



Ministerie van Infrastructuur
en Waterstaat

Handreiking risicobeheer in OT

Versie: Final – Handreiking 2.0 | 05.11.2025



Colofon:

Uitgegeven door:

Ministerie van Infrastructuur en Waterstaat

Opgesteld door:

F. Ruedisueli, Principal OT Security Consultant, Bureau Veritas Cybersecurity

T. Dotinga, OT Security Consultant, Bureau Veritas Cybersecurity

Met medewerking van:

T. Jansen, OT Security Consultant, Bureau Veritas Cybersecurity

B. van Altena, Chief Information Security Officer, Air France KLM

T. Huisman, Deputy Chief Information Security Officer, Air France KLM

D. Dirks, Information Security Officer, Rotterdam the Hague Airport

E. Pit, Information Security Manager Operational Technology, Van Oord

J. Brebde, Process Control Engineer, Van Oord

A. Kejriwal, Process Control Engineer, Van Oord

A. van Herk, Senior Business Development Manager, Kotug International

M. Luchs, OT Security Enthusiast - Pilz

S. Brands, Senior adviseur en Kwartiermaker OT Security, Gemeente Den Haag

S. Debets, Chief Information Security Officer, HTM

L. Strijd, Security Officer, HTM

J. Buiten, Business Information Security Officer, NS

M. Leenen, Risk & Compliance Manager Cyber, NS

R. Geurts, Cybersecurity Coördinator AM OT, ProRail

S. van der Aa, Information Security Manager OT, ProRail

M. Bunschoten, Information Security Officer OT, ProRail

T. Yildirim, Senior Adviseur Industriële Automatisering, Rijkswaterstaat

J. Jellesma, Senior Adviseur Industriële Automatisering, Rijkswaterstaat

Versiebeheer en wijzigingshistorie

1.0 23-04-2024 Initiële versie

2.0 05-11-2025 Aanvullingen, verdieping en verbreding

www.versterkenweerbaarheid.nl/programmacyberweerbaarheid

Rechten en vrijwaring:

Opstellers zijn zich bewust van hun verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kunnen opstellers geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. Opstellers aanvaarden ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

TLP:white

Samenvatting

Het ministerie van Infrastructuur en Waterstaat werkt sinds enkele jaren met cyberweerbaarheidsprogramma's voor haar vitale sectoren. Door de groeiende afhankelijkheid van digitale systemen en technologieën is de bescherming tegen cyberdreigingen essentieel. Cybersecurityincidenten in Operationele Technologie (OT) kunnen naast financiële schade ook ernstige gevolgen hebben voor persoonlijke veiligheid, milieu en de omgeving. Het is daarom van belang dat cybersecurityrisico-management als integraal onderdeel binnen de organisatie een plek krijgt, met sturing vanaf het directieniveau.

Wet- en regelgeving, zoals de Cyberbeveiligingswet (Cbw) en sectorspecifieke regelgeving, verhogen de druk om de weerbaarheid te verbeteren. Tegelijkertijd staat de OT-sector voor specifieke uitdagingen: de lange levensduur van systemen waardoor deze vaak verouderd zijn, complexe toeleveringsketens, veiligheid en beschikbaarheid als prioriteit en toenemende connectiviteit. Deze factoren zorgen ervoor dat de cybersecurityrisico's in OT-omgevingen toenemen en een gespecialiseerde aanpak vereisen. Niets doen is dus geen optie.

Deze handreiking biedt een praktische aanpak voor risicobeheer in OT en benadrukt dat organisaties laagdrempelig kunnen beginnen, ongeacht het huidige volwassenheidsniveau. Het doel is om cybersecurityrisico's te identificeren en naar een acceptabel niveau te verlagen. Het document bevat ook kaders met daarin (internationale) casestudies, praktijkvoorbeelden, tips en aandachtspunten. Deze handreiking is een product van samenwerking tussen de cyberweerbaarheidsprogramma's van het ministerie van Infrastructuur en Waterstaat, securityexperts en participanten uit de sectoren.

Hoofdstuk 2 beschrijft de cruciale eerste stappen voor organisaties die nog aan de start staan van het implementeren van OT-risicomanagement. Dit omvat het creëren van een high-level overzicht van systemen en hun bedrijfsbelang, het implementeren van een baseline met fundamentele basismaatregelen, en het borgen van de organisatorische voorwaarden, zoals managementbetrokkenheid, beschikbare middelen en capaciteit, en het vaststellen van duidelijke rollen.

Hoofdstuk 3 legt de basis voor de formele processen en juiste voorbereiding. Dit omvat het kaderen van risico's binnen de organisatie (o.a. het bepalen van 'kroonjuwelen' en het

opzetten van een risicomatrix), het vaststellen van een duidelijke scope, en het uitvoeren van een impactanalyse (Business Impact Analysis) om de potentiële impact op de bedrijfsvoering te bepalen.

Hierna volgt de structurele en cyclische aanpak van risicobeheer, opgedeeld in vier hoofdstappen:

- 1. Identificeren (hoofdstuk 4):** Het systematisch in kaart brengen van assets, kwetsbaarheden, bestaande maatregelen en relevante dreigingen.
- 2. Analyseren (hoofdstuk 5):** Het bepalen van het daadwerkelijke risico door de kans (op basis van dreiging en kwetsbaarheid) en de impact te combineren. De handreiking biedt methoden voor verschillende volwassenheidsniveaus.
- 3. Beheren (hoofdstuk 6):** Het kiezen van een passende risicobehandeling op basis van de analyse. De opties zijn: Reduceren (maatregelen treffen), Accepteren (het restrisico formeel aanvaarden binnen de 'risk appetite'), Overdragen (bijv. via verzekeringen), of Vermijden (stoppen met de activiteit).
- 4. Monitoren en Rapporteren (hoofdstuk 7):** Deze stap borgt dat risicobeheer een continu proces is. Dit wordt verzekerd via operationele processen, tactische sturing (zoals leveranciersmanagement en formele risicoacceptatie) en strategische processen (zoals beleidsvorming en resourcetoewijzing).

Tot slot is het beheren van cybersecurityrisico's een continu verbeterproces. Veranderingen binnen de organisatie en in het externe dreigingslandschap vereisen dat risico's regelmatig worden heroverwogen. Dit geeft het belang aan dat het risicobeheerproces, inclusief een PDCA-cyclus, een continu onderdeel moet zijn van de bedrijfsstrategie, gedragen en gestuurd door het management.

Inhoud

Samenvatting	3
Inleiding	5
Handreiking Risicobeheer in OT - Stappenplan en leeswijzer	6
1. Nut en noodzaak van cybersecurityrisicoanalyses in OT	8
1.1. Wet- en regelgeving	9
1.2. Uitdagingen van OT-cybersecurity en risicobeheersing	10
1.3. Noodzaak van een proportionele aanpak	11
1.4. Risicoanalyse en methodiek	12
2. De eerste stappen in risicobeheer	13
2.1. Overzicht	13
2.2. Basismaatregelen	14
2.4. Opzetten OT-Security Management System	18
3. Strategie en voorbereidingen	20
3.1 Kaderen van risico's binnen de organisatie	20
3.2 Vaststellen van de scope	23
3.3 Impactanalyse (Business Impact Analysis)	24
3.4 Maatregelen en vervolgstappen	26
3.5 Benodigde kennis en expertise	31
4. Identificeren	32
4.1 Identificeren van Assets	32
4.3 Identificeren van bestaande maatregelen	36
4.4 Identificeren dreigingen	37
5. Analyseren	40
5.1 De context van cybersecurityrisico's	40
5.2 Methoden voor Risicoanalyse	42
5.3 Analyseren van de kans & impact	45
5.4 Analyseren van het risico	47
6. Beheren	48
6.2 Accepteren	50
6.2.1 Risicotolerantie (Risk appetite)	50
6.2.2 Afwijkingen	50
6.3 Overdragen	52
6.3.1 Verzekeringen	52
6.3.2 Outsourcing	53
6.4 Vermijden	55
6.5 Aanbevelingen voor de implementatie van maatregelen	55
7. Monitoren en rapporteren	56
7.1 Operationeel proces	57
7.1.1 Validatie van Risicoaannames (gap-analyse)	57
7.1.2 Kwetsbaarheden monitoring (Effectiviteit Toetsen)	57
7.1.3 Patch- en Configuratiemanagement	59
7.1.4 Verandermanagement	59
7.1.5 Leren van incidenten	60
7.1.6 Continu verbeteren (PDCA)	60
7.2 Tactisch proces	60
7.2.1 Leveranciersmanagement en contractuele cybersecurity	61
7.2.2 Formele risicoacceptatie	62
7.2.3 Continu verbeteren (PDCA)	62
7.3 Strategisch proces	63
7.3.1 Continu verbeteren (PDCA)	64
Afkortingen en verklarende woordenlijst (op alfabetische volgorde)	65
Bijlage – Verwijzing naar verdere bronnen	68

Inleiding

Het ministerie van Infrastructuur en Waterstaat werkt met verschillende programma's om de cyberweerbaarheid in verschillende vitale sectoren te versterken. Door de groeiende afhankelijkheid van digitale systemen en technologieën is de bescherming tegen cyberdreigingen essentieel. Binnen dit cyberweerbaarheidsprogramma werkt het ministerie samen met stakeholders, experts en organisaties uit al deze betrokken sectoren om de kennis en aandacht over cyberdreigingen te bevorderen. Ook voorziet zij in trainingen en ondersteuning, en stimuleert het delen van 'best practices' om de digitale weerbaarheid van de sectoren te versterken.

Deze Handreiking Risicobeheer in OT is het product van samenwerking tussen het ministerie van Infrastructuur en Waterstaat, onafhankelijke securityexperts, en deelnemers uit de sectoren luchtvaart, maritiem, weg en spoor. Het document is specifiek gericht op beheersing van cybersecurityrisico's in OT, en is hiermee onderdeel van de bredere praktijk van risicobeheersing.

Van nature wil iedere organisatie haar operatie beschermen en datgene waar zij van afhankelijk is operationeel houden. Risicomanagement betreft het continue proces van het identificeren en kwantificeren van risico's binnen een organisatie, en het opstellen van maatregelen om deze risico's te beheersen. Een gedegen risicomanagementproces draagt bij aan het waarborgen van bedrijfscontinuïteit.

Het beheersen van cybersecurityrisico's in OT is een van de vele facetten van risicomanagement waar leidinggevend bestuur verantwoordelijkheid voor draagt en dat onder de Cbw ook een wettelijke verplichting wordt. Risicomanagement, zoals bovenstaand, omvat de hele organisatie en de complete bedrijfsvoering: binnen dit raamwerk vallen ook IT- en OT-risicobeheer. IT-risicobeheer richt zich op bescherming van digitale informatie, systemen en processen die betrokken zijn bij informatietechnologie. Denk aan beveiliging van netwerken, gegevens, applicaties, en gebruikersapparaten. OT-risicobeheer

doelt op beheer van operationele technologie, wat betrekking heeft op systemen en processen die cruciaal zijn voor de fysieke werking van de organisatie, zoals industriële besturingssystemen, machines en sensoren. De integratie van IT en OT in risicobeheer is essentieel vanwege toenemende convergentie tussen informatie- en operationele technologie. De verbondenheid van deze systemen betekent dat zwakheden in het ene domein potentieel een risico vormen voor het andere domein. Daarom moeten organisaties een holistische benadering aannemen om deze risico's te begrijpen, evalueren en aanpakken.

Als laatste toevoeging is belangrijk te erkennen dat risicobeheer in OT geen gemakkelijke opgave is. Dit komt mede doordat OT-risicobeheer vraagt om diepgaande technische kennis, significante investeringen van bedrijfsmiddelen en aanpassingen aan systemen die continu moeten werken. Dit leidt tot lange implementatietijden en complexe besluitvorming. Het credo luidt in dit geval ook: "Begin klein, en zo gecontroleerd als de situatie toestaat, maar begin ergens en werk iteratief voorwaarts".

Zodoende, en met bovenstaande in het achterhoofd, heeft deze Handreiking Risicobeheer in OT als doel een specifiek onderdeel te vormen van het overkoepelende risicobeheersproces van een organisatie, en concrete, praktische handvatten te bieden voor het identificeren, analyseren, controleren en monitoren van OT-cybersecurityrisico's. Een robuust cybersecurityrisicobeheer beschermt niet alleen de eigen organisatie, processen en producten, maar ook de klanten, partners en leveranciersketens. Uiteindelijk heeft dit zijn weerslag op de maatschappij en economie: continue verbetering van digitale weerbaarheid in de vitale sectoren is essentieel.



Programma
**Versterken
Cyberweerbaarheid
in de watersector**



Programma
**Versterken Cyberweerbaarheid
in de Luchtvaart- en Maritieme
sector**



Programma
**Versterken Cyberweerbaarheid
in de Weg- en Spoorvervoer
sectoren**



Programma
**Versterken
Cyberweerbaarheid
Milieu en Internationaal**

Handreiking Risicobeheer in OT - Stappenplan en leeswijzer

Het stappenplan hieronder biedt een leidraad voor het geleidelijk opzetten en uitbouwen van een OT-beveiligingsprogramma. In de handreiking wordt dit beschreven in de eerste drie hoofdstukken. De stappen beschrijven het proces van organisatievoorbereiding tot een eerste, pragmatische uitvoering van een risicoanalyse. Onder dit stappenplan staan nog twee voorbeelden van de iteratieve en verdiepende stappen voor het uitvoeren van een BIA (Business Impact Analyse) en het opstellen van securitybaselines.

In het tweede diagram op de volgende pagina staan de stappen voor het formele risicobeheerproces. Deze zijn in de handreiking beschreven

in de hoofdstukken 4 tot en met 7. Dit is een continu proces met de stappen identificeren, analyseren, beheeren en monitoren. Veel van deze substappen kunnen, afhankelijk van het volwassenheidsniveau of het risicoprofiel van de organisatie, op verschillende detailniveaus worden geïmplementeerd.

De stappen in de flowcharts verwijzen naar hoofdstukken, paragrafen of tekstkaders uit de handreiking. De gepresenteerde volgorde staat niet vast, maar is een praktische routekaart voor een pragmatische en iteratieve aanpak.

Stappenplan voor het fundament en de eerste stappen voor OT-risicomanagement

	Stap 1	Stap 2	Stap 3
Identificeren	Inventarisatie van doel en noodzaak van OT-risicobeheer binnen de organisatie. (H1) en de initiële identificatie van toepasselijke wet- en regelgeving (1.1)	Starten met een hoog-over inventarisatie van de belangrijkste OT-assets, verbindingen en leveranciers (2.1)	Een volledig overzicht van de belangrijkste processen & assets: de kroonjuwelen (3.1) en de scope vaststellen voor een risico-assessment (3.2)
Analyseren	Inzicht krijgen in de uitdagingen en afhankelijkheden binnen OT (1.2). Vervolgens een proportionele, iteratieve aanpak opzetten (1.3) inclusief een passende risicomanagementmethodiek (1.4)	Voer een initiële analyse uit om het belang van elke OT-asset voor de bedrijfsvoering vast te stellen. Wijs een verantwoordelijke systeemeigenaar aan (2.1)	Definieer en voer een eenvoudige BIA uit om de impact van verstoringen op de bedrijfsprocessen vast te stellen (3.3). Bepaal welke kennis en expertise noodzakelijk is voor een gedegen risicoanalyse (3.5). Zie voorbeeld A
Beheeren	Vorbereidingen op de eerste stappen van OT-risicobeheer (H2)	Definieer een verplichte, minimale set aan beveiligingsmaatregelen als baseline voor de gehele OT-omgeving. Implementeer deze voor alle OT-assets (2.2)	Definieer gelaagde en risicoafhankelijke baselines van beveiligingsmaatregelen en pas deze toe o.b.v. de uitkomst van de BIA (3.4). Zie voorbeeld B
Organiseren	Eerste stappen voor het inrichten van de interne organisatie. Gebruik informatie uit eerdere stappen om draagvlak bij management te creëren (2.3)	Definieer en wijs de benodigde rollen en verantwoordelijkheden toe voor het beheer van OT-risico's, en bepaal de risicotolerantie van de organisatie (2.3). Ontwikkel een risicomatrix (3.1)	Leg alle bevindingen vast en plan periodieke herzieningen (3.4). Start met opzet van een formeel OT Security Management System, incl. bevordering van een cybersecuritycultuur (2.4)

Voorbeeld A: volwassenheidspad Business Impact Analyse

1. Start met een eenvoudige Business Impact Analyse (BIA) (3.3)	2. Integreer het BIA-proces in de bedrijfscultuur en bestaande bedrijfsprocessen (3.3) Zie kader 3.3	3. Verdere verdieping van het BIA-proces (3.4, Aanvullende overwegingen) en gedetailleerde impactanalyse (3.4) Zie kader 3.4c
---	--	---

Voorbeeld B: volwassenheidspad Maatregelen (Baselines)

1. Start met één standaard set met basismaatregelen (3.4) met een beperkte diepgang. Zie kader 2.2b, jaar 1	2. Vervolg met meerdere en risicoafhankelijke sets aan maatregelen (3.4) en breid de diepgang per maatregel verder uit. Zie kader 2.2b, jaar 2	3. Stel een interne catalogus samen met extra maatwerkoplossingen (3.4). Ga verder met verbeteren en professionaliseren van deze maatregelen Zie kader 2.2b jaar 3
---	--	--

Stappenplan voor het gedetailleerde proces OT-risicomanagement

Processtappen	Niveau 1	Niveau 2	Niveau 3
Identificeren	4.1 Asset inventory & netwerktekeningen Basis assetregister Zie kader 4.1a, stap 1		
	Extra informatie toevoegen Zie kader 4.1a, stap 2		
	Volledige details Zie kader 4.1a, stap 3		
	Gedetailleerde logische & fysieke netwerkdiagrammen		
Analyseren	4.2 Kwetsbaarheden Baseline gap-analyse Zie kader 4.2		
	Documentanalyse, interviews & observaties		
	Fysieke inspecties en netwerkanalyses		
Beheren	4.3 Bestaande maatregelen Identificeer aanwezige baseline controls (techniek, mens & proces)		
	Identificeer effectiviteit bestaande maatregelen (techniek, mens & proces)		
Monitoren	4.4 Dreigingen Op basis van algemene of sector-specifieke dreigingbeelden		
	M.b.v. set standaard dreigingsscenario's Zie kader 4.4b		
	Gestructureerde analyses, OSINT & automatisering		
Beheren	5 & 5.1 Context Relatie tussen kwetsbaarheden en maatregelen, de motivatie, capaciteit en mogelijkheid van dreigingsactoren en potentiële impact het uiteindelijke risico bepalen. Zie schema in 5.2		
	5.2 Risicoanalyse Gap-analyse t.o.v. de geselecteerde baselines		
	Dreigingsscenario's, evt. aangevuld met Bowtie-analyse		
Beheren	5.3 & 5.4 Kans & Impact Analyse en bepalen van kans, impact en het risico t.o.v. de vastgestelde risicomatrix, -niveaus en -tolerantie.		
	H6 - Risicobeheer Toepassen van optie(s) voor risicoreductie. Afweging maken o.b.v. effectiviteit, complexiteit, kosten aanschaf en beheer. Hierbij is juiste expertise en beslissingsbevoegdheid nodig.		
	6.1 - Reduceren Extra preventieve of responsieve maatregelen		
Beheren	6.2 - Accepteren Formele acceptatie op basis van risicotolerantie		
	6.3 - Overdragen De verantwoordelijkheid voor risico's overdragen. Let op bij uitbesteden.		
	6.4 - Vermijden Risico weghalen door systemen of functionaliteit te verwijderen		
Beheren	6.5 - Testen & Terugkoppeling Verifieer de effectiviteit en volledigheid van nieuwe, aangepaste, tijdelijke of compenserende maatregelen. Koppel de resultaten terug naar de risicobeheerder.		
	H7 Monitoren & Rapportage Belangrijk voor compliance en audit en voor bijsturen en continu verbeteren (PDCA). Risicomanagement is een continu proces		
	7.1 Operationeel proces Regelmatig controleren aannames. Gap-analyses, focus op compliance (7.1.1)		
Monitoren	Meer focus op effectiviteit. Routinematige controle op kwetsbaarheden (7.1.2)		
	Risicomanagement afstemmen met andere operationele processen. Leren van incidenten (7.1.3-7.1.5)		
	7.2 Tactisch proces Prioritering van inzet en middelen, formele acceptatie van risico's en vaststellen baselines.		
Monitoren	Processen voor leveranciersmanagement waarborgen (7.2.1 fase 1). Verdiepen & beoordelen risicoacceptatieproces (7.2.2-7.2.3)		
	Verdiepen risicobeheersproces t.o.v. leveranciersmanagement (7.2.1 fase 2) Monitoren KPI en KRI (7.2.3)		
	7.3 Strategisch proces Bepalen risicotolerantie en ambitie, afstemmen van resources en vaststellen van OT-securitybeleid		
Monitoren	Afwegen toekomstige wet- en regelgeving, fusies, dreigingslandschap. Technische levensduur installaties		
	Prestatie-indicatoren en trendrapportages voor managementbetrokkenheid. Interne verantwoording (zie kaders 7.3.1a en 7.3.1b)		

1. Nut en noodzaak van cybersecurityrisicoanalyses in OT

Operationele Technologie (OT) is een verzamelnaam voor systemen voor de besturing van fysieke processen en objecten. Het Nationaal Cyber Security Centrum (NCSC) hanteert de volgende specifieke definitie: “Operationele Technologie (OT) is een verzameling van technologieën bestaande uit software en hardware systemen die in samenhang verantwoordelijk zijn voor het besturen, bewaken en beheren van fysieke processen”. Binnen deze brede definitie vallen diverse gerelateerde termen, zoals Industrial Control Systems (ICS), Industrial Automation and Control Systems (IACS) en SCADA (Supervisory Control and Data Acquisition)¹.

Deze OT-systemen zijn oorspronkelijk ontworpen als geïsoleerde netwerken, gebaseerd op specifieke technische principes gericht op het beheersen van technische risico's en het waarborgen van de (fysieke) veiligheid, efficiëntie en betrouwbaarheid van de processen. Om deze redenen bleef cybersecurity-risicobeheersing voor OT-systemen lange tijd (gedeeltelijk) buiten beeld. Tegenwoordig worden echter veel van deze OT-installaties en netwerken verbonden met IT-netwerken, die op hun beurt weer verbonden zijn met internet. Het cruciale verschil met IT-systemen, en daarmee het bijbehorende risico, is dat verstoringen in OT directe fysieke impact kunnen hebben op de omgeving of persoonlijke veiligheid. Een verstoring in een OT-systeem heeft onmiddellijke gevolgen voor de primaire bedrijfsprocessen van een organisatie en kan zelfs de veiligheidssystemen die mens en milieu moeten beschermen, beïnvloeden.

Hieruit volgt direct het nut en de noodzaak van cyberrisicobeheersing binnen de OT-omgeving: de groeiende connectiviteit van OT en het snel veranderende dreigingslandschap vormen een reëel risico voor het behoud van de werking van kritieke systemen, fysieke veiligheid en zelfs de publieke veiligheid. In de toekomst zullen IT, OT en IoT (Internet of Things) veel vaker geïntegreerd zijn en vanuit één centrale verantwoordelijkheid worden beheerd. Deze convergentie brengt de volgende

uitdagingen met zich mee: Welke OT-systemen draaien waar? Kunnen en mogen deze gekoppeld worden aan de IT-infrastructuur, en op welke manier? Hoe liggen de verantwoordelijkheden binnen de organisatie?

Bovendien zorgt ook het upgraden of migreren van verouderde OT-systemen voor specifieke uitdagingen. De kennis en kunde om in te breken op OT-installaties nemen sneller toe dan de expertise over de installaties zelf en de mogelijkheden om aanvallen te stoppen. Tot slot speelt ook de complexe toeleveringsketen (supplychain) een cruciale rol. Verschillende leveranciers, onderaannemers en producenten leveren allemaal een deel van de totale oplossing. Vaak hebben deze partijen rechtstreeks toegang tot hun apparatuur voor bijvoorbeeld onderhoudswerkzaamheden op afstand. OT-netwerken zijn vaak samengesteld uit diverse systemen van verschillende leveranciers, wat het totaaloverzicht vertroebelt en waardoor de algehele veiligheid niet altijd direct inzichtelijk is.

Het is daarom cruciaal voor organisaties om een gedetailleerd overzicht te hebben van de gehele OT-infrastructuur – inclusief alle koppelingen, afhankelijkheden en leveranciers. Organisaties moeten zich bewust zijn van de voortdurend evoluerende dreigingen en risico's in deze complexe omgevingen. Hieruit ontstaat de noodzaak om de bijbehorende cybersecurityrisico's nauwkeurig in kaart te brengen en deze vervolgens tot een acceptabel niveau te reduceren.

¹ Veelgebruikte termen, afhankelijk van context, zijn SCADA (Supervisory Control and Data Acquisition), ICS (Industrial Control System) of IACS (Industrial Automation and Control Systems); ondanks het verschil in technische details tussen de verschillende systemen zijn de essentiële functies grotendeels hetzelfde.

Casestudy: Voorbeeld uit de luchtvaartsector, de noodzaak van een OT-cybersecurityrisicoanalyse

De Engineering & Maintenance divisie van een luchtvaartbedrijf maakt gebruik van Operationele Technologie (OT) voor het beheren van industriële machines die cruciaal zijn voor het bouwen en onderhouden van vliegtuigonderdelen. Deze machines worden aangestuurd door standalone pc's die niet verbonden zijn met de IT-infrastructuur. Echter, om efficiënter te werken en gegevens van SAP te integreren, wordt overwogen om de OT-systemen te verbinden met het interne netwerk.

Dit brengt beveiligingsuitdagingen met zich mee, zoals verouderde OS-versies op de standalone pc's, ongecontroleerde externe verbindingen met leveranciers, en de verschuiving van verantwoordelijkheden voor beveiliging

naar IT en de CISO. Het gebrek aan regelmatige updates en beveiligingsmaatregelen vormt ook een risico voor het IT-netwerk, terwijl de connectiviteit van OT-systemen de controle bemoeilijkt en nieuwe bedreigingen introduceert.

Oplossingen omvatten het implementeren van een virtuele omhulling rond de OT-systemen, segmentatie met firewalls en het delen van informatie van SAP op protocolniveau. Hcertificatie moet worden geïntegreerd in het ontwerp van OT-systemen en worden opgenomen in de verantwoordelijkheid van leveranciers.

Deze case benadrukt de complexiteit van het beheren van OT-cyberberrisico's in een omgeving waarin verouderde technologieën en de behoefte aan integratie met moderne IT-systemen samenkomen, en illustreert de noodzaak van een nauwe samenwerking tussen de business, IT en leveranciers om effectieve beveiligingsoplossingen te implementeren.

Kader 1

1.1. Wet- en regelgeving

Cybersecuritywetgeving en -regulering speelt een steeds crucialere rol in het beschermen van IT- en OT-systemen. Deze wetgeving is ontworpen om een kader te bieden dat organisaties beweegt om passende beveiligingsmaatregelen te implementeren en te onderhouden om zo hun digitale infrastructuren te beschermen tegen aanvallen en datalekken.

Wet- en regelgeving rond cybersecurity kent twee belangrijke niveaus:

- Algemene richtlijn, zoals NIS2 en de daaruit voortvloeiende Cyberbeveiligingswet (Cbw), vormt een overkoepelend kader dat geldt voor meerdere sectoren. Deze wetgeving stelt brede cybersecurityeisen met als doel de bescherming van kritieke infrastructuren op nationaal en Europees niveau. Dit geldt ook voor privacywetgeving (AVG) dat zeker ook van toepassing kan zijn in OT. Ten slotte kan ook de toekomstige CRA (Cyber Resilience Act) en Machineverordening nog van invloed zijn, al is deze met name van toepassing op leveranciers en fabrikanten.

- Sectorspecifieke wet- en regelgeving heeft meestal andere primaire doelstellingen dan cybersecurity, zoals veiligheid, milieu of operationele continuïteit. Cybersecurity is in deze context een ondersteunende component die bijdraagt aan de centrale doelstellingen van deze wetgeving. Hoewel deze wetten niet specifiek zijn ontworpen voor cybersecurity, is het belang ervan steeds prominenter geworden als integraal onderdeel van de bredere sectorale regelgeving.

Voor het navolgen van deze wetten en voorschriften is het essentieel om zowel IT- als OT-netwerken te beschermen tegen toenemende cyberdreigingen. Organisaties moeten zich bewust zijn van regelgeving en bijbehorende verantwoordelijkheden, en een robuuste beveiligingsstrategie hebben die voldoet aan vereisten van zowel eigen organisatie als toezichthouder. Door middel van een op risico gebaseerde aanpak enerzijds en een sturende wet- en regelgeving op het gebied van cyber anderzijds, wordt er gestuurd op een optimaal klimaat van IT- en OT-bescherming en -weerbaarheid.

Voorbeelden van sectorspecifieke standaarden, voorschriften en wet- en regelgeving

Maritiem:

- Classificatiebureau notaties en Lloyds, DNV en Bureau Veritas
- IMO Resolution MSC.428: verplichting voor eigenaren in maritieme sector aan adequate risicoanalyse en -beheersing te doen
- IACS UR E26 and UR E27: gericht op de cybersecurity-weerbaarheid van schepen
- NR659: Regels voor cybersecurity voor classificatie van maritieme objecten, focus met name op software en hardware-supporting software ter preventie van cyberincidenten
- SPS: Internationale code voor de beveiliging van schepen en havenfaciliteiten

Luchtvaart:

- Luchtvaart: EASA Delegation Act 2022/1645 (Oktober 2025)
- Luchtvaart: EASA Implementing Act 2023/203 (Februari 2026)

Spoor & Weg:

- EN 50126-1: European standard for railway applications that specifies and demonstrates the process for Reliability, Availability, Maintainability, and Safety (RAMS)
- CLC/TS 50701:2023 is a European Technical Specification for Cybersecurity in Railway Applications
- CER, Critical Entities Resilience directive (2022)
 - ECM, Entity in charge of maintenance, (EU) 2019/779 (2022)
 - PCI-DSS, Payment Card Industry Data Security Standard

Let op: Deze lijst is ter illustratie en moet niet gezien worden als een compleet overzicht voor elke organisatie in de sector.

Kader 1.1

1.2. Uitdagingen van OT-cybersecurity en risicobeheersing

Ondanks dat wetgeving veelal spreekt van ‘bescherming tegen cyberdreigingen’ in het algemeen, hebben risicobeheer van IT en OT zich in de praktijk afzonderlijk ontwikkeld. Logisch, aangezien beide gebieden kampen met verschillende risico- en beveiligingsuitdagingen. Ondanks deze onderliggende verschillen tussen IT en OT maakt het voor de organisatie uiteindelijk niet uit waar de risico’s ontstaan, de gevolgen zijn voor de organisatie hetzelfde. Op bestuursniveau moeten daarom al deze risico’s worden afgewogen en daar ligt dan ook de centrale besluitvorming en verantwoordelijkheid.

IT is van nature datagericht. De voornaamste risico’s vloeien voort uit het stelen, manipuleren of ontoegankelijk maken van data. Incidenten kunnen daardoor diverse gevolgen hebben, zoals financiële schade, reputatieverlies, juridische claims en in extreme gevallen ook een impact op de gezondheid of veiligheid van personen, bijvoorbeeld bij de manipulatie van medische dossiers.

OT is daarentegen gericht op het beheer van fysieke processen en systemen. De risico’s richten zich op de beschikbaarheid en integriteit van deze processen. Een incident kan hierdoor direct fysieke en operationele gevolgen hebben, zoals het stilleggen van de productie, schade aan installaties, gevaar voor werknemers of milieuschade.

Dit fundamentele verschil toont zich ook in het beheer van netwerken en objecten: waar IT-systemen regelmatig bijge-

werkt kunnen worden in functionaliteit en beveiliging, kan elke verandering in een OT-netwerk de automatisering verstoren en de productie schaden. Het aanpassen van antivirusbescherming, installeren van beveiligingsupdates of het besturingssysteem upgraden is in een OT-omgeving een afgewogen keuze, geen vanzelfsprekendheid.

Vaak kampen OT-omgevingen met (ten minste enkele van) de volgende beperkende technische factoren:

- **Verouderde en kwetsbare systemen:** OT-systemen hebben vaak een lange levenscyclus (15-20 jaar), wat resulteert in het gebruik van verouderde hardware en software. Deze systemen zijn vaak niet ontworpen met moderne beveiligingsmaatregelen in gedachten (“insecure by design”) of kunnen deze simpelweg niet ondersteunen.
- **Complexe compatibiliteit en technische afhankelijkheden:** De specialistische aard van OT-systemen zorgt ervoor dat ze niet altijd compatibel zijn met standaard IT-beveiligingsoplossingen. Bovendien zijn er vaak complexe technische afhankelijkheden tussen verschillende systemen, waardoor vervanging of aanpassing een kostbare en risicovolle onderneming is.
- **Uitdagingen met beschikbaarheid en beheer:** De hoge beschikbaarheidseisen in OT-omgevingen maken gepland onderhoud of het installeren van updates lastig of onmogelijk. Daarnaast zijn beveiligingsprocessen vaak handmatig en moeilijk te automatiseren, wat leidt tot een lager volwassenheidsniveau in vergelijking met IT.
- **Leveranciersafhankelijkheid en beperkte transparantie:** OT-omgevingen zijn vaak sterk afhankelijk van specifieke leveranciers voor onderhoud, garantie en soms zelfs

certificering. Dit beperkt de mogelijkheden om zelf aanpassingen door te voeren die de cyberbeveiliging verbeteren, omdat veranderingen mogelijk de garantie of CE-markering ongeldig maken. Met name in dit laatste geval zal de eigenaar verantwoordelijk zijn voor hercertificering van de CE-markering. Naast deze strikte beperkingen komt het ook vaak voor dat extra cyberbeveiligingseisen gewoonweg niet worden ondersteund door de leverancier. Soms is dit onwetendheid, soms een geval van technische compatibiliteit, maar meestal is het niet getest waardoor een leverancier de beschikbaarheid en integriteit van het OT-systeem niet meer kan waarborgen.

- **Toenemende connectiviteit:** De groeiende verbindingen met IT-, IoT- en cloudomgevingen en de toenemende behoefte aan remote access introduceren nieuwe aanvalsvectoren. Deze connectiviteit kan leiden tot een verlies van overzicht over wie welke systemen beheert en welke beveiliging is geïmplementeerd.

Voor al deze punten geldt dat dit niet altijd een kritiek probleem hoeft te zijn. Afhankelijk van diverse factoren, zoals bijvoorbeeld connectiviteit en afhankelijkheid van andere systemen en/of (IT-)netwerken, kan het risico alsnog acceptabel zijn.

Voorbeeld uit de sector: Gecertificeerde systemen

Veel OT-systemen in de luchtvaart- en spoorsector zijn gecertificeerd op basis van een specifieke (software/configuratie) versie. Op het moment dat er bijvoorbeeld een software-update heeft plaatsgevonden, vervalt de certificering en dient deze hernieuwd te worden voor de 'nieuwe' staat. Deze certificeringen zijn vaak kostbare en langlopende trajecten. Dit proces van certificeren en hercertificeren vormt op dit moment een additionele complicerende factor, en is een van de redenen waarom de IT- van OT-systemen vaak verouderd zijn.

Kader 1.1a

Casestudy betreffende uitdagingen van OT-cybersecurity en risicobeheersing: Maritieme sector

Een vaartuig verlaat de haven, nadat een onderhoudsbeurt aan hun Veiligheids-PLC's van de ladingssystemen is uitgevoerd door een ingenieur van een derde partij. De ingenieur gebruikte een speciale laptop voor deze klus. Omdat het schip twee dagen vertraagd was, gebruikte de ingenieur de laptop om films te downloaden voor vermaak tijdens het verblijf in het hotel, waarvan er één malware bevatte.

Deze malware vond zijn weg naar de veiligheidssystemen van de laadinstallatie. Dit bleef onopgemerkt, omdat alle reguliere controles na de onderhoudscyclus positief waren, en de laadoperaties in de haven succesvol verliepen. Tijdens de overtocht merkten de boordwerktuigkundigen echter onverwacht gedrag van de laadinstallatie op, waardoor het moeilijk werd om de lading te controleren en te onderhouden. Volgens de nieuwste technologie is er geen volledige mechanische en handmatige bediening/uitschakeling voor de ingenieurs om de controle terug te krijgen. Bovendien hebben ze niet de specialistische kennis om deze sterk gedigitaliseerde systemen te bedienen. Het potentiële effect hangt af van de specifieke lading die wordt vervoerd.

Kader 1.1b

1.3. Noodzaak van een proportionele aanpak

Risicomanagement in OT-omgevingen is onmisbaar voor het beschermen van de primaire bedrijfsprocessen van een organisatie. Gezien de eerder beschreven complexiteit vraagt het beheer van deze risico's om een iteratieve en proportionele aanpak. Dit betekent dat je risico's gericht aanpakt: de meest kritieke systemen en processen verdienen de meeste aandacht. Een proportionele benadering is gebaseerd op het inzicht dat niet alle systemen even belangrijk zijn voor de bedrijfscontinuïteit. Door te focussen op de potentieel grootste impact, bijvoorbeeld op operatie of veiligheid, kan een organisatie haar middelen en inspanningen efficiënter inzetten.

Het nut van een risicogestuurde aanpak:

- **Strategische besluitvorming:** Een helder beeld van de risico's en de weerbaarheid van de organisatie stelt het hoger management in staat om strategische keuzes te maken over investeringen. Risicoanalyses helpen bij het stellen van prioriteiten, bijvoorbeeld de potentiële impact van risico's en de effectiviteit van voorgestelde maatregelen. Dit leidt tot een efficiënter gebruik van middelen en een hogere cyberweerbaarheid.

- **Voldoen aan wet- en regelgeving:** Gedegen OT-risicomanagement helpt bij het naleven van regels en standaarden op het gebied van cybersecurity. Alle nieuwe wetgeving eist een risk assessment en risicomanagement. Dit stelt de organisatie in staat om gerichte maatregelen te nemen om risico's te verminderen.
- **Juiste context binnen de organisatie:** Het is essentieel om OT-cyberbeveiligingsrisico's in het juiste perspectief te blijven plaatsen binnen de overkoepelende verantwoordelijkheid voor risicobeheer van de hele organisatie. Ze zijn slechts een onderdeel van de vele risico's waarmee een organisatie te maken krijgt, maar wel een onderdeel met de potentie om zeer ernstige, fysieke gevolgen te hebben.

Kortom: Risicomanagement biedt een strategisch kader om gerichte beslissingen te nemen, middelen efficiënt toe te wijzen en de veerkracht van de organisatie tegen cyberdreigingen te vergroten, wat essentieel is voor het waarborgen van operationele stabiliteit en bedrijfscontinuïteit.

1.4. Risicoanalyse en methodiek

Effectief risicobeheer in OT-omgevingen volgt een cyclisch proces. Het is een continue activiteit en geen eenmalige taak. De aanpak in deze handreiking sluit aan bij internationaal erkende standaarden zoals ISO 27005, NIST SP 800-30 en IEC 62443-3-2, en vormt een praktische opstap naar het toepassen van deze kaders.

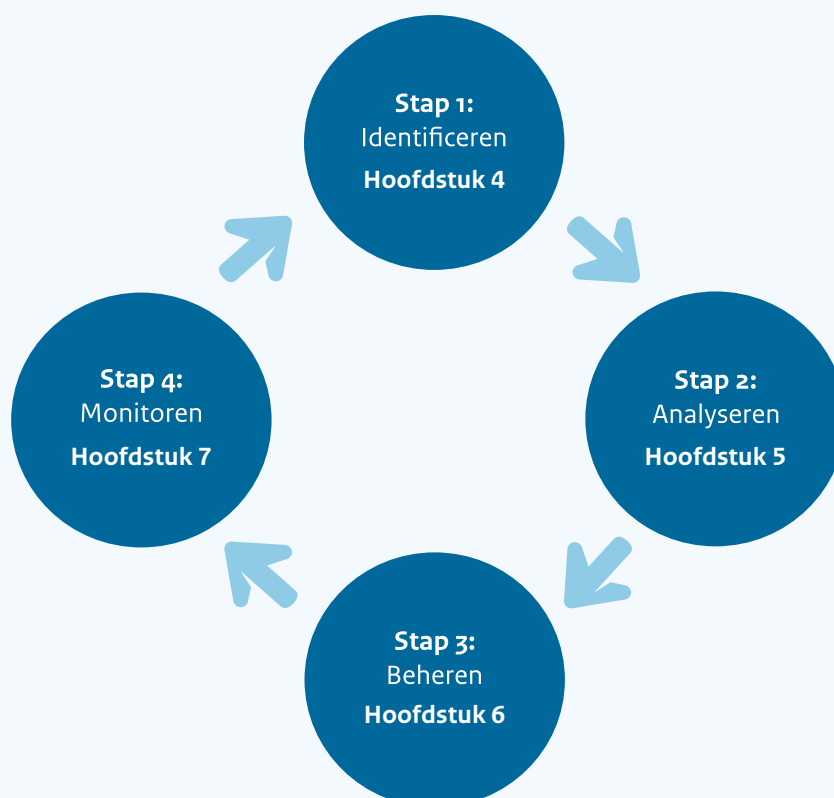
Deze handreiking hanteert een pragmatische aanpak, waarbij het risicobeheerproces is opgedeeld in vier stappen. Per stap is er verdieping beschikbaar, zodat zowel organisaties die net beginnen als organisaties met meer ervaring concrete handvatten hebben.

De vier stappen zijn:

1. **Risico-identificatie:** De eerste stap bestaat uit het in kaart brengen van de unieke risico's binnen een OT-omgeving. Dit omvat het identificeren van kritieke assets, dreigingen, kwetsbaarheden en de mogelijke impact.
2. **Risico-evaluatie:** Nadat de risico's bekend zijn, volgt een analyse om de waarschijnlijkheid en de potentiële impact ervan te bepalen. Dit stelt organisaties in staat om risico's te prioriteren en te bepalen welke de meeste aandacht vereisen.
3. **Risicobehandeling:** In deze stap worden passende maatregelen gekozen en geïmplementeerd om de geïdentificeerde risico's te verminderen. Denk hierbij aan het implementeren van technische controles, procesverbeteringen en organisatorische maatregelen.
4. **Monitoring en rapportage:** Risicobeheer is een doorlopend proces. Het monitoren van risico's en de effectiviteit van de genomen maatregelen is cruciaal. Regelmatige rapportage helpt het management op de hoogte te houden en de risicogestuurde aanpak binnen de organisatie te borgen.

Deze methodiek, die uitgebreid wordt behandeld in de volgende hoofdstukken, vormt de basis voor een structurele en effectieve aanpak van OT-risicobeheer.

Stappenplan voor cyclisch risicobeheer



2. De eerste stappen in risicobeheer

Deze handreiking beschrijft een gestructureerd risicobeheerproces. De praktijk leert echter dat veel organisaties, vooral die nog geen formeel of structureel risicomanagementproces voor OT hebben geïmplementeerd, een aantal cruciale voorbereidingen moeten treffen voordat dit proces effectief kan worden doorlopen. Het is niet productief om direct te starten met complexe risicoanalyses als de fundamentele basis nog ontbreekt.

Dit hoofdstuk is speciaal ontworpen om organisaties te helpen bij deze eerste, cruciale, stappen. Het doel is om een praktisch fundament te leggen voor OT-risicomanagement, ook als de ideale omstandigheden nog niet aanwezig zijn. De tekst biedt handvatten om de drempels te verlagen en een vliegende start te maken, zodat stapsgewijs kan worden toegewerkt naar een volwassen risicobeheerproces.

Om te kunnen starten, zijn de volgende drie factoren van essentieel belang:

- **Strategisch kader:** Er moet een minimale basis zijn van een informatiebeveiligingsstrategie of -beleid, zelfs als dit beleid nog voornamelijk op IT is gericht. Dit kader is noodzakelijk om OT-cyberbeveiliging te kunnen integreren en te rechtvaardigen. Mocht dit nog niet (voldoende) op niveau zijn dan is het belangrijk om dit parallel op te zetten. Dit valt echter buiten de scope van deze handreiking. Meer informatie rondom het starten met cybersecurity is te vinden op de websites van het NCSC en het DTC. Zie de bijlage voor alle relevante weblinks.
- **Betrokkenheid van het management:** OT-risicomanagement is geen eenmalige exercitie, maar vereist continue investering en aandacht. De bereidheid van het management om budget en tijd vrij te maken voor de lange termijn is cruciaal voor het slagen van het proces.
- **Voldoende capaciteit en mandaat:** Er moet binnen de organisatie een medewerker worden aangewezen die verantwoordelijk is voor het opzetten en beheren van het risicomanagementproces. Dit hoeft niet per se een fulltime-functie te zijn. Het is wel belangrijk dat deze persoon voldoende tijd en het juiste mandaat krijgt om de rol effectief te kunnen vervullen.

De volgende paragrafen beschrijven hoe deze eerste stappen kunnen worden gezet, ook als (nog) niet volledig aan alle voorwaarden wordt voldaan.

2.1. Overzicht

In deze fase is een gedetailleerde inventarisatie nog niet vereist. Het doel is om een high-level overzicht te creëren dat de afhankelijkheden en potentiële impact op de bedrijfsprocessen inzichtelijk maakt. Dit overzicht dient als basis om het management te overtuigen van de noodzaak en om budget en capaciteit vrij te maken voor de volgende stappen.

Een effectief hoog-over overzicht omvat de volgende elementen:

- **Systeemlijst:** Maak een lijst van de belangrijkste systemen en installaties. In deze fase is het niet nodig om alle details van elk afzonderlijk component te documenteren. Denk hierbij aan de basisgegevens van PLC's, SCADA-systemen, HMI's en netwerkkapapparaat.
- **Bedrijfsbelang en impact:** Bepaal de rol van elk systeem en de impact op de organisatie bij uitval of verstoring. Stel de volgende vragen:
 - "Hoe lang kan dit systeem niet beschikbaar zijn?"
 - "Wat kost het om het systeem te vervangen/weer operationeel te krijgen?"
 - "Wat is het ergste dat er zou kunnen gebeuren als dit systeem niet meer functioneert?"
- **Netwerkverbindingen:** Breng de koppelingen van de systemen met andere netwerken, zoals het IT-netwerk, en externe partijen in kaart. Dit geeft inzicht in de potentiële aanvals vectoren.
- **Verantwoordelijkheid:** Wijs de systeemeigenaar aan. Dit is de persoon of afdeling binnen de organisatie die verantwoordelijk is voor het systeem, ook als het onderhoud door een externe leverancier wordt gedaan. De systeemeigenaar is diegene die vanuit de organisatie mag beslissen over wijzigingen en is verantwoordelijk voor het beheer, onderhoud en veiligheid van het systeem. Mocht deze rol nog niet bestaan, dan is voorlopig het bestuur verantwoordelijk. Deze zal later de rol formaliseren en deze taak delegeren. (Zie paragraaf 2.3)
- **Leveranciers:** Als de OT-systemen (deels) door derden worden beheerd, inventariseer dan de (externe) beheerssystemen, netwerkontsluitingen en de bestaande beheercontracten. Dit laatste met name om te onderzoeken hoe cybersecurity is gewaarborgd.

Dit overzicht, dat als nulmeting fungeert, is bedoeld om de afhankelijkheden en potentiële impact van de OT-omgeving op de kernactiviteiten van de organisatie inzichtelijk te maken. Dit is geen gedetailleerde risicoanalyse, maar een middel om de noodzaak te onderbouwen en draagvlak te creëren. De diepere,

gedetailleerde analyse van risico's volgt in de latere hoofdstukken.

Op basis van deze inzichten kan aan het management worden aangetoond waarom er budget en capaciteit nodig zijn om een formeel risicomanagementprogramma te starten. Eventueel kan hierna gestart worden met een pilot om een risicoanalyse uit te voeren op een of enkele van de meeste belangrijke assets. Dit helpt om de scope klein te houden en toch ervaring op te doen. Deze input en ervaring kan in vervolggesprekken met het management waardevol zijn om zo de volgende stappen in het traject te bepalen.

2.2. Basismaatregelen

Het is aan te bevelen om te beginnen met het implementeren van een kleine set aan basale cybersecuritymaatregelen die universeel van toepassing zijn op vrijwel elke OT-omgeving. Deze aanpak, die ook wel het opzetten van een baseline wordt genoemd, is effectief omdat deze maatregelen fundamenteel zijn en vrijwel zeker uit een diepgaande risicoanalyse naar voren zouden komen. Door nu al te starten, worden niet alleen de meest voor de hand liggende risico's direct gereduceerd, maar wordt ook het vervolgproces van risicoanalyses vereenvoudigd.

Aanbevelingen voor het opzetten van een baseline:

- **Definieer en implementeer:** Leg een kleine set aan maatregelen vast en implementeer deze waar mogelijk op alle OT-componenten. Verderop in deze paragraaf staan een aantal voorbeelden. Overleg met en ondersteuning van leveranciers is hierbij vaak noodzakelijk.
- **Harmoniseer bestaande maatregelen:** Als er al diverse (versnipperde) beveiligingsmaatregelen zijn, zorg er dan voor dat deze minimaal voldoen aan de vastgestelde baseline. Dit zorgt voor consistentie en voorkomt gaten in de beveiliging.
- **Houd rekening met de context:** De baseline kan in de toekomst evolueren. Het is een delicate balans: zorg dat de set niet te zwaar is voor laag-ricosystemen, maar ook niet te licht voor de meest kritieke componenten. Overweeg of verschillende sets nodig zijn voor systemen met uiteenlopende risicoprofielen.
- **Geen vervanging van risicomanagement:** Een algemene baseline is geen vervanging voor een volledig risicogestuurde aanpak en is mogelijk niet voldoende om volledig aan wet- en regelgeving te voldoen. Het moet worden gezien als een cruciale eerste stap richting een volwassen risicobeheerproces.

LET OP: De uitdaging met leveranciers of externe diensten

In OT-omgevingen is het gebruik van externe leveranciers en dienstverleners de norm; niet de uitzondering. Deze partijen zijn vaak essentieel voor het onderhoud en de werking van de systemen. De basismaatregelen in dit document gelden daarom ook voor deze geleverde diensten en systemen. Dit kan een uitdaging vormen, zeker bij langlopende contracten die niet zomaar aangepast kunnen worden.

Toch is het belangrijk om hierover pro-actief het gesprek aan te gaan. De meeste leveranciers zijn zich bewust van de groeiende noodzaak voor cybersecurity en zijn bereid om mee te denken. Ga dus altijd in gesprek, zelfs bij bestaande contracten, om te onderzoeken wat er mogelijk is. Een contract hoeft niet per se te worden opgebroken; vaak kan de beveiliging worden verhoogd via een aanvullende overeenkomst of meerwerk.

In uiterste gevallen is het noodzakelijk om bepaalde punten af te dwingen. Denk hierbij aan hoe toegang op afstand wordt geregeld. Een organisatie kan bijvoorbeeld eisen dat externe toegang alleen is toegestaan via een door de organisatie beheerde VPN-oplossing met tweefactorauthenticatie, of dat er in plaats daarvan voor een fysiek bezoek kan worden gekozen.

Leveranciersmanagement en certificering

Het stellen van eisen gaat verder dan de technische maatregelen. Het is ook van belang om vast te stellen hoe de leverancier zelf omgaat met cybersecurity. Dit wordt vaak vastgelegd in een contract. Sommige bedrijven tonen dit aan met een certificering, zoals ISO 27001.

Voor kleinere leveranciers is dit niet altijd haalbaar. Er zijn echter initiatieven en certificaten, zoals CCV CYRA of het 'NIS2 Quality Mark', die gebruikt kunnen worden om aan te tonen dat er aan een bepaalde standaard wordt voldaan. Uiteindelijk moeten de verwachtingen en verplichtingen helder en contractueel worden vastgelegd.

Deze set van basismaatregelen is een praktisch voorbeeld dat voor de meeste organisaties van toepassing is. De focus ligt op het aanpakken van de meest voorkomende risico's om direct de cyberweerbaarheid te verhogen:

- **Netwerksegmentering:** Beperk de toegang tot OT-systemen door het netwerk minimaal te segmenteren van IT-netwerken en internet. Pas de netwerkkarchitectuur zo aan dat alleen essentiële communicatie met andere systemen is toegestaan en dat alle andere communicatie wordt geblokkeerd door bijvoorbeeld een firewall.
- **Veilige toegang op afstand:** Implementeer sterke beveiliging voor toegang op afstand. Mocht dit noodzakelijk zijn, dan moet toegang op afstand alleen mogelijk zijn via een VPN met individuele gebruikersrechten en tweefactorauthenticatie, liefst via een jumpserver in een demilitarized zone (DMZ). Directe verbindingen van OT-apparatuur met internet moeten onmogelijk worden gemaakt.
- **Bewustzijn en gedrag:** Bevorder een cultuur van veilig gedrag. Cyberweerbaarheid is niet alleen de verantwoordelijkheid van de IT- of OT-afdeling, maar van iedereen, inclusief het management en leveranciers. OT is ook echt anders dan IT, pas dus de bewustzijnprogramma's hierop aan door middel van specifieke trainingen over OT-security-awareness.
- **Back-ups:** Zorg ervoor dat er betrouwbare back-ups van alle systemen aanwezig zijn en dat deze veilig bewaard en regelmatig getest worden. Wees er zeker van dat systemen kunnen worden hersteld in het geval van een security-incident.
- **Hardening en configuratie:** Beperk het aanvalsoppervlak van systemen. Volg, indien beschikbaar, de hardening guidelines van de leverancier. Verwijder niet-essentiële softwarecomponenten, wijzig standaardwachtwoorden en pak bekende kwetsbaarheden aan door de belangrijkste software up-to-date te houden.

Dit overzicht van basismaatregelen is bewust beknopt gehouden. Het is bedoeld als een praktisch startpunt en is gebaseerd op de vijf basisprincipes van het NCSC. (Zie voor meer informatie de webpagina van het NCSC 'Aan de slag met het beveiligen van OT', deze en andere links zijn opgenomen in de bijlage.) In volgende iteraties kan deze set aan maatregelen verder worden uitgebreid, bijvoorbeeld op basis van de BIACS, CSIR, IEC 62443 of NIST-CSF.

Het is aan elke organisatie om hierin een eigen afweging te maken. Zorg er wel voor dat de baselines zo concreet en praktisch mogelijk worden gemaakt. Voorkom generalistische of overkoepelende maatregelen die de kans op inconsistentie vergroten. Verwijzingen naar beschikbare kaders zijn prima, maar bedenk dat deze vaak algemeen zijn omschreven. Maatregelen voor de eigen organisatie kunnen vaak duidelijker en concreter worden gemaakt, en daardoor makkelijker geïmplementeerd en gecontroleerd.

TIP: De baseline in de praktijk

De vijf basismaatregelen vormen een krachtig startpunt, maar de uitvoering ervan hoeft niet in één keer perfect te zijn. De baseline kan worden gezien als een levend document dat met de organisatie meegroeit.

Denk bijvoorbeeld aan securitypatches en het updaten van software:

Jaar 1: Begin met de absolute basis. Prioriteer de systemen met de meeste connectiviteit, zoals Human-Machine Interfaces (HMI's) of edge firewalls. Maak een handmatige inventarisatie van de besturingssystemen (OS). Kwetsbaarheden in deze systemen zijn vaak gemakkelijker te misbruiken, waardoor ze een logisch startpunt zijn voor een patchingstrategie. De installatie van patches vereist altijd een zorgvuldige risicoafweging om verstoring van kritieke processen te voorkomen. Controleer daarom periodiek of er kritieke patches beschikbaar zijn en plan de installatie in nauw overleg met de leverancier.

Jaar 2: Verfijn het proces. Breid de inventarisatie uit naar de firmware van cruciale hardware, zoals PLC's, én naar de applicaties die op de systemen draaien. Veel organisaties hebben geen testomgeving, dus wees extra voorzichtig. Als een testomgeving ontbreekt, overweeg dan om de patches te testen op een niet-kritiek, redundant systeem of in de rustigste uren. Werk nauw samen met de leverancier om de risico's zo veel mogelijk te beperken.

Jaar 3 en verder: Verhoog de lat. Overweeg een geautomatiseerd proces voor patchmanagement en continue monitoring op kwetsbaarheden. Werk aan een gestructureerde aanpak voor het bijhouden van de softwareversies van alle componenten in het OT-netwerk.

Door stapsgewijs te werken, is de belasting voor het team en het budget elk jaar behapbaar, terwijl de cyberweerbaarheid gestaag toeneemt. Het gaat erom dat de eerste stap wordt gezet, en vervolgens elk jaar een stapje verder wordt gegaan.

Kader 2.2b

2.3. Organisatie en voorwaarden voor risicomanagement

Een succesvol risicobeheerproces in OT-omgevingen staat of valt met de juiste organisatorische voorwaarden. Voordat met de risicobeheerstappen wordt begonnen, is het cruciaal dat beleid, processen en de juiste context binnen de organisatie aanwezig zijn. De belangrijkste benodigdheden worden in deze paragraaf beschreven, inclusief handvatten om deze te implementeren waar nodig.

Betrokkenheid van het management

Het beheer van OT-cyberbeveiligingsrisico's is geen louter technisch vraagstuk, maar een integraal onderdeel van de bedrijfsvoering en strategische planning. De meest kritieke bedrijfsprocessen van een organisatie leunen vaak zwaar op de betrouwbaarheid van de onderliggende OT-systemen. Deze processen dragen direct bij aan het bestaansrecht en de missie van de organisatie. De eindverantwoordelijkheid hiervoor ligt bij het management.

Zonder draagvlak vanuit het management zal een risicobeheerproces vastlopen. De eerste stap is daarom om te verzekeren dat het management het belang van het beheersen van deze risico's onderkent. De volgende punten kunnen daarbij helpen:

- **Inzicht in potentiële impact:** Gebruik het eerder gemaakte hoog-over overzicht om de ergst mogelijke effecten op OT-installaties en bedrijfsprocessen te visualiseren. Benadruk daarbij niet alleen de financiële gevolgen, maar ook de potentiële impact op menselijke veiligheid, het milieu en de reputatie. Daarnaast kan een overzicht van cyberincidenten en near-misses, zowel binnen de organisatie als in de bredere sector, het belang van risicomanagement verder onderstrepen.
- **Wet- en regelgeving:** Wijs op de verantwoordelijkheden die voortvloeien uit relevante wet- en regelgeving die organisaties verplicht tot het nemen van 'passende' maatregelen. Zonder een formeel risicomanagementproces is het onmogelijk om te bepalen wat als een passende maatregel wordt gezien.
- **Link met de missie en visie:** Koppel OT-cyberbeveiliging, met name de twee bovenstaande punten, aan de overkoepelende missie en visie van de organisatie. Thema's als betrouwbaarheid, integriteit en maatschappelijke betrokkenheid, die vaak in beleidsstukken worden genoemd, vormen hierbij een sterke basis.
- **Uitbesteding:** Benadruk dat de eindverantwoordelijkheid voor risicobeheer altijd bij de organisatie blijft liggen, ook wanneer OT-beheer wordt uitbesteed aan externe dienstverleners.

Uiteindelijk is het management verantwoordelijk voor het maken van de beste afwegingen. Zonder informatie en terugkoppeling vanuit gedegen risicobeheerprocessen is dat vrijwel onmogelijk. Dit onderstreept de noodzaak om een

formeel proces op te zetten en de bijbehorende middelen en het mandaat te verkrijgen.

Risicotolerantie van de organisatie

Het is onmogelijk om alle risico's te mitigeren, dus enige vorm van risicoacceptatie is altijd noodzakelijk. Het bepalen van de risicobereidheid (ook bekend als risk appetite) en het risicotolerantieniveau is daarom een cruciale taak van het management. Dit maakt het mogelijk om OT-cyberbeveiligingsrisico's te vergelijken met andere risicogebieden, zoals financiële risico's of veiligheidsrisico's (HSE), op een manier die past bij de cultuur en doelstellingen van de organisatie.

De risicobereidheid is een overkoepelende, strategische verklaring over het type en de hoeveelheid risico die de organisatie bereid is te accepteren. Het is het strategische plafond. Het risicotolerantieniveau is de gedetailleerde, operationele grens die de organisatie niet wil overschrijden. Het vertaalt de risicobereidheid naar concrete, meetbare drempels voor specifieke risico's.

Casestudy voorwaarden voor risicomanagement

De Engineering & Maintenance Business wil efficiënter werken en op gebeurtenissen gebaseerd werken met gegevens van SAP. In dit specifieke geval moet het OT-landschap 'verbonden' worden met het IT-netwerk om informatie te kunnen verzenden en ontvangen van de SAP-omgeving. Dus het initiële verzoek aan IT was om een netwerkverbinding te krijgen voor de standalone pc's. Dit verzoek bracht veel vragen met zich mee:

- Als de standalone pc's verouderde versies van het OS draaien, die niet beveiligd zijn en niet kunnen worden beveiligd met (moderne) beveiligingstools zoals AV en EDR, veroorzaakt dit een hoog risico voor het IT-netwerk. Hoe kunnen we dit hoge risico beperken?
- Hoe houden we controle over de OT-systemen met verschillende externe inbelverbindingen, zodra ze zijn verbonden met de IT-omgeving? Kan dit worden gedaan door netwerksegmentatie? En wie zal deze omgevingen beheren en veilig houden; IT of de business?
- En eenmaal verbonden, verschuift de verantwoordelijkheid voor beveiliging, continuïteit en beschikbaarheid dan van de eigenaar van de Business (OT) naar de CISO en IT?

Duidelijke antwoorden op deze vragen zijn vereisten voor het correct en veilig aandragen, opzetten en integreren van eventuele oplossingen.

Veel organisaties hebben al een uniforme risicomatrix of een bedrijfswaardematrix opgesteld. Deze matrix beschrijft de schaal van impact voor verschillende gebieden. Bijvoorbeeld: wat wordt gezien als een 'lage' financiële impact? Is dat € 5.000, € 50.000 of € 500.000? Deze matrix maakt het mogelijk om OT-cyberincidenten te beoordelen met dezelfde criteria als bijvoorbeeld diefstal.

Als er nog geen uniforme matrix bestaat of als deze niet geschikt is voor OT-cyberbeveiligingsrisico's, kan aansluiting worden gezocht bij bestaande processen binnen de organisatie. Dit levert niet alleen uniformiteit op, maar maakt ook gebruik van aanwezige kennis en ervaring.

- **Veiligheid (HSE):** In OT-omgevingen ligt van oudsher een sterke focus op veiligheid. Vaak zijn er al volwassen risicobeheerprocessen vanuit de HSE-discipline. De uitdaging hier is de beperkte link met cyberbeveiliging. OT-risico's worden vaak als technisch of digitaal gezien en vallen buiten de scope van traditionele veiligheidsprocessen. Het is aan te bevelen om te onderzoeken hoe deze processen zijn ingericht en of er aansluiting kan worden gevonden.
- **IT-afdeling:** De IT-afdeling is vaak al verder met cyberrisico-management. De uitdaging hier is het gebrek aan OT-domeinkennis. IT-processen missen vaak de link met de fysieke impact van een cyberincident op menselijke veiligheid, het milieu of zware kostbare machines. Het is nuttig om te leren van hun processen en deze geschikt te maken voor OT door relevante impactgebieden toe te voegen.
- **Overkoepelend risicobeheer (ERM/CRM):** Grotere organisaties hebben mogelijk al een overkoepelend raamwerk voor risicobeheer. Als dit bestaat, is het zaak om hierbij aan te sluiten en OT-risico's te integreren. De uitdaging kan zijn dat OT-risico's, en de unieke impact ervan, nog geen onderdeel zijn van het bestaande raamwerk.

Wanneer er nog geen formeel raamwerk voor risicobeheer bestaat, kan een begin worden gemaakt met het opstellen van een uniforme matrix. Dit hoeft geen complex proces te zijn; het doel is om een gezamenlijke taal en meetlat te creëren. Gebruik de volgende input om een matrix op te zetten:

- **Start met de basis:** Begin met een eenvoudige matrix. Beperk het aantal impactgebieden (bijvoorbeeld financieel, veiligheid, milieu, reputatie) en kies een beperkt aantal risiconiveaus (bijvoorbeeld laag, medium, hoog). Dit maakt het proces overzichtelijk en haalbaar.
- **Gebruik bestaande kennis:** Ook al ontbreekt een formeel proces, meestal is er in de organisatie wel informele kennis aanwezig. Deel ervaringen met de IT-afdeling of de veiligheidsafdeling (HSE), aangezien zij te maken hebben met vergelijkbare uitdagingen. Door samen te werken, kan een eerste gezamenlijke opzet worden gecreëerd.
- **Afstemming acceptatieniveau:** Stel initiële acceptatieniveaus vast na overleg met het management. Wat wordt beschouwd als een lage of hoge impact? Stel dit vast voor alle impactgebieden.
- **Ga iteratief te werk:** Het is vrijwel onmogelijk om een matrix

in één keer perfect te maken. Ga iteratief aan de slag, evalueer de resultaten en verwacht meerdere herzieningen voordat een definitieve versie kan worden bekrachtigd door het management.

- **Formele goedkeuring:** De risicomatrix bepaalt de schalen en niveaus die de organisatie als acceptabel of onacceptabel beschouwt. Het is de verantwoordelijkheid van het management om de ingebouwde risicobereidheid en de risicotolerantieniveaus officieel te bekrachtigen.

Rollen en verantwoordelijkheden

Een goed risicobeheerproces valt of staat met duidelijke rollen en verantwoordelijkheden. Hoewel het management de eindverantwoordelijkheid draagt, moet op alle niveaus van de organisatie helder zijn wie welke taak uitvoert. Het is essentieel om te voorkomen dat taken en verantwoordelijkheden 'tussen wal en schip' vallen.

In de praktijk bestaat er vaak al een beeld van wie welke taken uitvoert, gebaseerd op informele afspraken of algemene HR-functiebeschrijvingen. Dit is echter niet altijd toereikend. Zo wordt de rol van Asset Owner vaak gebruikt om iemand eindverantwoordelijk te maken voor een installatie, maar is het binnen de organisatie niet altijd duidelijk of cyberbeveiligingsrisico's ook onder deze verantwoordelijkheid vallen. Hierdoor ontstaat onduidelijkheid over wie de leiding neemt bij het beheer van cyberdreigingen, wat de effectiviteit van het risicobeheerproces in de weg staat.

De volgende punten kunnen helpen bij het inrichten van rollen en verantwoordelijkheden voor OT-cybersecurity:

- **Definieer de rollen:** Definieer een set van benodigde rollen binnen de organisatie die essentieel zijn voor het uitvoeren van OT-cyberbeveiliging. Dit zorgt voor een duidelijke taakverdeling en voorkomt onduidelijkheid. In kleinere organisaties kunnen diverse rollen worden gecombineerd. Denk bijvoorbeeld aan de volgende rollen:
 - CISO (verantwoordelijk voor cybersecurity binnen de organisatie, echter niet altijd duidelijk of OT-security hier ook onder valt)
 - OT-Security Manager (overall verantwoordelijk en rapporteert aan management)
 - OT-Security analyst (uitvoeren van risicoanalyses, identificeren van kwetsbaarheden)
 - Technische experts (implementatie en onderhoud van beveiligingsmaatregelen)
 - Risicomanager (identificatie, classificatie en rapportage van risico's)
 - Compliance Officer (naleven van processen, normen, wet- en regelgeving)
 - Assesteigenaren (verantwoordelijk voor bepaalde assets, inclusief cybersecurity)
- **Beleg de taken:** Zorg ervoor dat alle praktische taken die nodig zijn voor het risicobeheerproces duidelijk zijn toegewezen aan personen of rollen. Dit gaat verder dan de algemene functiebeschrijvingen van HR. Het expliciet beleggen van deze

taken is essentieel voor een effectief en werkbaar risicobeheerproces. Beschrijf bijvoorbeeld:

- Wie is verantwoordelijk voor de uitvoering van risicoanalyses?
- Wie bepaalt de prioriteit van de te implementeren maatregelen?
- Wie mag het uiteindelijke restrisico accepteren?
- En wie escaleert naar het management als de voortgang stagneert of als er problemen zijn?
- **Aandacht voor competenties:** Een veelvoorkomend probleem in de praktijk is het kennisdilemma tussen IT- en OT-personeel. Waar IT-medewerkers vaak over de benodigde cybersecurity- en compliance-expertise beschikken, missen ze soms de specifieke domeinkennis van de OT-omgeving. Het omgekeerde is ook waar: OT-personeel heeft diepgaande kennis van de fysieke processen, maar minder ervaring met cybersecurity. Dit kan leiden tot miscommunicatie en ineffectieve beveiligingsmaatregelen. Overweeg betere samenwerking, cross-training, het opzetten van een hybride IT/OT-rol of gebruik te maken van externe specialistische ondersteuning.
- **Uitbesteding van taken:** Bij uitbesteding van OT-beheer blijft de verantwoordelijkheid voor het toezicht en de opvolging bij de organisatie. Dit moet duidelijk worden vastgelegd.
- **Formele vastlegging:** Idealiter worden rollen en verantwoordelijkheden formeel vastgelegd in documenten die door de organisatie en de betrokken individuen worden gecommitteerd. Vanuit verschillende wet- en regelgeving is dit ook een verplichting. Een minder formele aanpak, waarbij taken en verantwoordelijkheden in een overkoepelend document worden beschreven, kan als tussenoplossing dienen.
- **Mandaat en middelen:** Het is cruciaal dat de betreffende rollen het mandaat en de middelen hebben om hun taken naar behoren uit te voeren. Zonder deze bevoegdheid zal het risicobeheerproces in de praktijk niet werken.

2.4. Opzetten OT-Security Management System

Deze handreiking focust specifiek op het opzetten van OT-risicobeheer. Het is belangrijk om te benadrukken dat dit proces een onderdeel is van een groter geheel: een OT-Security Management System (ISMS of CSMS). Dit omvat alle processen rondom cybersecurity, van beleid en procedure tot technische maatregelen en de continue verbetering van de beveiliging. Het opzetten van een dergelijk systeem zou het uiteindelijke doel van elke organisatie moeten zijn, omdat alle losse puzzelstukken dan pas echt op hun plaats vallen.

Ook hier geldt: begin klein en leer van de IT-afdeling, waar een ISMS vaak al is geïmplementeerd. Het is mogelijk om een ISMS specifiek voor OT op te zetten, maar een geïntegreerde aanpak is meestal efficiënter.

Hier zijn een aantal belangrijke overwegingen:

- **Verschillen tussen IT en OT:** Kopieer niet zomaar een IT ISMS. De focus van IT ligt op de vertrouwelijkheid van data en informatie, terwijl bij OT de nadruk ligt op (persoonlijke) veiligheid en de beschikbaarheid en integriteit van fysieke processen. Technieken die in IT vanzelfsprekend zijn, kunnen in OT onmogelijk of onwenselijk zijn.
- **Juiste standaarden:** Een IT ISMS is vaak gebaseerd op de ISO 27000-reeks, terwijl het OT-equivalent vaak gebaseerd is op de IEC 62443-2-1-standaard. De IEC-standaard is specifiek ontwikkeld voor de unieke uitdagingen in OT-omgevingen. Door een internationaal erkende standaard te volgen, kan de organisatie ook gemakkelijker aantonen te voldoen aan wet- en regelgeving.
- **Integratie en efficiëntie:** Het aansluiten op een bestaand ISMS is de meest efficiënte aanpak en voorkomt veel overlap. Ga voor uniformiteit waar het kan en specialisatie waar het moet.
- **Een langetermijndoel:** Realiseer dat het opzetten van een compleet ISMS jaren kan duren. Dit betekent echter niet dat het een onbegonnen taak is; kleine stappen kunnen direct effect sorteren. Begin realistisch, verbreed en verbeter gaandeweg, en communiceer de verwachte tijdsduur duidelijk naar het management.

TIP: IT/OT ISMS

Een handige aanpak is om ervoor te zorgen dat de policies IT/OT-agnostisch zijn en dat de specifieke details in de procedures en guidelines zijn opgenomen.

Bijvoorbeeld: In plaats van specifieke patchmanagement frequenties voor OT-systemen op te nemen, kan de policy voorschrijven dat patches binnen het standaard op risico gebaseerde interval moet plaatsvinden. Dit kan zowel voor IT als voor diverse OT-componenten leiden tot verschillende frequenties. Details kunnen uitgewerkt worden in OT-procedures.

Kader 2.4a

TIP: Cybersecuritycultuur als fundament

Naast een formeel ISMS, betrokkenheid van het management en uitgewerkte rollen en verantwoordelijkheden, is een gezonde cybersecuritycultuur binnen de organisatie van cruciaal belang. Deze cultuur vormt tevens een goede indicator voor de volwassenheid van de organisatie op het gebied van risicomanagement.

Belang van bewustwording en motivatie

Het is essentieel om het belang van cybersecurity effectief over te brengen, medewerkers te motiveren en de gehele organisatie mee te nemen in dit proces. Hierbij is structurele ondersteuning vanuit de organisatie onmisbaar. Zorg voor adequate training en bewustwording bij alle stakeholders. Zolang stakeholders het belang van security niet inzien, blijft implementatie een moeizaam proces. Het is cruciaal te voorkomen dat security wordt gezien als een formaliteit, dat stappen worden overgeslagen vanwege toegenomen werkdruk, of dat risico's bewust lager worden ingeschat om aan toegenomen verplichtingen te ontkomen.

“Compliant moet je zijn, secure moet je willen zijn.”

De securityorganisatie als partner

Positioneer de securityorganisatie primair als adviseur en partner, niet als auditor. In plaats van voortdurend kritische vragen te stellen, kan het helpen om de eigen

verantwoordelijkheid van de uitvoerende organisatie te benadrukken. Een gefaciliteerd gesprek gebaseerd op wederzijds begrip kan juist zorgen voor de benodigde motivatie en betrokkenheid.

TIP: Security Champions programma

Implementeer een Security Champions programma: Selecteer enthousiaste medewerkers uit verschillende afdelingen die als ambassadeurs fungeren voor cybersecurity. Deze champions ontvangen extra training en worden verantwoordelijk voor het delen van kennis binnen hun teams. Zij kunnen collega's informeren over nieuwe dreigingen, best practices delen en fungeren als eerste aanspreekpunt voor securityvragen. Dit creëert een netwerk van betrokken medewerkers die security van binnenuit promoten, wat veel effectiever is dan top-downcommunicatie.

TIP: De brug slaan tussen HSE en cybersecurity

In een OT-omgeving hebben cyberaanvallen niet alleen impact op beschikbaarheid, maar kunnen ze ook directe gevolgen hebben voor de fysieke veiligheid. Door cybersecurity te presenteren als een cruciaal onderdeel van de bredere veiligheidscultuur – naast fysieke veiligheid en milieubescherming – wordt de urgentie en relevantie ervan direct duidelijk. Meestal zijn HSE-processen al beter verankerd in de cultuur van een organisatie en kan het daarom helpen om hierop aan te sluiten.

Kader 2.4b



3. Strategie en voorbereidingen

Dit hoofdstuk gaat dieper in op de juiste voorbereidingen voor een volledige risicoanalyse. Voor beginnende organisaties is de informatie uit het voorgaande hoofdstuk waarschijnlijk voldoende om te starten. In volgende iteraties, of voor organisaties die al iets verder zijn in het proces, wordt het belangrijker om de diepgang uit dit hoofdstuk mee te nemen.

3.1 Kaderen van risico's binnen de organisatie

De strategie van een organisatie voor cybersecurityrisicobeheer richt zich op het beoordelen, reageren (door risico's te mitigeren, ontwijken, overdragen of accepteren) en monitoren van risico's die specifiek verbonden zijn aan OT-systemen. Deze strategie geeft een expliciete invulling aan aannames, beperkingen, de mate van risicotolerantie en prioriteiten die een rol spelen bij belangrijke beslissingen. Bij het opstellen van een strategie voor cybersecurityrisicobeheer worden kans (likelihood) en impact de assen van de risicomatrix. Deze benadering zorgt ervoor dat risicobeheer een gestructureerd proces wordt.

De risicobereidheid (risk appetite) van een organisatie moet gekoppeld worden aan de risicomatrix. Risicobereidheid betekent de hoeveelheid risico die een bedrijf bereid is te accepteren bij het nastreven van haar doelen. Sommige risico's kunnen geaccepteerd worden, andere moeten worden verantwoord, en weer andere zullen ontoelaatbaar zijn. Het bepaalt grenzen voor het nemen van risico's en helpt bij het vaststellen van prioriteiten. Het bestuur of hoger management bepaalt de risicobereidheid en vertaalt dit naar specifieke richtlijnen voor risicobeheer. Deze richtlijnen beïnvloeden vervolgens de besluitvorming over welke risico's moeten worden aangepakt, geaccepteerd of gemitigeerd. Risicobereidheid speelt dus een cruciale rol bij het bepalen van de tolereerbare niveaus van risico die een organisatie wil dragen.

Behalve de risicobereidheid, is het belangrijk om na te denken over hoe de prioriteiten en doelstellingen van een bedrijf in het geding kunnen komen. Hierbij kan gedacht worden aan dreigingen van buitenaf (van 'script kiddies' tot 'nation state actors'), interne dreigingen (van apparaat-/systeemfalen tot ontevreden medewerkers), maar ook aan wettelijke verplichtingen en regelgevingen (zoals Cbw en AVG). Het is cruciaal om te bepalen welke risico's de organisatie wil accepteren en waarom, en welke absoluut niet. Hierbij is wederom een top-downaanpak vereist om te beslissen over de bescherming van belangrijke zaken en de uitleg waarom dit nodig is.

Voor veel organisaties is het een flinke opgave om tot een gedetailleerde risicoanalyse en -prioritering te komen. Een iteratieve aanpak is daarom vaak noodzakelijk. Wat zijn de grootste zorgen binnen de organisatie en hoe sluit een weerbare OT-omgeving hierbij aan? Een doordachte, gestructureerde scopebepaling is van belang om de risicoanalyse behapbaar te houden en optimaal het beschikbare budget, kennis en middelen in te zetten. Zodra dit goed loopt kunnen vervolgstappen gepland worden.

LET OP: Praktische overwegingen bij de risicomatrix

Bij het invullen van de risicomatrix zijn er een aantal belangrijke vragen en overwegingen:

- Zijn alle specifieke effectcategorieën van toepassing op OT-risico's en volgen deze een gelijke schaalverdeling ten opzichte van andere risico's in uw organisatie?
- Zijn voor de as van kans specifieke schalen gemaakt die passen bij moedwillige OT-aanvallen? (Zie ook paragraaf 5.3 Analyseren van de kans en impact)
- Is de bestaande risicomatrix van de organisatie geschikt voor OT-risico's, of is een OT-specifieke aanpassing nodig?

De vastgestelde risicobereidheid kan met behulp van de risicomatrix gevisualiseerd worden. Hierbij kan een organisatie meerdere risiconiveaus hanteren, afhankelijk van haar specifieke behoeften en risicotolerantie.

Het voorbeeld dat veel organisaties hanteren is als volgt: risico's met een lage score (groen) worden geaccepteerd, middenrisico's (oranje) vereisen een verplicht 'pas-toe-of-leg-uit'-beleid, terwijl hoge risico's (rood) altijd onacceptabel zijn en gemitigeerd moeten worden. Dit kan echter worden aangepast naar wens.

Kader 3.1a

Vervolgens is het zaak om inzichtelijk te krijgen hoe alle systemen binnen de OT-omgeving bijdragen aan de bedrijfsprocessen. De eerste stap hierin is het vaststellen van de belangrijkste objecten, processen of onderdelen binnen de organisatie: de zogenaamde 'kroonjuwelen'. Deze kunnen verspreid zijn over verschillende bedrijfsonderdelen, met elk hun eigen eigenaren en verantwoordelijken.

Kroonjuwelen kunnen zowel tastbare als ontastbare assets zijn. De meest relevante assets binnen de context van een OT-risicoanalyse zijn over het algemeen:

- **Fysieke apparaten:** Zoals machines, specifieke sensoren, of kritieke componenten.
- **Logische netwerken:** Essentieel voor communicatie tussen systemen en de kern van veel OT-processen.

Andere assets, zoals intellectueel eigendom of personeel, kunnen ook kroonjuwelen zijn, maar vallen vaak buiten de directe scope van een OT-specifieke analyse. De focus ligt op de systemen en processen die direct een grote impact kunnen hebben op de veiligheid of de bedrijfscontinuïteit. Uiteindelijk bepaalt het belang van een asset de juiste prioritering en rechtvaardigt dit de te nemen maatregelen.

Praktijkvoorbeeld: Kroonjuwelen

De OT-systemen die als 'kroonjuwelen' worden beschouwd, zijn sterk afhankelijk van de sector en de specifieke bedrijfsdoelstellingen.

Voorbeeld maritiem: In de maritieme sector kunnen dit bijvoorbeeld navigatiesystemen, communicatienetwerken, of lading- en voorraadbeheersystemen zijn. Schepen zijn bijzonder afhankelijk van systemen zoals GPS, elektronische kaartweergave en informatiesystemen (ECDIS) of automatische identificatiesystemen (AIS). Ook satellietcommunicatie, on-board wifi en andere communicatiesystemen voor diverse on- en offshoreoperaties kunnen kritiek zijn.

Het is van belang om te onthouden dat de definitie van een kroonjuweel kan verschillen per stakeholder. Vanuit het perspectief van de scheepsbemanning zijn de kroonjuwelen de systemen die een veilige navigatie en besturing van het schip garanderen. Vanuit de projectorganisatie, die verantwoordelijk is voor de commerciële operatie, kunnen systemen zoals baggerpompen of gasinstallaties ook als kroonjuweel worden beschouwd, omdat zij essentieel zijn voor het succes van het project. Dit verschil in perspectief is cruciaal voor een volledige risicoanalyse.

Voorbeeld luchtvaart: In de luchtvaartsector worden als kroonjuwelen vaak de vluchtbesturingssystemen, avionica-systemen of vluchtgegevens (operationeel/ onderhoud/plannen/passagiersinformatie) aangehaald.

Systemen die de vlucht controleren, autopilotsystemen en fly-by-wire technologie, maar ook communicatie-, navigatie- en surveillancesystemen kunnen van cruciaal belang zijn – zowel aan boord als in luchtverkeersleidings-systemen (ATC). Aangezien vliegtuigen steeds meer verbonden worden met grondnetwerken en het internet voor diensten zoals in-flight wifi of gegevensoverdracht, is het belangrijk om deze systemen te monitoren op (ongeautoriseerde) toegang of wijzigingen. Het gebruik van on-board wifi zonder goede segmentatie kan risico's met zich meebrengen, vooral omdat piloten bijvoorbeeld een tablet kunnen aansluiten op het vliegtuignetwerk, waardoor het compromitteren van de tablet kan leiden tot verstoringen van het netwerk.

Voorbeeld weg & spoor: OT-systemen worden steeds belangrijker in trein, tram en bus, zowel binnen het voertuig als connecties en afhankelijkheden van systemen erbuiten. In eerste instantie is het duidelijk dat de spanningsvoorziening op bovenleidingen van treinen en trams cruciaal zijn voor de bedrijfsvoering en deze systemen daarom als kroonjuweel worden beschouwd. Soortgelijk is de EV-laadinfrastructuur voor elektrische bussen.

Maar ook de communicatiesystemen tussen voertuig en de centrale verkeersleiding zijn belangrijk voor de dienstregeling, opvolging van calamiteiten en het waarborgen van de veiligheid van de reizigers. Zonder deze communicatie kunnen (of mogen) deze voertuigen niet meer verder rijden. Op basis van deze grootschalige effecten zijn dit soort systemen dus ook een kroonjuweel.

Casestudy: Een ongeluk zit in een klein systeem

In een experiment van de Cockrell School of Engineering van de Universiteit van Texas is een jacht van \$ 80 miljoen succesvol van koers veranderd met behulp van een aangepast GPS-apparaat. Dit experiment, uitgevoerd in de Middellandse Zee, maakte gebruik van een techniek genaamd 'spoofing', waarbij valse signalen werden verzonden om controle te krijgen over het GPS-systeem van het schip zonder dat dit werd gedetecteerd.

Dit experiment benadrukt de potentiële dreiging van spoofing voor zowel de maritieme als de luchtvaartsector. In drukke wateren zoals de Noordzee kan het verstoren van het GPS-signaal leiden tot desoriëntatie van het schip, met mogelijk catastrofale gevolgen zoals aanvaringen

met andere vaartuigen, navigatie naar ondiepe wateren of zelfs het raken van obstakels zoals windmolenparken. In de luchtvaart kan spoofing ertoe leiden dat vliegtuigen onjuiste positie-informatie ontvangen, wat risico's met zich meebrengt voor de navigatie in drukbevolkte luchtruimen. Het niet nauwkeurig kunnen bepalen van de positie van een object kan leiden tot ernstige ongelukken met mogelijk verlies van mensenlevens en milieuschade.

Er zijn wel opties beschikbaar om spoofing te detecteren of zelfs te voorkomen, maar die zijn vaak kostbaar of lastig te implementeren. Experts benadrukken het belang van menselijke interventie om inconsistenties in navigatiesystemen te detecteren en te corrigeren.

Casestudy: Een klein foutje, grote gevolgen

In 2024 was op het Centraal Station in Arnhem op een van de informatieschermen voor korte tijd een pornografische video zichtbaar, in plaats van de gebruikelijke bustijden. Er werd snel actie ondernomen door het scherm af te plakken om de reputatieschade te beperken. Later konden technische specialisten het probleem volledig oplossen. Achteraf bleek het niet te gaan om een geavanceerde hack, maar om een simpele instelling die niet was uitgezet. Hierdoor kon iedereen via een openbare verbinding een willekeurige video naar het scherm streamen.

Dit voorval laat zien dat een klein administratief foutje misbruikt kan worden met onvoorziene gevolgen. Hoewel de directe impact in dit geval beperkt bleef tot reputatieschade, had het incident veel ernstigere gevolgen kunnen hebben. Dezelfde kwetsbaarheid had gebruikt kunnen worden om gemanipuleerde gegevens te tonen, bijvoorbeeld over een vals veiligheidsincident, om zo chaos te veroorzaken op het station. Helemaal wanneer dezelfde informatie op meerdere of alle schermen getoond wordt, kan dit leiden tot paniek en onveilige situaties.

Casestudy: De link tussen fysieke en cyberrisico's in het spoor

Ondanks dat deze handreiking primair gaat over het beheersen van cybersecurityrisico's, is het belangrijk om ook stil te staan bij mogelijke fysieke risico's.

Neem bijvoorbeeld de bovenleiding van een tram: deze kan zowel moedwillig als per ongeluk worden beschadigd. Als de bovenleiding wordt ontworcht, krijgen de trams geen stroom meer en zullen ze abrupt tot stilstand komen. Dit kan midden op een druk kruispunt plaatsvinden, met als gevolg dat de stad volledig kan vastlopen.

Het effect van zo'n incident is verstrekkend: het ontworcht de stedelijke mobiliteit op meerdere niveaus. Niet alleen worden reizigers getroffen door vertraging en ongemak, maar ook hulpdiensten zoals ambulances en politie worden belemmerd in hun bewegingsvrijheid. De economische en maatschappelijke impact is aanzienlijk: werknemers kunnen niet op tijd komen, toeleveringsketens worden verstoord en de algehele stedelijke infrastructuur wordt ontworcht.

Dit voorbeeld illustreert hoe een ogenschijnlijk enkelvoudig incident verregaande gevolgen kan hebben voor de samenleving als geheel. Het onderstreept het belang van een holistische benadering van risicomanagement, waarbij zowel digitale als fysieke dreigingen worden meegewogen.

3.2 Vaststellen van de scope

Een risicoanalyse moet altijd worden uitgevoerd op basis van een duidelijk afgebakende scope. Dit beantwoordt de vraag: “Waar hebben we het over en wat nemen we wel of niet mee in deze analyse?” De scopebepaling is cruciaal voor een efficiënt proces en het benutten van de beschikbare middelen.

Binnen de IEC 62443-standaard wordt deze scope het ‘System under Consideration’ (SuC) genoemd. Dit is dan de afgebakende scope waarvoor een cyberbeveiligingsanalyse wordt uitgevoerd. Hierbij moeten ook de in- en uitgaande datastromen (‘inflow’ en ‘outflow’) gedefinieerd worden. Dus welke data van buitenaf het systeem binnenkomt en welke data het systeem verlaat; wat essentieel is voor het identificeren van kwetsbaarheden en het bepalen van de benodigde beveiligingsmaatregelen.

Bij het vaststellen van de scope is het van belang om te bepalen of alle systemen binnen het mandaat van de eigen organisatie of afdeling vallen. Denk hierbij aan (centrale) objecten die zich in het buitenland bevinden of onder de verantwoordelijkheid van partners en joint ventures vallen. Dit helpt bij het in kaart brengen van de grenzen van de analyse. Voor meer informatie over de omgang met externe partijen, zie het kader over Third-party Systemen en Diensten.

Afhankelijk van de organisatie kunnen vervolgens verschillende benaderingen worden gekozen om de scope vast te stellen.

- **Op basis van een groot, fysiek object:** De scope ligt op een groot en complex object, zoals een schip, verkeerscentrale of een complete fabriekshal. De vraag is hier of het logischer is om het object in zijn geheel te bekijken, of dat het wordt opgedeeld in kleinere gebieden met verschillende risicoprofielen. De mate van detail moet van tevoren worden bepaald. Een mogelijke toepassing is de ‘zone and conduit’-benadering, zoals beschreven in de IEC 62443. Hier wordt het proces in twee stappen opgeknipt. Een initiële analyse om te bepalen waar de grootste risico’s zitten en op basis hiervan het systeem op te delen in zones waar vervolgens een detailanalyse op wordt uitgevoerd.
- **Op basis van een klein losstaand object:** De scope wordt afgebakend op één enkel object of systeem, zoals een verkeersregelinstallatie of een specifiek navigatiesysteem op een schip. Het is hierbij essentieel om te bepalen of het object werkelijk losstaand is. Soms lijken kleine objecten onafhankelijk, terwijl er onverwachte afhankelijkheden zijn met andere systemen of processen, wat kan leiden tot overkoepelende risico’s. Extra nadruk op cascade-effecten is dus belangrijk.
- **Op basis van functionele processen:** Hier wordt de scope afgebakend op een specifieke bedrijfsfunctie of een proces waarin OT-systemen een integraal onderdeel zijn. In dit geval kunnen diverse installaties op verschillende fysieke locaties als één geheel worden beschouwd. Een voordeel hiervan is dat de negatieve effecten eenvoudiger te relateren zijn aan

de bedrijfsfunctie. Een potentieel nadeel is dat de complexiteit kan toenemen wanneer meerdere typen installaties, netwerken en afhankelijkheden tegelijkertijd moeten worden geanalyseerd.

- **Op basis van een project:** Deze aanpak wordt gebruikt wanneer risicoanalyses worden uitgevoerd op nieuwe of aangepaste systemen. De scope voor risicoanalyse is dan gelijk aan de projectscope. Hoewel de scope dus in dit geval duidelijk lijkt, is het belangrijk om alsnog de risico’s af te bakenen. Denk hierbij bijvoorbeeld aan de impact op een centrale controlekamer of andere centrale systemen die buiten de directe projectscope vallen, maar wel beïnvloed kunnen worden.

LET OP: Gedeelde systemen en afhankelijkheden

Tijdens het vaststellen van de scope ontstaan vrijwel altijd afhankelijkheden van andere systemen. De uitdaging hierbij is dat de verantwoordelijkheid voor risico’s gemakkelijk wordt afgeschoven op andere partijen of afdelingen.

Dit geldt met name voor ondersteunende systemen zoals de netwerkinfrastructuur, virtualisatieplatformen, centrale softwareoplossingen en andere gedeelde diensten. Deze systemen zijn vaak complex te analyseren vanwege hun gedeelde karakter, terwijl het essentieel is dat ook zij een duidelijke risico-eigenaar hebben.

Complexe situaties ontstaan bijvoorbeeld wanneer hoogrisico- en laagrisicosystemen hetzelfde netwerk delen, of wanneer meerdere laagrisicosystemen tegelijkertijd kunnen worden beïnvloed door één centraal systeem. Dergelijke risico’s worden vaak onderschat, omdat de afzonderlijke impact klein lijkt, terwijl de geaggregeerde schade cumulatief en onacceptabel groot kan zijn.

Daarom moet worden vastgesteld dat alle risico’s bij de juiste eigenaar worden belegd. Met name in grote organisaties kan dit zeer complex zijn en vraagt het om extra aandacht tijdens de scopedefinitie. Goede registratie van afhankelijkheden en geautomatiseerde overzichten vanuit ondersteunende systemen kunnen dit proces aanzienlijk vergemakkelijken.

LET OP: Aandachtspunten voor third-party systemen en diensten

Bij alle scopingbenaderingen is het cruciaal om systemen en diensten van derden expliciet mee te nemen in de analyse. Deze externe componenten, die variëren van cloudoplossingen en software tot onderhouds- en remote monitoringsystemen, vormen vaak kritieke schakels in de OT-omgeving en brengen specifieke risico's met zich mee.

Vaak ontstaat een gedeeld verantwoordelijkheidsmodel waarbij de organisatie en de leverancier specifieke securityverplichtingen hebben. Het is essentieel om helder te definiëren welke delen onder de eigen verantwoordelijkheid vallen en waar de grenzen liggen. Een gebrek aan duidelijke afspraken kan ertoe leiden dat beveiligingsmaatregelen tussen wal en schip vallen.

Daarom is het van belang om cybersecurity-eisen vast te leggen in contractuele afspraken en inkoop-eisen. Dit zorgt ervoor dat alle partijen hun verantwoordelijkheden kennen en dat er geen onduidelijkheid is over wie welke risico's beheert.

Kader 3.2b

3.3 Impactanalyse (Business Impact Analysis)

Na het bepalen van de scope volgt een impactanalyse, ook wel Business Impact Analysis (BIA) genoemd. Hierbij wordt bepaald wat de ergst mogelijke impact zou kunnen zijn als een OT-systeem uitvalt, ongeacht de oorzaak. Het element van kans wordt ook bewust achterwege gelaten. Het doel van deze analyse is om inzicht te krijgen in de potentiële problemen die kunnen ontstaan als er iets misgaat. Deze aanpak is met name gericht op het bepalen of aanvullende maatregelen nodig zijn, bovenop de reeds vastgestelde baselinemaatregelen.

De aanpak

Een impactanalyse hoeft geen complexe, tijdrovende exercitie te zijn. Natuurlijk is er informatie en betrokkenheid nodig van diverse specialisten, omdat zij de meeste kennis hebben van de systemen en de bijbehorende processen. Idealiter is dit een standaardproces waar de projecteigenaren, systeemeigenaren of businessowners verantwoordelijk zijn voor het uitvoeren, zij hebben ten slotte de meeste kennis van het systeem en zijn verantwoordelijk voor de risico's. De rol van het (OT-)cybersecurityteam is hierbij voornamelijk faciliterend en ondersteunend. Het team zorgt voor het overkoepelende overzicht en kan achteraf steekproefsgewijs de resultaten controleren of vergelijken met eerdere analyses.

Er is een delicate balans tussen het uitvragen van meer informatie en het behouden van het gemak voor de organisatie. Hoe meer detail wordt gevraagd, hoe meer kennis en expertise er nodig is, wat het proces tijd- en middelenintensief maakt. Hierbij is het van belang om lange en complexe vragenlijsten aan alle stakeholders te vermijden. Met name vragen die lastig zijn om te beantwoorden en vaak geen waardevolle acties opleveren. Dit kan leiden tot frustratie en het verlies van 'goodwill', waardoor vervolgstappen alleen maar meer moeite kosten. Deel het proces op in kleine stapjes en haal gericht informatie op met gerichte interviews.

Dit proces kan prima worden begeleid met een eenvoudige Excel-lijst waarin door middel van diverse vragen de analyse wordt vastgelegd en de uitkomst wordt bepaald. Deze vragen moeten helpen bij het bepalen van de potentiële impact van een worstcasescenario. De analyse richt zich puur op de effecten, en laat de kans op het incident bewust buiten beschouwing.

Om zeker te zijn dat alle invalshoeken worden meegenomen, wordt dit opgesplitst in categorieën. Idealiter sluit dit aan bij de bestaande bedrijfswaardenmatrix van de organisatie waar categorieën zoals veiligheid, milieu, financieel, beschikbaarheid, reputatie al met gedefinieerde schalen zijn beschreven. In dat geval bepaalt de maximale score op een van de gebieden de uiteindelijke uitkomst.

Een alternatief is het gebruik van de bekende IT-begrippen BIV (Beschikbaarheid, Integriteit, Vertrouwelijkheid), met optioneel privacy (BIVP). Hoewel deze begrippen van oorsprong uit de IT-wereld komen, zijn ze ook toepasbaar op OT-systemen en kunnen ze het proces voor sommige organisaties eenvoudiger maken, met name als deze bestaande processen al gebruikt worden. Het kan dan eenvoudiger zijn om hierop aan te sluiten. In dit geval kan de BIV-vraagstelling worden uitgebreid met OT-specifieke impactgebieden zoals veiligheid en milieu.

Denk hierbij aan vragen als:

- Heeft de beschikbaarheid van dit systeem impact op de veiligheid of kan het leiden tot milieu-incidenten?
- Kan de aantasting van de integriteit van dit systeem leiden tot schade aan apparatuur of veiligheidsrisico's?

Ongeacht de gekozen methodiek is het aan te raden gebruik te maken van concrete en simpele vragen gericht op de specifieke discipline. Stel bijvoorbeeld vragen als:

- Wat gebeurt er als het systeem een dag of week lang niet werkt? Een concrete tijdsduur benoemen is voor dit soort vragen extra belangrijk.
- Wat gebeurt er als deze gegevens bij een concurrent terecht komen of publiekelijk beschikbaar worden?
- Wat gebeurt er als een onbekwaam individu toegang krijgt tot de bediening van deze installatie?

Het (OT-)cybersecurityteam zal hierbij een ondersteunende rol houden en support bieden aan de stakeholders om deze analyse juist uit te voeren. Hierbij is belangrijk om objectieve informatie te verkrijgen. Sommige medewerkers onderschatten de mogelijke impact of risico's (bijvoorbeeld met de redenering "Dit is toch nog nooit gebeurd"), terwijl anderen de belangrijkheid juist overdrijven.

Resultaat

De uitkomst van de impactanalyse kan worden uitgedrukt in eenvoudige categorieën, zoals Laag, Midden en Hoog of Kritiek, Belangrijk en Ondersteunend. Bijvoorbeeld:

- **Hoog/kritiek:** Het systeem faciliteert een primair bedrijfsproces en kan worden gezien als een 'kroonjuweel'. Een OT-cyberincident kan verstrekkende gevolgen hebben voor de organisatie.

- **Middel/belangrijk:** Het systeem is ondersteunend aan een primair proces of faciliteert een ondersteunend proces. De impact van een OT-cyberincident is merkbaar, maar beheersbaar.
- **Laag/ondersteunend:** Het systeem is ondersteunend aan overige processen en heeft geen directe invloed op het primaire bedrijfsproces. De impact van een OT-cyberincident is in dit geval beperkt.

De uitkomst van de analyse kan worden gebruikt voor interne prioritering en als startpunt voor toekomstige, meer gedetailleerde risicoanalyses.

TIP: Integreer in de bedrijfscultuur

Het implementeren van een nieuwe aanpak kost tijd en kan in het begin stroef verlopen. Het belangrijkste is om te starten. Begin bijvoorbeeld met een vastgestelde timebox of kleinere groep stakeholders. Zo kan de organisatie leren welke expertise mist en/of dat er meer tijd nodig is.

Blijf het proces verbeteren en consequent herhalen. De ervaring leert dat de organisatie uiteindelijk een omslag kan maken, waardoor cybersecurity-onderdeel wordt van de bedrijfscultuur. Systeemeigenaren zullen dan, bijvoorbeeld bij nieuwe projecten, uit zichzelf naar de analyse vragen.

Dit proces kan worden versneld door cybersecurity-ambassadeurs aan te stellen. Deze ambassadeurs kunnen de ondersteunende functies overnemen, zodat het centrale cybersecurityteam zich kan richten op een meer controlerende en overkoepelende rol binnen de organisatie.

TIP: Integreer in het projectproces

Maak deze impactanalyse onderdeel van het projectmanagementproces. Door deze stap vast te leggen in de projectaanpak, wordt cybersecurity al in de beginfase van nieuwe projecten meegenomen. Hierdoor is dit proces ook makkelijker en sneller uit te rollen binnen de organisatie en wordt voorkomen dat er telkens nieuwe risico's worden geïntroduceerd.

TIP: Uitvoeren impactanalyse voor aankoop

Het is belangrijk om de impactanalyse uit te voeren nog voordat een nieuw product of systeem wordt aangeschaft. Dit maakt inzichtelijk wat het afhankelijkheidsrisico is en hoe de verantwoordelijkheden belegd moeten worden. Op basis van deze analyse kunnen bovendien de juiste cybersecurity-eisen worden meegenomen in het aanbestedings- of inkooptraject. Dit kunnen ook eisen zijn dat leveranciers en/of systemen voldoen aan wet- en regelgeving of bepaalde standaarden moeten volgen.

3.4 Maatregelen en vervolgstappen

Op basis van de impactanalyse wordt, samen met de proceseigenaar en overige stakeholders, bepaald welke aanvullende maatregelen nodig zijn naast de reeds vastgestelde baselines. Hierbij is het van belang om een kosten-batenanalyse uit te voeren. Houd hierbij niet alleen rekening met eenmalige kosten, maar ook met de voortdurende onderhoudskosten.

Deze extra kosten moeten uiteindelijk geaccepteerd worden door de verantwoordelijke persoon, wat in veel gevallen dezelfde proceseigenaar is. Dit heeft als voordeel dat onnodig veel extra maatregelen worden voorkomen. Een mogelijke uitdaging is dat de proceseigenaar, vanuit financiële overwegingen, de effecten anders kan gaan inschatten. Hier komt de ondersteunende rol van het OT-securityteam naar voren, dat de resultaten kan controleren en bij conflict kan escaleren.

De aanpak

Een mogelijke aanpak is om de uitkomst van de impactanalyse te koppelen aan de eerdergenoemde baselinemaatregelen, waarbij afhankelijk van de score een extra set aan maatregelen verplicht kan worden. De baseline wordt daarmee afhankelijk van het risico.

Om daarna nog eventuele restrisico's af te dekken, kan er uiteindelijk gekozen worden voor extra maatregelen, bovenop deze set aan baselines.

Ten slotte kan de uitkomst ook worden gebruikt voor interne prioritering, of als startpunt voor meer gedetailleerde risicoanalyses. Zo kan bijvoorbeeld een aanvullende risicoanalyse verplicht zijn wanneer een risico als 'hoog' is ingeschat.

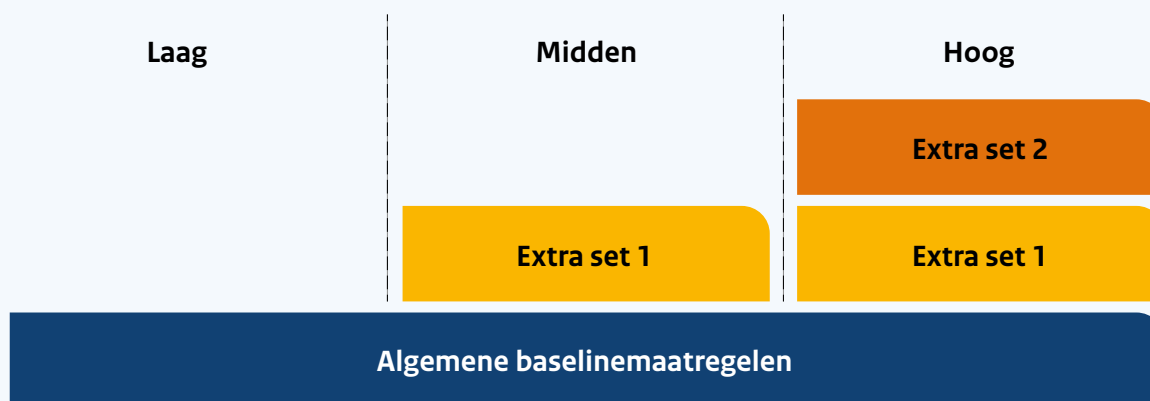
TIP: Gebruik een catalogus met gestandaardiseerde maatregelen

Wanneer extra maatregelen nodig zijn, is het verstandig om te zorgen voor een interne 'catalogus' met zoveel mogelijk gestandaardiseerde oplossingen. Dit voorkomt een wildgroei aan speciale maatregelen die uiteindelijk niet goed onderhoudbaar zijn voor de organisatie. Probeer daarom unieke oplossingen alleen als allerlaatste optie te gebruiken.

Deze catalogus kan gefaseerd worden opgezet op basis van bestaande en nieuw geïmplementeerde oplossingen. Bovendien kan deze inzicht geven in de verwachte extra kosten voor zowel de implementatie als het doorlopende onderhoud.

Kader 3.4a

Gelaagde maatregelenpakketten gebaseerd op BIA-score





Let op: Baseline is geen vervanging van een volledige risicoanalyse

Een op risico gebaseerde set aan baselines is een prima eerste stap, maar geen vervanging van een volledige risicoanalyse. Een baseline bestaat meestal uit een minimale, vaste set van basismaatregelen, terwijl elke installatie uniek is. Er is dus geen garantie dat de som van de maatregelen in dit specifieke geval de risico's voldoende afdekt. Een volledige risicoanalyse (zie hoofdstukken 4, 5 en 6) is daarvoor de volgende stap. De uitkomst van de effectanalyse kan natuurlijk wel de prioriteit van die risicoanalyse bepalen.

Kader 3.4b

Documentatie en herclassificatie

Ten slotte is het documenteren van alle stappen in dit proces van cruciaal belang. Dit omvat ook de gemaakte aannames over bijvoorbeeld de impact op beschikbaarheid, veiligheid en milieu. Uiteindelijk verklaart deze documentatie waarom bepaalde maatregelen wel of niet zijn genomen, en dient het als een waardevol startpunt wanneer de analyse in de toekomst wordt herhaald.

Het is verstandig om de impactanalyse periodiek te herhalen. De frequentie hiervan kan bijvoorbeeld worden afgestemd op de uitkomst: systemen met een hoge score kunnen vaker worden geanalyseerd dan systemen met een lage score. Een juist tegenovergestelde aanpak is om alle systemen met dezelfde frequentie opnieuw te analyseren. De gedachte hierachter is dat door ogenschijnlijk kleine aanpassingen of veranderingen het risicoprofiel van een systeem in de tussentijd

zodanig kan veranderen dat het van 'laag' naar 'hoog' verschuift.

Aanvullende overwegingen

Voor organisaties met een hogere volwassenheid op het gebied van risicobeheer, kan de BIA verder worden verdiept. Hieronder enkele aanvullende overwegingen voor een meer gedetailleerde analyse:

- **Meer genuanceerde scores:** Overweeg meer diverse uitkomsten of een gedetailleerde schaal, bijvoorbeeld van 1 tot 100, om de resultaten nauwkeuriger te kunnen prioriteren.
- **Gedetailleerde vragen:** Stel specifieke vragen om de risico's beter in kaart te brengen, zoals:
 - Kan het worstcasescenario ook daadwerkelijk door een cyberincident worden getriggerd?
 - Zijn er specifieke non-cybermaatregelen die de impact kunnen voorkomen of verkleinen?
 - Zijn er barrières meegenomen in de afweging die zelf ook beïnvloed kunnen worden door cyberaanvallen?
- **Relateer impact aan RAMSSHEEP:** Analyseer de impact op de bedrijfsprocessen aan de hand van de RAMSSHEEP-categorieën (Reliability, Availability, Maintainability, Safety, Security, Health, Environment, Economy, Politics), die een breder beeld geven dan alleen de traditionele BIV-categorieën. Zie het extra kader en tabel voor extra informatie over RAMSSHEEP.
- **Afhankelijkheden en cascade-effecten:** In grotere en complexere omgevingen kunnen systemen op elkaar ingrijpen. Het is van belang om afhankelijkheden van nevensystemen, 'common causes' en cascade-effecten mee te nemen in de analyse.
- **Integratie met business continuity management (BCM):** Een BIA is een cruciaal onderdeel van BCM. De inzichten uit de analyse, zoals de impact op de bedrijfsvoering bij uitval, kunnen direct worden gebruikt in BCM-plannen om de bedrijfscontinuïteit te waarborgen.

RAMSSHEEP - Impactcategorieën

Zoals eerder genoemd, kan een cyberincident in OT verder gaan dan alleen financiële schade, of impact hebben op de beschikbaarheid, integriteit of vertrouwelijkheid van een systeem.

Zowel directe als indirecte impact kan leiden tot verstoring van vitale systemen, productieverlies, veiligheidsrisico's en zelfs milieuproblemen. De maximale impact wordt dan ook bepaald door de gehele infrastructuur en eventuele onderlinge afhankelijkheden.

Om deze impact volledig te duiden, is het van belang om het worstcase-effect van alle relevante impactcategorieën te analyseren. Vanuit IT wordt vaak alleen gekeken naar de categorieën BIV (Beschikbaarheid, Integriteit, Vertrouwelijkheid). Voor OT kan dit ook worden gebruikt, maar in veel gevallen is dit niet voldoende. Er zijn meer impactcategorieën van toepassing, zoals Reliability, Availability, Maintainability, Safety, Security, Health, Environment, Economy en Politics – vaak afgekort als RAMSSHEEP. De volgende tabel geeft een gedetailleerde uitleg van deze categorieën.

Integriteit (Reliability)	Cyberincidenten kunnen de integriteit van objecten beïnvloeden, zoals sabotage of aanpassingen in automatisering. Terwijl productieverlies door cyberincidenten of storingen kan optreden, vormt bewuste sabotage een apart risico. Aanvallers kunnen systemen overnemen, commando's uitvoeren en beveiligingsmechanismen omzeilen. Documenteer aannames en mogelijkheden vanuit cyberperspectief.
Beschikbaarheid (Availability)	Het is van cruciaal belang om realistische hersteltijden vast te stellen en noodplannen te maken voor incidenten. Dit omvat het mobiliseren van personeel, het herstellen van back-ups en het opnieuw opstarten van systemen. Proeven tonen aan dat hersteltijden van twee tot vier weken gebruikelijk zijn, maar dit moet goed gedocumenteerd worden. Handmatige bediening als back-up moet niet alleen theoretisch, maar ook praktisch haalbaar zijn, met geteste procedures en voldoende gekwalificeerd personeel.
Onderhoudbaarheid (Maintainability)	Het vermogen om een systeem of apparatuur gemakkelijk en kosteneffectief in een staat te houden waarin het gerepareerd, onderhouden of bijgewerkt kan worden gedurende de hele levenscyclus. Onderhoudsvriendelijkheid speelt een belangrijke rol, omdat een systeem dat moeilijk of kostbaar is om te onderhouden kan leiden tot meer downtime, verminderde beschikbaarheid, hogere operationele kosten en mogelijk compromissen kan sluiten over veiligheid en andere kritische factoren.
Veiligheid (Safety)	Dit omvat risico's die kunnen leiden tot fysieke schade, letsel of verlies van mensenlevens binnen de operationele omgeving.
Beveiliging (Security)	De bescherming van systemen en informatie tegen onbevoegde toegang, gebruik, openbaarmaking, verstoring, wijziging of vernietiging. Dit omvat ook het lekken van persoonlijke gegevens of OT-gerelateerde data. Broncode, leveranciersgegevens of inloggegevens van apparaten/objecten zijn doelwitten voor hackers om te verkopen en/of toegang te verschaffen in het netwerk.
Gezondheid (Health)	Hierbij wordt gekeken naar risico's die de gezondheid van medewerkers of betrokkenen in het OT-systeem kunnen beïnvloeden, zoals blootstelling aan gevaarlijke stoffen.
Milieu (Environment)	Dit omvat de risico's die impact hebben op het milieu, zoals vervuiling, lozing van schadelijke stoffen of ecologische schade.
Economie (Economy)	Risico's die financiële gevolgen hebben, zoals verlies van inkomsten, productievertragingen of kosten voor herstel na een incident. Ook moet schade aan derden meegenomen worden, in de maritieme sector kan hierbij bijvoorbeeld gedacht worden aan een aanvaring.
Politiek (Politics)	Hierbij gaat het om risico's die verband houden met politieke aspecten, zoals wettelijke naleving, regelgevende problemen of geopolitieke factoren die de bedrijfsvoering kunnen beïnvloeden.

Casestudy: Cascade-effecten bovenleiding op de verkeersdoorstroming

Wat is het ergste dat er kan gebeuren? Stel jezelf die vraag bij een risicoanalyse voor het bovenleidingsysteem van een tram. Als het centrale SCADA-systeem uitvalt, zal dit impact hebben op de stroomvoorziening. In dat geval krijgt de tram ook geen stroom meer en staat abrupt stil. In het ergste geval natuurlijk net op een punt, een kruising, waar het voor flinke hinder in de doorstroming kan zorgen.

Misschien wel op diverse plekken in de stad. Op ongunstige, drukke tijden kan dit al snel het gevolg hebben dat het verkeer begint vast te lopen, omdat auto's en bussen er lastig of niet door kunnen komen. Er ontstaan steeds meer files. Uiteindelijk zou dit zelfs problemen kunnen opleveren voor hulpdiensten die daardoor niet meer tijdig op hun bestemming kunnen aankomen. Kortom, een systeemfout die uiteindelijk kan uitlopen op een groter maatschappelijk probleem.

Een soortgelijk scenario zou bijvoorbeeld ook kunnen ontstaan door falende verkeersregelinstanties, bruggen en sluizen die open blijven staan of tunnelsystemen die belangrijke toegangswegen kunnen afsluiten.

Casestudy: Ludieke teksten op informatiescherm

Dit voorbeeld is van wat langer geleden en gaat over het 'hacken' van de informatiedisplays in een trein van NBMS (België), waar normaal gesproken de volgende bestemming wordt getoond. Hier kwamen tot twee keer toe ludieke teksten te staan, die vervolgens veelvuldig op social media werden gedeeld. Vanuit publiekelijk beschikbare informatie is het niet duidelijk geworden hoe (en of) de systemen gehackt zijn. In oktober 2014, na het eerste incident, was de reactie van NMBS: "Dit kan echt niet" en "De bewuste trein werd stilgezet om de boodschap te verwijderen". En de NMBS is een onderzoek gestart dat moet uitwijzen hoe dit heeft kunnen gebeuren.

Tevergeefs, want in april 2015 gebeurde hetzelfde. NMBS geeft nogmaals aan dit verder te onderzoeken. "De boodschappen zijn er om onze reizigers te informeren en hebben ook een bepaalde veiligheidsfunctie", aldus NMBS. De berichten zijn nogmaals verwijderd.

Naast de impact op stilstand, het niet beschikbaar zijn van schermen die ook een veiligheidsfunctie hebben en de kosten van het onderzoek gaat het hier toch voornamelijk over reputatieschade.

Kader 3.4d

Kader 3.4e



Casestudy: Van kwaad tot erger: een maritiem worstcasescenario

Via een USB-stick ingevoegd door de bemanning vindt malware zijn weg naar de OT-systemen van het ballastwatersysteem. Deze systemen zijn cruciaal voor het handhaven van de stabiliteit van het vaartuig, vooral tijdens kritieke momenten zoals ruwe zeeën of bepaalde offshore-operaties. De impact van de malware kan leiden tot vertragingen in de controlesignalen op het netwerk, wat resulteert in verminderde responsiviteit en veerkracht van het ballastsysteem. Dit verhoogt het risico op instabiliteit tijdens al gevoelige situaties, wat kan resulteren in gevaarlijke situaties, zoals kapseizen of verlies van lading.

Verder kan het downloaden van malware op de veiligheidssystemen van de laadinstallatie leiden tot onverwacht gedrag tijdens de reis. Dit kan variëren van ongeautoriseerde toegang tot de ladingssystemen tot plotselinge uitschakelingen of storingen, waardoor het moeilijk wordt om de lading te controleren en te onderhouden. Als gevolg hiervan kan de veiligheid van het vaartuig en de bemanning in gevaar komen, vooral als de lading gevaarlijke stoffen betreft die een risico vormen bij lekkage of explosie.

Stel nu een combinatie voor van beide bovenstaande situaties, waarbij ook de hoofdmotor van het vaartuig plotseling uitvalt door beschermingsmechanismen, en als reactie op de gedetecteerde malware. Tijdens manoeuvres in de haven kan een volledige stroomuitval resulteren in het verlies van controle over het vaartuig, wat kan leiden tot aanvaringen met andere schepen, beschadiging van de haveninfrastructuur en milieuschade door gelekte brandstof of lading. Het kan ook gevolgen hebben voor de veiligheid van de bemanning, met mogelijk letsel of verlies van mensenlevens als gevolg van een ongeval.

Een worstcasescenario als dit kan ondergebracht worden in de volgende categorieën:

Milieu: Het gebruik van malware kan leiden tot instabiliteit van het vaartuig, wat op zijn beurt gevaarlijke situaties kan veroorzaken, met mogelijke schade aan de omgeving en het ecosysteem.

Veiligheid & gezondheid: De veiligheid van het vaartuig en de bemanning kan in gevaar komen door onverwachte storingen of uitschakelingen van vitale systemen als gevolg van malware-infectie.

(Financiële) middelen (assets): beschermingssysteem en vitale infrastructuur van het vaartuig kunnen beschadigd raken, wat leidt tot verlies van bedrijfsmiddelen en herstelkosten.

Reputatie & legislatie: Een dergelijk incident kan de reputatie van de rederij of het scheepvaartbedrijf schaden, vooral als het leidt tot ongevallen, milieuschade of verlies van mensenlevens.

Cascade-effecten: Het uitvallen van belangrijke systemen kan leiden tot een kettingreactie van gebeurtenissen, zoals stroomuitval, aanvaringen met andere schepen en milieurampen, met verstrekkende gevolgen voor zowel het vaartuig als de omgeving.

	Financieel	Assets	Omgeving	Veiligheid	Legislatie	Reputatie	Cascade-effecten
0	Geen schade	Geen schade	Geen schade	Geen schade	Geen schade	Geen schade	Geen schade
1	Minimaal	Minimaal	Minimaal	Minimaal	Minimaal	Minimaal	Minimaal
2	Matig	Matig	Matig	Matig	Matig	Matig	Matig
3	Aanzienlijk	Aanzienlijk	Aanzienlijk	Aanzienlijk	Aanzienlijk	Aanzienlijk	Aanzienlijk
4	Ernstig	Ernstig	Ernstig	Ernstig	Ernstig	Ernstig	Ernstig
5	Catastrofaal	Catastrofaal	Catastrofaal	Catastrofaal	Catastrofaal	Catastrofaal	Catastrofaal

3.5 Benodigde kennis en expertise

Voor een nauwkeurige beoordeling van de impact van een incident is de juiste expertise van cruciaal belang. Naast de technologische aspecten gaat het ook om de veiligheidsimplies en mogelijke financiële, juridische en ecologische gevolgen. De input van een multidisciplinair team is daarom een vereiste. Ontoereikende inzichten kunnen essentiële zaken over het hoofd zien en de inschatting van de worstcase-impact vertroebelen.

Dit betekent echter niet dat men altijd met twintig personen uren moet vergaderen. Het is vooral van belang dat gericht de juiste kennis wordt opgehaald en dat wordt gegarandeerd dat alle relevante aspecten worden meegenomen in de analyse. Ook hier is het weer belangrijk om klein te beginnen, een kleine groep om ervaring op te doen en informatie op te halen. Mocht blijken dat veel vragen elke keer onbeantwoord blijven, dan is het misschien toch efficiënter de groep iets uit te breiden.

Hiernaast staan een aantal voorbeelden van belangrijke rollen die nuttig kunnen zijn bij het maken van een juiste en complete securityanalyse. Dit zijn dus niet allemaal OT-specifieke rollen. In veel organisaties, en met name in kleinere organisaties, is het aannemelijk dat niet alle disciplines aanwezig zijn. Soms worden taken door anderen uitgevoerd. Gebruik de lijst hiernaast als een soort checklist om zeker te zijn dat alle relevante invalshoeken worden meegenomen.

Relevante rollen voor OT-risicoanalyse

Risicobeheerder: Bepaalt de risiconiveaus, keurt maatregelen goed en accepteert resterende risico's.

Chief information security officer (CISO): Waarborgt de kwaliteit van (IT-)risicoanalyse en -beheer, met diepgaande kennis van cybersecurity. Mogelijk is de CISO ook verantwoordelijk voor compliance.

Financieel expert: Beoordeelt de financiële gevolgen en integreert deze in bestuurlijke beslissingen en rapportages.

Technisch specialist: Heeft diepgaande technische kennis van OT-systemen en kan de impact van falende componenten inschatten.

Procesexpert: Begrijpt het operationele proces en kan de impact van falende processen beoordelen. Voor de maritieme sector kan dit bijvoorbeeld een maritiem officier zijn.

Automatiseringsdeskundige: Begrijpt procesautomatisering en beoordeelt de technische impact van dreigingen op geautomatiseerde processen.

Leverancier/externe dienstverlener: Bezit specifieke kennis van de OT-systemen die de organisatie afneemt en kan inzicht geven in de kwetsbaarheden en de impact van storingen.

Juridisch adviseur: Kent juridische aspecten van privacy, aansprakelijkheid en compliance binnen OT-cyberbeveiliging.

Milieuexpert: Beoordeelt mogelijke milieuimpact van cyberincidenten en de kosten voor herstel.

Netwerkarchitect of -beheerder: Kent de netwerkarctitectuur van OT-systemen en beoordeelt de impact op ICT-gebied.

Incident response specialist: Heeft expertise in het omgaan met incidenten en het herstellen van systemen na een cyberaanval.



4. Identificeren

4.1 Identificeren van Assets

De eerste stap in elk risicobeheerproces is het verkrijgen van een compleet en actueel inzicht in het OT-landschap van de organisatie. Het principe is eenvoudig: je kunt niet beschermen wat je niet kent.

Definitie NCSC: *“Operationele Technologie (OT) is een verzameling van technologieën bestaande uit software- en hardwaresystemen die in samenhang verantwoordelijk zijn voor het besturen, bewaken en beheren van fysieke processen.”*

Denk aan alle technologie die nodig is om schepen te besturen, treinen te laten rijden, bruggen en sluizen operationeel te houden en vliegtuigen veilig te laten landen.

Het is van belang om stipt om te gaan met systemen die in een grijs gebied vallen, zoals bijvoorbeeld betaalsystemen, camera's of informatieschermen. Er is niet per se een goed of fout antwoord, omdat hun classificatie vaak afhangt van de impact die ze hebben op de bedrijfsvoering. Een systeem wordt meestal als IT geclassificeerd als het primair gericht is op het verwerken en beveiligen van data, zoals een kassa die transacties registreert. Hetzelfde systeem wordt vaker als OT beschouwd als het directe invloed heeft op een fysiek proces.

Een aantal voorbeelden:

- Een informatiescherm dat puur reclame toont, wordt meestal als IT aangemerkt. Maar als datzelfde scherm ook wordt gebruikt om vluchtroutes te tonen tijdens een noodsituatie, heeft het een duidelijke impact op de veiligheid en wordt het vaker als OT gezien.
- Een camerasysteem dat alleen toezicht houdt op personeel is meestal geclassificeerd als IT. Maar als de camera tevens een automatisch hek of een alarmsysteem aanstuurt om veiligheidsrisico's te beheren, krijgt het een OT-component.
- Een betaalsysteem is meestal IT, maar wanneer dit ook deuren, poortjes of sloten bedient, heeft het een fysieke impact en wordt het vaak beschouwd als OT.

Het belangrijkste van deze IT/OT-classificatie is te voorkomen dat systemen buiten het zicht van beide disciplines vallen en vergeten worden in de risicobeoordeling. Een goede interne definitie voor IT en OT is daarom een voorwaarde.

Assetregister

Een grondig en volledig overzicht van alle assets is van cruciaal belang. Het assetregister is de centrale plek waar alle informatie over de OT-systemen wordt vastgelegd. Dit register vormt de basis voor alle verdere stappen in het risicomanagementproces.

Voor een bruikbaar assetregister concentreer je je op de volgende informatie:

- **Asseteigenaar:** Wie is er verantwoordelijk voor de asset en heeft het mandaat om beslissingen te nemen en/of maatregelen te laten doorvoeren?
- **Technische specificaties:** Focus op de details die je nodig hebt voor risicoanalyse, zoals model, hardwaretype, firmware- en softwareversies en netwerkadressen. Dit maakt het makkelijker om kwetsbaarheden te herkennen en te beheren. Het is hierbij van belang dat de hoeveelheid details wordt afgestemd op het volwassenheidsniveau van de risicoanalyse. Voorkom het aanleggen van complexe lijsten die (op dit moment) niet nodig zijn.
- **Functionele waarde en bedrijfsprocesrelatie:** Wat doet het systeem en welk bedrijfsproces wordt erdoor ondersteund? Deze informatie helpt te begrijpen hoe een asset bijdraagt aan de bedrijfscontinuïteit en het belang ervan te bepalen.
- **Kritikaliteit:** Categoriseer assets op basis van hun potentiële impact. Wat is het ergst mogelijke gevolg als het systeem uitvalt of wordt gecompromitteerd? Dit kan worden aangegeven met labels als 'laag', 'midden' of 'hoog'. Zo is direct duidelijk waar de meeste aandacht aan moet worden besteed.
- **Optionele assets:** Overweeg om ook niet-tastbare assets op te nemen, zoals bedrijfskritische informatie of intellectueel eigendom. Dit is vooral relevant als deze assets direct gerelateerd zijn aan de OT-omgeving.

Voorbeeld: Opzetten van het assetregister

Stap 1 – De minimale basis

Start met de basisinformatie die direct nodig is voor de risicoanalyse. Laat andere, minder relevante informatie achterwege. Een goed voorbeeld is het serienummer. Hoewel dit vaak wordt vereist in een assetregister, voegt het in de meeste gevallen weinig toe aan de risicobeoordeling. Bovendien is het bij OT-apparatuur vaak alleen handmatig te verkrijgen, wat een tijdrovende klus is. Mogelijk zijn ook niet meteen alle assets nodig en kan gestart worden met alleen de assets die verbonden zijn aan het netwerk (IP-enabled). De volgende gegevens zijn een goed begin en kunnen later worden uitgebreid, afhankelijk van de behoeften van de organisatie:

- **Assetnaam:** Een duidelijke, unieke naam, bijvoorbeeld Besturingspaneel Schip 1 - Motor 1.
- **Locatie:** De fysieke locatie van de asset (bijvoorbeeld Machinekamer B, Controlekamer).
- **Rol/functie:** Een korte omschrijving van wat de asset doet (bijvoorbeeld 'Monitort motortemperatuur' of 'Stuurt navigatiesysteem aan').
- **Eigenaar:** De persoon of afdeling die verantwoordelijk is voor de asset.
- **Netwerkverbinding:** Vermeld het netwerkadres (bijvoorbeeld IP-adres) of de netwerkn naam.
- **Fabrikant & model:** De naam van de fabrikant en het modelnummer.
- **Besturingssysteem/software:** Vermeld het gebruikte besturingssysteem en de belangrijkste softwareversies.
- Deze informatie biedt direct inzicht in de kritieke assets en hun functionele waarde.

Stap 2 – Extra verdieping

Zodra deze basis is vastgelegd, kan later, afhankelijk van de risicoclassificatie, worden besloten of extra informatie nodig is. Details zoals serienummers kunnen later alsnog belangrijk worden, bijvoorbeeld wanneer ze gekoppeld zijn aan licenties of supportcontracten. Ook andere specifieke informatie, zoals MAC-adressen, alle geïnstalleerde software, firmwareversies en de patchstatus, kan op een later moment nodig zijn bij het verhogen van het volwassenheidsniveau van het risicobeheer. Er zijn tools beschikbaar die dit proces deels kunnen automatiseren.

Stap 3 – De laatste details

Afhankelijk van het risicoprofiel en het volwassenheidsniveau van een organisatie kunnen extra details nodig zijn voor het uitvoeren van een complete en diepgaande risicoanalyse.

Om een volledig gedetailleerd overzicht te krijgen, is het essentieel om inzicht te hebben in alle subsystemen die door een leverancier zijn geïnstalleerd. Hiervoor is een Hardware Bill of Materials (HBOM) of Software Bill of Materials (SBOM) noodzakelijk. Zonder deze informatie kan het gehele systeem alleen als een 'black box' worden beschouwd.

Dit soort documentatie is van groot belang voor het aanpakken van supplychainrisico's. Zonder deze informatie is het voor een organisatie onmogelijk om de zwakheden van specifieke apparaten (bijvoorbeeld een machine met een geïntegreerde communicatiegateway) of softwarecomponenten (bijvoorbeeld zwakheden in softwarebibliotheken) in te schatten.

Kader 4.1a

Netwerktekeningen:

Naast het assetregister is het cruciaal om de afhankelijkheden en connectiviteit tussen assets goed te begrijpen.

Netwerktekeningen zijn hierbij onmisbaar, met name om de scheiding tussen IT- en OT-systemen en de onderlinge verbindingen van alle OT-systemen inzichtelijk te maken.

Gewone (as-built) systeemtekeningen kunnen nuttig zijn, maar zijn in de praktijk vaak niet gedetailleerd genoeg voor cybersecuritydoelstellingen. Afhankelijk van de complexiteit van het

systeem zijn specifieke logische en fysieke netwerktekeningen aan te raden.

- **Logische netwerktekeningen:** Deze tekeningen focussen op hoe data stroomt tussen systemen, los van de fysieke locaties en kabelverbindingen. Ze zijn ideaal om de architectuur en de scheiding in zones te visualiseren. Volg meteen het Purdue model om segmentering (of gebrek daaraan) direct zichtbaar te maken. Dit type tekening is met name van belang bij het gebruik van virtualisatie, VLANs en geavan-

ceerde netwerkconfiguraties. IP- en netwerkadressen zijn vaak handig om hieraan toe te voegen, omdat dit de abstracte structuur direct koppelt aan de technische realiteit.

- **Fysieke netwerktekeningen:** Deze tekeningen geven de daadwerkelijke fysieke lay-out weer, inclusief locaties van apparatuur, racks en kabelverbindingen. Ze zijn essentieel voor fysieke beveiliging en bij het oplossen van storingen. Om ze nog gedetailleerder te maken, kan hier ook informatie over kabelnummers en fysieke netwerkpoorten aan worden toegevoegd.

LET OP:

Enkel in bezit zijn van het assetregister en netwerktekeningen is niet voldoende: onderhoud en updaten van bestaande tekeningen is cruciaal om vat te houden op de omvang van, en objecten binnen, aanwezige netwerken. **Ook uitgaan van de correctheid van (oude) as-built tekeningen kan een risico met zich meebrengen.**

Kader 4.1b

Een belangrijk aspect is het vastleggen van functionele afhankelijkheid tussen netwerken om zo de mogelijke impact van een storing of aanval op de gehele bedrijfsvoering in te kunnen schatten. Dit helpt bij het identificeren van cascaderende effecten. Om deze tekeningen efficiënt te maken, is het aan te raden om dezelfde benamingen te gebruiken als in het assetregister. Dit zorgt voor consistentie en maakt het makkelijker om tussen de documenten te navigeren.

TIP: Een pragmatische aanpak voor netwerktekeningen

Start niet met een poging om elke kabel te tekenen. Begin met een eenvoudig overzicht dat direct inzicht geeft in de communicatielijnen tussen de assets en netwerken. Zeker in kleinere systemen is het wellicht mogelijk om fysieke en logische details in één overzicht op te nemen.

- **Plot alle assets:** Plot alle assets uit het register op de tekening in een logische volgorde. Dit kan fysiek, op basis van IP- en netwerkadressen, of op basis van functionele rol. Het doel is om deze assets in groepen te verdelen, de zogenaamde logische zones en segmenten. De realiteit is echter dat veel netwerken niet volgens dit ideale model zijn gebouwd. Het doel van de tekening is dan om de afwijkingen van dit model te visualiseren, zodat zwakke plekken duidelijk worden.
- **Scheiding IT en OT:** Geef op de tekening de scheiding tussen de IT- en OT-netwerken duidelijk aan. Markeer waar de verbindingen tussen beide domeinen lopen en via welke apparatuur, zoals firewalls. Dit is de basis van elk OT-beveiligingsmodel.
- **Focus op kritieke verbindingen:** Geef de communicatiepaden van de meest kritieke verbindingen duidelijk aan op de tekening. Denk hierbij aan de verbindingen tussen de controlekamer en PLC's, toegang op afstand, of verbindingen naar externe netwerken.

Deze aanpak levert direct inzicht in de risico's van de netwerkkarchitectuur en helpt bij het identificeren van zwakke plekken. Gedetailleerde, fysieke netwerktekeningen kunnen later worden gemaakt, maar een heldere, logische tekening is de basis voor elke risicoanalyse.

Kader 4.1c

4.2 Identificeren van kwetsbaarheden

Een dreiging kan pas een risico vormen als deze kan profiteren van bestaande zwaktes. Hoewel een systeem in theorie vrij kan zijn van kwetsbaarheden, kent de realiteit altijd bekende en onbekende zwakheden. Deze zwakheden kunnen zich op verschillende niveaus voordoen, namelijk:

- **Mensen:** De menselijke factor is cruciaal. Kwetsbaarheden hierbij zijn gerelateerd aan kennis, expertise, gedrag en de bedrijfscultuur die de omgang met cybersecurity beïnvloedt.
- **Processen:** Dit verwijst naar het ontbreken of het niet naleven van beveiligingsprocessen, bijvoorbeeld rondom onderhoud, wijzigingen of eigendom.
- **Technologie:** Hierbij gaat het om gebrekkige scheiding van OT-netwerken, verouderde apparatuur, niet-geïnstalleerde beveiligingspatches en andere technische tekortkomingen.

Voor een effectieve risicoanalyse is het verzamelen van nauwkeurige informatie over de OT-omgeving essentieel. Een stapsgewijze en gelaagde aanpak is hiervoor de meest effectieve methode. De al opgestelde documenten, zoals het assetregister en de netwerktekeningen, vormen hiervoor een essentieel startpunt. De volwassenheid van een organisatie bepaalt de frequentie en de diepgang waarmee deze stappen worden doorlopen.

- **Documentanalyse:** Begin met het raadplegen van alle beschikbare documenten, zoals ‘as-built’ tekeningen, handleidingen en onderhoudslogboeken. Deze methode is snel en kosteneffectief en geeft direct een eerste overzicht. Het nadeel is dat documentatie vaak onvolledig of verouderd is en de actuele situatie niet weerspiegelt. Gegevens uit het assetregister kunnen ook worden gebruikt om een koppeling te maken met bekende kwetsbaarheden (CVE's), zoals gepubliceerd door instanties als het NCSC, CISA of in de NVD (National Vulnerability Database).
- **Interviews en observatie:** Praat met de OT-engineers, operators en ander personeel dat dagelijks met de systemen werkt. Zij bezitten vaak cruciale, informele kennis die niet in documenten te vinden is. Dit onthult waardevolle informatie, maar de verkregen kennis kan subjectief of onvolledig zijn en vraagt om tijd van het personeel.
- **Inventarisatie en veldwerk:** Voer een fysieke inspectie uit in de OT-omgeving. Met de informatie uit de documenten en interviews kan deze inspectie gerichter worden uitgevoerd. Veldwerk is zeer nauwkeurig en essentieel voor het vastleggen van ongedocumenteerde assets. Het is echter arbeidsintensief en kan de operatie tijdelijk verstoren.

- **Netwerkanalyse:** Maak gebruik van geautomatiseerde tools om het netwerk te analyseren. Dit omvat passieve monitoring om verkeer te ontdekken en, indien verantwoord, actieve scans om kwetsbaarheden te vinden. Deze methode is efficiënt voor het ontdekken van alle aangesloten systemen. Het vereist wel technische expertise en is in gevoelige OT-omgevingen potentieel risicovol.

Een grondige analyse vereist goed inzicht in de kwetsbaarheden in de OT-omgeving en hoe deze bijdragen aan het geheel. Hierbij is het van belang om een balans te vinden in de mate van detail. Het vaststellen van een oneindige lijst van kwetsbaarheden is zelden het doel. Op een gegeven moment leiden nog meer geïdentificeerde zwakheden niet tot fundamenteel andere maatregelen of acties. De focus dient daarom te liggen op het vinden van de meest kritieke kwetsbaarheden die het risicoprofiel significant beïnvloeden en waarop direct actie ondernomen kan worden.

TIP: Start met een baseline gap-analyse

Zoals eerder beschreven, is het voor veel organisaties efficiënt om te beginnen met een pragmatische set van basismaatregelen. Het streven is dat deze overal zijn geïmplementeerd. In daaropvolgende iteraties kan deze set worden uitgebreid om, wanneer nodig, uiteindelijk te voldoen aan een norm zoals IEC 62443 of CSIR.

De eerste stap is dan een baseline gap-analyse waarbij de huidige beveiliging wordt vergeleken met deze baseline. Dit geeft een direct overzicht van de meest fundamentele tekortkomingen. De focus ligt hierbij op het identificeren van de ‘quick wins’ en het verhogen van het basisbeveiligingsniveau. De pragmatische aanpak dient als een beheersbaar startpunt en richt zich op de naleving van de baseline.

Hoewel een gap-analyse een uitstekend startpunt is, is deze niet hetzelfde als een volledige kwetsbaarheidsanalyse. Een gap-analyse toetst de naleving van bekende maatregelen. Een volledige analyse omvat ook onderzoek naar onbekende kwetsbaarheden of specifieke software- en firmwarekwetsbaarheden die niet per se in de norm of baseline staan, maar wel een risico vormen.

4.3 Identificeren van bestaande maatregelen

Het in kaart brengen van bestaande maatregelen is een cruciale stap in de risicoanalyse. Deze maatregelen verminderen de waarschijnlijkheid en impact van risico's en vormen een belangrijke factor bij de uiteindelijke risicobeoordeling. Door een inventarisatie te maken, voorkomt u bovendien dat er onnodig dubbel werk wordt gedaan. Het is efficiënt om deze inventarisatie gelijktijdig met de identificatie van kwetsbaarheden uit te voeren, aangezien beide processen vergelijkbaar zijn en elkaar aanvullen.

Bestaande maatregelen zijn over het algemeen onder te verdelen in de volgende categorieën:

- **Fysieke maatregelen:** Denk aan beveiliging van gebouwen, toegangscontrole met deuren en sloten, en fysieke scheiding van netwerken.
- **Technische maatregelen:** Dit omvat firewalls, netwerk- en systeemarchitectuur, en het gebruik van detectie- en loggingtools.
- **Processen en organisatorische maatregelen:** Hieronder vallen onderhoudsprocedures, incident response-plannen, beleid voor toegang tot systemen, en beleid voor het onboarden en offboarden van personeel.
- **Menselijke maatregelen:** Dit heeft betrekking op trainingen, screenings en bewustwordingscampagnes die de menselijke factor versterken.

De gap-analyse ten opzichte van een baseline, die eerder als startpunt werd genoemd voor het identificeren van kwetsbaarheden, is een eerste stap. Deze inventarisatie richt zich vooral op het vaststellen van de aanwezigheid van een aantal fundamentele maatregelen.

Voor organisaties met een hogere volwassenheid is het echter noodzakelijk om verder te gaan dan deze baseline. In dat geval wordt een uitgebreidere beoordeling uitgevoerd aan de hand van industriestandaarden zoals IEC 62443, of algemene best practices. Deze beoordeling gaat dieper dan alleen het vaststellen dat maatregelen aanwezig zijn. Het draait ook om het bepalen van hun effectiviteit en het volwassenheidsniveau van de bijbehorende processen. Dit biedt een diepgaand inzicht in de werking van de maatregelen en identificeert eventuele hiaten in hun implementatie.

TIP: Overlap met andere disciplines

Cyber risico's bestaan niet in een vacuüm. Het is essentieel om te onderkennen dat bepaalde risico's ook al zijn vastgesteld en beheerd door andere disciplines, zoals Business Continuity Management, fysieke beveiliging of HSE (Health, Safety, & Environment). De maatregelen die daarvoor genomen zijn, hebben vaak een directe invloed op het OT-cyberrisicoprofiel, zowel in positieve als negatieve zin.

Positieve synergie: Eisen vanuit fysieke beveiliging en HSE (Health, Safety, and Environment) kunnen de maximale impact van een cyberincident helpen reduceren. Door deze disciplines te betrekken, kunnen maatregelen die oorspronkelijk voor andere doeleinden zijn genomen, een onbedoeld maar waardevol beveiligingsvoordeel opleveren.

- Vanuit fysieke beveiliging: Strikte maatregelen zoals paslezers en elektronische sloten die de toegang tot een controlekamer beperken, beveiligen het OT-systeem ook tegen ongeautoriseerde fysieke toegang. Dit neemt een potentiële aanvalsvector weg die ook door cybercriminelen kan worden gebruikt.
- Vanuit HSE: Veiligheidseisen kunnen fysieke maatregelen vereisen die indirect de impact van een cyberaanval verkleinen. Zo kunnen automatische uitschakelsystemen bij oververhitting, of detectoren voor gaslekages en brandmelders, snel reageren op fysieke schade die mogelijk ook door een cyberincident veroorzaakt zou kunnen worden.

Potentiële conflicten: Soms kunnen vereisten uit andere disciplines in conflict komen met cyberbeveiligingsmaatregelen. Denk bijvoorbeeld aan vluchtroutevoorschriften voor een machinekamer op een schip. Deze vereisen dat een deur te allen tijde geopend kan worden, wat het onmogelijk maakt om diezelfde ruimte volledig fysiek af te sluiten met elektronische sloten en paslezers. In dergelijke gevallen verhoogt de veiligheidseis de kwetsbaarheid en daarmee het cyber risico. Het vinden van een balans tussen deze disciplines is dan ook cruciaal.

4.4 Identificeren dreigingen

De eerste stap is het bepalen van de typen dreigingen die relevant zijn voor deze OT-omgeving. Dit vormt de basis voor de analyse en zorgt voor een gerichte aanpak.

- **Opzettelijke dreigingen:** Dit zijn dreigingen die voortkomen uit bewuste, vijandige acties. Denk aan aanvallen door cybercriminelen, statelijke actoren, of kwaadwillende insiders. In de context van cybersecurity worden deze dreigingen vrijwel altijd meegenomen in de analyse.
- **Onopzettelijke dreigingen:** Deze dreigingen zijn het gevolg van incidenten die 'per ongeluk' gebeuren, vaak door onkunde of onoplettendheid van medewerkers. Gezien het menselijke element in veel OT-omgevingen, maken ook deze incidenten vaak een integraal onderdeel uit van de dreigingsscope.
- **Systeem- en infrastructuurfalen:** Deze categorie omvat risico's die inherent zijn aan de systemen zelf, zoals het falen van hardware en software door veroudering, of de uitval van interne stroomvoorziening. Hoewel de oorzaak niet bij cyber ligt, kunnen deze incidenten leiden tot hetzelfde verlies van functionaliteit, beschikbaarheid of integriteit. Het meenemen van deze risico's in een OT-risicoanalyse is daarom een strategische keuze om de operationele veerkracht van de organisatie holistisch te beoordelen en niet enkel te focussen op één type dreiging.
- **Omgevingsrisico's:** Dit zijn externe factoren die de systemen kunnen beïnvloeden, zoals natuurrampen (bijvoorbeeld overstromingen), brand, of maatschappelijke factoren (bijvoorbeeld beslissingen van nutsbedrijven). Hoewel de impact op de OT-omgeving enorm kan zijn, worden deze risico's vaak beheerd binnen andere risicomanagementkaders, zoals business continuity management of fysieke beveiliging. Het is essentieel om expliciet te beslissen of deze risico's wel of niet worden meegenomen in de OT-risicoanalyse, om dubbel werk te voorkomen en de verantwoordelijkheden duidelijk te beleggen.

Het vaststellen van de dreigingsscope is een strategische keuze die moet worden afgestemd op de doelen van de risicoanalyse en de bredere risicomanagementstrategie van de organisatie.

Casestudy: De menselijke factor als zwakte: Maritiem

Dit voorbeeld van onopzettelijke dreiging laat zien hoe een zwakte kan ontstaan zonder dat er sprake is van een kwaadwillende actor.

Via een gratis verkregen USB-stick van een bemanningslid vindt malware zijn weg naar de OT-systemen van het ballastwatersysteem. Dit systeem is essentieel voor het handhaven van de stabiliteit van het vaartuig. Het gevolg is dat de controlesignalen op het netwerk vertraagd zijn, wat de responsiviteit en veerkracht van het ballastsysteem beïnvloedt. Dit creëert een risico voor momenten waarop de stabiliteit van het vaartuig cruciaal is, zoals in ruwe zee of tijdens bepaalde offshore-operaties.

Dit incident onderstreept het feit dat de menselijke factor een belangrijke zwakte kan zijn. Onbedoeld en onwetend kan er veel schade worden aangericht. Daarom is bewustzijnsstraining voor zowel personeel aan boord als aan land essentieel bij het identificeren en mitigeren van zwakheden.

Kader 4.4a



De volgende stap is inzicht te krijgen in de specifieke dreigingen voor de eigen organisatie. “Waar moeten en willen we ons tegen beschermen?” Dreigingen kunnen vanuit diverse invalshoeken komen, zowel van externe als interne bronnen. Het type dreigingsactor is daarbij van belang, aangezien hun motivatie, middelen en capaciteiten daaraan gekoppeld zijn. Inzicht wordt verkregen door informatie uit de volgende bronnen te verzamelen:

- **Algemene dreigingsbeelden:** Informatie opgesteld door nationale en internationale instanties, zoals het ENISA of het NCSC.
- **Sectorspecifieke dreigingsbeelden:** Beschikbare informatie via sectoren, bijvoorbeeld via ISAC's (Information Sharing and Analysis Centers) of commerciële partijen.

- **Leveranciersinformatie:** Beveiligingsadviezen en updates van leveranciers van OT-systemen en software.
- **Interne informatie:** Kennis uit eerdere incidenten, logbestanden of observaties van het personeel.
- **Gestructureerde analyse:** Het uitvoeren van een dreigingsanalyse met behulp van algemene of sectorspecifieke dreigingslijsten.
- **Open source intelligence (OSINT):** Informatie verkregen uit openbare bronnen, zoals beveiligingsblogs en fora.
- **Geautomatiseerde tools:** Data uit securitytools, zoals vulnerability scanners en intrusion detection systemen.

TIP: Dreigingsscenario's zijn een handig hulpmiddel voor starters

Voor organisaties die net beginnen met risicobeheer, kan het verzamelen en verwerken van deze informatie overweldigend zijn. Een praktische aanpak is om te starten met een set standaarddreigingsscenario's. Een scenario beschrijft de stappen die leiden tot een incident: een dreiging die een of meerdere kwetsbaarheden misbruikt, vaak met een specifieke intentie en wat leidt tot een concrete impact.

Deze dreigingsscenario's kunnen worden gebruikt als uitgangspunt om na te denken over de kans en impact, zonder dat er direct diepgaand technisch onderzoek nodig is. Om te garanderen dat alle relevante aspecten worden meegenomen, is het aan te raden de scenario's eerst op te delen in externe en interne dreigingen. Vervolgens kan binnen beide categorieën een verdere verdeling worden gemaakt naar opzettelijke en onopzettelijke dreigingen. Als extra hulpmiddel kan worden gecontroleerd of de scenario's voldoende aandacht besteden aan fysieke, menselijke, procesmatige of technische kwetsbaarheden.

Uiteindelijk moet hier ook een balans worden gevonden. Een overcomplete lijst met scenario's zal uiteindelijk niet leiden tot andere maatregelen. Het is mogelijk dat veel scenario's ook op elkaar lijken en voor de analyse niet veel toevoegen. Begin daarom met een compacte lijst die wel is afgestemd op de organisatie en die rekening houdt met de bovengenoemde dreigingscategorieën. Een lijst van 10-15 scenario's is vaak al een behoorlijk goed startpunt.

Hieronder staan een aantal voorbeeldscenario's uitgewerkt. Deze geven een beeld van hoe de risico's kunnen worden gecategoriseerd, van de dreiging tot de uiteindelijke impact:

- **Externe dreiging (opzettelijk):** Een externe cybercrimineel krijgt ongeautoriseerde toegang tot het centrale OT-netwerk via een kwetsbaarheid in een oudere server. De aanvaller installeert ransomware met de intentie om losgeld te eisen, waardoor alle systemen en bijbehorende bedrijfsprocessen niet meer functioneren.
- **Interne dreiging (opzettelijk):** Een ontevreden medewerker met legitieme toegang tot de systemen van het controlecentrum verandert een instelling in de software. Het doel is om onrust en vertraging te veroorzaken. De veranderde instelling leidt tot storingen en onverwacht gedrag van automatiseringsprocessen, wat financiële schade en reputatieverlies tot gevolg heeft.
- **Interne dreiging (onopzettelijk):** Een technicus maakt tijdens onderhoudswerkzaamheden per ongeluk een fout in de configuratie van een netwerkcomponent. De fout leidt tot een onderbreking van de communicatie met een cruciaal OT-systeem. De impact is een verlies van omzet en extra kosten voor herstel.

Dit soort scenario's zijn perfect om inzicht te krijgen in de mogelijke risico's en de bijbehorende effecten, en om de juiste personen erover te laten meedenken.

Casestudy: Een hypothetisch voorbeeld van algemeen naar specifiek

Stel dat 'Maritiem OT B.V.' de eigenaar is van een vloot containerschepen. Het is bekend dat de maritieme sector een belangrijk doelwit is voor cyberaanvallen.

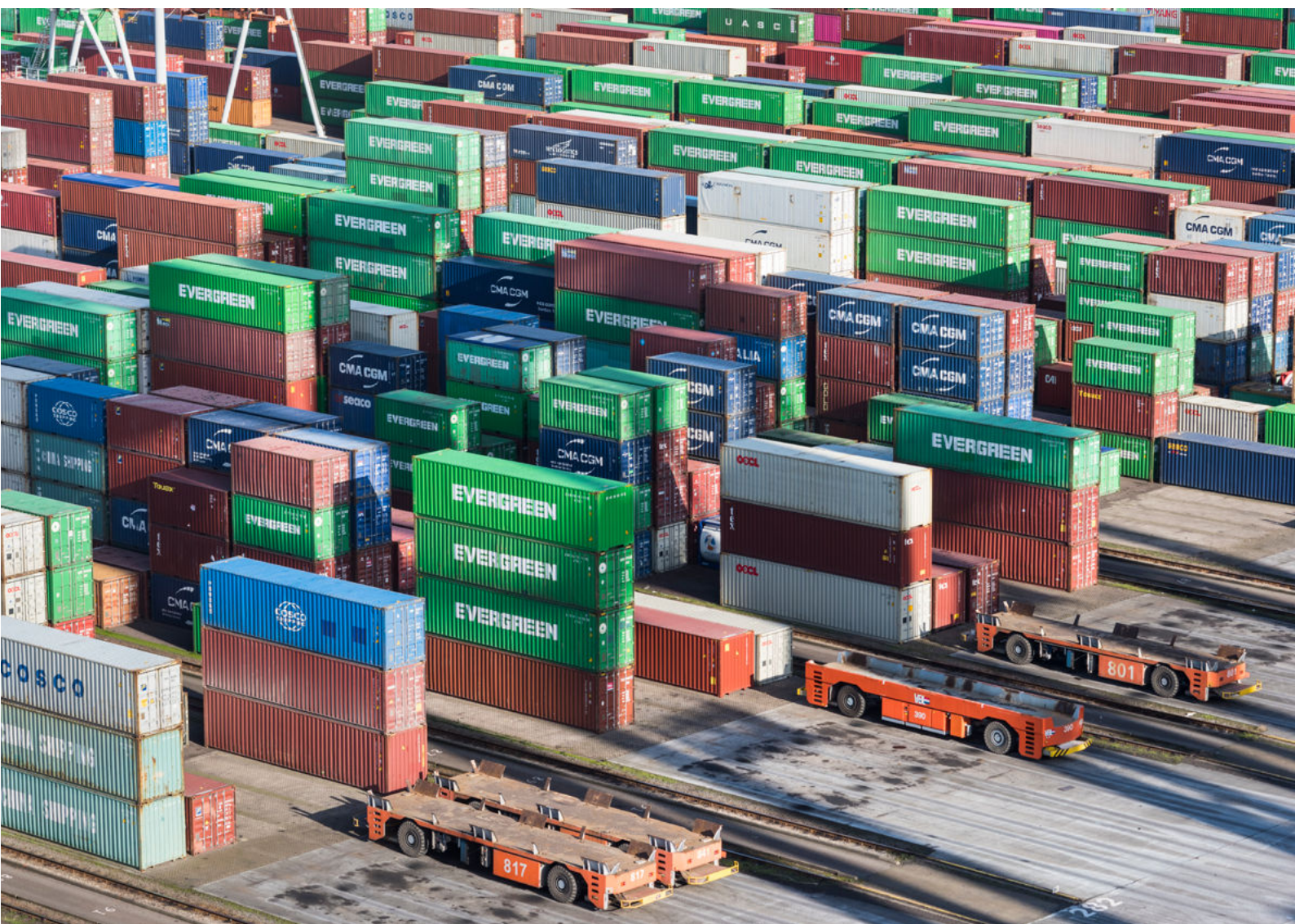
- **Algemene dreigingsbeelden (NCSC):** De risicomanager leest een jaarrapport van het NCSC. Daarin staat dat er een algemene toename is van ransomware-aanvallen op kritieke infrastructuur, waaronder de transportsector. Dit is een nuttige waarschuwing, maar de informatie is te breed om direct actie op te ondernemen.
- **Sectorspecifieke dreigingsbeelden (ISAC):** Vervolgens deelt het Maritieme ISAC een specifiek dreigingsbeeld. Het rapport beschrijft dat aanvallers gebruikmaken van een onbekende kwetsbaarheid in een specifieke merknaam van satellietssystemen, die veel voorkomt in de maritieme sector. Deze informatie is al relevanter, maar er is nog geen concrete oplossing.
- **Leveranciersinformatie:** Kort na het ISAC-rapport stuurt de leverancier van het satellietstelsel een beveiligingsadvies (security advisory). Hierin staat dat er

een kritieke kwetsbaarheid is ontdekt in de firmware van bepaalde modellen. De leverancier heeft nu een patch beschikbaar gesteld en geeft concrete instructies voor het beveiligen van het systeem. Dit is directe, bruikbare informatie die een urgente actie vereist.

- **Interne informatie:** De OT-engineer van Maritiem OT B.V. herinnert zich een eerdere, onverklaarbare communicatiestoring op een van de schepen, die nooit volledig is opgelost. Na het zien van de dreigingsinformatie en het vendor-advies, kan de engineer de incidenten aan elkaar koppelen en vaststellen dat er mogelijk al een eerdere poging tot aanval is geweest.

Conclusie: Door alleen te vertrouwen op de algemene dreigingsbeelden zou Maritiem OT B.V. wel bewust zijn van het risico van ransomware, maar niet weten dat de vloot specifiek in gevaar was. Alleen door de informatie van het NCSC, het ISAC, de leverancier en de eigen interne kennis te combineren, kan de organisatie op tijd de nodige maatregelen nemen.

Kader 4.4c



5. Analyseren

Dit hoofdstuk beschrijft de benodigde stappen voor een verdere, verdiepende analyse van OT-cybersecurityrisico's. De analyse is de fase waarin de kans op een incident en de impact van dat incident worden samengebracht om het daadwerkelijke risico te bepalen.

Voor een effectieve en betrouwbare risicoanalyse zijn de volgende uitgangspunten van cruciaal belang. Ze bouwen voort op de voorbereidende stappen uit de vorige hoofdstukken:

- **De juiste basis (scoping en impactanalyse):** Een correcte uitvoering van de scoping en impactanalyse (zoals beschreven in het vorige hoofdstuk) vormt het fundament. Zonder dit fundament kunnen risico's verkeerd worden ingeschat of blijven belangrijke bedreigingen onontdekt.
- **Organisatorische cultuur en ondersteuning:** De juiste procesondersteuning en een sterke cybersecuritycultuur binnen de organisatie zijn essentieel. Adequate ondersteuning versnelt het proces en waarborgt de kwaliteit, terwijl een goede cultuur voorkomt dat risico's bewust buiten scope worden geplaatst of te laag worden ingeschat om extra werkbelasting te vermijden.
- **Duidelijke rollen en besluitvorming:** De aanwezigheid van duidelijke rollen, verantwoordelijkheden en processen is noodzakelijk. Deze governancestructuur is essentieel om beslissingen over risicoacceptatie te nemen, acties op te volgen en risico's tijdig te escaleren naar het juiste managementniveau.

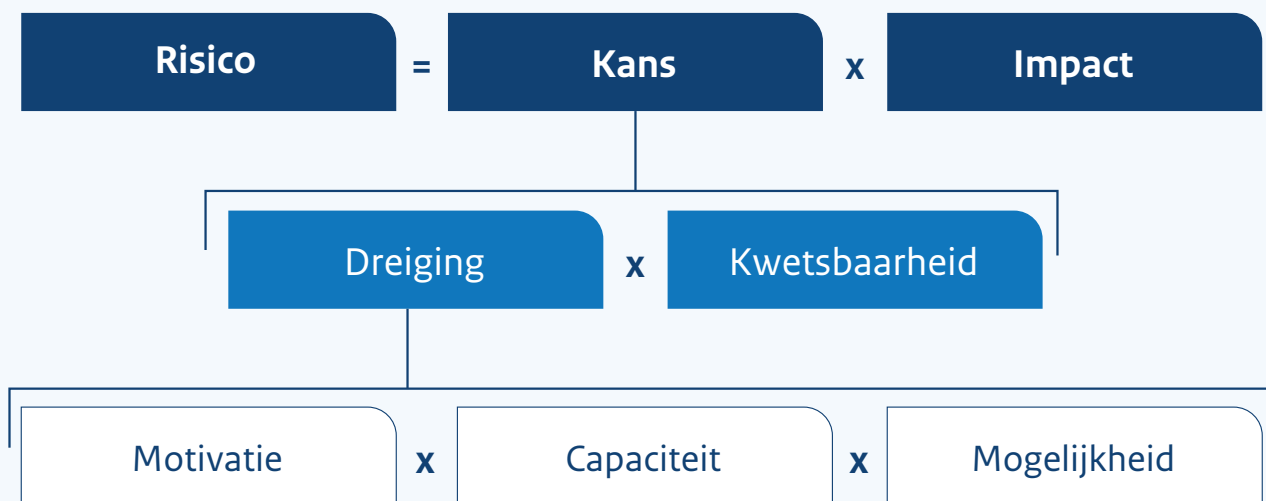
5.1 De context van cybersecurityrisico's

Het doel van de analyse is om het risico van potentiële incidenten te kwantificeren. Het risico wordt traditioneel bepaald door de combinatie van de kans dat een gebeurtenis plaatsvindt en de impact ervan, eerder ook weergegeven met de volgende formule: **risico = kans x impact**.

In de context van cybersecurity is kans echter geen statistische waarschijnlijkheid, maar een kwalitatieve inschatting van de waarschijnlijkheid dat een bepaalde dreiging een bestaande kwetsbaarheid van het systeem misbruikt. Die 'dreiging' is weer een samenspel van de factoren motivatie, capaciteit en de mogelijkheid. Dit is schematisch weergegeven in het diagram onder aan deze pagina.

Dit betekent dat de risico's van de gevonden kwetsbaarheden pas echt duidelijk worden als ze worden geanalyseerd in de unieke context van de gedefinieerde scope van de OT-omgeving. Een volledige analyse beoordeelt de kans en impact van elke kwetsbaarheid, en houdt ook nog rekening met de specifieke dreigingen, de waarde van de asset en de potentiële impact op mens en milieu.

Model voor Dreiging, Kwetsbaarheid en Risicoanalyse



Dreigingsprofiel (Motivatie en Capaciteit)

Het begrijpen van de relatie tussen het dreigingsprofiel, zoals eerder geïdentificeerd (zie paragraaf 4.4) en het profiel van de aanvaller is essentieel voor effectief cyberrisicobeheer. Het dreigingsprofiel omvat de specifieke risico's waarmee de organisatie wordt geconfronteerd op basis van zijn sector, grootte en infrastructuur. Het profiel van de aanvaller omvat hun motivatie en capaciteiten.

Dreigingsactoren zijn zeer divers en variëren sterk in hun motivaties en doelen. Een aantal voorbeelden van de meest voorkomende actoren zijn:

- **Criminele organisaties:** Streven financiële winst na via ransomware en datadiefstal.
- **Nationale staten:** Richtten zich op spionage of geopolitieke belangen.
- **Hacktivist:** Focussen zich op milieukwesties of politieke agenda's.
- **Interne betrokkenen (insiders):** Kunnen ontevreden werknemers zijn die gevoelige informatie lekken of toegangsprivileges misbruiken.

Het is cruciaal te benadrukken dat al deze actoren verschillende capaciteiten (technische kennis en kunde) en motivatie hebben.

Zo beschikken meerdere nationale staten waarschijnlijk over voldoende capaciteiten om de OT-infrastructuur zodanig aan te vallen dat dit zorgt voor significante disruptie of zelfs impact op mens en milieu. Toch ontbreekt vaak de motivatie om dit te doen, waarbij factoren als de geopolitieke situatie en de specifieke sector doorslaggevend zijn. Daartegenover staat de interne medewerker, die mogelijk een lage technische capaciteit heeft, maar wel beschikt over legitieme toegang, interne kennis en wachtwoorden, wat de drempel voor een aanval enorm verlaagt. Beide voorbeelden benadrukken de unieke dynamiek van de dreigingsactoren en laten zien dat kans een complexe afweging is tussen deze factoren.

Mogelijkheid

De mogelijkheid duidt op de mate waarin een dreigingsactor een bestaande kwetsbaarheid succesvol kan misbruiken. De gevonden zwakheden geven een potentiële mogelijkheid, maar de context van bestaande maatregelen kunnen deze mogelijkheid weer (deels) beperken. De ontdekte kwetsbaarheden en netwerktekeningen (zie hoofdstuk 4) dienen als input om de mogelijkheid van een succesvolle aanval te beoordelen.

De mogelijkheid is afhankelijk van twee factoren:

- **Bereikbaarheid:** Zijn de kwetsbare assets geïsoleerd of zijn ze verbonden met externe netwerken? Hoe makkelijk is het voor de dreigingsactor om de barrières (zoals netwerksegmentatie of fysieke beveiliging) te omzeilen?

- **Complexiteit/moeilijkheid:** Niet alle ontdekte zwakheden zijn even eenvoudig te misbruiken. Een zwakte in gespecialiseerde industriële apparatuur is vaak moeilijker te misbruiken dan bekende kwetsbaarheden in algemene software, waarvoor vaak kant-en-klare exploits bestaan.

Om de twee factoren van de mogelijkheid – de bereikbaarheid en de complexiteit/moeilijkheid – gestructureerd te beoordelen, kan een eenvoudige matrix worden gebruikt. Deze methode helpt om een kwalitatieve score voor de totale mogelijkheid te bepalen, wat cruciaal is voor de inschatting van de kans.

De onderstaande figuur illustreert hoe de combinatie van de bereikbaarheid van de asset en de moeilijkheid van het exploiteren van de zwakheid leidt tot een gezamenlijke inschatting (laag, middel of hoog) van de aanvalsmogelijkheid.

Moeilijkheid	Bereikbaarheid Makkelijk	Bereikbaarheid Middel	Bereikbaarheid Moeilijk
	Middel	Hoog	Hoog
Makkelijk	Middel	Hoog	Hoog
Middel	Laag	Middel	Hoog
Moeilijk	Laag	Laag	Middel

Deze visuele weergave onderstreept dat de aanvalsmogelijkheid hoog is wanneer een kwetsbaarheid bijvoorbeeld zowel makkelijk bereikbaar als eenvoudig te misbruiken is. Deze kwalitatieve score is een directe component van de totale kans op een gerealiseerde aanval.

- **Hoge mogelijkheid** (zoals de combinatie makkelijk/makkelijk in de matrix) betekent dat de drempel voor een dreigingsactor om succesvol te zijn, zeer laag is. Zelfs een actor met beperkte capaciteiten en lage motivatie kan een risico vormen. Dit vertaalt zich in een hogere kans op een incident.
- **Lage mogelijkheid** (zoals de combinatie moeilijk/moeilijk) betekent dat de kwetsbaarheid alleen door zeer capabele en sterk gemotiveerde actoren, zoals een nationale staat, kan worden misbruikt. Dit beperkt de groep potentiële aanvallers, wat de algehele kans op een succesvol incident verlaagt.

Door de mogelijkheid gestructureerd te beoordelen, wordt de subjectieve inschatting van kans gestaafd, wat essentieel is voor een realistische risicobeoordeling.

Voorbeeld: Dreigingsprofiel, motivatie en capaciteiten

Veel OT-systemen zijn vanwege hun levensduur verouderd en kunnen daarom niet meer gepatcht worden, wat een groot aantal eenvoudig te misbruiken kwetsbaarheden oplevert. Een veelgebruikte oplossing is om deze systemen dan volledig te isoleren van externe netwerken (air-gapped), wat de drempel voor aanvallers sterk verhoogt.

Dit creëert een belangrijk spanningsveld in de analyse:

- **Hoge kwetsbaarheid en lage bereikbaarheid:** Een ongepatcht, niet-verbonden systeem is uitermate lastig te exploiteren voor een externe dreigingsactor, ondanks de vele makkelijke zwakheden. De bereikbaarheid is zeer laag.
- **De verschuiving van risico:** De conclusie dat hiermee alle risico is vermeden, is onterecht. Het risico is alleen verschoven naar andere vectoren en actoren. Het systeem is nog steeds lokaal te beïnvloeden door middel van:
 - Verwijderbare media (zoals USB-sticks). Zo'n aanval vereist extreem hoge capaciteiten en motivatie (zoals bij de Stuxnet-aanval door nationale staten).
 - Insiders. Interne actoren hebben fysieke toegang, waardoor de vereiste capaciteit om een aanval uit te voeren plotseling laag is.

Dit voorbeeld benadrukt dat het isoleren van een systeem weliswaar de meest voorkomende aanvalsvectoren elimineert, maar de risicoanalyse noodzakelijk blijft om de overgebleven, vaak unieke, dreigings-scenario's in kaart te brengen.

5.2 Methoden voor Risicoanalyse

Zoals eerder beschreven, wordt het risico bepaald door de combinatie van de dreiging, de mogelijkheid om zwakheden te exploiteren, en de potentiële impact die dit kan veroorzaken. De reeds geïmplementeerde maatregelen hebben een directe impact op dit risico, omdat zij zowel de mogelijkheid als het effect reduceren.

De volledige analyse kan als volgt schematisch worden weergegeven (zie afbeelding hieronder op deze pagina).

Een grondige risicoanalyse is een intensief proces dat aanzienlijke tijd en gespecialiseerde expertise vereist. Omdat de aanpak sterk varieert, afhankelijk van het risicoprofiel en de volwassenheid van de organisatie, zijn er verschillende niveaus van diepgang mogelijk.

De volgende drie methoden vertegenwoordigen een oplopende schaal van complexiteit en diepgang:

- **Gap-analyse en bepaling baseline** (Eenvoudig)
- **Dreigingsscenario's en Bowtie-analyse** (Middel)
- **Threat Modeling en Kill Chain Analysis** (Geavanceerd)

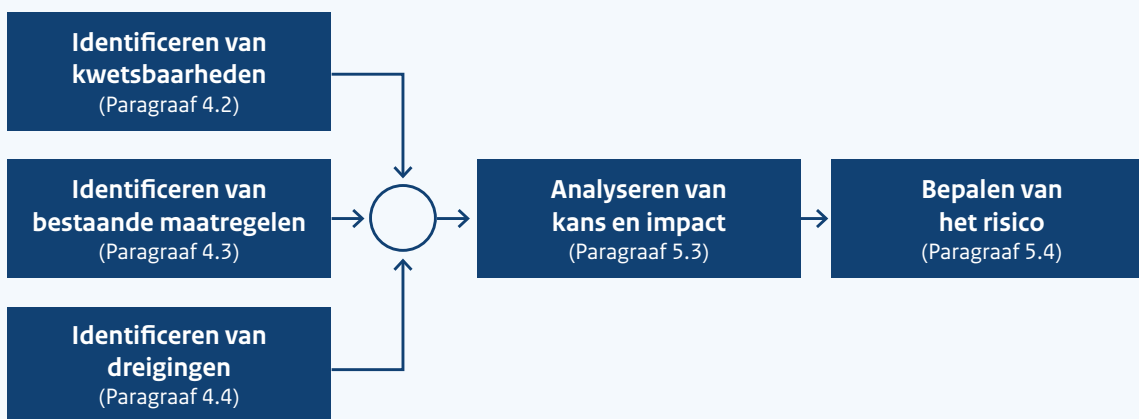
Gap-analyse en bepaling baseline (Eenvoudig)

Dit is de meest eenvoudige en snelste methode om te beginnen met risicobeheer. Zoals beschreven in eerdere hoofdstukken, vereist deze aanpak dat de organisatie een duidelijke security-baseline heeft vastgesteld. Het detailniveau van deze baseline wordt afgestemd op de volwassenheid van de organisatie en kan zowel technische als procesmatige maatregelen bevatten.

De gap-analyse beperkt zich tot het inventariseren van de baselinemaatregelen die niet zijn geïmplementeerd. Deze methode is de eenvoudigste manier om kwetsbaarheden te

Kader 5.1

Operationeel Stappenplan Risicoanalyse





identificeren (zoals eerder beschreven in hoofdstuk 4), aangezien elke ontbrekende maatregel ('gap') direct als een kwetsbaarheid wordt beschouwd. Elke gap vertegenwoordigt een tekortkoming in de controle, wat de mogelijkheid op een gerealiseerde aanval verhoogt. Het risico wordt vervolgens bepaald op basis van deze geïdentificeerde gaps.

Deze aanpak werkt vaak volgens het 'pas-toe-of-leg-uit'-principe. Het uitgangspunt is dat de organisatie de maatregel moet implementeren, tenzij er een geldige, risico-onderbouwde uitleg is waarom de maatregel ontbreekt (de gap). Er zijn kunnen verschillende redenen zijn waarom een bepaalde maatregel niet is geïmplementeerd:

- **Niet van toepassing:** Maatregelen die betrekking hebben op toegang op afstand zijn bijvoorbeeld niet relevant als dit helemaal geen onderdeel is van de betreffende scope.
- **Niet mogelijk:** De maatregel kan niet worden geïmplementeerd omdat de OT-apparatuur (bijvoorbeeld de PLC of software) de benodigde functionaliteit simpelweg niet ondersteunt (denk aan sterke wachtwoorden of tweefactorauthenticatie)
- **Kosten/complexiteit:** De maatregel leidt tot zulke hoge kosten of een ongewenste complexiteit, dat implementatie niet wenselijk is vanuit bedrijfsperspectief.
- **Tijd/resources:** De organisatie is nog niet in staat geweest om de eerder vastgestelde maatregelen te implementeren door een gebrek aan middelen of beschikbare tijd.

Als een maatregel niet van toepassing is, leidt de afwezigheid ervan niet tot een risico. Bij de overige redenen ontstaat echter

wel een risico. Het is nu cruciaal om de impact en het uiteindelijke risico te bepalen. Deze analyse bepaalt of de non-implementatie in een latere fase (Risicobeheer) geaccepteerd kan worden als een formele uitzondering op de baseline. De bepaling van de impact gebeurt met dezelfde methodiek (inclusief impactcategorieën en schalen) als beschreven in de Impactanalyse (zie paragraaf 3.3).

TIP: Kosten bepalen

Het inschatten van de kosten voor eventuele implementatie van de ontbrekende maatregelen is een waardevolle stap in dit proces. Deze informatie is essentieel voor de volgende fase: het behandelen van het risico.

Kader 5.2

Hoewel deze methode een beheersbaar startpunt biedt, geeft een gap-analyse 'slechts' aan welke maatregelen ontbreken. Het geeft geen volledig beeld van het daadwerkelijke contextuele risico, omdat unieke dreigingen, afhankelijkheden of de specifieke motivatie van de dreigingsactor niet expliciet worden meegenomen. Een meer diepgaande analyse (zoals beschreven in de volgende paragrafen) is nodig voor een holistisch risicoprofiel. Deze kunnen op een later moment worden gebruikt, zodra de organisatie een meer volwassen risicomangementproces heeft.

Dreigingsscenario's en Bowtie-analyse (Middel)

Deze methode biedt een kwalitatieve en meer contextuele benadering van risico's dan de eenvoudige gap- analyse. De risico's worden nu geëvalueerd aan de hand van realistische dreigingsscenario's (zoals eerder beschreven in het hoofdstuk Identificeren dreigingen). Over het algemeen is het voor een organisatie niet haalbaar of kosteneffectief om elke mogelijke dreigingsactor aan elke kwetsbaarheid te koppelen. Daarom is het aan te bevelen om de scenario's af te stemmen op de belangrijkste risico's.

Binnen deze scenario's kunnen bestaande maatregelen, de context en de netwerkinfrastructuur beter worden meegenomen. Dit geeft direct meer inzicht in de kansfactoren moeilijkheid en bereikbaarheid (zie voorgaande paragraaf) van een aanval. Daarnaast is het doorgaans gemakkelijker voor operationele medewerkers om zich een duidelijk scenario met impact voor te stellen dan een abstracte 'gap' in de baseline.

Met deze inzichten zijn de kans en impact, en daarmee het uiteindelijke risico, beter inzichtelijk te maken:

- **Kans:** Hoe meer effectieve maatregelen, netwerkbarrières en goed uitgevoerde processen er zijn, hoe moeilijker de aanval en dus hoe kleiner de kans op een gerealiseerde aanval.
- **Impact:** Hoe meer systemen er gecompromitteerd kunnen worden, en hoe belangrijker het systeem is in het proces, hoe groter de impact.

Om dit proces visueel te ondersteunen, kan gebruikgemaakt worden van de Bowtie-methode. Dit is een nuttig visueel

hulpmiddel dat de relatie tussen de dreiging, het incident (ook wel topscenario, de daadwerkelijke inbreuk) en de geïmplementeerde maatregelen overzichtelijk in kaart brengt. Hieronder is een voorbeeld weergegeven.

Het diagram visualiseert de volgende kerncomponenten:

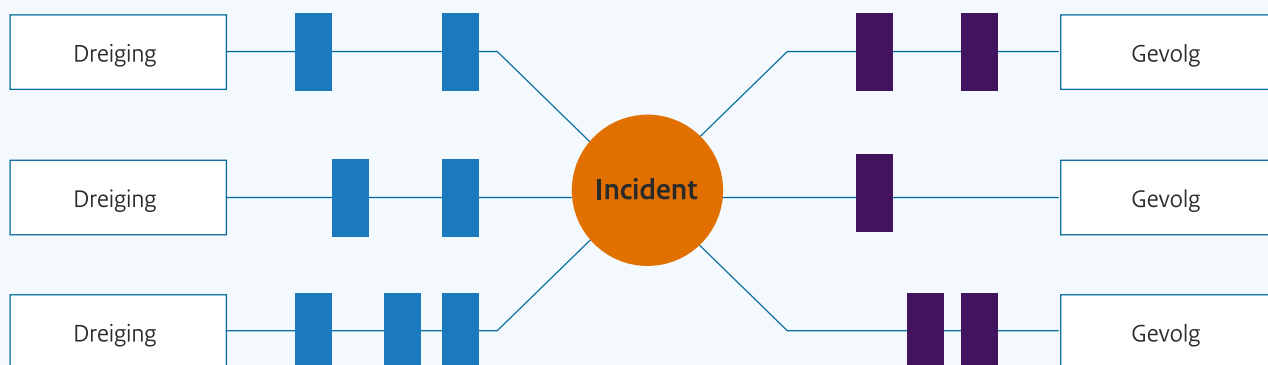
- **Dreigingen (links):** De mogelijke oorzaken die leiden tot het incident (ook wel trigger event). De methode biedt de mogelijkheid om meerdere dreigingen die tot hetzelfde incident kunnen leiden te bundelen. Zo kan een ransomware-incident uitgevoerd worden door cybercriminelen via externe toegang, maar bijvoorbeeld ook door malware via een leveranciersportal, of lokaal door een medewerker via USB of laptop.
- **Incident/topscenario (midden):** Het kritieke punt, of de daadwerkelijke inbreuk, dat de organisatie wil voorkomen. In dit voorbeeld is dat dus de ransomware-besmetting.
- **Gevolgen (rechts):** De mogelijke consequenties die uit dit scenario voortvloeien. De ransomware-uitbraak kan direct leiden tot verlies van beschikbaarheid. Maar dezelfde aanval kan ook datadiefstal als additionele impact hebben (bekend als double extortion). Ten slotte kan er ook nog sprake zijn van een cascade-impact, bijvoorbeeld door het via bestaande netwerkverbindingen besmetten van een partner of leverancier.

Door de effectiviteit van de preventieve en mitigerende maatregelen voor elk specifiek scenario te beoordelen, wordt een realistisch beeld verkregen van het resterende risico.

Visuele weergave van risico's via de Bowtie-Methode

Preventieve maatregelen

Responsieve (impact reducerende) maatregelen



Threat Modeling en Kill Chain Analysis

Dit is de meest uitgebreide en gedetailleerde methode, gereserveerd voor organisaties met een hoge volwassenheid of voor de meest kritieke assets ('kroonjuwelen'). Deze aanpak gaat aanzienlijk dieper dan de dreigingsscenario's, omdat het niet uitgaat van algemene scenario's, maar van een systematische ontleding van het systeem zelf.

Het belangrijkste voordeel is dat met deze diepgang unieke en voorheen onbekende kwetsbaarheden aan het licht kunnen komen. De methode onderzoekt de volledige aanvalsketen, van de laagste technische details tot de exploitatie. Het is doorgaans de meest intensieve methode en wordt alleen geadviseerd als de basissecurity al op orde is. Het vergt veel technische expertise, is tijd- en budgetintensief, en vereist de meest gedetailleerde input, zoals een nauwkeurig assetregister en de meest recente netwerktekeningen. Vanwege de specialistische kennis die nodig is, wordt hiervoor vaak externe expertise ingeschakeld.

De volgende technieken kunnen hier gebruikt worden:

- **Threat Modeling:** Hierbij wordt systematisch het systeemontwerp geanalyseerd om potentiële kwetsbaarheden en aanvalsvectoren in kaart te brengen. Idealiter gebeurt dit al in de ontwerpfasen van een nieuw systeem, maar het kan ook achteraf op een bestaand systeem worden uitgevoerd.
- **Aanvalspadanalyse (Attack Trees en Kill Chain):** Door bijvoorbeeld een Attack Tree op te stellen of een Cyber Kill Chain Analysis uit te voeren, wordt onderzocht welke stappen een aanval exact moet nemen om tot een bepaald gevolg te komen. Hierbij wordt het volledige aanvalspad onderzocht.
- **MITRE ATT&CK for ICS Framework:** Dit framework kan worden gebruikt om de analyse nog specifiek te duiden. Het brengt de technieken en tactieken in kaart die aanvallers gebruiken om OT-omgevingen te compromitteren.
- **Integratie van maatregelen:** Tegelijkertijd worden de effecten van bestaande maatregelen meegenomen in het aanvalspad. Dit leidt tot een inzichtelijk beeld van de huidige stand van zaken rondom risico's en bedreigingen.

Na het opstellen van een gedetailleerd Threat Model, kan een Penetration Test (Pentest) worden uitgevoerd. Dit is een gecontroleerde, praktische test om de theoretisch gevonden kwetsbaarheden daadwerkelijk te misbruiken. Dit is de meest realistische manier om de effectiviteit van de geïmplementeerde beveiligingsmaatregelen te valideren.

De uitkomst van deze diepgaande analyse is een gedetailleerd risicoprofiel, inclusief een schatting van de totale blootstelling aan risico's. Dit is cruciaal voor strategische besluitvorming over grote investeringen en biedt de organisatie de kans om weloverwogen gepaste maatregelen te nemen.

5.3 Analyseren van de kans & impact

Om uiteindelijk het risico te kunnen bepalen, zijn de factoren kans en impact cruciaal. De eerdergenoemde formule, $\text{risico} = \text{kans} \times \text{impact}$, maakt dit duidelijk. Meestal wordt voor beide schalen een gedefinieerde risicomatrix gebruikt. Er zijn echter verschillende manieren waarop deze schaal kan worden opgezet, wat soms voor verwarring of zelfs verkeerde interpretaties kan zorgen.

Het is essentieel om te onthouden dat het gaat om de kans dat de betreffende impact wordt gerealiseerd, niet om de kans dat de dreiging zich voordoet.

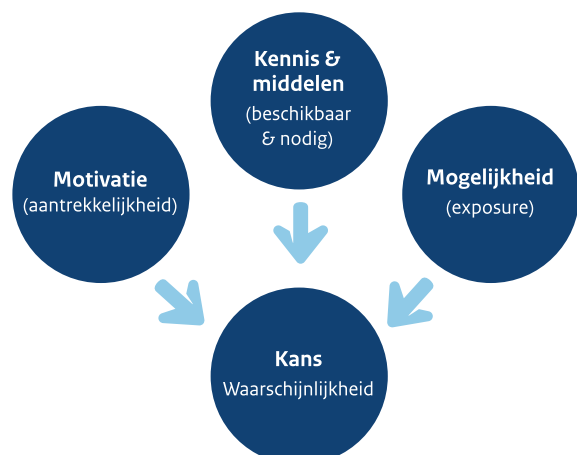
Kans

Specifiek voor OT-cybersecurity is het bepalen van de kans erg complex. Vanuit regulier risicomanagement wordt de kans vaak bepaald op basis van historische gegevens. Dit wordt mede mogelijk gemaakt doordat kans in deze gevallen vaak een bepaalde toevalsfactor heeft (bijvoorbeeld hoe vaak een zware orkaan in een bepaald gebied voorkomt). In zo'n context wordt kans vaak als een vorm van frequentie (bijvoorbeeld 1x per maand of 1x per jaar) weergegeven. Daarom bevatten veel matrices een van de volgende kansschalen:

Risicomatrix: Kansschaal/frequentie

Niveau	Omschrijving	Frequentie
Heel laag	Incident vindt zeer zelden plaats	1 × per 10 jaar
Laag	Incident vindt af en toe plaats	1 × per jaar
Middel	Incident vindt regelmatig plaats	1 × per maand
Hoog	Incident vindt vaak plaats	1 × per week
Heel hoog	Incident vindt (bijna) dagelijks plaats	1 × per dag

Het wordt al snel duidelijk dat dit soort schalen niet goed passen om de kans op OT-cybersecurity-incidenten te bepalen. Voor cybersecurity is de inslag namelijk zelden toeval, maar eerder het resultaat van (on)gerichte of (on)bewuste sabotage. Zoals eerder beschreven, wordt de kans hierbij gevormd door de motivatie, kennis en middelen van een dreigingsactor in combinatie met de staat van de aanwezige kwetsbaarheden en maatregelen.



Dit maakt het traditionele gebruik van frequentie als kans-schaal zeer lastig toepasbaar op OT-cybersecurity-incidenten. Deze is immers niet afhankelijk van de kalender, toeval of frequentie, maar van de intentie van een tegenstander. Een risicomatrix kan daarom beter gebruikmaken van een andere, kwalitatieve, schaalverdeling.

Een praktische aanpak die ook vaak gebruikt wordt is een objectieve schaal op basis van voorkomen. Dit is vaak een stuk eenvoudiger om te gebruiken en werkt goed als startpunt voor een eerste analyse. Bijvoorbeeld:

Risicomatrix: Kansschaal/frequentie

Niveau	Omschrijving	Frequentie / context
Heel laag	Dit type incident is nog nooit voorgekomen in de sector.	Mogelijk alleen in de toekomst; geen historische gevallen.
Laag	Dit type incident is weleens ergens in de sector voorgekomen.	In het afgelopen jaar ergens één keer geconstateerd.
Middel	Dit type incident is weleens binnen de organisatie voorgekomen.	In het afgelopen jaar binnen de organisatie of sector vastgesteld.
Hoog	Dit type incident komt weleens voor bij dit object.	Afgelopen jaar geconstateerd in een vergelijkbaar bedrijf.
Heel hoog	Dit incident komt regelmatig binnen de organisatie of bij dit object voor.	In het afgelopen jaar binnen dit bedrijf vastgesteld.

Voor een eerste analyse werkt deze schaal erg praktisch. Het grote nadeel is echter dat de kansschaal niet kan worden beïnvloed door het meenemen van bestaande of extra maatregelen. Daarnaast zijn niet alle dreigingen afhankelijk van een specifieke sector.

In een volwassen risicomanagementproces zou de kans op een risico gehetwaardigd (gereduceerd) moeten worden na de implementatie van mitigerende maatregelen. Als een incident echter eenmaal is voorgekomen (bijvoorbeeld scoort als Midden, want het is voorgekomen in de organisatie), blijft de score op deze schaal Midden, ongeacht de zwaarte van de extra geïmplementeerde securitycontroles. Dit klopt natuurlijk niet, want mitigerende maatregelen bemoeilijken de succesvolle uitvoering van een cyberaanval en zouden de kans dus moeten reduceren.

Een alternatieve, meer gedetailleerde, schaalverdeling is daarom noodzakelijk. Deze schaal houdt wel rekening met de motivatie en capaciteiten van de dreigingsactor ten opzichte van de aanwezige cybersecuritymaatregelen van een systeem of netwerk.

Risicomatrix: Kansschaal/frequentie

Niveau	Omschrijving	Maatregelen / invloed
Heel laag	De dreigingsactor heeft geen motivatie, kennis of capaciteiten om kwetsbaarheden te misbruiken.	Er zijn effectieve maatregelen die misbruik voorkomen.
Laag	De dreigingsactor heeft weinig motivatie en beperkte capaciteiten.	Redelijk effectieve maatregelen zijn aanwezig tegen misbruik.
Middel	De dreigingsactor is enigszins gemotiveerd en beschikt over enige kennis en capaciteiten.	Er zijn enkele of matige maatregelen die misbruik kunnen beperken.
Hoog	De dreigingsactor is behoorlijk gemotiveerd en heeft voldoende kennis en capaciteiten.	Er zijn slechts beperkte maatregelen om misbruik te voorkomen.
Heel hoog	De dreigingsactor is zeer gemotiveerd en heeft uitgebreide kennis en capaciteiten.	Er zijn geen effectieve maatregelen om misbruik van zwaktes te voorkomen.

Impact

De impact omvat de diverse negatieve gevolgen na een incident, variërend van financiële gevolgen tot menselijke, milieu- of omgevingseffecten. Het is essentieel om deze impact op verschillende niveaus te kunnen schalen. Zoals beschreven in de Impactanalyse (paragraaf 3.3), moet elke organisatie passende niveaus vaststellen (eventueel aangevuld met items uit RAMSSHEEP) om alle risico's binnen de organisatie consistent te kunnen vergelijken.

Bij een cyberincident komt het vaak voor dat meerdere impactgebieden van toepassing zijn, elk met een eigen score. De uitkomst van de impactanalyse wordt bepaald door de hoogste score per impactgebied.

Hier kan echter nog een belangrijke nuance in aangebracht worden. De kans op een incident moet namelijk altijd worden beoordeeld ten opzichte van de specifieke impact die wordt geanalyseerd.

Neem het voorbeeld van een gecompromitteerd OT-systeem. Dit kan twee mogelijke, uiteenlopende perspectieven op risico opleveren:

- **Onbeschikbaarheid:** Stel dat de impact als Midden, en de kans ook als Midden wordt ingeschat. Bijvoorbeeld omdat een aanvaller met gemiddelde skills deze verstoring kan uitvoeren (lagere drempel).
- **Veiligheid (safety):** De impact wordt hierbij als Hoog of Heel Hoog ingeschaald. Tegelijkertijd is de kans is veel kleiner omdat het veroorzaken van fysieke schade of letsel zeer specifieke kennis en kunde vereist. Dit kan alleen worden gerealiseerd door een specialistische dreigingsactor, waarbij bovendien de motivatie vaak ontbreekt.

Door dus alleen naar de maximale impact van een scenario te kijken en daarbij de algemene kans de gebruiken waarbij dit scenario kan optreden kom je waarschijnlijk uit op een te hoog risico.

Het is vaak niet praktisch om alle mogelijke combinaties van dreigingsactoren en kwetsbaarheden te analyseren. Het groeperen van kwetsbaarheden of het uitgaan van een ‘gemiddelde’ dreigingsactor kan de analyse vereenvoudigen. Om de bovengenoemde nuance over impact en kans mee te nemen, is het echter waardevol om gebruik te maken van goed gedefinieerde scenario’s (Methode 2 en 3). Deze scenario’s moeten expliciet een dreigingsactor koppelen aan een beoogde impact (bijvoorbeeld: “Een nationale staat veroorzaakt schade aan de pompinstallatie”).

5.4 Analyseren van het risico

Het evaluatieproces van cybersecurityrisico’s wordt afgerond door de vastgestelde kans op een gerealiseerde aanval te combineren met de verwachte impact. Dit wordt doorgaans gevisualiseerd met behulp van een risicomatrix, waarbij deze twee factoren op de respectievelijke assen worden geplott.

In dit conceptvoorbeeld zijn vier risiconiveaus (Verwaarloosbaar, Laag, Gematigd en Hoog) gebruikt, maar meer of minder niveaus zijn natuurlijk ook mogelijk. De risicobereidheid (risk appetite) van de organisatie is het

leidende principe en bepaalt vervolgens wat er met het risico moet gebeuren. De interpretatie van de plot en de vereiste acties kan als volgt worden gebruikt:

- **Lichtgroen/verwaarloosbaar:** Zeer laag risico met minimale (of geen enkele) impact en daarom ruim binnen de acceptabele grenzen. Er zijn geen aanvullende actie vereist.
- **Groen/laag:** Laag risico dat binnen de vastgestelde risk appetite valt, maar met mogelijke verbeterpunten. Acceptabel zonder onmiddellijke aanvullende maatregelen. Wellicht is er nog wel interne controle of toetsing nodig. Risico’s worden wel geregistreerd en formeel geaccepteerd.
- **Oranje/gematigd:** Gematigd risico dat extra maatregelen vereist om binnen de vastgestelde risk appetite te blijven. Acties binnen vastgestelde tijd zijn nodig. Registratie en formele actiepunten worden uitgezet. Dit risico kan escaleren naar ‘Hoog’ als maatregelen te lang worden uitgesteld.
- **Rood/onaanvaardbaar:** Onaanvaardbaar risico dat een directe bedreiging vormt voor de organisatie en buiten de vastgestelde risk appetite valt. Onmiddellijke en dringende maatregelen zijn vereist. Rapportage en escalatie naar management als acties te lang worden uitgesteld.

De beslissing over risicoacceptatie en de te nemen maatregelen (risicobehandeling) is de volgende cruciale stap in het risicomangementproces en wordt verder beschreven in hoofdstuk 6.

Voorbeeld kwalitatieve risicoanalysematrix voor OT-omgevingen

Impact		Veiligheid	Financieel	Omgeving	Reputatie	Kans/waarschijnlijkheid				
						A	B	C	D	E
						Heel laag	Laag	Midden	Hoog	Heel hoog
0										
1										
2										
3										
4										
5										

6. Beheren

Dit hoofdstuk beschrijft hoe de risico's beheerst kunnen worden. Dit geldt zowel voor acceptabele lage risico's als onacceptabele hoge risico's. Voor elk risico zullen een of meerdere beheersmaatregelen genomen moeten worden, zoals beschreven in de onderstaande tabel.

Maatregel	Omschrijving
Reduceren	Extra mitigerende maatregelen zijn nodig om het risico te reduceren. Dit kan door de kans, impact of beide te beïnvloeden.
Accepteren	Het risico is lager dan de risk appetite van de organisatie, of kosten van overige maatregelen zijn zodanig hoog t.o.v. het risico dat het daarom geaccepteerd kan worden.
Overdragen	Het risico wordt overgedragen aan een andere partij, vaak een cybersecurityverzekering.
Vermijden	Het elimineren van het risico door de dreiging in zijn geheel te verwijderen. Bijvoorbeeld door het stoppen/uitfaseren van bepaalde systemen.

Meestal is een combinatie van maatregelen nodig, omdat geen enkele maatregel 100% feilloos is en het hele risico volledig af kan dekken (behalve wellicht het compleet verwijderen van het risico). Het risicobeheersproces moet deze besluitvorming faciliteren. Het is belangrijk dat de juiste personen, expertise en beslissingsbevoegdheid hiervoor aanwezig zijn. Er zijn vaak meerdere oplossingen, verschillende maatregelen beschikbaar met elk hun eigen voor- en nadelen, zoals effectiviteit, complexiteit en kosten voor aanschaf en beheer. In de volgende paragrafen wordt elke maatregel verder beschreven.

6.1 Reduceren

Om het risico te reduceren naar een acceptabel niveau zijn meestal een of meerdere maatregelen nodig. Deze kunnen zowel technisch als organisatorisch van aard zijn (mens, proces, techniek). Ter verduidelijking zijn er een aantal voorbeelden opgenomen in de onderstaande tabel:

Type	Omschrijving
Techniek	- Het implementeren van een juiste netwerkscheiding tussen IT en OT, bijvoorbeeld door het volgen van het Purdue Model. - Het installeren van antivirus- of beveiligingssoftware, patches, software-updates op OT-systemen.
Proces	- Het opnemen en implementeren van formele securityprocedures in het Bedrijfs-IMS (Integraal Managementsysteem), zoals een vierogenbeleid en het scheiden van verantwoordelijkheden (Segregation of Duties). - Het regelmatig maken van systeem- en configuratie-back-ups van alle OT-systemen, inclusief het periodiek testen van de herstelprocedure (restoreprocedure).
Mens	Het verplicht stellen van een op rol en verantwoordelijkheid gebaseerde training OT-cybersecurity-awareness voor alle personen die aan of met OT-systemen werken, inclusief derde partijen.

Het is sterk aan te bevelen om zoveel mogelijk gebruik te maken van een standaardlijst aan maatregelen, zoals de eerdere genoemde sets aan baselinemaatregelen, eventueel aangevuld met extra maatregelen uit een interne catalogus. Dit



is cruciaal voor de onderhoudbaarheid van de procedures en de technische oplossingen. In de meest volwassen organisaties is ook centrale logging en monitoring (door bijvoorbeeld een Security Operations Center) geïmplementeerd. Ook hiervoor is het efficiënter om zoveel mogelijk standaardoplossingen te hebben. Unieke oplossingen per systeem of situatie zijn altijd een laatste optie, maar introduceren extra onderhoud, complexiteit en hogere kosten op de lange termijn.

LET OP: Beperkingen van OT-systemen

In een OT-omgeving ligt het toepassen van oplossingen vaak gecompliceerder door het eigenaarschap van de betreffende asset. Het kan voorkomen dat een leverancier van een bepaald OT-systeem de gekozen security-oplossingen (zoals EDR of XDR) niet ondersteunt. Voordat een dergelijke oplossing als standaard op alle systemen kan worden uitgerold, moet dit vaak eerst in overeenstemming met alle betreffende leveranciers worden afgesproken.

Kader 6.1a

Maatregelen kunnen grofweg in twee functionele categorieën worden onderverdeeld:

- **Preventieve maatregelen:** Deze zijn erop gericht te voorkomen dat een incident plaatsvindt of de kans te verkleinen. Dit omvat ook afschrikkende of vertragende maatregelen.
- **Responsieve/mitigerende maatregelen:** Deze zijn voornamelijk gericht op het reduceren van de impact wanneer een incident zich voordoet. Voorbeelden zijn detectie, incident-respons en herstelprocedures.

Specifiek voor OT is het van belang om te kijken naar de mogelijke fysieke impact. Het kan soms veel effectiever zijn om de behaalde functionaliteit fysiek te beperken (bijvoorbeeld het uitschakelen van een poort of het beperken van fysieke toegang) in plaats van extra softwarematige preventieve maatregelen te nemen.

Ten slotte nog een aantal overwegingen:

- **Introductie nieuwe risico's:** Bij het nemen van maatregelen moet altijd rekening worden gehouden met eventuele nieuwe risico's die worden geïntroduceerd. Als er bijvoorbeeld nieuwe apparatuur, zoals een firewall, wordt geïnstalleerd, zal deze ook bekende kwetsbaarheden hebben die beheerd moeten worden. Of dat een automatische back-up ook zorgt voor extra netwerkconnecties.
- **Restrisico:** Zelfs als alle mitigerende maatregelen zijn genomen, blijft er altijd een restrisico bestaan. Zodra dit risico echter onder de tolerantiedrempel komt, kan dit restrisico geaccepteerd worden door de organisatie. De risicoacceptatie wordt verder beschreven in het volgende hoofdstuk.

- **Total cost of ownership:** Ten slotte is het belangrijk om een volledig kostenoverzicht van de nieuw voorgestelde maatregelen op te stellen. Dit omvat niet alleen de initiële aanschaf- en installatiekosten, maar ook de kosten voor de operationele taken en het onderhoud op de lange termijn. Uiteindelijk moeten deze kosten worden meegenomen in de afweging of een maatregel kosteneffectief is om het risico te reduceren.
- **Benefits:** Naast risicoreductie, het primaire doel van de extra maatregel, zijn er mogelijk ook operationele en financiële voordelen, al zijn deze niet altijd goed meetbaar. Een up-to-date assetregister kan bijvoorbeeld veel tijd besparen bij diverse onderhoudstaken en cybersecuritymonitoring kan ook operationele problemen snel detecteren en daarmee kosten besparen.

Casestudy: Risicoreductie, een omgekeerde wereld

Een voorbeeld waarbij het niet wenselijk is om OT-systemen verder te digitaliseren, maar juist terug te keren naar analoge systemen, is een overdrukventiel op leidingen. In sommige industriële omgevingen, zoals in de chemische industrie of bij de behandeling van gevaarlijke stoffen, zijn overdrukventielen van cruciaal belang om te voorkomen dat leidingen barsten of exploderen als gevolg van drukopbouw.

Hoewel het verleidelijk kan zijn om deze overdrukventielen te digitaliseren en te koppelen aan geautomatiseerde systemen voor monitoring en controle, brengt dit ook risico's met zich mee. Digitale systemen zijn vatbaar voor cyberaanvallen en storingen, waardoor de betrouwbaarheid van het overdrukventiel kan worden aangetast.

In plaats daarvan kan het behouden van een analogoos overdrukventiel, dat zijn werk doet op basis van mechanische principes zonder afhankelijk te zijn van digitale signalen, een betrouwbaardere optie zijn. Dit minimaliseert het risico op cyberaanvallen en biedt een robuuste fysieke fail-safe in geval van drukopbouw in de leidingen. Hoewel dit misschien niet de meest geavanceerde technologie is, kan het in sommige gevallen de meest veilige en betrouwbare optie zijn om de integriteit van het systeem te waarborgen.

Kader 6.1b

6.2 Accepteren

Risicoacceptatie is een cruciaal onderdeel van risicobeheersing, waarbij een organisatie bewust bepaalde risico's aanvaardt als onvermijdelijk of beheersbaar. Het accepteren van een risico is een besluit dat vastgelegd moet worden.

Een formeel aangestelde risico-eigenaar of risicomanager met mandaat speelt hierbij een sleutelrol. Deze persoon moet niet alleen het mandaat hebben om de risico's te accepteren, maar moet ook het gehele risicolandschap voor de organisatie kunnen overzien. Dit betekent dat de persoon een passend verantwoordelijkheidsniveau binnen de organisatie moet bekleden, zoals het niveau van de Business Owner of zelfs bestuur van de organisatie.

Het is van essentieel belang dat beslissingen met betrekking tot risicoacceptatie worden genomen door personen met de vereiste autoriteit en expertise. Dit waarborgt dat de organisatie risico's op een effectieve manier beheert en de operationele continuïteit en veiligheid van de operationele technologie (OT) kan waarborgen.

	Veiligheid	Financieel	Omgeving	Reputatie	Kans / waarschijnlijkheid				
					A	B	C	D	E
0									
1									
2									
3									
4									
5									

6.2.1 Risicotolerantie (Risk appetite)

Accepteren van risico's is niet hetzelfde als risico's negeren. Elke organisatie heeft een bepaald risicotolerantieniveau – ook wel de risk appetite genoemd – dat eerder is beschreven als een belangrijke voorwaarde voor risicomanagement.

Zolang risico's goed en duidelijk in kaart zijn gebracht, geanalyseerd en onder deze drempelwaarde blijven (het restrisico), kunnen ze worden geaccepteerd. In het eerder gebruikte voorbeeld zouden dus alle risico's boven de zware lijn acceptabel zijn zonder extra maatregelen.

Het is en blijft cruciaal om de risicoanalyse, tezamen met alle aannames en het acceptatiebesluit, te documenteren. Zo kan

later altijd aangetoond worden waarom bepaalde maatregelen wel of niet genomen zijn, wat essentieel is voor verantwoording en compliance.

6.2.2 Afwijkingen

In de praktijk kan het voorkomen dat risico's boven het bepaalde risicotolerantieniveau toch niet direct gemitigeerd kunnen worden. Redenen hiervoor kunnen zijn:

- **Techniek:** Technisch niet mogelijk binnen de huidige OT-architectuur.
- **Kosten:** De kosten van implementatie zijn te hoog ten opzichte van het risico.
- **Planning:** Noodzakelijke veranderingen kunnen pas later in de tijd worden doorgevoerd (bijvoorbeeld tijdens een geplande shutdown).

Voor deze gevallen is een (tijdelijke) acceptatie, of een afwijking, mogelijk. Binnen veel organisaties geldt de regel dat Hoge of Onaanvaardbare risico's (Rood in eerdere voorbeelden) nooit zonder meer geaccepteerd mogen worden. Er zal altijd eerst een van de andere beheersmaatregelen (transfer, reductie, vermijden) moeten worden overwogen.

Pas-toe-of-leg-uit

Voor het formeel afwijken of accepteren van risico's zijn een aantal strikte stappen nodig:

- **Justificatie beschrijven:** Leg gedetailleerd vast waarom het niet mogelijk is om het risico op een andere manier te beheersen.
- **Compenserende maatregelen onderzoeken:** Onderzoek of er andere compenserende (dempende) maatregelen te nemen zijn die een deel van het risico (mens, proces, techniek) kunnen reduceren. Denk hierbij aan extra (manuele) controles, procedures of speciale operationele omstandigheden.
- **Gedetailleerde heranalyse:** Voer een specifiek en gedetailleerde risicoanalyse uit, waarbij alle specifieke aannames en de invloed van de aanvullende compenserende maatregelen worden meegewogen.
- **Formele acceptatie en vastlegging:** Het specifieke risico moet formeel worden geaccepteerd en ondertekend door de verantwoordelijke risicobeheerder die dit mandaat heeft. Hierbij is belangrijk dat:
 - Het risico wordt beoordeeld door kundige en ervaren specialisten.
 - De afwijking wordt opgeslagen in een formeel document-beheerssysteem voor traceerbaarheid en verantwoording.
- **Periodieke herbeoordeling:** Alle afwijkingen moeten regelmatig (minimaal jaarlijks) opnieuw worden beoordeeld, waarbij rekening wordt gehouden met:
 - Het huidige risicotolerantieniveau en dreigingslandschap.
 - De status van de compenserende maatregelen.
 - Eventuele invloeden van andere gedocumenteerde afwijkingen.

Het correct vastleggen van afwijkingen in een formeel beheers-systeem is cruciaal om de organisatie te beschermen tegen mogelijke schade, en schept zowel intern duidelijkheid als tegenover toezichthoudende instanties.

Casestudy: Een verouderd SCADA-systeem

Een centraal SCADA-systeem is verouderd. Het is hierdoor technisch niet meer mogelijk om aan alle cybersecurityvereisten te voldoen, zoals het installeren van beveiligingsupdates of nieuwere beveiligingssoftware. De standaardmaatregelen zijn dus niet uitvoerbaar. Het systeem is van cruciaal belang voor de meest kritische bedrijfsprocessen. Het risico wordt daarom geclassificeerd als hoog.

Vervangen van het systeem is te kostbaar en op korte termijn zelfs onmogelijk. Als alternatief worden compenserende maatregelen geïmplementeerd om de kans op misbruik te reduceren en de detectie te verhogen:

- **Techniek:** Aanscherpen van firewallregels, toegang op afstand beperken, en de implementatie van extra beveiligingsmonitoring (IDS/IPS) betreffende het netwerksegment.
- **Proces/Mens:** Striktere procedures en een vierogenbeleid voor het gebruik van removable media (zoals USB-sticks).

Door de implementatie en de geschatte effectiviteit van deze compenserende maatregelen wordt het resterende risico geherwaardeerd naar het lagere niveau Midden (Oranje).

Het restrisico van Midden valt binnen de vastgestelde risicotolerantie van de organisatie mits er een formele acceptatie is (pas-toe-of-leg-uit). Het risico wordt tijdelijk geaccepteerd en formeel vastgelegd door de risico-eigenaar, met de duidelijke eis dat het SCADA-systeem binnen een gestelde termijn (bijvoorbeeld 12 maanden) wordt vervangen.

Kader 6.2.2a

TIP: Effectief exception management

Een goed uitgewerkte exception policy is cruciaal voor succesvol risicobeheer. Het vinden van de juiste balans vormt echter een uitdaging: te strenge procedures leiden ertoe dat organisaties proberen om via creatieve interpretaties aan securityeisen te 'voldoen', terwijl te soepele procedures resulteren in het routinematig aanvragen van excepties zonder de intentie deze op te lossen.

De geldigheidsduur van excepties speelt een belangrijke rol in deze balans. Korte geldigheidsduren verhogen de drempel voor het aanvragen van excepties, terwijl lange termijnen de barrière verlagen. Maatwerk kan hierbij helpen, maar moet altijd duidelijk worden beargumenteerd aan de hand van het resterende risico. Registratie van alle uitzonderingen is in elk geval belangrijk.

Kader 6.2.2b

6.3 Overdragen

6.3.1 Verzekeringen

Het overdragen van cybersecurityrisico's kan door middel van een cybersecurityverzekering. Hierbij wordt het financiële risico van een bepaald incident overgedragen aan een derde partij, zoals een verzekeraar.

Deze methode wordt doorgaans ingezet voor het restrisico: het risico dat overblijft nadat alle redelijke reductiemaatregelen zijn genomen, en dat nog steeds te groot is voor de organisatie om zelf te dragen. Een voorbeeld hiervan is het financiële risico van een grootschalige ransomware-aanval.

Deze verzekeringen zijn meestal uit drie delen opgebouwd.

Onderdelen	Omschrijving
Preventie	Acceptatiecriteria De verzekeraar stelt verplichtingen aan de te nemen preventiemaatregelen. Door middel van intakes, interviews of audits zal bepaald worden of de verzekering kan worden afgesloten en wat de premie hiervoor is.
Herstellen	Schadereductie Als onderdeel van een verzekering kan ondersteuning voor herstel worden geboden. Dit is bedoeld om de (vervolg)schade na een incident zo snel mogelijk te minimaliseren (bijvoorbeeld door toegang tot gespecialiseerde incident response teams).
Vergoeden	Financiële compensatie Het belangrijkste onderdeel is dat de verzekering de financiële schade compenseert. Dit omvat vaak verloren omzet, boetes en directe herstelkosten en is doorgaans gemaximeerd tot een bepaald bedrag.

Een belangrijke overweging is dat niet alle risico's kunnen worden overgedragen.

- **Niet-financiële impact:** Wanneer er potentiële impact is op veiligheid (safety), het milieu, juridische/regelgeving of maatschappelijk belang, zijn bijvoorbeeld alleen de financiële consequenties van die schade te verzekeren. De operationele verstoring, de reputatieschade en de aansprakelijkheid van de organisatie blijven altijd risico's die de organisatie zelf draagt.
- **Complexiteit van voorwaarden:** Ten slotte kunnen de voorwaarden van een verzekering complex zijn. Organisaties moeten zich goed inlezen in:
 - Wat er wel of niet wordt vergoed (bijvoorbeeld in geval van verloren omzet of boetes).
 - In hoeverre cyber risico's zijn verzekerd en wat er wel of niet valt onder een oorlogs- of andere uitzonderingsclausule.

Het is van belang om vast te stellen dat verzekeren altijd een aanvulling is op, en geen vervanging van, adequate beveiligingsmaatregelen.



Casestudy: De complexiteit van de oorlogsuitsluitingsclausule

De NotPetya-malwareaanval uit 2017 op het farmaceutische bedrijf Merck illustreert de juridische complexiteit van cyberverzekeringen.

- Merck leed aanzienlijke schade en diende een claim van \$ 1,4 miljard in onder zijn algemene allriskdekking.
- De aanval werd breed toegeschreven aan Rusland. Mercks verzekeraars wezen de claim aanvankelijk af en beriepen zich op de standaard oorlogsuitsluitingsclausule – een clausule die schade als gevolg van oorlogshandelingen uitsluit.
- Na juridische procedures oordeelde een rechtbank in New Jersey echter in het voordeel van Merck. De rechtbank stelde dat de clausule voor oorlogsuitsluiting niet van toepassing was op deze specifieke cyberaanval.

Deze zaak belicht een cruciale onzekerheid: er is geen gestandaardiseerde, eenduidige definitie van ‘cyberoorlog’. Dit toont aan dat de uitsluitingsclausules in een verzekeringspolis in de praktijk juridisch complex kunnen zijn en een belangrijke overweging vormen bij het overdragen van het financiële restrisico.

Echter na de enorme financiële verliezen die verzekeraars leden als gevolg van de NotPetya-schadeclaims, heeft de markt hierop gereageerd. Vóór incidenten als NotPetya waren veel organisaties onbedoeld gedekt voor cyberinci-

denten onder hun algemene allrisk- of property- (eigendommen) polissen. Dit fenomeen werd Silent Cyber genoemd: de polis sprak niet expliciet over cyberdekking, maar sloot het ook niet uit. Momenteel geldt vaak het volgende:

- **Expliciete uitsluiting:** Verzekeraars hebben massaal de voorwaarden van hun algemene (all-risk)polissen aangescherpt met expliciete uitsluitingsclausules voor cyberrisico's.
- **Verplichte cyberverzekering:** Organisaties zijn genoodzaakt om specifieke cybersecurityverzekeringen af te sluiten om zich te beschermen tegen cyberrisico's.
- **Strengere voorwaarden en uitsluitingen:** De voorwaarden om deze specifieke cyberpolissen af te sluiten zijn strenger geworden (bijvoorbeeld door verplicht te stellen dat bepaalde basismaatregelen, zoals multifactorauthenticatie, al zijn geïmplementeerd). Bovendien zijn de uitsluitingsclausules in deze specifieke cyberpolissen, met name de oorlogsuitsluitingsclausule, preciezer geformuleerd in een poging om toekomstige juridische discussies (zoals in de Merck-zaak) te vermijden.

Kortom: De allriskpolis is na NotPetya grotendeels onbruikbaar geworden voor het dekken van grootschalige OT-cyberincidenten. Specifieke streng gereguleerde cyberpolissen zijn de nieuwe norm.

Kader 6.3.1

6.3.2 Outsourcing

Meer en meer diensten worden tegenwoordig uitbesteed aan derde partijen en serviceproviders. Denk hierbij aan cloudcomputingdiensten (zoals OT-data historian-diensten), online diagnostics van een leverancier, een uitbesteed OT SOC (Security Operations Center) of een leverancier die verantwoordelijk is voor lokaal (security)onderhoud. Hierbij wordt vaak onterecht aangenomen dat hiermee meteen alle risico's zijn afgedekt. **Het uitbesteden van bepaalde diensten is namelijk niet hetzelfde als het overdragen van risico's.**

Hoewel bepaalde werkzaamheden en bijbehorende verantwoordelijkheden verschuiven naar de externe partij, blijft het risico uiteindelijk altijd bij de organisatie zelf. Als er bijvoorbeeld een datalek plaatsvindt bij een externe dienstverlener, zal – ondanks een SLA en eventuele boeteclausule – de reputatieschade en de uiteindelijke vervolgschade neerkomen bij de uitbestedende organisatie.

In risicomanagement bestaat daarom de volgende rolverdeling:

- **Verantwoordelijk (Responsible):** Verwijst doorgaans naar individuen of teams die rechtstreeks betrokken zijn bij de uitvoering van specifieke taken of activiteiten (bijvoorbeeld het uitvoeren van toegewezen taken of het implementeren van risicobeperkende maatregelen).
- **Aansprakelijk/Eindverantwoordelijk (Accountable):** Verwijst naar individuen of rollen die de uiteindelijke verantwoordelijkheid en bevoegdheid dragen voor het algehele resultaat van risicomanagementprocessen. Dit is de risico-eigenaar binnen de organisatie die verantwoordelijk is voor het stellen van doelen en het formeel accepteren van het restrisico.

Het is essentieel om te beseffen dat de externe dienst, dienstverlener of serviceprovider ook nieuwe risico's kan introduceren, zogenaamde supplychainrisico's. Dit kan zelfs nog een stap verder gaan wanneer deze partijen een deel van het uitbesteede werk verder uitbesteden aan subleveranciers. Het is belangrijk dat deze risico's zijn meegenomen tijdens de inventarisatiefase (zie 3.2) en dat er rekening wordt gehouden met het volwassenheidsniveau van de leverancier bij de risicobeoordeling.

Casestudy: Risico's in de toeleveringsketen (supplychain)

Nogmaals hetzelfde voorbeeld - NotPetya - maar nu in een ander perspectief. De NotPetya-aanval in 2017 toonde de desastreuze impact aan van deze afhankelijkheid. De aanval raakte ook de Rotterdamse haven, waarbij een terminal compleet werd stilgelegd, met grote logistieke problemen tot gevolg (zoals het uitwijken van schepen naar andere havens).

Dit incident maakte de keten van afhankelijkheid pijnlijk duidelijk: een schip is afhankelijk van de haven, de haven van de laad- en lossystemen, en deze systemen waren uiteindelijk gecompromiteerd door een cyberaanval op een derde partij. De primaire bedrijfsprocessen van een organisatie zijn dus afhankelijk van een hele keten van processen die elders plaatsvinden.

Andere voorbeelden van ketenrisico's:

- **Service- en productdisruptie:** Toeleveranciers die door een cyberaanval (bijvoorbeeld ransomware) hun producten of diensten niet meer kunnen leveren. Dit varieert van het uitstellen van gepland onderhoud en te late levering van reserveonderdelen, tot het wegvallen van cruciale (online) diensten die ingrijpen op de primaire bedrijfsprocessen van de organisatie. De vraag is: hoe afhankelijk is de organisatie van deze diensten?
- **Toegangsrisico (third-party access):** Een van de leveranciers of dienstverleners is gehackt, waardoor de aanvaller onbedoeld toegang krijgt tot de systemen van de organisatie. Dit is met name risicovol omdat leveranciers en onderhoudspersoneel vaak legitieme toegang nodig hebben voor dagelijkse werkzaamheden. De cruciale vraag is dan: hoe goed heeft deze externe partij de cyberbeveiliging op orde?
- **Kwetsbaarheden in producten:** Er worden kritieke kwetsbaarheden gevonden in producten (hardware of software) die gebruikt worden binnen de organisatie. Dit geldt zowel voor commercieel beschikbare producten (zoals MS Windows en netwerkkapparatuur) als voor

specifieke OT-assets (PLC's, SCADA-software). Extra voorzichtigheid is geboden voor op maat gemaakte, unieke software, omdat deze vaak is opgebouwd uit vele bestaande programmabibliotheken of modules die elk weer eigen zwakheden kunnen bevatten. Het is essentieel om te weten welke hard- en software gebruikt wordt en of de juiste informatie en updates van de leveranciers worden ontvangen.

Casestudy: Sabotage in de rail-supplychain

Om de potentiële omvang en de complexiteit van supplychainrisico's te schetsen, is het incident uit de railsector in Polen in 2023 een extreem voorbeeld. In dit geval kwam aan het licht dat een leverancier van treinmaterieel zeer waarschijnlijk een vorm van logische sabotage had ingebouwd in de PLC's van de treinen, namelijk:

- **Sabotagefunctionaliteit:** De code liet de treinen op willekeurige momenten in storing vallen met nietszeggende storingscodes.
- **Vendor lock-in:** De storingen konden alleen door de leverancier zelf worden 'opgelost', vaak met behulp van een specifieke ongedocumenteerde invoerprocedure of een unieke code.
- **Geavanceerde detectie:** De firmware bevatte zelfs GPS-coördinaten van de onderhoudswerven van derde partijen. Dit stelde de trein in staat te detecteren of deze onderhoud kreeg op een niet-geautoriseerde locatie.

Hoewel de leverancier deze beschuldiging ontkende en claimde zelf gehackt te zijn, illustreert het incident in beide gevallen een kritieke kwetsbaarheid. Ongeacht de officiële oorzaak (opzettelijke sabotage door de leverancier of een succesvolle aanval via de supplychain) is het resultaat een catastrofale inbreuk op de integriteit en de operationele veiligheid van de systemen. Dit voorbeeld benadrukt de noodzaak van diepgaande integriteitscontroles bij leveranciers en de door hen geleverde producten.

6.4 Vermijden

Als laatste optie in de risicobehandeling is het mogelijk om het risico in zijn geheel te vermijden. Risicovermijding betekent dat de kans of de impact van een risico wordt gereduceerd tot nul. In de praktijk houdt dit meestal in dat men geheel stopt met een bestaande activiteit, of afziet van de introductie van nieuwe systemen of functionaliteiten.

Dit is doorgaans een actie voor de grootste onacceptabele risico's die zelfs met uitgebreide mitigerende maatregelen nog te hoog blijven. Het is ook een optie wanneer de kosten-batenanalyse aantoont dat de enige veilige manier om een activiteit uit te voeren simpelweg te duur is, of wanneer het risico de verwachte baten structureel overstijgt.

Bijvoorbeeld: Toegang op afstand op kritieke veiligheidssystemen kan een onacceptabel risico zijn. Het wegnemen van deze optie (bijvoorbeeld door de netwerkverbinding fysiek te verwijderen) zal de kans op misbruik tot nul reduceren. Daarmee is het risico in zijn geheel vermeden. Daarmee is echter ook de activiteit (onderhoud op afstand) niet meer mogelijk waardoor weer fysieke controles nodig zijn. Kortom, dit is meestal een vergaande oplossing.

6.5 Aanbevelingen voor de implementatie van maatregelen

Nadat de beheersmaatregelen zijn bepaald, volgt de cruciale fase van implementatie. Aangezien de middelen en mankracht zelden toereikend zijn om alle mitigerende maatregelen tegelijkertijd voor alle systemen uit te voeren, is prioriteitsstelling noodzakelijk.

De volgende aanbevelingen zijn behulpzaam bij het stellen van prioriteiten en het opstellen van een plan van aanpak:

- **Risicogewicht bepalen:** Gebruik het riskeregister om prioriteit te geven aan risico's met het hoogste risicogewicht en/of de meest kritieke objecten. Het is hierbij cruciaal om het totaalbeeld niet te vergeten: de som van meerdere kleine risico's kan uiteindelijk belangrijker zijn dan één geïdentificeerd hoog risico.
- **Planning en constraints:** Stel een gedetailleerd plan van aanpak op, afhankelijk van de beschikbare middelen en (productie- of onderhoud)planning. Houd rekening met

operationele en technische belemmeringen, zoals levertijden van leveranciers, wachten op nieuwe versies, certificeringen of geplande downtime. Dit plan vereist managementgoedkeuring.

- **Externe verplichtingen:** Neem eventuele toekomstige of bestaande verplichtingen meteen mee in de implementatieplanning, zoals vereisten voortkomend uit wetgeving (zoals de Cbw of AVG) of de voorwaarden voor een (cyber) verzekering.
- **Tijdelijke acceptatie:** Als blijkt dat de implementatie door omstandigheden (te) lang duurt, kan een tijdelijke risicoacceptatie noodzakelijk zijn (zie paragraaf 5.2, Acceptatie), mits deze formeel wordt vastgelegd.
- **Managementbeslissing:** Uiteindelijk is het een managementbeslissing hoe de prioriteiten voor implementatie worden afgewogen ten opzichte van het risicoprofiel en de beschikbare middelen.

De volgende overwegingen zijn nodig voor het borgen van de correcte implementatie en het garanderen van de effectiviteit van de gekozen maatregelen:

- **Testen van effectiviteit en volledigheid:** Voer systematische tests uit om de effectiviteit en volledigheid van elke geïmplementeerde maatregel te valideren. Dit is cruciaal om aan te tonen dat het restrisico daadwerkelijk tot het beoogde niveau is gereduceerd.
- **Verificatie bij nieuwe assets:** Bij de ingebruikname van nieuwe assets of systemen is het cruciaal om te controleren of alle maatregelen correct zijn geïmplementeerd. De implementatie kan worden geverifieerd tijdens een FAT (Factory Acceptance Test) of SAT (Site Acceptance Test), bijvoorbeeld door het uitvoeren van een penetratietest. Zorg ervoor dat resterende risico's bekend en geaccepteerd zijn voordat het systeem operationeel wordt. Paragraaf 6.3.1
- **De terugkoppelingslus:** Als blijkt dat de voorgestelde maatregelen in de praktijk anders uitpakken (de oplossing werkt niet of de situatie is veranderd), is directe terugkoppeling naar de risicobeheerder essentieel. De risicoanalyse moet in zo'n situatie opnieuw worden uitgevoerd om het nieuwe restrisico te bepalen.

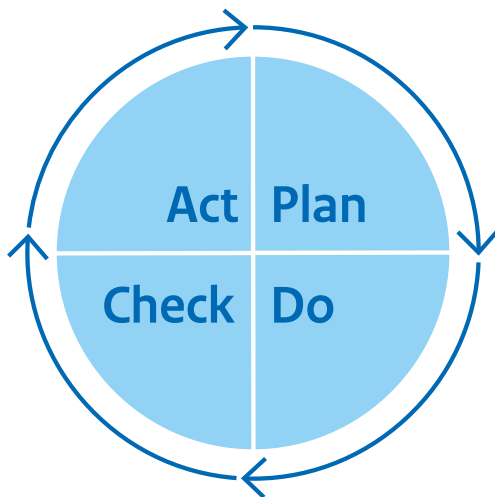
7. Monitoren en rapporteren

Risicobeoordeling en -beheer is geen eenmalige activiteit, maar een continu proces dat constante herziening vereist. Zelfs als er niets verandert aan de infrastructuur en systemen binnen de organisatie, staat de buitenwereld – het dreigingslandschap – nooit stil.

Dit vereist continue monitoring om twee belangrijke redenen:

- **Externe dreigingen:** Dit is onverminderd van toepassing, zelfs als er intern geen wijzigingen plaatsvinden. Externe actoren ontwikkelen continu nieuwe aanvalstechnieken en exploiteren dagelijks nieuwe zwakheden in bestaande systemen.
- **Interne veranderingen:** De interne organisatie staat niet stil. Nieuwe technologieën en systemen introduceren mogelijk nieuwe zwakheden of risico's die gemist kunnen worden als een risicoanalyse niet wordt herzien.

Om de risico's continu passend te beheren, zijn periodieke herevaluaties nodig via bijvoorbeeld zelf-assessments, interne audits, of controles door externe partijen. In de meeste organisaties worden deze continue processen geborgd binnen de PDCA-cyclus (Plan-Do-Check-Act).



De benodigde bedrijfsprocessen voor monitoring en rapportage zijn grofweg te verdelen in drie niveaus: Operationeel, Tactisch en Strategisch. Deze niveaus zullen elk in de volgende paragrafen worden beschreven.

TIP: Compliance als krachtige motor voor monitoring

Veel organisaties, zeker in kritieke sectoren, hebben te maken met wet- en regelgeving. Deze regelgeving creëert een expliciete plicht om aan te tonen dat er passende cyberbeveiligingsmaatregelen zijn getroffen en dat het risicomanagementproces continu is.

Deze externe druk is vaak de belangrijkste reden om een formeel monitoring- en rapportageproces op te zetten. Managementteams zullen de status van deze beheersprocessen en de monitoring van risicotrends (afwijkingen, acceptaties, etc.) daarom actief opvragen. Deze rapportages dienen als cruciale input voor strategische besluitvorming (welke risico's worden geaccepteerd?) en compliance-verantwoording (voldoen we aan de wettelijke eisen?).

Procesintegratie en efficiëntie

Om al deze processen zo efficiënt mogelijk te maken, wordt aangeraden om de beveiligingsprocessen waar mogelijk te integreren in reeds bestaande bedrijfsprocessen (zoals verandermanagement, onderhoud en inkoop). Door mee te liften op de bestaande, goed werkende managementstructuren, voorkomt men het creëren van dubbele processen. Het is hierbij essentieel dat lijsten met openstaande risico's en actiepunten actief worden bijgehouden en gemanaged.

Afhankelijk van de omvang, complexiteit en volwassenheid van de organisatie, kan het beheer van deze risicolijsten en compliance-eisen een enorme taak worden. In dat geval kan ondersteunende software, zoals GRC-tools (Governance, Risk & Compliance), worden ingezet om de rapportage, documentatie en continue monitoring te stroomlijnen.

Kader 7

7.1 Operationeel proces

Deze processen omvatten alle operationele activiteiten en maatregelen die verband houden met cyberbeveiliging. Hierbij draait het vooral om de implementatie, het beheer en de routinematige uitvoering van deze maatregelen.

LET OP: Verificatie is cruciaal

Zonder de zekerheid dat de beheersmaatregelen daadwerkelijk zijn geïmplementeerd en goed functioneren, zijn de eerder gedane risicoaannames ongeldig. De acceptatie van een restrisico is immers gebaseerd op de veronderstelling dat de maatregelen de kans en impact succesvol hebben gereduceerd. Wanneer de effectiviteit niet is bewezen, kan de organisatie niet met zekerheid stellen dat het risico aanvaardbaar is. Verificatie is daarom essentieel om de geldigheid van de risicoacceptatie te borgen.

Kader 7.1

7.1.1 Validatie van Risicoaannames (gap-analyse)

De validatie van risicoaannames is het meest fundamentele operationele monitoringproces. Het richt zich op het borgen van de restrisico's. De operationele aanname is dat het risico aanvaardbaar is, omdat de geïmplementeerde beheersmaatregelen effectief zijn. Het doel is om continu te bevestigen dat deze aanname klopt.

Validatie vereist zowel een controle op de aanwezigheid van maatregelen als op de effectieve werking ervan in de praktijk.

- **Gap-analyse (technische compliance):** Dit proces is reeds in eerdere hoofdstukken beschreven en is de primaire tool om te controleren of alle systemen nog voldoen aan de vastgestelde baselines en maatregelen. De frequentie en mate van detail van deze analyse kunnen risicoafhankelijk worden bepaald. Belangrijke assets worden vaker en vollediger gecontroleerd, terwijl minder kritische objecten steekproefsgewijs kunnen worden gecontroleerd.
- **Proceseffectiviteit:** Deze kwalitatieve checks zijn essentieel om te bepalen hoe de maatregelen in de praktijk functioneren. Dit wordt uitgevoerd via interne audits en assessments om te controleren of vastgelegde procedures (bijvoorbeeld rond toegangsbeheer of onderhoud) daadwerkelijk gevolgd worden.
- **Menselijke factor en cultuur:** Security-awareness en de daadwerkelijke beveiligingscultuur zijn bepalend voor hoe de organisatie omgaat met cybersecurity. Dit wordt in kaart gebracht door middel van observatie en interviews met

medewerkers en het observeren van routinewerkzaamheden.

De bevindingen uit deze validatieprocessen leiden tot twee mogelijke vervolgacties, ongeacht of de bevinding technisch, procedureel of menselijk van aard is:

- **Directe operationele correctie:** Dit betreft de afwijkingen waarbij iets is gevonden dat conform de vastgestelde maatregelen had moeten zijn, maar is nagelaten (bijvoorbeeld een ontbrekende patch of een overgeslagen procedure). Deze afwijkingen moeten door het operationele team direct worden opgepakt en opgelost. Escalatie is enkel nodig indien de directe oplossing niet lukt of vertraging oploopt.
- **Formele herziening van risicoaannames:** Dit pad wordt gevolgd wanneer een bevinding aantoont dat de onderliggende risicoaannames niet (meer) kloppen. Dit kan zijn door een fundamentele zwakte in het ontwerp, een nieuw inzicht in de dreiging, of de vaststelling dat een maatregel (techniek, proces of mens) structureel ineffectief is. Dergelijke bevindingen vereisen een formele herziening van het restrisico door de risicobeheerder en moeten worden geëscaleerd naar het tactische niveau. Dit leidt mogelijk tot een aanpassing van het risicoregister of het risicobehandelplan.

7.1.2 Kwetsbaarheden monitoring (Effectiviteit Toetsen)

Het is belangrijk te benadrukken dat compliance (waar de nadruk op lag in de vorige paragraaf) niet hetzelfde is als effectiviteit: alle maatregelen kunnen aanwezig zijn, maar toch onvoldoende risicoreductie bieden.

Kwetsbaarhedenmonitoring is de directe en continue test van de effectiviteit van de geïmplementeerde maatregelen. Dit proces is vergelijkbaar met de initiële inventarisatie van kwetsbaarheden (zie hoofdstuk 4), maar richt zich nu op het routinematig controleren op nieuwe of onbekende zwakheden in bestaande gecontroleerde systemen.

Dit kan bijvoorbeeld worden gedaan door regelmatig gerichte 'vulnerability scans' of 'penetration tests' uit te voeren. Een vulnerability scan is een geautomatiseerde check die technisch bekende kwetsbaarheden identificeert in systemen, netwerken of applicaties die misbruikt kunnen worden. Voor OT-omgevingen bestaan er specifieke, passieve scanoplossingen die de systemen monitoren via netwerkverkeer, zonder deze direct actief te benaderen of te verstoren. Een penetratietest is een actieve aanvalssimulatie waarbij ethische hackers proberen binnen te dringen om de effectiviteit van de beveiligingsmaatregelen in de praktijk te testen.

LET OP: Kwetsbaarheidstesten in OT-omgevingen

Standaard IT-testmethoden zijn vaak niet een-op-een te gebruiken binnen OT-omgevingen. Het uitvoeren van vulnerability scans en penetratietests kan hierdoor onbedoeld negatieve gevolgen hebben, zoals verstoring van de productie, instabiliteit van systemen of zelfs uitval.

Daarom vereisen dit soort onderzoeken in OT-omgevingen extra zorgvuldige voorbereiding, gedetailleerde planning en expliciete goedkeuring van het management. In de meeste gevallen worden deze onderzoeken daarom uitbesteed aan externe experts die gespecialiseerd zijn in veilige en niet-destructieve OT-testen.

In het meest ideale geval zorgt de organisatie voor spare componenten en/of een acceptatie omgeving waar dit onderzoek op plaats kan vinden. Dit voorkomt dat de productieomgeving negatief wordt beïnvloed.

Kader 7.1.2a

Opvolging van Bevindingen

Bevindingen uit kwetsbaarhedenmonitoring zijn complexer om op te volgen dan een simpele gap in compliance, omdat het systeem volledig compliant kan zijn, maar alsnog ernstige zwakheden kan bevatten. De volgende afwegingen zijn hierbij relevant:

- **Directe actie bij kritieke impact:** In sommige gevallen is het direct duidelijk dat de gevonden zwakheden een ernstige impact hebben op kritieke bedrijfsprocessen (eerder vastgesteld met de BIA). Als de kwetsbaarheid de continuïteit van deze processen direct bedreigt, is het risico overduidelijk onacceptabel. De noodzaak tot een oplossing is in dit geval zo groot dat een verdere, gedetailleerde risicoanalyse wordt overgeslagen en direct actie tot mitigatie wordt ondernomen.
- **Analyse via risicobeheer:** In de meeste gevallen is er echter meer technisch en inhoudelijk onderzoek nodig om vast te stellen hoe een bepaalde zwakheid daadwerkelijk kan leiden tot de gevreesde impact. Voor deze detailanalyse is vaak extra expertise (intern of van de leverancier) nodig. Deze bevindingen moeten via het risicobeheerproces worden opgepakt om alle afwegingen te maken (mitigeren, extra compenserende maatregelen of accepteren).

- **Escalatie en acceptatie:** Het kan voorkomen dat er tegenstrijdige inzichten zijn, of dat de asseteigenaar het niet eens is met de kosten of de vermindering van gebruiksgemak van de voorgestelde oplossing. In dit soort gevallen moet het escalatieproces via het management gevolgd worden. Uiteindelijk moet het officiële risicoacceptatieproces (zie paragraaf 5.2) worden doorlopen om eventuele restrisico's formeel te accepteren.

Casestudy: Akira ransomware op KNP Logistics

In 2023 werd transport- en logistiekbedrijf KNP Logistics slachtoffer van de Akira ransomware-aanval. Dit incident toonde aan dat één simpele tekortkoming in de basisbeveiliging catastrofale gevolgen kan hebben. Dit incident was uiteindelijk mede de oorzaak van het faillissement van KNP.

De initiële toegang tot de systemen werd namelijk verkregen door één zwak gebruikersaccount. Het wachtwoord hiervan was erg eenvoudig en multifactorauthenticatie (MFA) hierop was niet geactiveerd.

Dit incident onderstreept twee cruciale leerpunten:

- **Disproportionele gevolgen:** Eén zwakke schakel leidde tot onherstelbare schade, in dit geval bijdragend aan het faillissement van de organisatie.
- **Beperking cyberverzekering:** Hoewel cyberinsurance (zie hoofdstuk 5) was afgesloten en hielp bij de incidentrespons, kon deze de enorme economische schade door wekenlange operationele stilstand en verlies van contracten niet compenseren.

Deze casus is een scherpe herinnering aan de noodzaak om bestaande maatregelen continu te valideren en de effectiviteit ervan te controleren.

Kader 7.1.2b

7.1.3 Patch- en Configuratiemanagement

Dit betreft het routinematige onderhoud van de systemen. Het tijdig aanbrengen van patches en het borgen van de juiste basisconfiguraties zijn de meest essentiële maatregelen in elk beveiligingsbeleid. Dit omvat:

- **Patchmanagement:** Dit is de uitvoering van de installatie en verificatie van beveiligingsupdates (patches) conform de gedefinieerde planning en het beleid (dat op tactisch niveau is vastgesteld). De operationele taak is het correct aanbrengen en controleren van de stabiliteit van het systeem na installatie.
- **Configuratiemanagement:** Dit omvat het periodiek bijhouden, opschonen en controleren van de actieve configuraties op afwijkingen en onnodige risico's. Daarbij gaat het bijvoorbeeld om het identificeren en deactiveren van verouderde of niet-gebruikte gebruikersaccounts, het verwijderen van oude, ongebruikte firewallregels, en het controleren op en uitschakelen van onnodige netwerkprotocollen of services op systemen.

7.1.4 Verandermanagement

Elke wijziging in de infrastructuur, zoals nieuwe software, nieuwe netwerkkoppelingen of configuratiewijzigingen, kan de cybersecurity direct beïnvloeden. Dit kan leiden tot de introductie van nieuwe risico's of, wat minstens zo belangrijk is, invloed hebben op eerdere aannames die zijn gebruikt bij de risicoanalyse en risicoacceptatie. Significante veranderingen kunnen zelfs impact hebben op certificeringen of de CE-markering.

Een goed verandermanagementproces is daarom cruciaal. Het omvat procedures voor het beoordelen, goedkeuren, imple-

menteren en monitoren van wijzigingen waarbij, voordat de verandering wordt doorgevoerd, rekening wordt gehouden met de mogelijke beveiligingsimplicaties en de validiteit van het bestaande risicoprofiel.

TIP: Verandermanagement als basis voor efficiëntie

Een robuust verandermanagementproces is de beste preventieve maatregel tegen 'configuration drift' (het onbedoeld afwijken van de beveiligingsbaseline). Door elke wijziging grondig te toetsen, voorkomt de organisatie dat er onnodig zwakheden worden geïntroduceerd.

Hoewel verandermanagement in eerste instantie vaak als een lastige bureaucratische taak wordt beschouwd, levert het uiteindelijk aanzienlijke efficiëntievoordelen op:

- **Minder manuele controles:** Er is minder vaak de noodzaak voor uitgebreide configuratiemanagementcontroles (zie 6.1.3), omdat de basisconfiguratie betrouwbaarder blijft.
- **Minder heranalyses:** De betrouwbaarheid van de veranderprocessen vergroot de zekerheid van de oorspronkelijke risicoacceptatie, waardoor minder vaak een volledige herevaluatie van het risicoprofiel noodzakelijk is.

Door te investeren in een efficiënt proces, bespaart de organisatie op de lange termijn aanzienlijk op herstelwerk en onverwachte risico-evaluaties.

Kader 7.1.4



7.1.5 Leren van incidenten

Mocht er ondanks alle genomen maatregelen toch een incident plaatsvinden, dan is de fase van ‘lessons learned’ een vast en cruciaal onderdeel van het Incident Response proces. Het doel is om te leren van het incident, niet alleen om de operationele procedures te verbeteren, maar vooral om het risicobeheerproces te valideren en aan te passen.

Met name de volgende vragen zijn interessant voor risicomanagement:

- **Effectiviteit van maatregelen:** Hoe kon het incident plaatsvinden? Waren de genomen maatregelen niet geïmplementeerd of waren ze ineffectief in de praktijk? Moet de set aan baselinemaatregelen worden aangepast?
- **Impact:** Was de daadwerkelijke impact zoals voorspeld tijdens eerdere impactanalyses (BIA)? Of is het nodig om de inschatting van de impact te herijken op basis van de opgedane ervaring?

Casestudy: Eén centrale storing, enorme impact

Veel kritieke OT-systemen zijn tegenwoordig afhankelijk van overkoepelende, centrale communicatie- en aansturingssystemen (denk aan verkeersleiding of controlekamers). Een storing in deze centrale functie kan het hele systeem tot stilstand brengen, met directe en enorme impact op het grote publiek:

Enkele voorbeelden uit het nieuws:

- “Vliegverkeer Schiphol stilgelegd na communicatiestoring” (2018)
- “Metroverkeer GVB langzaam weer opgestart na storing communicatiesysteem” (2018)
- “Treinverkeer plat door communicatiestoring bij ProRail” (2021)
- “NS-storing legt alle treinverkeer van vervoerders plat” (2022)
- “Communicatiestoring bij HTM legt dienstregeling plat” (2024)
- “Busvervoer Qbuzz plat door storing communicatiesysteem” (2024)

Ondanks de initiële risicoanalyse en genomen maatregelen kan het dus alsnog misgaan. Het is nu zaak om te bepalen: waren de juiste maatregelen genomen, of moet er iets veranderen om dit in de toekomst te voorkomen? Uiteindelijk heeft dit ook een koppeling met het risicobeheerproces.

7.1.6 Continu verbeteren (PDCA)

De processen die in dit hoofdstuk zijn beschreven (validatie, monitoring, leren van incidenten, etc.) vormen samen een ambitieus ideaalbeeld voor operationeel risicobeheer. Voor veel organisaties is dit een vergezicht. De essentie is dat er ergens begonnen wordt met monitoren en dat de cyclus van verbeteren niet stopt.

De resultaten van al deze operationele controles moeten uiteindelijk worden geïntegreerd in het bredere risicomanagementproces. Dit zorgt ervoor dat de cyberbeveiligingsmaatregelen voortdurend worden geëvalueerd, bijgewerkt en aangepast om de veiligheid van de organisatie te waarborgen.

De operationele processen vormen de ‘Check’ en ‘Act’-fasen van de PDCA-cyclus (Plan-Do-Check-Act) op de werkvloer. De verschillende controles (6.1.1 t/m 6.1.5) verschaffen de input voor deze cyclus:

Check

De controles geven antwoord op de volgende essentiële vragen:

- Zijn alle voorgestelde maatregelen (techniek, mens, proces) aanwezig en up-to-date?
- Zijn de maatregelen effectief in de praktijk, en worden ze correct gebruikt?
- Worden hiermee de restrisico’s daadwerkelijk gemitigeerd, of is de initiële risicoanalyse onjuist gebleken?

Act

Op basis van deze bevindingen worden aanpassingen gemaakt om te verbeteren en bij te sturen. Dit leidt tot de volgende operationele acties:

- Het actualiseren van werkinstructies en het borgen van de naleving van (aangepaste) procedures.
- Het implementeren van verbeteringen en het nemen van preventieve maatregelen.
- Het doorvoeren van technisch onderhoud om de operationele risico’s te beheersen en te verminderen.

7.2 Tactisch proces

Het tactische proces fungeert als de brug tussen de strategische governance (de waarom en wat van risicobeleid) en de operationele uitvoering (de hoe). Het richt zich op de middellange termijn (doorgaans 1 tot 3 jaar) en de concrete invloed van cybersecurity op kritieke bedrijfsprocessen en assets binnen de OT-omgeving.

Op dit niveau worden de belangrijke beslissingen genomen over de prioritering en inzet van middelen. Alle risicobeheerprocessen die in de eerdere hoofdstukken zijn beschreven worden hier geconcretiseerd, bewaakt en bijgestuurd. De

tactische sturing is essentieel om te garanderen dat de dagelijkse operationele taken daadwerkelijk bijdragen aan de strategische risicodoelstellingen van de organisatie.

De verantwoordelijkheid van het tactische niveau omvat onder andere:

- **Beheer van de baseline:** Het opstellen, formeel vaststellen én het dynamisch aanpassen van de standaard (baseline) maatregelen, op basis van operationele feedback en veranderende dreigingslandschappen.
- **Prioritering en planning (securityroadmap):** Het vertalen van strategische doelen en de baseline naar een concreet uitvoeringsplan (de securityroadmap). Dit omvat het vaststellen van prioriteiten, het toewijzen van middelen en het bepalen van mijlpalen en deadlines voor de implementatie van maatregelen.
- **Formele risicoacceptatie:** Het beoordelen van (tijdelijke) afwijkingen en het formeel accepteren van restrisico's, in lijn met de strategische risicotolerantie (zie 6.2.2)
- **Dynamische aanpassing:** Alle processen moeten continu worden aangepast om in lijn te blijven met veranderende bedrijfsprocessen en strategische waarden. (zie 6.2.3)

7.2.1 Leveranciersmanagement en contractuele cybersecurity

Het goed beheren van leveranciersrisico's is een kritiek onderdeel van OT-cybersecurity. Third-party risico's vereisen specifieke beheersmaatregelen die verder gaan dan het traditionele contractmanagement. Hoewel de richting en het beleid wordt bepaald in het strategische proces, is het tactische niveau verantwoordelijk voor de concrete implementatie van het leveranciers- of supplychainmanagement voor de middel-lange termijn. De aanpak kan worden opgebouwd in verschillende fases van volwassenheid.

Fase 1: Eerste Stappen

Voor organisaties die beginnen met leveranciersmanagement is het cruciaal om te starten met de meest essentiële activiteiten. Deze benadering zorgt voor snelle risicoreductie zonder de organisatie te overbelasten. De focus ligt op de meest kritieke leveranciers en basiswaarborgen:

- **Inventarisatie en prioritering:** Inventariseer alle third-party leveranciers en prioriteer ze op basis van hun kritikaliteit voor de OT-omgeving. Focus specifiek op leveranciers met directe toegang tot OT-systemen of die kritieke ondersteunende diensten leveren.
- **Minimale contractuele waarborgen:** Implementeer minimale contractuele eisen, zoals een incidentmeldingsplicht, afspraken over toegangsbeveiliging en audit-rechten. Let op: contractuele eisen zijn belangrijk, maar zonder regelmatig toezicht betekenen ze weinig in de praktijk.

- **Standaardclausules:** Gebruik standaard cybersecurityclausules die eenvoudig bij nieuwe contracten of contractverlenging kunnen worden toegevoegd.
- **Eenvoudige Monitoring:** Voer eenvoudige operationele monitoring uit op de meest kritieke leveranciers. Dit omvat onder meer het bijhouden van periodieke verificatie van de toegangsrechten, certificeringen en incidentrapportages. Controleer tevens of de medewerkers de relevante trainingen OT-cybersecurity-awareness hebben ontvangen.

Fase 2: Gedetailleerde Aanpak

Organisaties die reeds een volwassener risicobeheerproces hebben opgebouwd — inclusief de benodigde expertise en governancestructuren — kunnen een uitgebreidere aanpak implementeren die diepgaandere risicobeheersing biedt.

Deze aanpak vereist meer resources, maar levert ook betere risicoreductie en compliance op. De intensiteit van het proces moet bovendien altijd risicoafhankelijk zijn: het is niet noodzakelijk voor alle leveranciers; hoe meer risico een leverancier met zich meebrengt, hoe zwaarder het beoordelingsproces is.

De volgende onderwerpen zijn van belang voor deze gedetailleerde aanpak:

- **Gestructureerd evaluatieproces:** Implementeer een formeel evaluatieproces voor nieuwe leveranciers dat hun cybersecurityvolwassenheid, incident response capabilities en compliance-assessment omvat.
- **Periodieke herbeoordeling:** Voer periodieke herbeoordelingen uit van bestaande kritieke leveranciers met behulp van formele scoringsmethodieken.
- **Meetbare afspraken:** Stel specifieke cybersecurity-SLA's (Service Level Agreements) op met meetbare indicatoren en prestatiedashboards.
- **Contractuele verdieping:** Neem gedetailleerde dataprotectieafspraken en escalatieprocedures op in contracten. Dit omvat bijvoorbeeld afspraken over hoe leveranciers met de data van de organisatie om dienen te gaan (denk bijvoorbeeld aan leveranciers die back-ups maken).
- **Supplychainbeheer:** Neem contractuele verplichtingen op voor leveranciers om hun eigen supplychain te beheren en te rapporteren over de bijbehorende risico's.
- **Beheer en analyse:** Implementeer regelmatige overlegstructuren en trendanalyse van leveranciersprestaties.
- **Exitstrategie:** Leg verplichtingen vast in contracten voor het (eventueel) beëindigen van een dienst of leverancier. Denk aan het overdragen van kennis, documentatie, intellectueel eigendom, toegangsrechten, configuratie, broncode, etc.
- **Automatisering:** Zet geautomatiseerde monitoring in waar mogelijk en stel gestructureerde procedures op voor zowel contractbeëindiging als een leverancierswissel.

7.2.2 Formele risicoacceptatie

Het formele risicoacceptatieproces is het meest kritische tactische proces voor OT-risicobeheer. Het gaat hierbij om het gecontroleerd en formeel behandelen van alle restrisico's en tijdelijke afwijkingen die de organisatie bewust besluit te dragen. In de OT-omgeving, waar risico's complex zijn, fungeert dit als een mechanisme om de operationele realiteit en strategische risicotolerantie op elkaar af te stemmen. Het doel van het proces is om elk geaccepteerd risico transparant te maken en formeel te documenteren, om zo de accountability vast te leggen.

Elke risico-acceptatie – of het nu een afwijking van de baseline betreft, een tijdelijk operationeel risico, of een onvermijdelijk restrisico na een mitigatietraject – moet beginnen met een gedocumenteerde aanvraag. Deze aanvraag is pas compleet wanneer deze de aard van het risico, de duidelijke reden, de maximale duur en, cruciaal, de compenserende maatregelen bevat. Dit zijn de stappen die direct worden genomen om de potentiële impact te verlagen, bijvoorbeeld door extra monitoring of organisatorische procedures.

De tactisch eindverantwoordelijke – dit is de persoon of entiteit (zoals de OT-securitymanager, de risicobeheerder, of een bevoegde gedelegeerde stuurgroep) waaraan de formele beslissingsbevoegdheid is gedelegeerd – is verantwoordelijk voor de beoordeling. Zij valideren de effectiviteit van de compenserende maatregelen en bepalen de uiteindelijke risicoscore van het restrisico.

Bij veel organisaties is het zo ingericht dat deze score de benodigde autoriteit voor goedkeuring bepaalt: bij lage en middelgrote risico's ligt de beslissingsbevoegdheid op het

tactische niveau. Echter, bij hoge risico's vindt er altijd een formele escalatie plaats naar het strategische governance-niveau (CISO of directie) voor bevoegde acceptatie. Dit garandeert dat de eindverantwoordelijkheid voor risico's boven de tactische tolerantiegrens op het juiste niveau wordt gedragen. Het tactische niveau draagt tevens zorg voor een centrale registratie van alle geaccepteerde risico's. Dit is essentieel voor auditing en het borgen van de accountability voor elk bewust geaccepteerd restrisico.

7.2.3 Continu verbeteren (PDCA)

De tactische processen vereisen continue controle en verbetering om effectief te blijven. De fasen Check en Act van de PDCA-cyclus zijn cruciaal voor de dynamische sturing van OT-risicobeheer. Dit zorgt ervoor dat de ingezette middelen en de vastgestelde baselines relevant blijven in een continu veranderende omgeving.

Check

Systematische monitoring is essentieel om de effectiviteit van het risicobeheer te valideren. Dit gaat verder dan incidentregistratie; het is gericht op prestatiebeoordeling en het identificeren van structurele problemen.

- **Prestatiemeting en KPI's:** Het monitoren van de vastgestelde Key Performance Indicators (KPI's) en Key Risk Indicators (KRI's) om op feitelijke basis te bepalen of de geïmplementeerde maatregelen de restrisico's daadwerkelijk verlagen. Denk hierbij bijvoorbeeld aan: Percentage kritieke systemen met actuele patches, doorlooptijd van risicoacceptatieaanvragen of naleving van minimale contractuele waarborgen bij leveranciers.



- **Systematische beoordeling:** Hieronder valt het uitvoeren van audits en periodieke reviews van het Risicoacceptatieproces zelf. Hierbij wordt bijvoorbeeld gecontroleerd op de kwaliteit van de risicoargumentatie en de feitelijke naleving van gestelde eisen. Is de onderbouwing van het restrisico consistent en volledig? En zijn de tijdelijk geaccepteerde risico's daadwerkelijk afgesloten of geëscaleerd na het verstrijken van de termijn?

Het rapporteren van OT-cyber risico's is uitdagend omdat het een technische vertaalslag vereist van operationele bevindingen naar tastbare risico's, bedrijfsimpact en verwachte kosten voor de bestuurslaag. Om deze uitdagingen te overwinnen, dient de rapportage te focussen op bedrijfseffecten (zoals kwantificering van potentiële verstoringen en financiële verliezen). Organiseer daarnaast educatieve sessies om het bewustzijnsniveau van leidinggevendenden te verhogen, maar ook om te leren hoe de organisatie omgaat met andere risico's om hier zo goed mogelijk bij aan te sluiten.

TIP: Praktische monitoring zonder formele KPI's

Formele KPI's zijn niet altijd voorhanden en worden doorgaans alleen in de meest volwassen organisaties geïmplementeerd. Voor organisaties zonder uitgebreide meetsystemen bestaan echter praktische alternatieven.

Een effectieve benadering is het benutten van interne expertise door gebruik te maken van medewerkers in de eerste lijn, eventueel aangevuld met cybersecurity champions of ambassadeurs. Deze medewerkers hebben vaak een accuraat beeld van de werkelijke stand van zaken en kunnen waardevolle inzichten verschaffen over naleving van securityprocedures in de praktijk, knelpunten in de uitvoering, opkomende risico's of incidenten, en de effectiviteit van geïmplementeerde maatregelen.

Het belangrijkste aspect is het waarborgen van structurele terugkoppeling naar het management, zodat trends en patronen zichtbaar worden. Dit kan worden gerealiseerd door regelmatige gesprekken met sleutelmedewerkers, gestructureerde rapportageformats, periodieke evaluatiesessies en documentatie van waargenomen ontwikkelingen te implementeren.

Deze informatie vormt vervolgens input voor beleidsaanpassingen op strategisch niveau en helpt bij het prioriteren van verbeteracties binnen het tactische governance raamwerk.

Act

De bevindingen uit de 'Check'-fase leiden direct tot actie op twee cruciale niveaus: de interne tactische bijsturing van processen en de rapportage naar de strategische leiding.

- **Tactische aanpassingen:** Het direct herzien van de security-roadmap en/of baseline en het initiëren van corrigerende acties op uitvoerend niveau op basis van de evaluatieresultaten. Dit omvat bijvoorbeeld het bijwerken van de baseline als blijkt dat maatregelen niet proportioneel of haalbaar zijn.
- **Strategische rapportage:** Het rapporteren van trends in excepties en prestaties naar de strategische bestuurslaag van de organisatie. Door middel van trendanalyse van de verzamelde data kan besluitvorming over structurele investeringen en herziening van de risicotolerantie worden gefaciliteerd. De rapportage wijst op structurele problemen, zoals een toename van excepties die duidt op architectuurbeperkingen of onrealistische securityeisen, en op budgettaire tekortkomingen die duurzame oplossingen belemmeren.

7.3 Strategisch proces

Het strategisch proces richt zich op de organisatie als geheel en heeft een duidelijke focus op de lange termijn. Op deze bestuurslaag worden de fundamenteën van het risicobeheer gelegd door de context en scope van de organisatie te bepalen. Dit omvat alles wat de kernwaarden en de bedrijfscontinuïteit beïnvloedt, zoals nieuwe wet- of regelgeving, aanpassingen in de risicotolerantie (risk appetite) en grote gebeurtenissen zoals fusies of overnames.

De belangrijkste output van dit proces is het vaststellen van het OT-securitybeleid en de ambitie. Dit bepaalt het gewenste volwassenheidsniveau voor risicobeheer en de strategische doelen voor de beheersing van risico's binnen de organisatie. Strategische ambities, een veranderend dreigingslandschap (zoals de opkomst van AI-ondersteunde aanvallen), of maatschappelijke externe eisen kunnen aanleiding geven tot aanpassingen in dit beleid.

De strategische bestuurslaag moet beslissingen nemen met een langetermijnpact om te garanderen dat de ambitie voor OT-risicobeheer gehaald én behouden kan worden, twee voorbeelden:

- **Resource- en ambitieafstemming:** Het strategisch proces is verantwoordelijk voor het toewijzen van adequate budgetten en middelen (personeel, technologie) die passen bij het vastgestelde volwassenheidsniveau en de strategische ambitie. Dit garandeert dat de tactische en operationele lagen de middelen hebben om het beleid uit te voeren.
- **Technologisch levenscyclusbeheer:** De strategie moet vooruitkijken en besluiten nemen over investeringen en het beleid ten aanzien van verouderde (legacy) OT-systemen. De hoge kosten en downtime voor vervanging vereisen een strategische beslissing over hoe de technische omgeving in staat blijft om op de lange termijn aan het vastgestelde volwassenheidsniveau te kunnen voldoen.

7.3.1 Continu verbeteren (PDCA)

De voortgang en relevantie van het strategisch beleid wordt geborgd via de PDCA-cyclus. Deze cyclus verzekert dat beleid en ambitie dynamisch blijven en reageren op de interne en externe context.

Plan

De 'Plan'-fase van het strategisch proces moet antwoord geven op de volgende kernvragen om de koers te bepalen:

- Welke bedreigingen rondom cybersecurity zien we die invloed hebben op de missie van onze organisatie? En hoe veranderen deze in de tijd (dreigingslandschap)?
- Wat is ons risicotolerantieniveau (risk appetite) en hoe sluit deze aan bij de kernwaarden van onze organisatie?
- Aan welke wet- en regelgevingen moeten we voldoen? Gaat dit veranderen in de toekomst of beïnvloedt dit de toeleveringsketen?
- Wat is ons ambitieniveau voor risicobeheer en hoe waarborgen we dat in de organisatie? Wat verwachten we van onze ketenpartners?

LET OP: Auditeerbaarheid en verantwoording

Risicorapportage dient altijd auditeerbaar te zijn, wat cruciaal is voor de naleving van regelgeving (zoals bijvoorbeeld NIS2 of IEC 62443) en de verantwoordingsplicht. Auditbare rapporten bieden transparantie en bewijs van zorgvuldigheid bij het aanpakken van cyberdreigingen, wat het vertrouwen van alle stakeholders versterkt.

Kader 7.3.1a

TIP: Visualisatie van indicatoren

De geaggregeerde indicatoren uit de 'Check'-fase zijn de basis voor de tactische en strategische rapportage. Deze kunnen effectief worden weergegeven in dashboards, heatmaps of scorecards, waardoor ook onderlinge verbanden duidelijk worden. Belangrijke indicatoren kunnen bijvoorbeeld zijn: bewustzijnsniveau onder personeel, voortgang in implementatie van maatregelen, identificatie van gaps en het signaleren van opkomende trends. Het indexeren en inzichtelijk maken van deze indicatoren vergemakkelijkt proactieve besluitvorming en snelle bijsturing in een veranderend landschap.

Kader 7.3.1b

Check & Act

Het strategisch proces gebruikt de rapportage vanuit de tactische laag (6.2) om het beleid te valideren. Hiertoe evalueert de strategische bestuurslaag de effectiviteit van de genomen maatregelen aan de hand van meetbare prestatie-indicatoren (strategische KPI's) en de gerapporteerde trends in excepties en structurele problemen.

Op basis van de bevindingen uit deze evaluatie worden aanpassingen gemaakt aan de strategische benadering van risicobeheer. Dit kan inhouden: het herzien van strategische doelstellingen, het aanpassen van beleidslijnen, het opnieuw toewijzen van middelen, of het nemen van corrigerende maatregelen om te voldoen aan veranderende omstandigheden (zowel intern als extern). Dit proces is essentieel om de langetermijnweerbaarheid te garanderen.

Afkortingen en verklarende woordenlijst (op alfabetische volgorde)

Asset: Een waardevol bezit van een organisatie, zoals fysieke apparatuur, software, gegevens of intellectueel eigendom. Personen vallen ook onder de noemer ‘assets’.

AVG: Algemene Verordening Gegevensbescherming - Een Europese wetgeving die de bescherming van persoonsgegevens regelt en de rechten van individuen met betrekking tot hun persoonlijke gegevens versterkt, van toepassing op alle organisaties die persoonsgegevens verwerken binnen de Europese Unie.

Beschikbaarheid (BIV) : De B uit de afkorting BIV. De eigenschap dat een actief toegankelijk en bruikbaar is op aanvraag door een geautoriseerde entiteit.

Best Practice: Een erkende methode, techniek of proces die als effectief wordt beschouwd voor het bereiken van een specifiek doel of resultaat.

BIA: Business Impact Analysis. Vaststellen van kritieke bedrijfsprocessen en de afhankelijkheden.

BIV: Beschikbaarheid, Integriteit, Vertrouwelijkheid.

BOM (HBOM, SBOM): Bill of Materials. Een overzicht van alle subsystemen, componenten en softwarebibliotheken (zoals een Hardware Bill of Materials of Software Bill of Materials) die door een leverancier zijn geïnstalleerd. Noodzakelijk voor een complete risicoanalyse en het aanpakken van supplychainrisico's.

Cascaderende effecten: Het fenomeen waarbij een incident of storing in een systeem of proces leidt tot opeenvolgende problemen of storingen in andere systemen of processen, vergelijkbaar met een domino-effect.

Cbw: De Cyberbeveiligingswet is de Nederlandse wet die de Europese NIS2richtlijn implementeert. Het doel van deze wet is om de cyberbeveiliging en de weerbaarheid van essentiële en belangrijke diensten in Nederland te verbeteren.

CISA: Cybersecurity and Infrastructure Security Agency. Een agentschap van de Amerikaanse overheid dat verantwoordelijk is voor het beschermen van de nationale cybersecurity en de kritieke infrastructuur.

CISO: Chief Information Security Officer. De hooggeplaatste functionaris binnen een organisatie die verantwoordelijk is voor het ontwikkelen en uitvoeren van het informatiebeveiligingsbeleid.

Cloudcomputing: Diensten voor het leveren van computerbronnen, zoals rekenkracht, opslag en software, via het internet, waarbij gebruikers toegang hebben tot gedeelde pools van configureerbare systeembronnen.

CRA: Cyber Resilience Act. De CRA is een nieuwe Europese verordening die als doel heeft de cyberbeveiliging van digitale producten te verhogen. Het stelt verplichte eisen aan fabrikanten, importeurs en distributeurs van hardware en software die op de Europese markt worden gebracht.

CSMS: Cyber Security Management System – Een gespecialiseerde vorm van een informatiebeveiligingsbeheersysteem (ISMS), maar dan specifiek gericht op het beheer van cyberbeveiligingsrisico's binnen een organisatie.

CVE: Common Vulnerabilities and Exposures. Een gestandaardiseerd naamgevingssysteem voor publiekelijk bekende cyberbeveiligingskwetsbaarheden.

Cyber Kill Chain: Een model dat de opeenvolgende fasen van een cyberaanval beschrijft, van de eerste verkenning tot het uiteindelijk bereiken van het doelwit.

Datalek: Een incident waarbij gevoelige, vertrouwelijke of beschermde informatie onbedoeld wordt vrijgegeven, verloren raakt of wordt gestolen.

Diagnostics: Het proces van het identificeren en analyseren van problemen of storingen in systemen, apparaten of processen om de oorzaak vast te stellen en passende maatregelen te nemen.

EDR: Endpoint Detection and Response. Een beveiligingstechnologie die zich richt op het bewaken en detecteren van, en reageren op, verdachte activiteiten en mogelijke bedreigingen op eindpuntapparaten zoals computers, laptops en servers.

FAT: Factory Acceptance Test. Een test die wordt uitgevoerd bij de fabrikant voordat een systeem of apparaat wordt geleverd aan de klant. Het dient om te controleren of het systeem voldoet aan de specificaties en eisen van de klant.

Hacktivist: Een persoon of groep die hacken gebruikt als een vorm van protest of activisme om politieke of sociale doelen te bevorderen.

ICS/IACS: Industriële Controlesystemen/Industriële Automatisering en Controlesystemen. Systemen gebruikt in industrieën om processen te automatiseren, monitoren en regelen.

IEC 62443: Een reeks internationale normen die specifiek zijn gericht op de beveiliging van industriële automatiserings en controlesystemen (IACS), met richtlijnen voor het identificeren, beoordelen en beheren van beveiligingsrisico's.

Impact: Het effect of de gevolgen van een gebeurtenis of incident.

Integriteit (BIV): De I uit de afkorting BIV. De nauwkeurigheid, correctheid en volledigheid van activa.

IoT: Internet der Dingen. Het netwerk van fysieke apparaten, voertuigen, huishoudelijke apparaten en andere objecten die zijn ingebed met elektronica, software, sensoren en connectiviteit om gegevens te verzamelen en uit te wisselen.

ISO 27001: Een internationale norm voor informatiebeveiliging die een raamwerk biedt voor het vaststellen, implementeren, beheren en continu verbeteren van een informatiebeveiligings-beheersysteem (ISMS) binnen een organisatie.

ISO 27005: Een internationale norm die richtlijnen biedt voor het uitvoeren van risicobeoordelingen en het implementeren van risicobeheersingsmaatregelen binnen een organisatie.

ISMS: Information Security Management System. Een gestructureerde, systematische aanpak om de gevoelige informatie van een organisatie te beheren en te beschermen, met als doel de vertrouwelijkheid, integriteit en beschikbaarheid van die informatie te waarborgen.

IT: Informatietechnologie - Het gebruik van computers, netwerken, en andere technologische systemen voor het opslaan, verzenden en verwerken van gegevens en informatie.

KPI: Key Performance Indicator - Een meetbare waarde die de voortgang of prestatie van een organisatie op een bepaald gebied aangeeft, zoals cyberbeveiliging.

Kroonjuwelen: Kritieke bedrijfsmiddelen of -gegevens die van onschatbare waarde zijn voor een organisatie en die bijzonder goed moeten worden beschermd.

Likelihood: De kans dat een bepaald risico zich voordoet.

Machineverordening: Nieuwe Europese wetgeving die de vorige Machinerichtlijn vervangt. Het doel is om de gezondheid en veiligheid van mensen te beschermen bij het gebruik van machines, inclusief eisen voor cybersecurity en kunstmatige intelligentie (AI).

Nation state actor: Een entiteit die handelt namens of onder controle staat van een nationale overheid, en die betrokken is bij cyberaanvallen of spionageactiviteiten.

NCSC: Nationaal Cyber Security Centrum. Een organisatie op nationaal niveau die verantwoordelijk is voor het bevorderen van cyberbeveiliging en het bieden van ondersteuning.

NIS2: De Europese richtlijn inzake de beveiliging van netwerk- en informatiesystemen (NIS) die de veiligheid van netwerk- en informatiesystemen binnen de Europese Unie regelt.

NIST SP 800-30: Een publicatie van het National Institute of Standards and Technology (NIST) die richtlijnen biedt voor het uitvoeren van risicobeoordelingen, met de nadruk op informatietechnologie en cybersecurity.

NVD: National Vulnerability Database: Een openbare database die informatie bevat over bekende beveiligingskwetsbaarheden en hun risico's.

OS: Besturingssysteem - Software die de hardware van een computer beheert en andere softwaretoepassingen toelaat om op het apparaat te draaien.

OT: Operationele Technologie. Systemen en processen die worden gebruikt om fysieke apparaten en infrastructuur te controleren en te beheren, zoals industriële controlesystemen.

OT Data historian: Een systeem dat historische gegevens verzamelt, opslaat en analyseert van operationele technologie om trends te identificeren en operationele beslissingen te ondersteunen.

OT SMS: OT Security Management System. Een raamwerk van beleid, procedures en richtlijnen voor het beheren van OT-cyberbeveiligingsrisico's.

OT SOC: Operationele Technologie Security Operations Center. Een faciliteit die is opgezet om operationele technologieën te bewaken, te detecteren en te reageren op beveiligingsincidenten.

PCI-DSS: Payment Card Industry Data Security Standard. Een set van beveiligingsnormen die zijn opgesteld door de vijf grote creditcardmaatschappijen. Elke organisatie die kaartbetalingen accepteert, verwerkt, of waarbij de gegevens anderszins betrokken zijn, moet aan deze normen voldoen.

PDCA: Plan-Do-Check-Act. Een cyclus voor continu verbeteren.

Penetration test: Een gecontroleerde aanval op een computersysteem of netwerk om de kwetsbaarheden te identificeren en de effectiviteit van de beveiligingsmaatregelen te evalueren.

Purdue Model: Een hiërarchisch raamwerk dat wordt gebruikt om OT-architectuur te segmenteren, van fysieke processen op de laagste niveaus tot de bedrijfsnetwerken op de hoogste niveaus.

RACI: Acroniem voor een verantwoordelijkheidsmatrix: Responsible (Verantwoordelijk), Accountable (Eindverantwoordelijk), Consulted (Geraadpleegd) en Informed (Geïnformeerd).

RAMSSHEEP: Een acroniem dat wordt gebruikt om verschillen in de categorieën van cyberdreigingen te classificeren.

Ransomware: Schadelijke software die computersystemen vergrendelt of gegevens versleutelt, waarbij de aanvaller losgeld eist.

Risk appetite: De mate van risico die een organisatie bereid is te nemen bij het nastreven van haar doelstellingen.

SAT: Site Acceptance Test. Een test die wordt uitgevoerd op de locatie waar het systeem daadwerkelijk zal worden gebruikt. Controleert of het systeem correct functioneert in de specifieke operationele omgeving van de klant.

SCADA: Supervisory Control And Data Acquisition. Een systeem voor het controleren en beheren van industriële processen. Scope: De grenzen en het bereik van een project, onderzoek of activiteit.

Script kiddie: Een persoon die geautomatiseerde hulpmiddelen of scripts gebruikt om kwetsbaarheden in computersystemen uit te buiten, zonder veel kennis of vaardigheden.

Securityroadmap: Een strategisch plan dat de stappen en initiatieven beschrijft die een organisatie zal nemen om haar cyberbeveiligingsdoelstellingen te bereiken.

Segmentatie: Het opdelen van een netwerk in kleinere, geïsoleerde secties om risico's te beperken.

SLA: Service Level Agreement. Een contractuele overeenkomst tussen een dienstverlener en een klant die de kwaliteit en prestaties van de geleverde diensten definieert.

Standalone: Een systeem dat niet is verbonden met andere systemen of netwerken, en dus geïsoleerd is.

SOC: Security Operations Center. Een centrale faciliteit waar een team van beveiligingsprofessionals de IT- en OT-infrastructuur van een organisatie 24/7 bewaakt, analyseert en verdedigt tegen cyberdreigingen.

Vendor Lock-in: Een situatie waarin een organisatie zo afhankelijk wordt van één leverancier, product of technologie, dat het overstappen naar een alternatief aanzienlijke kosten, moeite of verstoringen met zich meebrengt.

Vertrouwelijkheid (BIV): De V uit de afkorting BIV. De eigenschap dat informatie niet beschikbaar wordt gesteld of wordt onthuld aan onbevoegde individuen, entiteiten of processen.

VLAN: Virtual Local Area Network. Een logisch gescheiden netwerk binnen een fysiek netwerk.

Vulnerability scan: Een geautomatiseerd proces voor het identificeren en beoordelen van kwetsbaarheden in computersystemen of -netwerken.

XDR: Extended Detection and Response. Een geïntegreerde beveiligingsoplossing die meerdere beveiligingslagen combineert om bedreigingen te detecteren, te analyseren en te beantwoorden.

Bijlage – Verwijzing naar verdere bronnen

Deze bijlage verwijst door naar andere bronnen die als aanvulling kunnen dienen bij het uitvoeren van OT -risicomanagement. Hiervoor biedt het bronnen m.b.t. informatiebeveiliging in de brede zin, en voor specifiek OT-security.

Informatiebeveiliging (IT & OT)

Doel: Basis leggen voor cybersecurity- en risicomanagement.

- **Starten met cybersecurity (Digital Trust Center)** [Webpagina]
<https://www.digitaltrustcenter.nl/starten>
Geeft een overzicht van eerste stappen en basisprincipes voor (kleinere) organisaties die cybersecurity willen implementeren.
- **CyberVeilig check voor ZZZ en MKB (Digital Trust Center)** [Vragenlijst]
<https://tools.digitaltrustcenter.nl/cyberveilig-check/>
Een snelle zelfscan om inzicht te krijgen in de huidige cyberveiligheid en verbeterpunten.
- **Risicoklassenindeling Digitale Veiligheid (Digital Trust Center)** [Vragenlijst]
<https://tools.digitaltrustcenter.nl/check-je-risicoklasse/>
Helpt organisaties hun risicoklasse te bepalen en passende maatregelen te kiezen.
- **Routekaart risicomanagement (NCSC)** [Webpagina]
<https://www.ncsc.nl/wat-kun-je-zelf-doen/routekaart-risico-management>
Biedt een gestructureerde aanpak voor risicomanagement, inclusief stappen en hulpmiddelen.
- **Hoe maak je een beleidsplan Risicoanalyse? (Digital Trust Center)** [Webpagina]
<https://www.digitaltrustcenter.nl/nis2/hoe-maak-je-een-beleidsplan-risicoanalyse>
Praktische handleiding voor het opstellen van een beleidsplan voor het uitvoeren van risicoanalyses volgens NIS2.

Beveiligen van OT

Doel: Specifieke maatregelen en richtlijnen voor Operational Technology (OT) en industriële automatiseringssystemen (IACS).

- **Operational Technology (Digital Trust Center)** [Webpagina]
<https://www.digitaltrustcenter.nl/operational-technology>
Introductie over OT en de specifieke cybersecurity-uitdagingen die daarbij horen.

- **Security Check Procesautomatisering (Digital Trust Center)** [Vragenlijst]
<https://tools.digitaltrustcenter.nl/security-check-procesautomatisering/>
Zelftest om de beveiliging van procesautomatisering te beoordelen.
- **Aan de slag met het beveiligen van OT/IACS (NCSC)** [Publicatie]
<https://www.ncsc.nl/documenten/publicaties/2025/januari/28/aan-de-slag-met-het-beveiligen-van-ot-iacs>
Praktische stappen en best practices voor het beveiligen van OT/IACS-omgevingen.
- **Basismaatregelen voor cybersecurity van IACS (NCSC)** [Publicatie]
<https://www.ncsc.nl/documenten/publicaties/2022-oktober/10/basismaatregelen-voor-cybersecurity-van-iacs>
Fundamentele beveiligingsmaatregelen voor industriële automatiseringssystemen. Ook wel bekend onder de afkorting BIACS.
- **Handleiding procesautomatisering PA-beleid (IBD)** [Handleiding]
<https://www.informatiebeveiligingsdienst.nl/product/handleiding-procesautomatisering-pa-beleid/>
Richtlijnen voor het opstellen van beleid rond procesautomatisering en OT-beveiliging.
- **Partnerpublicaties en internationale richtlijnen (NCSC UK)** [Blogs & Whitepapers]
Internationale best practices en ontwerpprincipes voor OT-beveiliging en governance.
 - <https://www.ncsc.gov.uk/collection/cyber-security-design-principles/examples/study-operational-tech>
 - <https://www.ncsc.gov.uk/blog-post/cni-system-design-secure-remote-access>
 - <https://www.ncsc.gov.uk/blog-post/protect-your-management-interfaces>
 - <https://www.ncsc.gov.uk/blog-post/cyber-security-toolkit-for-boards-updated-briefing-pack-released>
 - <https://www.ncsc.gov.uk/blog-post/introducing-new-paws-principles>
 - https://www.ncsc.gov.uk/whitepaper/security-architecture-anti-patterns#section_5

Deze brochure is een uitgave van:

Ministerie van Infrastructuur en Waterstaat
Postbus 20901 | 2500 EX Den Haag

Ontwerp: Tappan

December 2025