren**
Kloof IT en OT: bevorderen van kennisdeling	Ruimte voor persoonlijkheden die graag kennis delen	Geef collega's die graag kennis uitdragen de ruimte en gelegenheid daarvoor.
		Door kennisdeling onderdeel te maken van de functioneringsgesprekken worden individuele medewerkers gestimuleerd en uitgedaagd om hierin uit te blinken.
	Kennisdeling en informatie-uitwisseling buiten de organisatie om	Het face-to-face deelnemen aan (nationale en internationale) bijeenkomsten zorgt voor kennisdeling buiten de eigen praktijken om.
		Een informeel netwerk met gelijkgestemden (binnen en buiten de eigen sector) draagt bij aan het delen van kennis en het up-to date houden ervan.
	Zelfde soort programma's en apparatuur gebruiken	Het is van toegevoegde waarde om door het management het gebruik van homogene programma's en apparatuur te laten ondersteunen en hier een doelstelling van te maken.
		Het streven naar standaardisatie van programma's en apparatuur kan het beste worden vormgegeven in de life cycle management processen.
		Uit de resultaten komt geen succesfactor naar voren hoe de keuze gemaakt wordt voor dezelfde soort programma's en apparatuur. Wel kan life cycle management in combinatie met wat er aangeboden wordt in de markt invloed uitoefenen op deze keuze en is het van belang om de functionele eisen vanuit IT en OT op te stellen en uit te zetten.
Kennis en kunde: vergaren en versterken van kennis en kunde	Eigen mensen binnenhalen en opleiden	Weet welke kennis benodigd is voor veilige OT en werf hier actief op.
		Geef ruimte aan medewerkers die uit eigen interesse willen groeien en die vooroplopen in de benodigde kennis.
		Reserveer middelen om medewerkers voortdurend bij te scholen.
	IT- en OT-security deskundigheid	Maak gebruik van medewerkers die de organisatie door en door kennen en zet hen voorop in het verspreiden van de benodigde deskundigheid.
		De diversiteit van de competenties en deskundigheid van de medewerkers moet inzichtelijk en beschikbaar zijn voor een CISO. Organiseer de (face-to-face) interactie die hiervoor benodigd is en kennis en kunde kan versterken.
	Gezamenlijk oefenen	Ontwikkel een *ingrijpend* en *realistisch* scenario, oefen het reactieplan en evalueer hoeveel tijd er nodig is om de procesautomatisering weer volledig te herbouwen. Dit gezamenlijk doen zorgt voor het vergaren en versterken van kennis en kunde.
	Assessments met expertise	Betrek OT-specialisten bij assessments.
	Het belang en toegevoegde waarde van OT-security wordt door het management uitgedragen	Borg OT-security als een jaarlijkse bedrijfsdoelstelling.
		Het management faciliteert het delen van ervaring en kennis op dit onderwerp met andere bedrijven.
	Audits creëren aandacht	Gebruik audits om de mogelijke kwetsbaarheden als startpunt te gebruiken om OT-security onder de aandacht te brengen bij het management.