Ministerie van Infrastructuur
en Waterstaat

Handreiking Risicobeheer in OT

Sectoren Luchtvaart & Maritiem

TLP: white

Programma
Versterken Cyberweerbaarheid in de Luchtvaart- en Maritieme sector

Colofon

Uitgegeven door:
Programma Versterken Cyberweerbaarheid in de Luchtvaart- en Maritieme sector, Ministerie van Infrastructuur en Waterstaat

Opgesteld door:
F. Ruedisueli, Principal OT Security Consultant, Secura
T. Jansen, OT Security Consultant, Secura

Met medewerking van:
A. van Herk, Senior Business Development Manager, Kotug International
E. Pit, Information Security Manager Operational Technology, Van Oord
M. Luchs, CISO & Digital Development Manager, Anthony Veder
B. van Altena, Chief Information Security Officer, CISO voor KLM
T. Huisman, Deputy Chief Information Security Officer, Air France KLM

Samenvatting

In 2023 is het ministerie van Infrastructuur en Waterstaat gestart met het programma om de cyberweerbaarheid in de luchtvaart en maritieme sector te versterken. Door de groeiende afhankelijkheid van digitale systemen en technologieën is het essentieel om systemen en data te beschermen tegen cyberdreigingen.

Cybersecurity-incidenten kunnen leiden tot serieuze impact op de bedrijfsprocessen en resulteren in financiële schade of invloed hebben op de reputatie. Specifiek in OT, zowel in de sector maritiem als luchtvaart, kan de impact verdere gevolgen hebben op persoonlijke veiligheid, milieu en de omgeving. Het is daarom van belang dat cybersecurityrisicomanagement als integraal onderdeel binnen de organisatie een plek krijgt, met sturing vanaf het directieniveau.

Wet- en regelgeving gericht op het (internationaal) verbeteren van cybersecurityweerbaarheid zal steeds veeleisender worden. Een goed voorbeeld hiervan is de recentelijk uitgebrachte NIS2, waarbij niet alleen de organisatie in beeld is, maar ook de leveranciersketen en de positie van de sector in de maatschappij. Naast NIS2 is er ook steeds meer sectorspecifieke regelgeving. Deze heeft met name impact op nieuwe objecten. Tegelijkertijd is onderkend dat er nog een flinke uitdaging ligt bij de bestaande vloot en installaties, die een lange levensduur hebben. Tegelijkertijd is er wel meer vraag naar connectiviteit, zoals toegang op afstand, en verandert het dreigingslandschap voortdurend. Hierdoor nemen cybersecurityrisico's alleen maar toe. Niets doen en afwachten is dus geen optie.

Deze handreiking beschrijft alle stappen voor risicobeheer in OT om cybersecurityrisico's te identificeren en vervolgens te mitigeren naar een acceptabel niveau. Afhankelijk van de huidige stand van zaken en het volwassenheidsniveau van de organisatie is hier meer of minder nodig. Vanaf nul een volledig programma opzetten, inclusief alle vereisten zoals beschreven in internationale standaarden, wordt vaak als een onoverkomelijke hoeveelheid werk gezien: iets dat haast onmogelijk lijkt. Om hierbij te helpen, zijn in deze handreiking ook pragmatische opties beschreven om het laagdrempeliger te maken om te starten met risicobeheer. Het belangrijkste is om een start te maken en een plan te ontwikkelen hoe stap voor stap het programma ingericht kan worden, zodat het voldoende aansluit bij het risicoprofiel van de organisatie.

Tot slot is het beheren van cybersecurityrisico's een continu verbeterproces. Overgebleven risico's, geaccepteerde risico's en veranderingen binnen de organisatie of systemen moeten regelmatig worden heroverwogen. Daarnaast is het ook belangrijk dat alle genomen beveiligingsmaatregelen, zowel technisch als organisatorisch, worden getest om zeker te weten dat ze het risico op een juiste manier reduceren. Dit geeft het belang aan dat het risicobeheerproces, inclusief een PDCA-cyclus, een onderdeel moet zijn van de bedrijfsstrategie, gedragen en gestuurd door het management.

Deze handreiking "Risicobeheer in OT" voor de sectoren luchtvaart en maritiem is een product van samenwerking tussen het ministerie, onafhankelijke securityexperts, en participanten uit de desbetreffende sectoren. Het document is specifiek gericht op beheersing van cybersecurityrisico's in OT, en is hiermee onderdeel van de bredere praktijk van risicobeheersing.

Inhoudsopgave

Inleiding

In maart 2023 is het ministerie van Infrastructuur en Waterstaat (IenW) gestart met het programma om de cyberweerbaarheid in de luchtvaart- en maritieme sector te versterken. Door de groeiende afhankelijkheid van digitale systemen en technologieën is het essentieel om systemen en data te beschermen tegen cyberdreigingen.

Binnen het programma werkt het ministerie van IenW samen met stakeholders, experts en organisaties uit de luchtvaart- en maritieme sector om de kennis en aandacht over cyberdreigingen te bevorderen. Ook voorzien zij in trainingen en ondersteuning, en stimuleren het delen van "best practices" om de digitale weerbaarheid van de sectoren te versterken.

Deze Handreiking Risicobeheer in OT voor de sectoren luchtvaart en maritiem is een product van samenwerking tussen het ministerie, onafhankelijke securityexperts, en participanten uit de desbetreffende sectoren. 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 in bedrijf 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. Risicomanagement, zoals bovenstaand, omvat het hele bedrijf 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 voor veel sectoren en bedrijven geen gemakkelijke opgave is. Het credo luidt in dit geval ook "begin klein, begin 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 eigen bedrijf en proces/product, maar ook maatschappij en economie: continue verbetering van digitale weerbaarheid in onze belangrijke sectoren is iets waar we als ministerie van Infrastructuur en Waterstaat achter staan, en waar we u praktisch in bij willen staan door middel van deze handreiking.

1. Nut en noodzaak van cybersecurityrisicoanalyses in OT

Operationele Technologie, ofwel OT (o.a. ICS/IACS/SCADA[1]), duidt in de breedte op systemen en netwerken die fysieke processen en objecten controleren. Deze systemen zijn oorspronkelijk ontworpen en gebouwd als geïsoleerde netwerken met bepaalde technische principes, om technische risico's te beheersen en de (fysieke) veiligheid, efficiëntie en betrouwbaarheid van de fysieke processen te beschermen. Risicobeheersing van cybersecurity op OT-systemen is wegens bovenstaande redenen voor een lange tijd (gedeeltelijk) buiten scope gebleven. Tegenwoordig zijn veel van deze OT-objecten en OT-netwerken verbonden met (of zullen in de toekomst verbonden worden met) computernetwerken, die op hun beurt weer verbonden zijn met internet. Het grote verschil met IT-systemen, en daarmee de bijbehorende risico's, is dat OT-systemen een fysieke impact om de omgeving of persoonlijke veiligheid kunnen hebben. Een verstoring werkt meestal direct door op de primaire bedrijfsprocessen van de betreffende organisatie.

Hieruit volgt het nut en de noodzaak van cyberrisicobeheersing binnen de OT-omgeving: de groeiende connectiviteit van OT en het snel veranderende cyberdreigingslandschap vormt een reëel risico voor behoud van werking van kritieke systemen, fysieke en zelfs publieke veiligheid. In de toekomst zullen IT, OT en IoT veel vaker geïntegreerd zijn en meer gemanaged vanuit één centrale verantwoordelijkheid. Daardoor ontstaan de volgende uitdagingen. Welke OT draait er waar? Kan deze gekoppeld worden aan de IT-infrastructuur, en hoe? Hoe liggen de verantwoordelijkheden binnen de organisatie?

Verder kan het upgraden of migreren van systemen uitdagingen met zich meebrengen in verouderde OT-systemen. De kennis en kunde van het inbreken op OT-installaties neemt harder toe dan de kennis van installaties en mogelijkheden tot het stoppen van deze aanvallen.

Hierbij speelt ook de toeleveringsketen een rol: leveranciers van (delen van) objecten en systemen hebben rechtstreeks toegang tot hun apparatuur op afstand om bijvoorbeeld updates uit te voeren of onderhoud te verrichten. Netwerken kunnen samenstellingen zijn van verschillende objecten geleverd door verschillende leveranciers, wat het overzicht vertroebelt en waarvan de veiligheid niet altijd direct inzichtelijk is. Het is daarom cruciaal voor organisaties om hun OT-infrastructuren goed te beveiligen en zich bewust te zijn van de voortdurend evoluerende dreigingen in deze complexe omgevingen.

Verder zijn, met de groeiende vraag naar data in verschillende sectoren, OT-gegevens waardevoller geworden voor zowel bedrijven als cybercriminelen. Deze gegevens kunnen worden gebruikt voor concurrentievoordeel of, in het geval van een aanval, gegijzeld worden in ruil voor losgeld.

Casestudy betreffende nut en noodzaak van cybersecurityrisicoanalyse in OT: Luchtvaartsector

De Engineering & Maintenance divisie van een luchtvaartbedrijf maakt gebruik van Operationele Technologie (OT) voor het beheren van industriële machines die noodzakelijk 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 het SAP-bedrijfsvoeringsysteem 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 inbelverbindingen 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. Her-certificatie moet worden geïntegreerd in het ontwerp van OT-systemen en worden opgenomen in de verantwoordelijkheid van leveranciers.

[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.

Deze case benadrukt de complexiteit van het beheren van OT-cyberrisico'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.

1.1 Wet- en regelgeving

Cybersecuritywetgeving en -regulering speelt een steeds crucialere rol in het beschermen van IT- (informatietechnologie) en OT-(operationele technologie)netwerken. 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. 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 risicogebaseerde aanpak enerzijds en een sturende wet- en regelgeving op het gebied van cybersecurity anderzijds, wordt er gestuurd op een optimaal klimaat van IT- en OT-bescherming en -weerbaarheid.

Voorbeelden van voorschriften en wetgeving zijn:
Maritiem:

- Classificatiebureau notaties en Lloyds, DNV en BV
- 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
- ISPS: 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)

1.2 Uitdagingen van OT-cybersecurity en risicobeheersing

Ondanks dat wetgeving veelal spreekt van 'bescherming tegen cyberdreigingen' in het algemeen, heeft risicobeheer van IT en OT zich in de praktijk afzonderlijk ontwikkeld. Logisch, aangezien beide gebieden kampen met verschillende risico- en beveiligingsuitdagingen. In tegenstelling tot cybersecurityrisico's op IT-systemen, die vaak uitsluitend economische of financiële consequenties hebben in navolging van het compromitteren van gegevens, gegevensdiefstal of financieel verlies, kunnen OT-cybersecurityincidenten verregaande (fysieke) gevolgen hebben voor mensen, installaties en omgeving/milieu.

Dit verschil toont zich ook in beheer van netwerken en objecten: waar IT-systemen regelmatig bijgewerkt kunnen worden in functionaliteit en beveiliging, kan elke verandering in een OT-netwerk mogelijk de automatisering verstoren en productie schaden. Het aanpassen van antivirusbescherming, installeren van beveiligingsupdates of het OS-systeem upgraden is in een OT-omgeving een afgewogen keuze, geen gegeven. Vaak kampen OT-omgevingen met (tenminste enkele van) de volgende beperkende technische factoren:

- Verouderde systemen met matige (tot geen) beveiliging en/of systemen die moderne beveiligingsmaatregelen niet ondersteunen. Dit wordt mede veroorzaakt door de lange levenscyclus van OT-systemen (15-20 jaar zijn geen uitzondering)
- Systemen, netwerken en applicaties met een zwakke beveiliging. (Soms aangegeven als "insecure by design".)
- Systemen met technische afhankelijkheden van andere systemen. Vervangen is daardoor vaak een kostbare aangelegenheid.
- Hoge beschikbaarheidseisen waardoor onderhoud slecht of niet te plannen is.
- Toenemende (inter)connectiviteit met IT-/IoT-/cloudapplicaties en remote access oplossingen. Denk hierbij bijvoorbeeld ook aan afhankelijkheid van leveranciers en beperkt inzicht in beveiliging van objecten of applicaties door (beheer door) verschillende partijen.
- Beveiligingbeheersprocessen zijn niet/slecht te automatiseren waardoor het volwassenheidsniveau vaak achterblijft.
- Afhankelijkheden van een leverancier, onderhoudscontracten, garantie of certificering. Hierdoor zijn aanpassingen die cybersecurity zouden kunnen verbeteren niet altijd mogelijk.

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: Veel OT-systemen in de luchtvaart zijn gecertificeerd voor 'die specifieke versie/status'. Op het moment dat er een software-update heeft plaatsgevonden, vervalt de certificering en dient deze hernieuwd te worden voor de 'nieuwe' staat. Deze certificeringen zijn vaak duur en hebben impact op productie. Dit proces van certificeren en hercertificeren vormt op dit moment een additionele complicerende factor, en is een van de redenen waarom de IT-software van OT-systemen vaak verouderd is.

OT-netwerken zijn complexe omgevingen, en voor beheer is diepgaande kennis van zowel technische aspecten als operationele gevolgen een vereiste. De bovenstaande opsomming maakt duidelijk dat niet alle standaard of generieke oplossingen mogelijk zijn. OT-risicomanagement moet specifiek afgestemd worden op deze unieke technische omgeving.

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.

1.3 Noodzaak van een proportionele aanpak

Risicomanagement in OT-omgevingen is onmisbaar voor het beschermen van de kernwaarden van een organisatie. Risicobeheersing in de praktijk, op kritische bedrijfsprocessen en vitale systemen, vraagt veelal om een iteratieve en proportionele aanpak. Bestaande OT-netwerken zijn complexe omgevingen waaraan veel onderliggende connecties, verschillende systemen, en een legio aan processen ten grondslag liggen. Nieuwe systemen zijn gemakkelijker af te stemmen op (wettelijke) verplichtingen en moderne richtlijnen dan bestaande omgevingen. Met name de uitdagingen genoemd in paragraaf 1.2 vormen de basis voor een proportionele benadering. Kortom: de meest kritieke systemen verdienen de meeste aandacht.

Belangrijk is om constant te blijven beseffen dat het doel van risicomanagement is om risico's inzichtelijk en beheersbaar te maken, en dat risicogestuurd denken en werken de boventoon voert.

- Door een holistisch beeld van cybersecurityrisico en cyberweerbaarheid van een organisatie te schetsen, is hoger management in staat om strategische beslissingen te nemen over investeringen in eigen cybersecurity. Hiermee kunnen organisaties effectiever hun budgetten toewijzen door prioriteiten te stellen op basis van potentiële impact op bedrijfscontinuïteit en -doelstellingen. Dit leidt tot effectiever gebruik van middelen en uiteindelijk een hogere cyberweerbaarheid.
- Verder helpt gedegen OT-risicomanagement bij naleving van regels en standaarden op het gebied van cybersecurity. Het identificeert gebieden die niet voldoen aan vereisten en stelt organisaties in staat om risico's te verminderen en naleving te verbeteren.

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

Tenslotte zijn de beveiligingsrisico's die verband houden met OT-systemen slechts onderdeel van de vele componenten waar de organisatie mee te maken krijgt bij overkoepelende verantwoordelijkheid op het gebied van risicobeheer. Vanuit de organisatie blijft het dus belangrijk om de OT-cybersecurityrisico's in het juiste perspectief te plaatsen.

1.4 Voorwaarden voor risicomanagement

Het initiëren van een risicobeheersproces, zoals beschreven in de hoofdstukken van deze handreiking, gaat uit van een aantal belangrijke aannames en processen die idealiter al geïmplementeerd zijn in de betreffende organisatie. Deze voorwaarden zijn generiek voor alle andere vormen van risicomanagement.

Omdat cybersecurity niet enkel een technisch vraagstuk is, maar een integraal onderdeel van de bedrijfsvoering en de strategische planning, is betrokkenheid van het management bij OT-cybersecurity en OT-risicobeheer van groot belang.

Deze voorwaarden vallen buiten de scope van deze handreiking maar zijn wel fundamenteel aan een succesvolle uitvoering, bijvoorbeeld:

- Het verzekeren dat het management het belang van het beheersen van OT-cyberbeveiligingsrisico's onderkennen en vervolgens passende bestuursstructuren en strategieën opzetten om dergelijke risico's te beheersen.
- Dat rollen en verantwoordelijkheden zijn beschreven en belegd zijn bij de juiste personen in de organisatie. Ook is het eigenaarschap van risicobeheer vastgelegd voor alle assets, objecten en processen.
- Dat er vanuit de organisatie een risicotolerantieniveau is vastgesteld en dat er formele processen zijn belegd voor het accepteren van risico's.
- Dat er het juiste mandaat is en dat er voldoende middelen aanwezig zijn om deze processen te waarborgen.

Casestudy voorwaarden voor risicomanagement: Luchtvaart

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, niet beveiligd zijn en niet kunnen worden beveiligd met (moderne) beveiligingstools zoals AV/EDR/etcetera, 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 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.

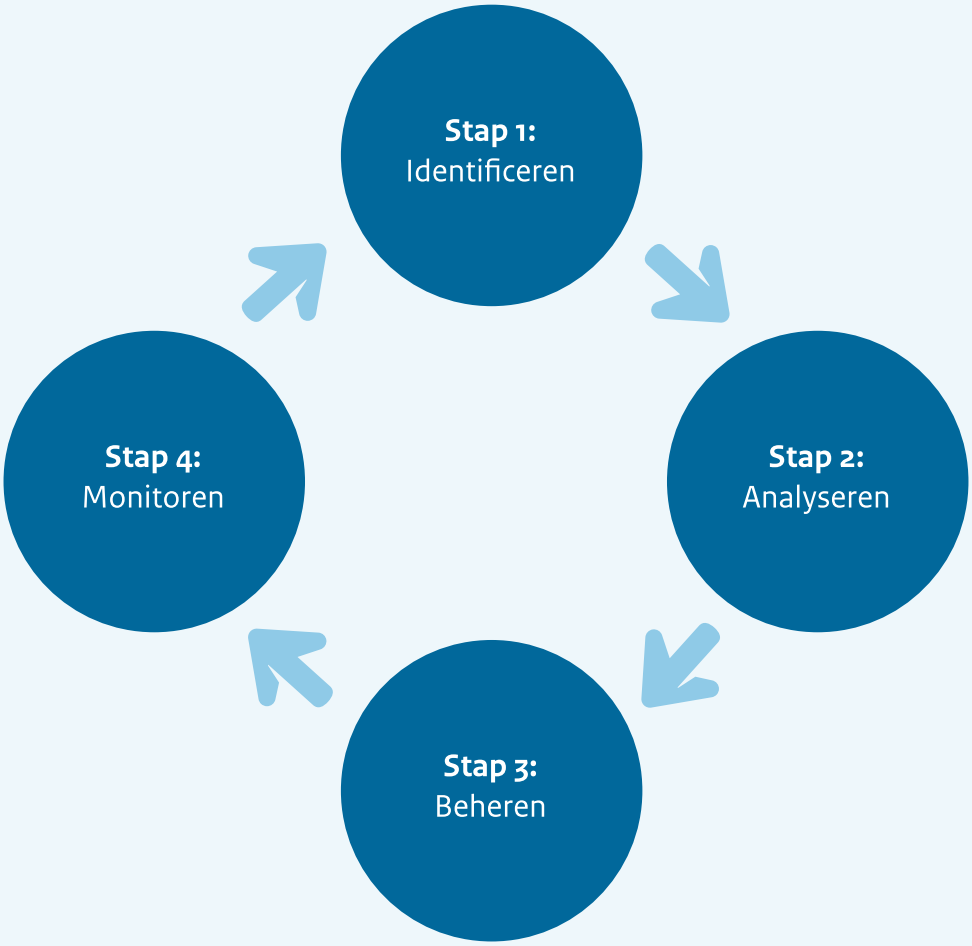
1.5 Risicoanalyse en methodiek

Het kernprincipe voor het beoordelen van cybersecurityrisico's is het bepalen van de kans dat een bepaalde dreiging gebruikmaakt van een zwakheid en het bijbehorende effect gerealiseerd wordt. Hiervoor wordt gebruikgemaakt van de bekende risicoformule, waarbij risico gelijk is aan de kans vermenigvuldigd met het effect: **risico = kans x effect**.

Deze formule biedt een gestructureerde, risicogebaseerde benadering om potentiële dreigingen te evalueren en de mogelijke gevolgen ervan te begrijpen en kaderen binnen organisaties. Hoewel deze formule voor zich lijkt te spreken, blijkt het vaststellen van zowel kans op- als impact van een beveiligingsincident in OT-omgevingen bijzonder uitdagend. Verder ligt aan elk element in de formule een complexere werkelijkheid ten grondslag. Hier wordt in de volgende hoofstukken dieper op ingegaan.

Er bestaan verschillende internationale standaarden en guidelines voor het uitvoeren van cybersecurityrisicoanalyses, zoals bijvoorbeeld ISO27005 en NIST SP800-30, en specifiek voor OT, bijvoorbeeld de IEC62443-3-2. In principe is elke methode prima te gebruiken en kan elke organisatie een eigen keuze maken. Uiteindelijk komen alle methoden ongeveer overeen en beschrijven het identificeren van dreigingen, het analyseren van de bijbehorende risico's, het implementeren van maatregelen om deze dreigingen te neutraliseren en het totale risicobeheersproces.

Deze handreiking zal de onderstaande algemene aanpak volgen en is opgesplitst in vier stappen, 'identificeren', 'analyseren', 'beheren' en 'monitoren', die elk per hoofdstuk beschreven worden.



2. Identificeren

De eerste stap is het inzichtelijk krijgen hoe de systemen uit het OT-landschap bijdragen aan de bedrijfsprocessen en te bepalen wat het ergst mogelijke effect zou kunnen zijn. Om hiermee te beginnen is het belangrijk om vast te stellen wat de belangrijkste objecten, bedrijfsprocessen of onderdelen zijn. Met andere woorden: wat zijn de zogenaamde 'kroonjuwelen' binnen de organisatie. Deze kunnen zich verspreid door de organisatie bevinden, in verschillende businessunits, met verschillende eigenaren/verantwoordelijke partijen. Kroonjuwelen kunnen duiden op zowel tastbare als ontastbare assets: fysieke apparaten, logische netwerken en intellectueel eigendom of personeel kunnen alleen deel uitmaken van deze definitie. Uiteindelijk bepaalt het belang de juiste prioritering en verantwoordt het belang het aantal te nemen maatregelen. Een kritiek document om gedegen uitvoering van de stappen van zowel hoofdstuk 2 (Identificeren) als hoofdstuk 3 (Analyseren) te verzekeren, is een compleet en bijgewerkt OT-assetoverzicht.

Bij kroonjuwelen kan gedacht worden aan navigatiesystemen, communicatienetwerken of lading- en voorraadbeheersystemen. Schepen zijn bijzonder afhankelijk van GPS, elektronische kaartweergave en informatiesystemen (ECDIS) of automatische identificatiesystemen (AIS), maar bijvoorbeeld ook van satellietcommunicatie, on-board wifi en andere communicatiesystemen voor diverse on- en offshoreoperaties. Afhankelijk van het doel van het schip kunnen systemen als baggerpompen of gasinstallaties ook onder deze definitie vallen. Verder zijn veel systemen tegenwoordig (noodgedwongen) op afstand toegankelijk en te monitoren door derde partijen.

Een vliegtuig is ook te definiëren als een OT-systeem. Moderne vliegtuigen zijn meer en meer verbonden met externe systemen op de grond. Hierdoor zijn zij mogelijk te beïnvloeden. Dit brengt cyberrisico's met zich mee. Daarom worden systemen voor de vlucht (bijvoorbeeld de tablets die gebruikt worden door piloten) strikt gescheiden van systemen die gebruikt worden door de crew en systemen die bedoeld zijn voor passagiers, zoals on-board wifi en entertainmentsystemen. Op deze manier kan een entertainmentsysteem de vluchtsystemen niet beïnvloeden. Ook voor onderhoud aan vliegtuigen is het essentieel om goede monitoring (aanbrengen van noodzakelijke wijzigingen) en zeer strikte toegangsautorisatie te gebruiken.

Zowel in de luchtvaart als in de maritieme sector is een allesomvattende aanpak, inclusief robuuste netwerkbeveiliging, software-updates, training van medewerkers en een best practice aanpak van belang. 'Allesomvattend' duidt hierbij ook op de aanwezigheid van een compleet OT-assetoverzicht: om te beschermen wat je hebt moet je gewaar zijn van wat je bezit. Vaak ontbreken er overzichten van IT/OT-assets die voorheen standalone waren, of verbindingen tussen netwerken die los van elkaar ontstaan zijn maar gedurende de tijd met elkaar verstrengeld zijn geraakt.

2.1 Kaderen van risico's binnen de organisatie

De strategie van een organisatie voor cybersecurityrisicobeheer richt zich op het beoordelen, reageren (mitigeren, ontwijken, overdragen, accepteren) en monitoren van risico's specifiek verbonden aan OT-systemen binnen de organisatie. Deze strategie benoemt uitdrukkelijk de aannames, beperkingen, risicotolerantie, en prioriteiten die een rol spelen bij investerings- en operationele beslissingen. Bij het opstellen van een strategie voor cybersecurityrisicobeheer vormen kans (likelihood) en effect (impact) de assen van de matrix.

Vaak zijn risicomatrices 3x3 of 4x4, en worden de risico's geplot op de assen als risicocategorieën: laag risico (lage kans, weinig effect), matig risico (gemiddelde kans en effect), en hoog risico (hoge kans en effect). In dit hoofdstuk zal effect behandeld worden, terwijl 'kans' later aan bod zal komen, in hoofdstuk 3. Binnen een organisatie bestaat vaak al een risicomatrix. Van belang is om na te gaan of die ook geschikt is voor de OT-risico's of om te overwegen of er een OT-specifieke versie nodig is. Met andere woorden: zijn de risico's binnen de OT-omgeving dusdanig correct vertegenwoordigd en in kaart gebracht dat een aparte matrix niet nodig is?

Verder zal de risicobereidheid/tolerantie (risk appetite) van een organisatie gekoppeld moeten worden aan de matrix. Risicobereidheid betekent de hoeveelheid risico die een organisatie bereid is te accepteren bij het nastreven van haar doelen. Sommige risico's kunnen geaccepteerd worden, andere zullen degelijk verantwoord moeten worden, en weer andere zullen ontoelaatbaar zijn. Het bepaalt grenzen voor het nemen van risico' s en helpt bij het vaststellen van prioriteiten bij het beheersen van risico's. Bestuur of hoger management bepaalt de

risicobereidheid, en vertaalt dit naar specifieke richtlijnen voor risicobeheer (zie omschreven voorwaarden in paragraaf 1.4). Deze richtlijnen beïnvloeden vervolgens de besluitvorming bij het bepalen welke risico' s moeten worden aangepakt, welke worden geaccepteerd en welke 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 bij een passende cybersecuritystrategie 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 'statelijke actoren'), interne dreigingen (van apparaat-/systeemfalen tot ontevreden medewerkers), maar ook bijvoorbeeld wettelijke verplichtingen en regelgevingen (NIS2, AVG, sectorspecifieke wetgeving). Hierbij is wederom een top-downaanpak vereist bij beslissen over bescherming van belangrijke zaken en de uitleg waarom dit nodig is. Het is noodzakelijk om te bepalen welke risico's de organisatie wil accepteren en waarom, en welke absoluut niet. Voor veel organisaties is tot een gedetailleerde risicoanalyse en -prioritering komen een flinke opgave. Veelal wordt er daarom (noodgedwongen) een iteratieve aanpak geadopteerd. Een doordachte, gestructureerde scopebepaling is van belang om risicoanalyse behapbaar te houden en zo optimaal mogelijk beschikbaar budget, kennis en middelen in te zetten.

Voorbeelden van belangrijke overwegingen:
Zijn alle specifieke effectcategorieën vertegenwoordigd in de risicomatrix en volgen deze een gelijke schalering ten opzichte van andere risico's? Zijn voor "kans" specifieke schalen gemaakt die passen bij moedwillige OT-aanvallen? (Zie hoofdstuk 3 voor meer verdieping.)De vastgestelde risicobereidheid kan van een risicomatrix gebruikmaken. Lage risico's (groen) worden geaccepteerd (dit is dus de formeel geaccepteerde risicotolerantie), middenrisico's (oranje) moeten een verplicht 'pas-toe-of-leg-uitbeleid' volgen en hoge risico's (rood) zijn altijd onacceptabel *en **moeten** dus gemitigeerd worden*.

2.2 Vaststellen van de scope

Bij het vaststellen van de risicobeoordelingsscope zijn verschillende factoren van belang. Afhankelijk van de organisatie, kan de scope één groot object of juist meerdere (evt. kleinere) objecten, assets of bedrijfsonderdelen omvatten waar OT-cyberdreigingen relevant zijn. Belangrijk is daarom om van tevoren vast te stellen om welke genoemde variant het gaat.

Bij één groot object is de vraag of het logischer is om het object in het geheel te bekijken, of dat het logischer is om de omgeving op te delen in kleinere stukken met verschillende risicoprofielen. De mate van granulariteit moet van tevoren worden vastgesteld. Uiteindelijk kan dit leiden tot het toepassen van de "zone and conduit" benadering zoals beschreven in de IEC 62443.

Bij meerdere losse objecten is het van belang te bepalen of deze werkelijk losstaand zijn of dat er afhankelijkheden zijn, zowel direct (zoals netwerkkoppelingen) als indirect (waarbij een object afhankelijk is van bedrijfsprocessen geleverd door een ander object). Het is essentieel om deze factoren mee te nemen in de beschouwing van individuele objecten.

Na het bepalen van object(en), is het belangrijk om de plaatsing (zowel fysiek als in het OT-netwerk) van objecten te bepalen. Is het bijvoorbeeld duidelijk of alle objecten binnen het mandaat van de eigen organisatie of afdeling vallen? Zijn er objecten in het buitenland of joint ventures die buiten de scope vallen? Is er een duidelijke scheiding tussen IT- en OT-componenten binnen dit object? Zijn er externe afhankelijkheden (systemen, diensten) die buiten de OT-riskassessmentscope vallen (bijvoorbeeld IT- of clouddiensten, leveranciers of partners)?

Tot slot is het van belang om duidelijk af te spreken welke typen dreigingen binnen de scope van de OT-risicoanalyse vallen. Een aantal voorbeelden, maar zeker geen compleet overzicht, volgt hieronder:

- Aanvallende (vijandige) actoren, zoals cybercriminelen, maar ook insiders: iedereen die moedwillig acties uitvoert. Dit ligt het meest voor de hand om te includeren.
- Accidenteel (incidenteel): incidenten die 'per ongeluk' gebeuren, soms door onkunde of onoplettendheid. Deze incidenten maken ook vaak onderdeel uit van de dreigingsscope.
- Structureel (objecten/elementen): incidenten en interne afhankelijkheden. Denk hierbij aan koeling of interne stroomvoorziening. Deze categorie includeert ook falen van de software en hardware van systemen en apparaten, door bijvoorbeeld veroudering, afwezigheid van vervangende materialen, et cetera.
- Omgeving (ecologisch/maatschappelijk): externe omgevingsfactoren buiten invloed van een organisatie, zoals natuurrampen of beslissingen van energiemaatschappijen.

Casestudy een ongeluk zit in een klein systeem: Maritieme sector

In een experiment geleid door professor Todd Humphreys en zijn studenten van de Cockrell School of Engineering aan de Universiteit van Texas, is een jacht ter waarde van $80 miljoen succesvol van koers veranderd met behulp van een aangepast GPS-apparaat. Het experiment vond plaats in de Middellandse Zee en 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 voor de maritieme sector door het gebruik van spoofing. Met 90% van het wereldwijde vrachtvervoer over zeeën en een groot deel van het personenvervoer door de lucht, is het begrijpen van de bredere implicaties van GPS-spoofing essentieel.

Jamming/GPS-spoofing kan ernstige gevolgen hebben voor de automatische navigatiesystemen aan boord van een vaartuig. 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. Het niet nauwkeurig kunnen bepalen van de positie van het schip kan leiden tot ernstige ongelukken met mogelijk verlies van mensenlevens en milieuschade.

Hoewel er nog geen technologie is ontwikkeld om spoofing te voorkomen, benadrukken experts het belang van menselijke interventie om inconsistenties in navigatiesystemen te detecteren en te corrigeren.

2.3 Effectanalyse

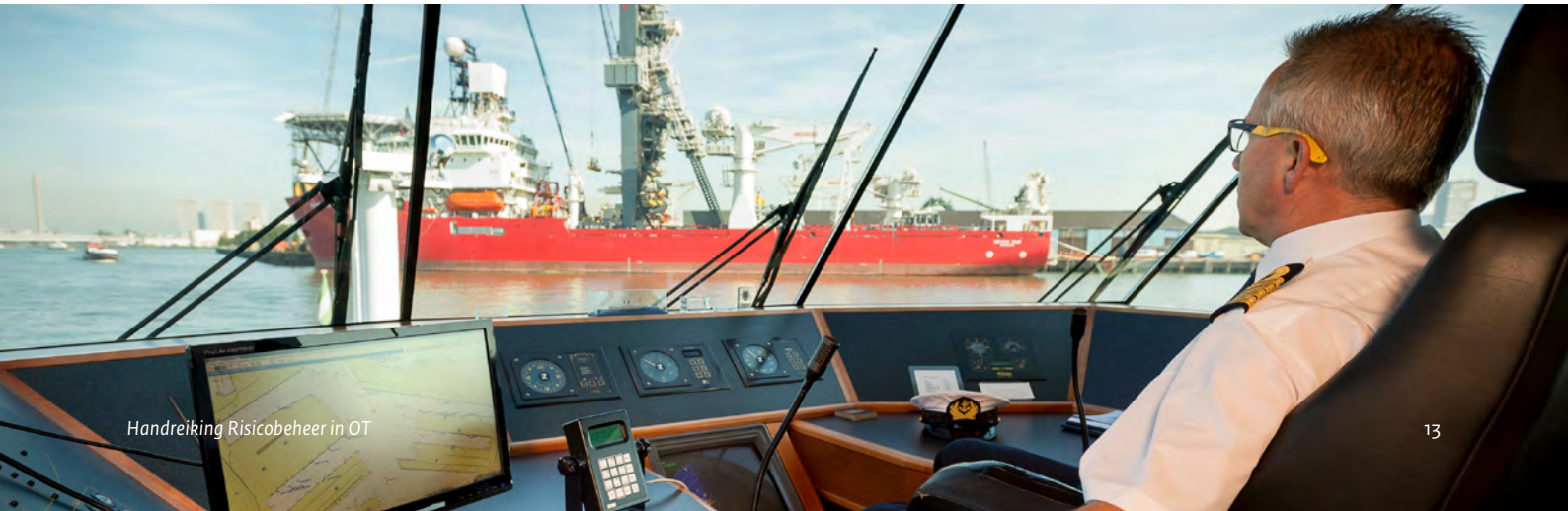
Na het bepalen van de scope volgt een worst-case impactanalyse: wat is het ergste dat er met dit object (of deel van het object) door een cyberincident kan gebeuren? Het element van kans wordt hier bewust achterwege gelaten: de impact beschrijft het mogelijke effect dat door het object veroorzaakt kan worden, ongeacht de oorzaak. Deze worst-case impactanalyse zal door dit document aangeduid worden als ‘effectanalyse’, en ‘impact’ als ‘effect’.

Voorbeelden:

- **Businessimpact:** Als uw OT-middelen falen, wat gaat er dan nog meer mis? Kan uw bedrijf doorgaan?
- **Veiligheid:** Als uw OT-middelen falen, wat gebeurt er dan met de veiligheid van uw processen?
- **Milieu/maatschappij:** Als uw OT-middelen falen, wat is dan de impact voor mens en milieu?

Een effectanalyse helpt bij het identificeren van de meest cruciale onderdelen of objecten binnen een organisatie. Zo wordt ook vaak gesproken van een Business Impact Analyse (BIA). Een BIA kijkt naar de gevolgen van gebeurtenissen op bedrijfsprocessen, waarbij wordt vastgesteld welke impact incidenten hebben op de operationele activiteiten, financiën en reputatie van een organisatie. Dit helpt bij het identificeren van vitale bedrijfsonderdelen en -processen en het begrijpen van afhankelijkheden tussen verschillende elementen binnen een organisatie.

In OT-omgevingen heeft een beveiligingsincident vaak directe gevolgen voor de meest essentiële bedrijfsprocessen. Het volledige effect is echter vaak moeilijk vast te stellen vanwege de directe fysieke consequenties die kunnen optreden. Tegelijkertijd kunnen er fysieke beveiligingen aanwezig zijn die niet door cyberaanvallen kunnen worden beïnvloed, maar wel moeten worden overwogen.



Effectcategorieën

Een cyberincident in OT kan, zoals al eerder genoemd, verder gaan dan alleen financiële schade of effect hebben op beschikbaarheid, integriteit of vertrouwelijkheid. Zowel directe als indirecte effecten kunnen leiden tot verstoring van vitale systemen, productieverlies, veiligheidsrisico's en zelfs milieuproblemen. De maximale impact wordt bepaald door de gehele infrastructuur en eventuele onderlinge afhankelijkheden.

Om deze impact te duiden, is het dus van belang om het worst-case effect van alle relevante impactcategorieën te analyseren. Vanuit IT wordt vaak alleen naar de categorieën beschikbaarheid, integriteit of vertrouwelijkheid (BIV) gekeken. Voor OT kan dit ook gebruikt worden, maar meestal is dit niet voldoende: er zijn meer impactcategorieën van toepassing, zoals Reliability, Availability, Maintainability, Safety, Health, Environment, Economy, Politics, vaak afgekort als RAMSHEEP.

Zorg voor een consistente schaal voor het beoordelen van de impact, zoals een schaal van 0 tot 5 of een omschrijvend label, passend bij de situatie. Het documenteren van alle aannames tijdens deze analyse is van vitaal belang. Dit omvat aannames over beschikbaarheid, veiligheid, en milieu-impact, en biedt een solide basis voor verdere risicoanalyse en besluitvorming.

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.
Vertrouwelijkheid (reliability)	Draait vooral om het lekken van persoonlijke gegevens of OT-gerelateerde data. Hoewel dit minder vaak voorkomt in OT, mag het niet genegeerd worden, omdat het toch impact kan hebben. Broncode, leveranciersgegevens of inloggegevens van apparaten/objecten zijn doelwitten voor aanvallers om te verkopen en toegang te verschaffen in het netwerk.
Beschikbaarheid (availability)	Het is van groot 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. Deze overwegingen en maatregelen zijn essentieel voor een effectieve respons op incidenten en het behoud van operationele continuïteit, zowel op zee als in de lucht.
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.
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 bijv. 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.Het is verstandig om de gebruikte categorisatie(s) en riskmatrices aan elkaar aan te passen, afgestemd op de organisatie.

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 voor 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):** beschermingssystemen 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.
- **Cascaderende-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.

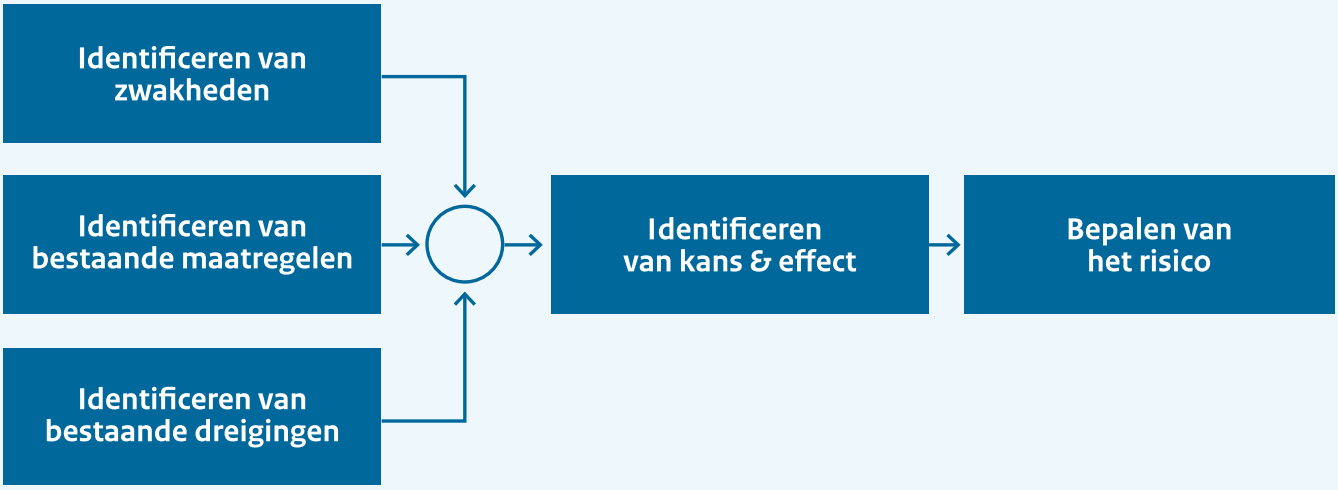
	Financieel	Assets	Omgeving	Veiligheid	Legislatie	Reputatie	Cascaderende effecten
0	Geen schade	Geen schade	Geen schade	Geen schade	Geen schade	Geen schade	Geen schade
1	Minimaal	Minimaal	Minimaal	Minimaal	Minimaal	Minimaal	Minimaal
2	Matig	Matig	Matig	Matig	Matig	Matig	Matig
3	Aanzienlijk	Aanzienlijk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

2.4 Benodigde kennis en expertise

Het is van groot belang dat bij de effectclassificatie de juiste expertise aanwezig is om de impact nauwkeurig te beoordelen. Naast technologische aspecten gaat het ook om veiligheidsimplicaties en mogelijke financiële, juridische en ecologische gevolgen. Ontoereikende inzichten kan ertoe leiden dat essentiële zaken over het hoofd worden gezien en de inschatting van de worst-case impact vertroebelen. Een multidisciplinair team is daarom een vereiste. Hieronder staan een aantal voorbeelden van belangrijke rollen bij het maken van een juiste en complete impactanalyse:

1. **Risicobeheerder:** bepaalt risiconiveaus, keurt maatregelen goed en accepteert resterende risico's.
2. **Chief Information Security Officer (CISO):** waarborgt kwaliteit van (IT-)risicoanalyse en -beheer, met diepgaande kennis van cybersecurity. Mogelijk is de CISO ook verantwoordelijk voor compliance.
3. **Financieel Expert:** beoordeelt financiële gevolgen en integreert deze in bestuurlijke beslissingen en rapportages.
4. **Technisch Specialist:** heeft diepgaande technische kennis van OT-systemen en kan de impact van falende componenten inschatten.
5. **Procesexpert:** begrijpt het operationele proces en kan de impact van falende processen beoordelen. Voor de maritieme sector kan dit bijvoorbeeld een maritiem officier zijn
6. **Automatiseringsdeskundige:** begrijpt procesautomatisering en beoordeelt technische impact van dreigingen op geautomatiseerde processen.
7. **Juridisch Adviseur:** kent juridische aspecten van privacy, aansprakelijkheid, en compliance binnen OT-cyberbeveiliging.
8. **Milieuexpert:** beoordeelt mogelijke milieueffecten van cyberincidenten en de kosten voor herstel.
9. **Netwerkbeheerder:** kent de netwerkarchitectuur van OT-systemen en beoordeelt impact op ICT-gebied.
10. **Incident Response Specialist:** heeft expertise in het omgaan met incidenten en het herstellen van systemen na een cyberincident.

3. Analyseren



Dit hoofdstuk beschrijft de nodige stappen om tot een gedetailleerde analyse van de OT-cybersecurityrisico's te komen. Zoals eerder beschreven wordt het risico bepaald door de dreiging, bestaande zwakheden, en de kans dat deze dreiging door middel van exploitatie van deze zwakheden een bepaalde impact kan veroorzaken. Om dit te analyseren zijn de bovenstaande stappen nodig, die elk in een van de volgende paragrafen beschreven wordt.

3.1 Identificeren van zwakheden

Een dreiging vormt pas een risico wanneer het kan profiteren van bestaande zwaktes. Stel je een hypothetisch scenario voor waarin een OT-systeem volledig vrij is van zwaktes en altijd perfect blijft werken; dan zou er geen risico zijn. Maar in de realiteit zullen er altijd bekende en onbekende zwakheden zijn. Deze zwakheden kunnen zich op verschillende niveaus voordoen, namelijk:

- **Menselijk:** dit omvat kennis, expertise, gedrag en bedrijfscultuur, die van invloed zijn op hoe mensen omgaan met cybersecurity.
- **Processen:** dit verwijst naar het ontbreken of niet naleven van beveiligingsprocessen rond onderhoud, wijzigingen of eigendom.
- **Technologie:** hierbij gaat het om zaken als gebrekkige scheiding van OT-netwerken, verouderde apparatuur, niet-geïnstalleerde beveiligingspatches, etcetera.

Een grondige analyse vereist goed inzicht in de OT-omgeving en hoe individuele systemen (assets) bijdragen aan het geheel. Het opstellen van een register van assets en netwerkdiagrammen vormt hiervoor een essentieel startpunt.

Casestudy identificeren van zwakheden: Maritiem

Deze casestudy geeft een voorbeeld van hoe na te denken over het identificeren van zwakheden. Er hoeft niet altijd uitgegaan te worden van kwaadwillende actoren!

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 hiervan is dat de controlesignalen op het netwerk vertraagd zijn, wat invloed heeft op de responsiviteit en veerkracht van het ballastsysteem. Dit creëert een risico voor momenten waarop de stabiliteit van het vaartuig een zorg is (bijv. ruwe zeeën, bepaalde offshore-operaties, etcetera).

De menselijke factor mag tijdens het identificeren van zwakheden niet worden vergeten! Aan boord en aan land is cybersecurity bewustzijn van belang. Onbedoeld en onwetend kan er veel schade aangericht worden!

Assetregister:

Een grondig en volledig overzicht van alle individuele assets en hun technische specificaties is van groot belang:

- De focus ligt voornamelijk op hardware en software, inclusief model, type, firmware- en softwareversies, en netwerkadressen. Ook is het belangrijk om de functionele specificaties vast te leggen zodat het duidelijk is wat de toegevoegde functionele waarde is van een bepaald asset.
- Andere, wellicht niet tastbare, assets, zoals vertrouwelijke of bedrijfkritische informatie of intellectueel eigendom, kunnen optioneel als assets worden beschouwd en in het register worden opgenomen.
- Het is tevens belangrijk om van elke asset te bepalen wat de potentiële impact kan zijn bij onbeschikbaarheid en/of wat de ergst mogelijke gevolgen zijn als de asset wordt gecompromitteerd door een cyberincident. Om deze effecten in kaart te brengen en te categoriseren wordt vaak een 'asset criticality label' gebruikt met indeling 'laag, midden, hoog'.
- Verder is het belangrijk om in kaart te hebben welke bedrijfsprocessen worden ondersteund door welke assets/systemen. Dat maakt het uitvoeren van een assessment op potentiële impact ook makkelijker en zorgt voor breder begrip hoe een bepaald systeem de continuïteit van de bedrijfsvoering direct en indirect beïnvloedt.

Netwerktekeningen:

Daarnaast is het cruciaal om de afhankelijkheden en connectiviteit tussen assets goed te begrijpen, vooral de scheiding tussen IT- en OT-systemen en hoe alle OT-systemen onderling aan elkaar verbonden zijn:

- Gewone (as-built) systeemtekeningen kunnen in sommige gevallen nuttig zijn, maar zijn in de praktijk vaak niet gedetailleerd genoeg.
- Afhankelijk van de complexiteit van het systeem, zijn specifieke logische en fysieke netwerktekeningen aan te raden. Met name bij het gebruik van veel virtualisatie, VLANs, etcetera kan een extra logische netwerktekening belangrijker worden voor het juiste overzicht.
- Verder kan het een overweging zijn om de functionele afhankelijkheid tussen netwerken van elkaar in kaart te brengen, ook in verband met cascaderende effecten.

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

Hoeveel detail is nodig?

In werkelijkheid is het erg lastig en arbeidsintensief om een assetregister en netwerktekening 100% compleet te maken, inclusief alle gewenste details. Zelfs met bestaande tools die deze acties deels kunnen automatiseren blijft het vaak een uitdaging, en dan is nog niet gesproken over het up-to-date houden van de registers en netwerken. Afhankelijk van het risicoprofiel kunnen er keuzes gemaakt worden om met minder details te starten. Bijvoorbeeld alleen de verbonden (IP-enabled) assets.

Ook de hoeveelheid details per asset kan verschillen. Het belangrijkste is er minimaal een compleet overzicht is van alle gekoppelde assets, bijvoorbeeld met de systeemnaam, hardwaremodel, operating system versie en het IP-adres. In een meer gedetailleerde versie kunnen (eventueel later) ook de volgende gegevens worden opgenomen; patchversies, geïnstalleerde software, gebruikers, MAC-adres, rol in het proces, belangrijkheid, beheerder.

Voor het volledig gedetailleerde overzicht is er ook inzicht nodig in alle subsystemen die door een leverancier geïnstalleerd zijn. Hiervoor is een HBOM (hardware bill-of-materials) of SBOM (software bill-of-materials) nodig. Zonder dit soort informatie moet het hele systeem als een black-box beschouwd moeten worden. Afhankelijk van het risicoprofiel en/of het volwassenheidsniveau van de organisatie zijn deze extra details nodig voor het uitvoeren van een complete risicoanalyse.

Inventarisatie zwakheden:

Deze stap draait om het identificeren van zoveel mogelijk zwakheden. Om deze zwakheden juist te kunnen bepalen is het cruciaal om in het bezit te zijn van een zo compleet mogelijk assetregister. Als er nog geen assetregister is, kan dit best een gewichtige oefening opleveren, en daarmee een die snel niet goed wordt uitgevoerd. Eerdergenoemde stappen uit bovenstaande hoofdstukken kunnen gebruikt worden als leidraad om pragmatisch en risicogedreven te werk te gaan. Verstandig is om een pragmatische aanpak toe te passen: houd de scope klein en behapbaar om vervolgens verder uit de bouwen. De inventarisatie kan op verschillende manieren worden aangepakt, zowel continu als gepland:

- Bij het vinden van technische zwakheden is voorzichtigheid geboden bij het gebruik van automatische scanners, omdat deze de OT-systemen negatief kunnen beïnvloeden. Soms zijn er mogelijkheden tijdens specifieke onderhoudsmomenten, spot-checks of met behulp van testsystemen of systeemback-ups.
- Een alternatief is het benutten van externe informatiebronnen zoals leveranciers en NCSC, CISA of NVD. Hierbij is een

compleet assetregister en juiste informatie per type essentieel voor analyse.
- Tot slot kunnen gap-analyses, securityassessments en/of security maturity analyses ten opzichte van standaarden of "best practices" zwakheden in technologie, mens en processen aan het licht brengen.

Analyse:

Niet alle ontdekte zwakheden zijn eenvoudig te misbruiken door een aanvaller. Daarnaast is een zwakte in specifieke industriële apparatuur vaak moeilijker te misbruiken dan bekende kwetsbaarheden in algemene software, omdat voor laatstgenoemde kant-en-klare tools bestaan. Kortom, de bereikbaarheid en de complexiteit van een zwakte spelen een rol. De ontdekte zwakheden, samen met de netwerktekeningen, kunnen dienen als input voor verdere analyse.

Complexiteit	Lage bereikbaarheid	Middel bereikbaarheid	Hoge bereikbaarheid
Makkelijk	Middel	Hoog	Hoog
Middel	Laag	Middel	Hoog
Moeilijk	Laag	Laag	Middel

Dreigingsprofiel vs. aanvaller

Het begrijpen van de relatie tussen het dreigingsprofiel van een organisatie en het profiel van de aanvaller is essentieel voor effectief cyberrisicobeheer. Het dreigingsprofiel van een organisatie omvat de specifieke risico's waarmee het wordt geconfronteerd op basis van haar branche, grootte, locatie en technologische infrastructuur. Het profiel van de aanvaller omvat hun motivaties, capaciteiten en gebruikelijke aanvalsmethoden. Door deze profielen te vergelijken, kunnen organisaties zich beter voorbereiden op mogelijke dreigingen en gerichte maatregelen nemen om zichzelf te beschermen tegen cyberaanvallen.

In beide sectoren zijn dreigingsactoren actief met uiteenlopende motivaties en doelen. Deze actoren kunnen onder meer bestaan uit hacktivisten, criminele organisaties, nationale overheden, interne betrokkenen, individuele hackers, concurrenten en terroristische groeperingen. Hacktivisten richten zich vaak op milieukwesties of geopolitieke zaken, terwijl criminele organisaties financiële winst nastreven via ransomware en datadiefstal. Nationale overheden kunnen organisaties als doel zien voor spionage of geopolitieke belangen. Interne bedreigingen kunnen voortkomen uit werknemers die gevoelige informatie lekken of toegangsprivileges misbruiken.

Voorbeeld: dreigingsprofiel, motivatie en capaciteiten
Een niet-gepatcht systeem dat niet is verbonden met een netwerk is uitermate lastig te exploiteren voor een externe dreigingsactor. Echter is niks onmogelijk, afhankelijk van hoeveel capaciteiten en motivatie een dreigingsactor heeft. In het voorbeeld van een niet-gepatcht, niet verbonden systeem kan er nog steeds lokaal invloed op uitgeoefend worden door middel van verwijderbare media zoals USB-sticks.

3.2 Identificeren van bestaande maatregelen

Bestaande maatregelen spelen een cruciale rol bij het verminderen van zowel bekende als onbekende zwakheden en het reduceren van daarmee samenhangende risico's. Ondanks dat er wellicht op dit moment weinig tot geen OT-specifieke regulatie of baseline is omtrent op de hoogte zijn en blijven van zwakheden en risico's – het is vaak een taak is van de leverancier – , moet er rekening gehouden worden met toekomstige voorschriften. Om deze stap effectief uit te voeren, is het essentieel om in kaart te brengen welke maatregelen zijn geïmplementeerd en hoe effectief ze zijn. Hierbij valt te denken aan een breed scala van maatregelen op verschillende vlakken, bijvoorbeeld zoals onderverdeeld in de internationale ISO27002 norm:

- **Fysieke maatregelen**: denk aan beveiliging van gebouwen, toegangscontrole, fysieke scheiding van netwerken, zoals deuren, hekken, sloten en meer. Zo kunnen er bijvoorbeeld fysieke beperkingen en toegangscontrolemechanismen worden geïmplementeerd om ongeautoriseerde fysieke toegang tot systemen te voorkomen.
- **Technische maatregelen:** hierbij spelen firewalls, netwerk- en systeemarchitectuur, detectie- en loggingtools een vitale rol. Zo speelt bijvoorbeeld het gebruik van firewalls en real-time monitoring van netwerkactiviteiten een rol om mogelijke bedreigingen te identificeren en te blokkeren.
- **Processen/organisatorische maatregelen:** dit omvat onderhoudsprocedures, incident responseplannen en beveiligingsbeleid. Bijvoorbeeld het belang van een goed gedefinieerd en regelmatig getest incident responseplan bij zowel on- als offshore werkzaamheden.
- **Menselijke maatregelen:** dit omvat het onboarden/offboarden van medewerkers, trainingen, screenings en bewustmakingscampagnes. Een gedegen cybersecuritybeleid omvat continue trainingen en bewustwordingsprogramma's om de menselijke factor te versterken en de risico's van sociaal-technische aanvallen te verminderen.

Bovenstaande gegevens worden vaak duidelijk uitgelicht in eerdere analyses, zoals de gap-analyse, securityassessment en/of security maturity analyse. Deze activiteiten bieden een diepgaand inzicht in de effectiviteit van de toegepaste maatregelen en

identificeren eventuele hiaten die moeten worden aangepakt. Bij ieder van de bovenstaande maatregelen geldt dan ook dat er een continu proces van meting van implementatie, werking en effectiviteit plaatsvindt, ook wel aangeduid de cyclus van 'plan-do-check-act' en 'continue verbetering'. Na het in effect treden van maatregelen is het aan te raden een analyse van de gevolgen te doen, om zo lessen voor in de toekomst mee te nemen en de cyberweerbaarheid iteratief te verbeteren.

3.3 Identificeren van bedreigingen

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. Om hier inzicht in te verkrijgen, is de eerste stap om informatie te verzamelen uit verschillende bronnen, zoals bijvoorbeeld:

- algemene dreigingsbeelden, zoals die opgesteld zijn door ENISA of het NCSC
- eventueel beschikbare sectorspecifieke dreigingsbeelden, zoals voor luchtvaart en maritieme sectoren, bijvoorbeeld via sectorspecifieke ISAC's of commerciële partijen
- interne informatie en kennis uit eerdere incidenten
- het uitvoeren van een dreigingsanalyse met behulp van algemene of bedrijfs- en sectorspecifieke dreigingslijsten

De pragmatische aanpak

Over het algemeen is het voor een bedrijf vaak niet haalbaar en/of kosteneffectief om elke mogelijke dreigingsactor aan elke kwetsbaarheid te koppelen. Het is eerst van belang om binnen de vastgestelde scope te blijven, bijvoorbeeld omdat bepaalde typen dreigingen en actoren buiten beschouwing worden gelaten. Bovendien kan de aanpak sterk variëren afhankelijk van de risicobereidheid en volwassenheid van de organisatie. In een meer pragmatische aanpak wordt verkregen informatie zonder verdere specifieke analyse meegenomen in de volgende stappen voor het bepalen van kans en risico. Een nadeel hiervan is dat bestaande maatregelen en afhankelijkheden niet voldoende worden meegenomen, wat kan leiden tot discussie, onjuiste inschattingen of benoemde risico's zonder gekoppelde risico-eigenaar.

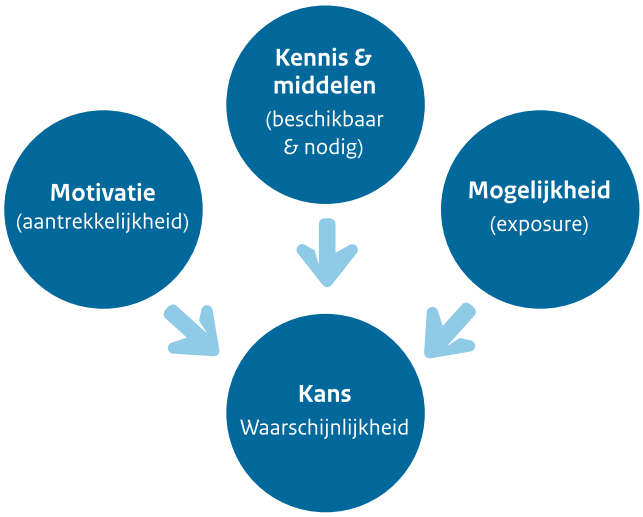
De gedetailleerde aanpak

In een gedetailleerdere aanpak wordt er, zoals de naam al aanduidt, specifieker en dieper ingegaan op dreigingen, kwetsbaarheden en de koppeling tussen deze factoren. Door bijvoorbeeld Threat Modeling of het opstellen van Attack Trees wordt onderzocht welke stappen een aanvaller moet nemen om tot een bepaald gevolg te komen. Hierbij wordt het volledige aanvalspad (ook wel Cyber Kill-chain genoemd) onderzocht, en soms zelfs nog specifieker geduid met behulp van het "MITRE ATT&CK for ICS framework". Tegelijkertijd worden de effecten van bestaande maatregelen meegenomen. Dit leidt tot een inzichtelijk beeld van de huidige stand van zaken rondom risico's en bedreigingen, en biedt een organisatie de kans om weloverwogen gepaste maatregelen te nemen. Het nadeel van deze methode is dat er veel technische kennis van het systeem vereist is en het proces zowel tijd- als budgetintensief kan zijn.

3.4 Analyseren van de kans & impact

Om uiteindelijk het risico te kunnen bepalen is de factor **kans** erg belangrijk. De eerdergenoemde formule, risico = kans x effect, maakt dit duidelijk. 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. Voor cybersecurity is de inslag meestal geen toeval maar meer (on)gerichte of (on)bewuste sabotage. De motivatie, kennis en middelen van een dreigingsactor, gecombineerd met het aantal aanwezige (makkelijk) te misbruiken zwakheden, bepalen uiteindelijk de waarschijnlijkheid op een incident.



Daarom is de kansschaal voor cybersecurityincidenten vaak lastig uit te drukken in tijdseenheden van bijvoorbeeld 1 x per week, 1 x per maand of 1 x per jaar. Een risicomatrix kan hierdoor beter een andere schaalverdeling gebruiken. Een praktische aanpak die gebruikt kan worden, zeker als bovenstaande gegevens niet volledig helder zijn, is een objectieve schaal op basis van voorkomen.

	Voorbeeld 1	Voorbeeld 2
Heel laag	Is nog nooit voorgekomen in de sector	Toekomstige waarschuwing
Laag	Is wel eens eerder voorgekomen in de sector	Is afgelopen jaar ergens een keer voorgekomen
Middel	Is wel eens voorgekomen in de organisatie	Is afgelopen jaar voorgekomen in de sector
Hoog	Is wel eens voorgekomen voor dit object	Is afgelopen jaar voorgekomen in een vergelijkbaar bedrijf
Heel hoog	Komt vaker voor binnen de organisatie/object	Is afgelopen jaar voorgekomen binnen dit bedrijf

Voor een eerste analyse werkt deze schaal erg praktisch en is deze goed te gebruiken als startpunt. Een nadeel is dat de kansschaal niet beïnvloed kan worden door het meenemen van bestaande of extra maatregelen. Mitigerende maatregelen bemoeilijken de succesvolle uitvoer van een cyberaanval, en zouden de kans moeten reduceren. Een alternatieve, meer gedetailleerde, schaalverdeling die rekening houdt met waarschijnlijkheid/kans zoals eerder genoemd, en de motivatie en capaciteiten van de dreigingsactor ten opzichte van de aanwezige cybersecuritymaatregelen van een systeem of netwerk, houdt hier wel rekening mee:

Niveau	Omschrijving
Heel laag	De dreigingsactor heeft geen motivatie, kennis of capaciteiten om de zwakte te benutten. Bovendien zijn er effectieve maatregelen die het misbruik van de zwakte voorkomen, waardoor het risico minimaal is.
Laag	De dreigingsactor heeft weinig motivatie en beperkte capaciteiten en er zijn redelijk effectieve maatregelen om de zwakte tegen te gaan.
Middel	De dreigingsactor is enigszins gemotiveerd en heeft enige kennis en capaciteiten, met matige maatregelen die het misbruik van de zwakte kunnen beperken.
Hoog	De dreigingsactor is behoorlijk gemotiveerd en beschikt over voldoende kennis en capaciteiten, terwijl er slechts beperkte maatregelen zijn om het misbruik van de zwakte te voorkomen.
Heel hoog	De dreigingsactor is zeer gemotiveerd en beschikt over uitgebreide kennis en capaciteiten, en er zijn geen effectieve maatregelen die voorkomen dat de zwakte wordt misbruikt.

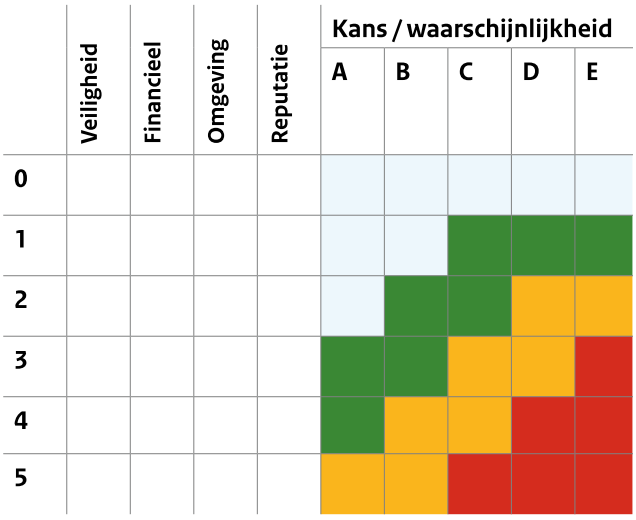
Uiteindelijk draait het om de combinatie van motivatie, vereiste kennis en expertise, en de capaciteit van de dreigingsactoren. Het is essentieel om te onthouden dat het gaat om ***de kans dat de betreffende impact wordt gerealiseerd, niet om de kans dat de dreiging zich voordoet***.

De impact omvat de diverse negatieve effecten na een incident, variërend van financiële gevolgen tot menselijke, milieu- of omgevingseffecten. Het is van belang om deze impact op verschillende niveaus te kunnen schalen. Elke organisatie moet passende niveaus vaststellen, zodat alle risico's binnen de organisatie kunnen worden vergeleken. Dit gestructureerde kader helpt bij het identificeren en managen van risico's op een effectieve manier.

Vaak is het niet praktisch om alle mogelijke combinaties van dreigingsactoren en kwetsbaarheden te analyseren. Het groeperen van kwetsbaarheden of uitgaan van een "gemiddelde" dreigingsactor kan hierbij helpen. Echter, het is waardevol om inzicht te krijgen in diverse actoren met verschillende kennis en middelen. Soms kan de ergst mogelijke impact van een risico alleen ontstaan door een specifiek type dreigingsactor met een zeer kleine kans, terwijl de kans om gehackt te worden door een minder vaardige actor groter is maar de kennis en motivatie ontbreekt om tot die ergste impact te komen.

3.5 Analyseren van het risico

Het evalueren van cybersecurityrisico's houdt in dat de kans wordt bepaald dat een dreiging een zwakheid exploiteert, met de daaruit voortvloeiende impact. Dit wordt doorgaans gedaan met behulp van een risicomatrix, waarbij kans en impact op de respectievelijke assen worden geplot. De impact kan diverse gevolgen hebben, zoals financiële, veiligheids- en omgevingsaspecten, (zie casestudy 'van kwaad tot erger' onder kopje 2.3). In de risicomatrix hebben deze elk een vastgestelde schaal, waarbij de ergste consequentie telt.



De bovenstaande risicomatrix is breed inzetbaar binnen een organisatie: voor cybersecurityrisico's vereist deze benadering een aangepaste interpretatie van kans, met mogelijk extra impactgebieden zoals veiligheid en milieu. Door risico's op de matrix te plaatsen, ontstaat een overzicht van vereiste acties, die worden geleid door de bedrijfswaarden en de risicobereidheid

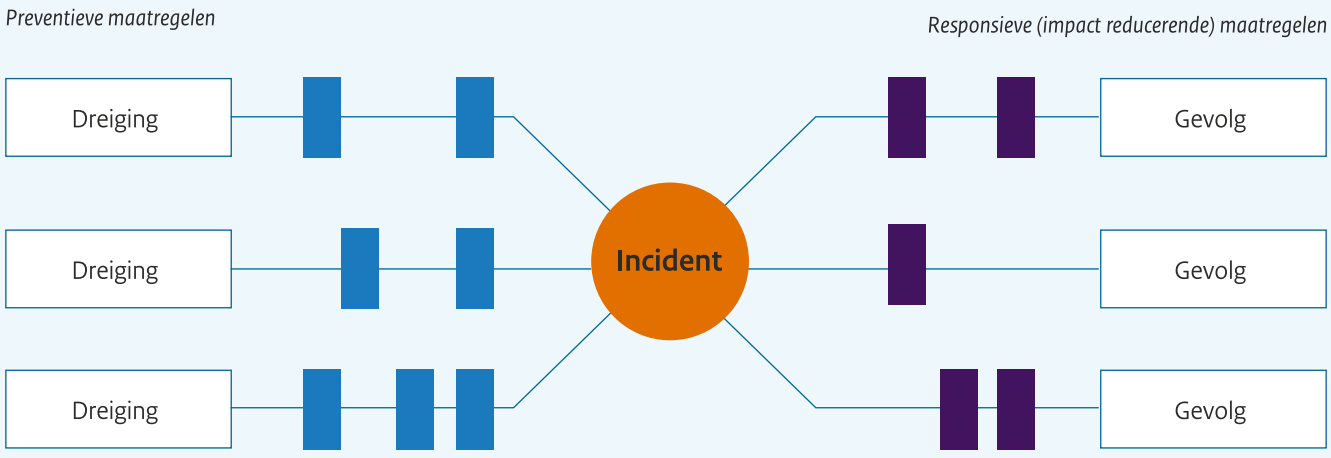
van een organisatie, oftewel de risk appetite. Bijvoorbeeld:

- **Lichtblauw:** verwaarloosbaar of zeer laag risico met minimale impact en binnen de acceptabele grenzen van de organisatie. Geen aanvullende actie vereist. Bijvoorbeeld een niet-gebruikt systeem zonder enige connectie met operationele activiteiten.
- **Groen:** Laag risico dat binnen de vastgestelde risk appetite valt, maar met mogelijke verbeterpunten. Acceptabel zonder onmiddellijke aanvullende maatregelen. Bijvoorbeeld een systeem met beperkte kwetsbaarheden maar met een solide beveiligingsinfrastructuur.
- **Oranje:** Gematigd risico dat extra maatregelen vereist om binnen de vastgestelde risk appetite te blijven. Bijvoorbeeld een systeem met enkele kwetsbaarheden waarvan de meeste beheersbaar zijn, maar waarvoor aanvullende beveiligingsupdates nodig zijn. Oranje kan echter escaleren naar hoog risico dat onmiddellijke aandacht en verbetering behoeft als eerdergenoemde maatregelen te lang uitgesteld of vergeten worden.
- **Rood:** Onaanvaardbaar risico met een directe bedreiging voor de organisatie en buiten de vastgestelde risk appetite. Onmiddellijke en dringende maatregelen zijn vereist. Bijvoorbeeld een systeem met kritieke kwetsbaarheden die een directe bedreiging vormen voor de operationele integriteit van de organisatie.

Risicoacceptatie en maatregelen worden verder beschreven in hoofdstuk 4.

Het is wel belangrijk om het onderscheid te maken tussen nieuwe/bestaande maatregelen die de kans of de impact beïnvloeden. Voor een volledige en gedetailleerde risicoanalyse is uiteindelijk inzicht nodig in al deze facetten. Hiervoor kan een zogenaamd Bow Tie-model gebuikt worden waar dreigingen, preventieve en responsieve maatregelen en potentiële gevolgen in relatie worden gebracht met elkaar.

De Bow Tie-methode is een visueel hulpmiddel in risicomanagement, vooral handig in OT. Het visualiseert risico's, oorzaken, gevolgen, en de preventieve maatregelen ertussen. Voor OT identificeert het risico's, hun oorzaken (zoals cyberaanvallen) en de gevolgen (zoals productiestilstand). Het benadrukt ook de noodzaak van preventieve maatregelen, zoals firewalls en training, om deze risico's te beheersen en kritieke systemen te beschermen.



4. 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 (Treat)	Extra mitigerende maatregelen zijn nodig om het risico te reduceren. Dit kan door de kans, impact of beide te beïnvloeden.
Accepteren (Tolerate)	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 (Transfer)	Het risico wordt overgedragen aan een andere partij, vaak een cybersecurityverzekering.
Vermijden (Terminate)	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 is. 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.

4.1 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 implemventeren van een procedures in bedrijfs-IMS zoals een vierogenbeleid en het scheiden van verantwoordelijkheid. • Het regelmatig maken van systeem of configuratie back-ups van alle OT-systemen en het met regelmaat testen van de restoreprocedure.
Mens	• Het verplicht stellen van een op rol en verantwoordelijkheid gebaseerde OT-cybersecurityawareness-training voor alle personen die aan of met OT-systemen werken, inclusief derde partijen.

Het is aan te bevelen om zoveel mogelijk gebruik te maken van een standaardlijst aan maatregelen. Dit is met name belangrijk voor de onderhoudbaarheid van de maatregelen, gebruikte technische oplossingen en procedures. Uiteindelijk, in de meest volwassen organisaties, is centrale logging en monitoring (door bijvoorbeeld een SOC) geïmplementeerd en ook hiervoor is het efficiënter om zoveel mogelijk standaardoplossingen te hebben.

Unieke oplossingen per systeem of situatie zijn als laatste optie altijd nog mogelijk, maar geven dus extra onderhoud, complexiteit en kosten op de langere termijn. In OT ligt het toepassen van oplossingen vaak nog wat gecompliceerder wegens eigenaarschap van het asset: zo kan het zijn dat een leverancier van een bepaald OT-systeem de gekozen oplossingen niet ondersteunt. Bijvoorbeeld een oplossing als EDR of XDR heeft een grotere risicoreductie dan reguliere antivirus, maar voordat deze oplossing als standaard op alle OT-systemen gebruikt kan worden, moet dit in overeenstemming met alle betreffende leveranciers worden afgesproken.

Maatregelen kunnen grofweg in twee categorieën worden ondergebracht: preventief en responsief (zie figuur in 3.4). Alle preventieve maatregelen zijn er om te voorkomen dat een incident gaat plaatsvinden (of de kans te verkleinen). Dit kunnen ook afschrikkende of vertragende maatregelen zijn. De tweede categorie, responsieve maatregelen, zijn er voornamelijk om de impact te reduceren. Voorbeelden zijn detectie en maatregelen om adequaat te reageren op cyberincidenten. Tenslotte, en specifiek voor OT, is het van belang om naar de mogelijk OT-impact te kijken. Het kan soms veel effectiever zijn om behaalde functionaliteit fysiek te beperken in plaats van extra preventieve maatregelen te nemen.

Vervolgens moet er ook rekening gehouden worden met eventuele nieuwe risico's die geïntroduceerd worden door de genomen maatregelen. Als er bijvoorbeeld nieuwe apparatuur zoals een firewall geïnstalleerd wordt, zal deze ook bekende zwakheden hebben. Daarnaast blijft er altijd een restrisico bestaan, zelfs als alle mitigerende maatregelen genomen zijn. Zodra dit risico onder de tolerantiedrempel komt, kan dit restrisico geaccepteerd worden. In de volgende paragraaf wordt verder ingegaan op risicoacceptatie.

Ten slotte is het belangrijk om een volledig kostenoverzicht van de nieuw voorgestelde maatregelen op te stellen. Dit zijn niet alleen de initiële aanschaf- en installatiekosten, maar ook de kosten voor de operationele taken en onderhoud. Uiteindelijk moeten deze kosten meegenomen worden in de afweging.

Casestudy voor risico reduceren: 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 groot 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 analoog 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.

4.2 Accepteren

Risicoacceptatie is een cruciaal onderdeel van risicobeheersing, waarbij een organisatie bewust bepaalde risico's aanvaardt als onvermijdelijk. Een formeel aangestelde risicobeheerder speelt hierbij een sleutelrol. Deze persoon heeft niet alleen het mandaat om de risico's te accepteren, maar kan ook het gehele risicolandschap voor de organisatie overzien. Dit betekent dat de persoon een passend verantwoordelijkheidsniveau binnen de organisatie moet bekleden, zoals bijvoorbeeld op het niveau van de business owner of zelfs op het niveau van de directie. Het is van essentieel belang om ervoor te zorgen dat beslissingen met betrekking tot risicoacceptatie worden genomen door personen met de vereiste autoriteit en expertise, en het mandaat dus bij de juiste persoon wordt belegd. Hierdoor kan de organisatie risico's op een effectieve manier beheren en haar operationele continuïteit en veiligheid van de operationele technologie waarborgen.

4.2.1 Risicotolerantie ("Risk appetite")

Accepteren van risico's is niet hetzelfde als risico's negeren. Bij elke organisatie zullen altijd bepaalde risico's blijven bestaan, het ondernemersrisico. Tegelijkertijd heeft elke organisatie een bepaald risicotolerantieniveau, ook wel "risk appetite" genoemd.

Dit is eerder beschreven in 1.4 als een belangrijke voorwaarde voor risicomanagement.

Zolang risico's goed en duidelijk in kaart zijn gebracht, geanalyseerd en onder deze drempelwaarde blijven kunnen ze worden geaccepteerd. Het is en blijft belangrijk om deze risicoanalyse, tezamen met alle aannames, te documenteren.

4.2.2 Afwijkingen

In de praktijk kan het voorkomen dat hogere risico's, boven het bepaalde risicotolerantieniveau, toch niet gemitigeerd kunnen worden. Extra maatregelen zijn bijvoorbeeld technisch niet mogelijk, kosten van implementatie zijn te hoog ten opzichte van het risico, of het is alleen mogelijk de veranderingen pas veel later in de tijd door te voeren. Afhankelijk van het risico is een (tijdelijke) acceptatie mogelijk.

Voor grote risico's (Rood in eerdergenoemde voorbeelden, zie 3.4), is (tijdelijke) acceptatie niet toegestaan. Er zal dus altijd eerst een van de andere beheersmaatregelen toegepast moeten worden.

Voor het formeel afwijken van het risicotolerantieniveau zijn een aantal extra stappen nodig volgens het 'pas-toe-of-leg-uitprincipe'.

1. Beschrijf waarom het niet mogelijk is om het risico op een andere manier te beheersen.
2. Onderzoek of er eventueel andere compenserende (dempende) maatregelen te nemen zijn die een deel van het risico (mens, proces, techniek) kunnen reduceren. Dit kunnen ook procedures zijn, extra (manuele) controles of speciale omstandigheden.
3. Voer een specifiek en gedetailleerde risicoanalyse uit, met inachtneming van alle specifieke aannames en aanvullende compenserende maatregelen.
4. Dit specifieke risico moet worden beoordeeld door de verantwoordelijke risicobeheerder, geaccepteerd en formeel worden vastgelegd. Hierbij is belangrijk dat:
   - het risico beoordeeld wordt door kundige en ervaren specialisten
   - het risico wordt geaccepteerd door een formeel aangestelde risicobeheerder die het gehele risico voor de organisatie kan overzien en ook het mandaat heeft deze risico's te accepteren
   - de afwijking wordt opgeslagen in een formeel (document) beheerssysteem
5. Alle afwijkingen moeten regelmatig (jaarlijks) opnieuw worden beoordeeld, rekening houdend met:
   - huidige risicotolerantieniveau en dreigingslandschap
   - huidige herevaluatie van het risico
   - status van compenserende maatregelen
   - eventuele invloeden van andere gedocumenteerde afwijkingen

Behalve het 'hoe' te behandelen van afwijkingen is het ook belangrijk om rekening te houden met het 'waarom': het is cruciaal dat specifieke risico's worden beoordeeld, geaccepteerd en formeel worden vastgelegd door de verantwoordelijke risicobeheerder om de organisatie te beschermen tegen mogelijke schade, verlies of verstoringen. Het vastleggen van afwijkingen in een formeel beheerssysteem zorgt voor traceerbaarheid en verantwoording, wat niet alleen intern duidelijkheid schept maar ook tegenover toezichthoudende instanties.

4.3 Overdragen

4.3.1 Verzekeringen

Het overdragen van cybersecurityrisico's kan door middel van een cybersecurityverzekering. Deze verzekeringen zijn meestal uit drie delen opgebouwd.

Onderdelen	Omschrijving
Preventie	De verzekeraar stelt verplichtingen aan de genomen preventiemaatregelen. Door middel van intakes, interviews of audits zal bepaald worden of de verzekering afgesloten kan worden en wat hiervoor de premie is.
Herstellen	Als onderdeel van een verzekering kan ondersteuning voor herstellen om zo de (vervolg)schade te minimaliseren.
Vergoeden	Het belangrijkste onderdeel is dat de verzekering de financiële schade compenseert, dit is inclusief verloren omzet en herstelkosten en is vaak gemaximeerd tot een bepaald bedrag.

Een belangrijke overweging is dat niet alle risico's kunnen worden overgedragen. Wanneer er potentiële impact is op veiligheid, omgeving, juridisch/regelgeving of maatschappelijk belang zijn bijvoorbeeld alleen de financiële consequenties te verzekeren. Verder gaat dit onderwerp vaak over het verzekeren van een restrisico, bijvoorbeeld het risico op ransomware, dat zelfs na alle geïmplementeerde maatregelen nog steeds een te groot (financieel) risico is voor de organisatie. Ten slotte kunnen de voorwaarden van een verzekering complex zijn: wat wordt er wel of niet vergoed, in hoeverre zijn cyberrisico's verzekerd en wat valt er wel of niet onder een oorlogs- of andere uitzonderingsclausule.

Casestudy verzekeren tegen cybersecurityaanvallen?

In 2017 leed het farmaceutische bedrijf Merck aanzienlijke schade door de NotPetya-malwareaanval. Ondanks het ontbreken van een cyberverzekering diende Merck een claim van $1,4 miljard in onder zijn allriskdekking. De aanval, toegeschreven aan Rusland, werd door velen gezien als een daad van cyberoorlog tegen Oekraïne. De impact van NotPetya verspreidde zich wereldwijd, wat leidde tot aanzienlijke financiële verliezen.

Mercks verzekeraars wezen de claim aanvankelijk af en beroepen zich op een standaardclausule voor oorlogsuitsluiting. Deze clausule sluit doorgaans schade uit als gevolg van oorlogshandelingen, waaronder cyberoorlogsvoering kan vallen. Merck betoogde echter dat de clausule voor oorlogsuitsluiting niet van toepassing was, omdat de aanval niet verbonden was met een militaire actie of doelstelling. Na juridische procedures oordeelde een rechtbank in New Jersey in het voordeel van Merck, waarbij werd gesteld dat de clausule voor oorlogsuitsluiting niet van toepassing was.

Deze zaak belicht de complexiteiten van cyberverzekeringen.

Maritieme organisaties worden geconfronteerd met unieke uitdagingen vanwege de onderlinge verbondenheid van wereldwijde scheepvaart en het potentieel voor cyberaanvallen om wereldwijd verstoring te veroorzaken. Desondanks worstelen verzekeraars met het beoordelen en verzekeren van cyberrisico's, aangezien er geen gestandaardiseerde definitie is van cyberoorlog. Zonder duidelijke criteria voor het beoordelen van claims gerelateerd aan cyberoorlog staan verzekeraars voor onzekerheid en zijn ze mogelijk terughoudend om dekking te bieden voor cybergerelateerde verliezen.

Bovendien bemoeilijkt de evoluerende aard van cyberdreigingen risicobeoordeling en -mitigatie. Cyberaanvallen kunnen afkomstig zijn van verschillende actoren, waaronder staten, criminele organisaties en hacktivisten, waardoor het moeilijk is om alle potentiële dreigingen te voorzien en te beschermen. De onderlinge verbondenheid van maritieme systemen vormt ook uitdagingen voor verzekeraars, aangezien een enkel cyberincident kan leiden tot wijdverbreide verstoring binnen de sector.

4.3.2 Outsourcing

Meer en meer diensten worden tegenwoordig uitbesteed aan derde partijen en serviceproviders. Voorbeelden zijn cloud-computing diensten (zoals OT-data historian diensten), cloudportalen van een leverancier (zoals online diagnostics van geïnstalleerde OT-systemen), 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 afgedekt zijn. Het uitbesteden van bepaalde diensten is niet hetzelfde als het overdragen van risico's. Het kan wel zijn dat bepaalde werkzaamheden (en daarmee bijbehorende verantwoordelijkheden) worden verschoven, maar uiteindelijk blijft het risico altijd bij de organisatie. Als er bijvoorbeeld een datalek heeft plaatsgevonden bij een externe dienstverlener, zal – ondanks een SLA en eventuele boeteclausule – de reputatieschade (en eventuele vervolgschade) uiteindelijk neerkomen bij de organisatie.

Gekoppeld aan bovenstaande wijzen van aanpak zijn de termen 'verantwoordelijk' (responsible) en 'aansprakelijk' (accountable):

- De term **verantwoordelijk** verwijst doorgaans naar individuen of teams die rechtstreeks betrokken zijn bij het uitvoeren van specifieke taken of activiteiten met betrekking tot risicomanagement. Deze personen zijn verantwoordelijk voor het uitvoeren van toegewezen taken, het implementeren van risicobeperkende maatregelen, en ervoor zorgen dat taken effectief en op tijd worden voltooid. Ze zijn actief betrokken bij de dagelijkse activiteiten van risicomanagement en spelen een praktische rol bij het beperken van risico's.
- Aan de andere kant verwijst de term **aansprakelijk** doorgaans naar individuen of rollen die uiteindelijk verantwoordelijkheid en bevoegdheid dragen voor het algehele resultaat van risicomanagementprocessen. Hoewel ze mogelijk niet rechtstreeks betrokken zijn bij het uitvoeren van specifieke taken, zijn aansprakelijke personen uiteindelijk verantwoordelijk voor het succes of falen van de inspanningen voor risicomanagement binnen hun verantwoordelijkheidsgebied. Ze zijn verantwoordelijk voor het stellen van doelen, het definiëren van strategieën, het toewijzen van middelen en ervoor zorgen dat passende maatregelen worden genomen om risico's effectief te beheren.

Ten slotte kan de externe dienst, dienstverlener of serviceprovider ook nieuwe risico's introduceren, bijvoorbeeld doordat een deel van het bestede werk ook weer door de leverancier wordt uitbesteed (supply chain risico's). Het is belangrijk dat deze risico's zijn meegenomen tijdens de inventarisatie fase (zie 3.2) en dat er rekening gehouden wordt met het volwassenheidsniveau van de leverancier.

4.4 Vermijden

Als laatste optie is het ook mogelijk het risico in zijn geheel te vermijden. Dit kan door de kans of de impact tot 0 te reduceren. In de praktijk betekent dit meestal het stoppen van een bepaalde activiteit. Meestal zal dit een mogelijke actie zijn voor de grootste (onacceptabele) risico's, die zelfs met mitigerende acties nog steeds te risicovol zijn. In dat geval kan het verstandig zijn om af te vragen of het risico wel genomen moet worden en/of het niet beter is om de activiteit te stoppen (of überhaupt niet te starten, aangezien het ook om nieuwe OT-technologie kan gaan).

Bijvoorbeeld het op afstand toegang verlenen tot kritieke veiligheidssystemen kan een onacceptabel risico zijn. Het wegnemen van deze optie (verwijderen van de netwerkverbinding) zal de kans reduceren tot 0 en daarmee is het risico in zijn geheel vermeden.

4.5 Implementatie maatregelen

Uiteindelijk, wanneer van alle risico's de beheersmaatregelen zijn bepaald, moeten de mitigerende maatregelen nog geïmplementeerd worden. In een ideaal geval zijn er voldoende middelen en mankracht beschikbaar om dit voor alle objecten of systemen uit te voeren. In werkelijkheid is dit meestal niet realistisch en moeten prioriteiten gesteld worden. De volgende punten kunnen hierbij behulpzaam zijn:

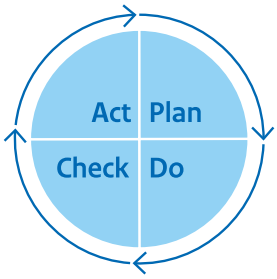
- Gebruik het risicoregister en geef prioriteit aan de belangrijkste (grootste) risico's en/of risico's op de meest belangrijke objecten/systemen. Tegelijkertijd moet het totaalbeeld niet vergeten worden, de som van meerdere kleine risico's kan uiteindelijk alsnog belangrijker zijn dan een van de geïdentificeerde hoge risico's.
- Afhankelijk van beschikbare middelen, mankracht en planning kan een plan van aanpak gemaakt worden. Hiervoor is dan ook managementgoedkeuring nodig. Het is niet altijd mogelijk om veranderingen (meteen) door te voeren. Soms moet worden gewacht op een leverancier, nieuwe versies, certificeringen, downtime, etcetera.
- Als toch blijkt dat het (te) lang duurt voordat maatregelen genomen kunnen worden, is een tijdelijke risicoacceptatie wellicht noodzakelijk. (Zie 4.2).
- In het geval van nieuwe assets of systemen is het belangrijk om te controleren of alle maatregelen juist geïmplementeerd zijn voordat het system in gebruik wordt genomen, of resterende risico's bekend en geaccepteerd zijn. Implementatie van maatregelen kan worden gecontroleerd tijdens een FAT of SAT door bijvoorbeeld het uitvoeren van een penetratietest.
- Uiteindelijk is het een managementbeslissing hoe de prioriteiten voor bovenstaande punten worden afgewogen ten opzichte van risico's en middelen.
- Overige verplichtingen of externe eisen zoals wetgeving of verplichting tot (cyber)verzekering staan wellicht nu nog vrij maar in de toekomst niet meer. Uiteraard moet in zulke gevallen deze verplichtingen bij implementatie ook meegenomen worden.

Ten slotte kan het voorkomen dat tijdens de implementatie van de voorgestelde maatregelen het in de praktijk iets anders uitpakt. Bijvoorbeeld als de voorgestelde oplossing niet (geheel) werkt, niet (overal) geïnstalleerd kan worden en/of de uitgangssituatie inmiddels anders is. In dit geval is het belangrijk dat dit wordt teruggekoppeld naar de risicobeheerder en dat de risicoanalyse opnieuw wordt uitgevoerd.

5. Monitoren en rapporteren

Risicobeoordeling en -beheer is een continu proces. Al zou er niets veranderen aan de infrastructuur en de systemen in de organisatie, de buitenwereld (het 'dreigingslandschap') verandert continu. Dit geldt op grote schaal, voor externe dreigingen, die nieuwe aanvalstechnieken ontwikkelen en op dagelijkse basis nieuwe zwakheden vinden in bestaande systemen. Daarnaast staat de interne organisatie ook niet stil, door bijvoorbeeld nieuwe technologieën en andere systemen te gebruiken. Deze introduceren mogelijk nieuwe zwakheden die gemist kunnen worden als een risicoanalyse niet herzien wordt. Een herevaluatie van de risicoanalyse kan op verschillende manieren, door bijvoorbeeld zelfassessments of interne audits, maar bijvoorbeeld ook door controles uit te laten voeren door externe partijen.

Om de risico's continu passend te beheren, zijn er verschillende bedrijfsprocessen nodig die grofweg in drie verschillende categorieën onder te verdelen zijn. Deze worden elk in een volgende paragraaf beschreven. In de meeste organisaties worden deze processen opgenomen in de zogenaamde PDCA-cyclus.



5.1 Operationeel proces

Dit proces omvat alle operationele activiteiten en maatregelen die verband houden met cyberbeveiliging. Hierbij draait het vooral om de implementatie, het beheer en de uitvoering van deze maatregelen. Een voorbeeld hiervan is het regelmatig uitvoeren van een gap-analyse op bestaande systemen. Een gap-analyse is een evaluatie om te bepalen of er discrepanties of 'gaten' bestaan tussen de huidige status van de beveiliging en de gewenste status. Dit biedt inzicht in de mate waarin alle systemen daadwerkelijk voldoen aan de vastgestelde beveiligingsmaatregelen.

Een tweede belangrijk aspect is het testen van de effectiviteit van de geïmplementeerde maatregelen. Dit kan bijvoorbeeld worden gedaan door regelmatig gerichte "vulnerability scans" of "penetration tests" uit te voeren. Al moet meteen gezegd worden dat dit vaak erg lastig is binnen OT-omgevingen, omdat dit soort onderzoeken negatieve gevolgen kan hebben op de systemen. Een vulnerability scan identificeert kwetsbaarheden in systemen, netwerken of applicaties die kunnen worden misbruikt door kwaadwillende actoren. Daarentegen is een penetratietest een actieve aanvalssimulatie waarbij ethische hackers proberen binnen te dringen in systemen om kwetsbaarheden te identificeren en de effectiviteit van de beveiligingsmaatregelen te testen. Wat werkt in IT is vaak niet een-op-een te gebruiken in OT. Dus, in OT-omgevingen vereisen dit soort onderzoeken extra aandacht, voorbereidingen en goedkeuring, maar zijn zeker niet onmogelijk.

Daarnaast valt changemanagement ook onder de operationele processen. Elke wijziging in de netwerkinfrastructuur, zoals software-updates of configuratiewijzigingen, kan namelijk invloed hebben op de cybersecurity en nieuwe risico's introduceren. Daarom is het belangrijk om elke aanpassing te toetsen op mogelijke effecten op de beveiliging. Een goed changemanagementproces omvat procedures voor het beoordelen, goedkeuren, implementeren en monitoren van wijzigingen, rekening houdend met mogelijke beveiligingsimplicaties.

De resultaten van deze processen moeten worden geïntegreerd in het risicomanagementproces. Op deze manier wordt ervoor gezorgd dat de cyberbeveiligingsmaatregelen voortdurend worden geëvalueerd, bijgewerkt en aangepast om de veiligheid van de organisatie te waarborgen.

PDCA-cyclus in het Operationele Proces
Deze processen moeten antwoord geven op de volgende vragen:

1. Zijn alle voorgestelde maatregelen (techniek, mens, proces) aanwezig?
2. Zijn deze maatregelen effectief, worden ze gebruikt, zijn ze nog up-to-date?
3. Is het gehele pakket aan maatregelen effectief en worden hiermee de risico's daadwerkelijk gemitigeerd?

Dit kan o.a. inhouden: monitoren van risico-indicatoren, het beoordelen van prestaties en het identificeren van verbeterpunten. Maar ook, de operationele processen om geïmplementeerde maatregelen te onderhouden. Op basis van de bevindingen uit de controlefase worden aanpassingen gemaakt aan de operationele risicobeheersmaatregelen. ***Dit kan het bijwerken van procedures, het implementeren van verbeteringen en het nemen van preventieve maatregelen omvatten om de operationele risico's te beheersen en te verminderen.***

5.2 Tactisch proces

Het tactisch proces richt zich op de bedrijfsprocessen en heeft vooral aandacht voor de middellange termijn en de invloed van cybersecurity op deze processen. Hier vallen alle risicobeheersprocessen onder die beschreven zijn in hoofdstuk 4. Voorbeelden hiervan zijn onder andere het opstellen en vaststellen van standaard (baseline)maatregelen, het prioriteren van de implementatie van maatregelen en het opstellen van een security roadmap. Een security roadmap is een strategisch plan dat de stappen en acties beschrijft die nodig zijn om de beveiliging van een organisatie te verbeteren en te versterken. Dit omvat doorgaans het identificeren van beveiligingsdoelstellingen, het vaststellen van prioriteiten, het toewijzen van middelen en het bepalen van mijlpalen en deadlines voor het implementeren van beveiligingsmaatregelen. Ook het beoordelen van (tijdelijke) afwijkingen en het accepteren van risico's behoort tot het tactisch proces.

Aangezien zowel de bedrijfsprocessen als de bedrijfswaarden (zoals beschreven in het strategische proces) veranderen, moeten alle bovengenoemde processen overeenkomstig worden aangepast om hiermee in lijn te blijven.

PDCA-cyclus in het tactisch proces
Deze processen moeten antwoord geven op de volgende vragen:

1. Met welke cybersecurityrisico's hebben we te maken en hoe groot zijn deze?
2. Welke maatregelen moeten worden geïmplementeerd om deze risico's te verlagen (tot onder het gestelde tolerantieniveau)?
3. Welke prioriteiten, keuzes en afwegingen worden gemaakt voor de inzet van middelen en het (tijdelijke) accepteren van risico's?

Dit kan o.a. inhouden: het monitoren van gestelde prestatie-indicatoren (KPI's), het uitvoeren van beoordelingen en het identificeren van eventuele afwijkingen van de plannen. Op basis van de bevindingen uit de controlefase worden aanpassingen gemaakt aan de tactische risicobeheersplannen. Dit kan het bijwerken van prioriteiten, het herzien van maatregelen en het nemen van corrigerende acties omvatten om de ***doelstellingen te bereiken en de effectiviteit te verbeteren***.

5.3 Strategisch proces

Het strategisch proces richt zich op de organisatie als geheel en heeft een focus op de lange termijn. Deze processen bepalen de ambities en volwassenheidsniveaus van risicobeheer, vaak in overeenstemming met de kernwaardes van de organisatie. Voorbeelden hiervan zijn nieuwe wet- of regelgeving, aanpassingen in de risicotolerantie (risk appetite) en mogelijke fusies of overnames. In wezen omvat dit alles wat de context of scope van de organisatie beïnvloedt, zoals beschreven in hoofdstukken 2 en 3. Daarnaast stelt het strategisch proces doelen vast voor het beheersen van risico's binnen de organisatie. Strategische ambities of veranderingen in het dreigingslandschap kunnen aanleiding geven tot aanpassingen in dit beleid.

PDCA-cyclus in het strategisch proces
Deze processen moeten antwoord geven op de volgende vragen:

1. Welke bedreigingen rondom cybersecurity zien we die invloed hebben op de missie van onze organisatie? En hoe veranderen deze in de tijd?
2. Wat is ons risicotolerantieniveau en hoe sluit deze aan bij de kernwaarden van onze organisatie?
3. Aan welke wet- en regelgevingen moeten we voldoen?
4. Wat is ons ambitieniveau voor risicobeheer en hoe waarborgen we dat in de organisatie?

Dit kan o.a. inhouden: het vaststellen van nieuwe beleidslijnen, het toewijzen van middelen voor risicobeheer en het opzetten van een raamwerk voor strategische risicobeoordeling. De voortgang van de strategische doelen wordt geëvalueerd aan de hand van meetbare prestatie-indicatoren, bijvoorbeeld KPI's (key performance indicators). Dit omvat het regelmatig monitoren en beoordelen van de effectiviteit van de genomen maatregelen en het bijsturen waar nodig. Op basis van de bevindingen uit de controlefase worden aanpassingen gemaakt aan de strategische benadering van risicobeheer. Dit kan het herzien van strategische doelstellingen, het aanpassen van beleidslijnen, en het nemen van corrigerende maatregelen omvatten om ***de prestaties te verbeteren en te voldoen aan veranderende omstandigheden van zowel intern (binnen de organisatie) als extern (plaats die een organisatie inneemt in de maatschappij en externe eisen aan de organisatie).***

Een algemene aanname is dat de ontwikkeling en toepassing van Artificial Intelligence (AI) de komende jaren zal zorgen voor verbeterde vormen van cyberaanvallen en cyberweerbaarheid, die voorbij zullen gaan de menselijk capaciteit van overzicht en beheersing. Nieuwe technologieën zullen nodig zijn om hier adequaat mee om te gaan.

5.4 Rapportage

Nauwkeurige risicorapportage is van vitaal belang voor het waarborgen van organisatorische veerkracht. Door gebruik te maken van risicoregisters, prestatie-indicatoren en auditbare rapporten kunnen organisaties proactief reageren op cyberdreigingen en het vertrouwen van stakeholders behouden. Up-to-date risicoregisters dienen als gedegen bronnen van geïdentificeerde risico's en bijbehorende beheersmaatregelen, waardoor een grondig inzicht in het dreigingslandschap, zowel intern als extern, mogelijk is.

Prestatie-indicatoren (KPI' s) vormen onmisbare elementen van cybersecurityrisicorapportage. Ze bieden management waardevolle inzichten in de doeltreffendheid van bestaande beveiligingsmaatregelen door meetbare resultaten te leveren. Deze kunnen weergegeven worden in dashboards, heatmaps of scorecards, waardoor ook onderlinge verbanden eventueel 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.

Het management speelt een cruciale rol bij het benutten van deze gegevens voor effectieve sturing van de organisatie. Het is van essentieel belang dat het management deze inzichten gebruikt om de organisatie te leiden naar versterkte veerkracht tegen cyberdreigingen. Door de informatie uit risicorapportage te benutten, kan het management geïnformeerde beslissingen nemen over prioriteiten en middelenallocatie.

Risicorapportage dient ook auditeerbaar te zijn, wat noodzakelijk is voor naleving van regelgeving en verantwoordingsplicht. Auditbare rapporten bieden transparantie en bewijs van zorgvuldigheid bij het aanpakken van cyberdreigingen, wat het vertrouwen van stakeholders versterkt.

5.4.1 Uitdagingen in risicorapportage

Het rapporteren van OT-cyberrisico's aan het hoger management kan uitdagend zijn vanwege de technische aard van het onderwerp en de complexiteit die ermee gepaard gaat. Het is op dit moment lastig om huidige en toekomstige OT-cyberrisico's inzichtelijk te maken, of hoe ze de organisatie kunnen beïnvloeden. Bovendien kunnen beperkte budgetten en middelen het moeilijk maken om deze risico's effectief aan te pakken. Daarnaast kunnen er barrières zijn tussen verschillende afdelingen binnen de organisatie, wat samenwerking op het gebied van cybersecurity bemoeilijkt. Het voldoen aan regelgeving kan nog een extra laag complexiteit toevoegen, en het communiceren van deze risico's op een manier die bij het hoger management aansluit, kan lastig zijn.

Om deze uitdagingen te overwinnen, kunnen organisaties verschillende oplossingen implementeren. Zo kunnen zij educatieve sessies aanbieden om leidinggevenden te helpen OT-cyberrisico's en hun potentiële impact beter te begrijpen. Speciale cybersecuritytrainingen die zijn afgestemd op de behoeften van leidinggevenden kunnen ook nuttig zijn. Het opzetten van multidisciplinaire teams en communicatiekanalen kan samenwerking tussen afdelingen bevorderen. Het uitvoeren van analyses van de organisatie-effecten kan helpen om de mogelijke gevolgen van cyberincidenten te kwantificeren in termen die voor leidinggevenden begrijpelijk zijn, zoals verstoringen van de operaties of financiële verliezen.

Daarnaast kan het zoeken naar begeleiding van cybersecurityexperts waardevolle inzichten en aanbevelingen opleveren. Door deze benaderingen te volgen, kunnen organisaties hun vermogen verbeteren om OT-cyberrisico's aan het hoger management te communiceren en proactieve maatregelen te nemen om ze te beheersen.

Afkortingen en verklarende woordenlijst (in volgorde zoals ze voorkomen)

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

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

I**oT:** Internet of Things - 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.

ICS/IACS: Industriële Controlesystemen / Industriële Automatisering en Controle Systemen - Systemen gebruikt in industrieën om processen te automatiseren, monitoren en regelen, zoals in de productie, energieopwekking en waterbehandeling.

SCADA: Supervisory Control and Data Acquisition - Een systeem voor het controleren en beheren van industriële processen, vaak gebruikt in sectoren zoals energie, transport en productie.

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

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

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

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

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

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

Likelihood: De kans dat een bepaald risico zich voordoet.

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

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

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

Statelijke actor: Een entiteit die handelt namens of onder controle staat van een nationale overheid, en die betrokken is bij cyberaanvallen of spionageactiviteiten op nationaal of internationaal niveau.

Scope: De grenzen en het bereik van een project, onderzoek of activiteit.

RAMSHEEP: Een acroniem dat wordt gebruikt om verschillende categorieën van cyberdreigingen te classificeren.

VLAN: Virtual Local Area Network - Een logisch gescheiden netwerk binnen een fysiek netwerk, waarmee apparaten met elkaar kunnen communiceren alsof ze zich in hetzelfde fysieke netwerksegment bevinden, zelfs als ze zich op verschillende locaties bevinden.

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.

NCSC: Nationaal Cyber Security Centrum - Een organisatie op nationaal niveau die verantwoordelijk is voor het bevorderen van cyberbeveiliging, het monitoren van bedreigingen en het bieden van ondersteuning aan overheidsinstanties en het bedrijfsleven.

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.

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

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

Ransomware: Schadelijke software die computersystemen vergrendelt of gegevens versleutelt, waarbij de aanvaller losgeld eist in ruil voor het herstellen van de toegang tot de systemen of gegevens.

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

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

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.

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

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

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

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

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

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

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

Standaarden:

ISO 27001: Een internationale norm voor informatiebeveiliging die een raamwerk biedt voor het vaststellen, implementeren, beheren en continu verbeteren van een informatiebeveiligingsbeheersysteem (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, als onderdeel van het bredere kader van informatiebeveiliging.

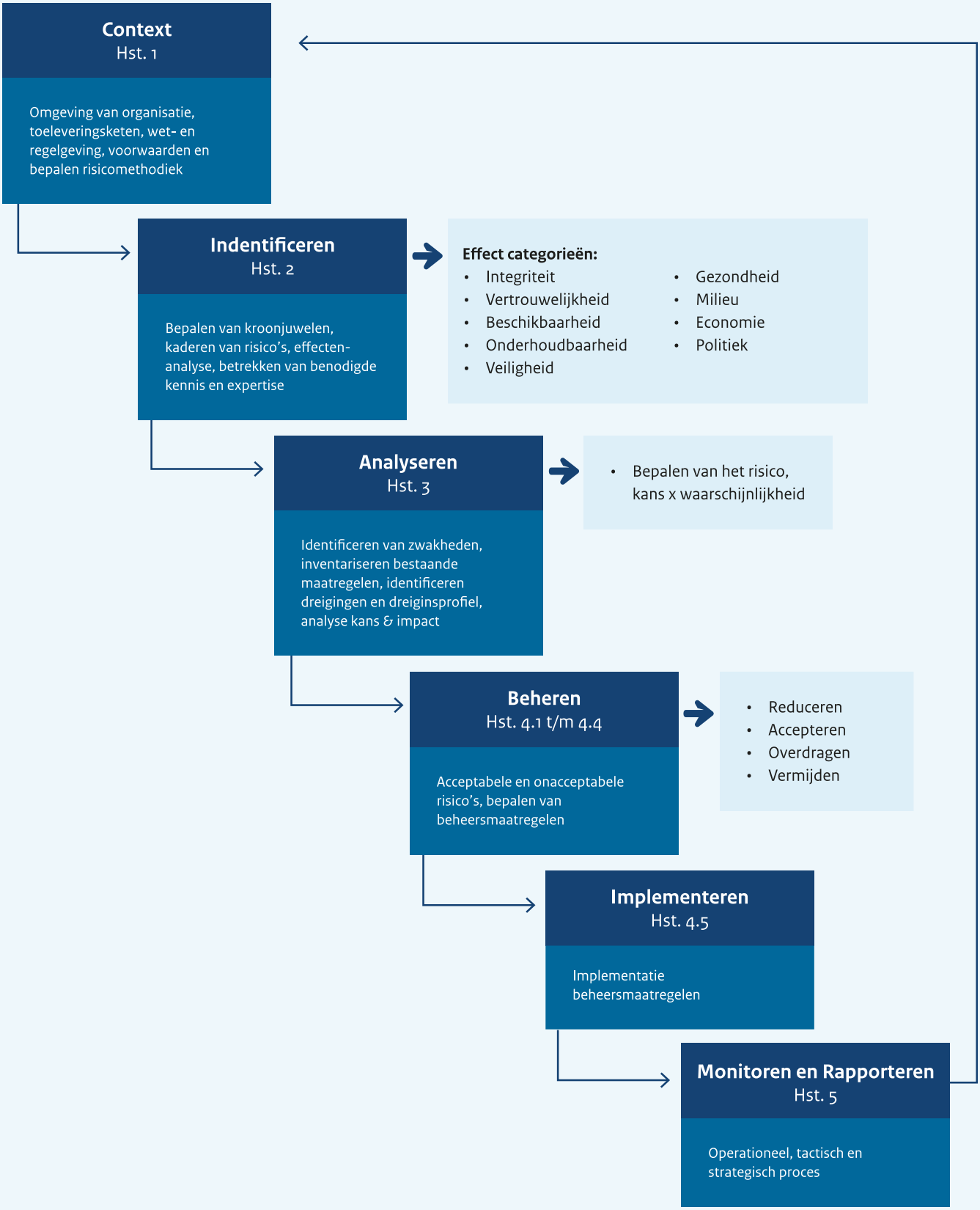
NIST SP 800-30: Een publicatie van het National Institute of Standards and Technology (NIST) die richtlijnen biedt voor het uitvoeren van risicobeoordelingen binnen organisaties, met de nadruk op informatietechnologie en cybersecurity.

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 in deze omgevingen. De delen 2-1, 3-2 en 3-3 van de normenreeks behandelen respectievelijk het ontwerp en de implementatie van beveiligingsmaatregelen voor IACS.

NIS2: De Europese richtlijn inzake de beveiliging van netwerk- en informatiesystemen (NIS) die de veiligheid van netwerk- en informatiesystemen binnen de Europese Unie regelt, met als doel het versterken van de cyberbeveiliging en het verminderen van de impact van incidenten op essentiële diensten en digitale infrastructuur.

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.

Flowchart en structuur van het document



Deze brochure is een uitgave van:

Ministerie van Infrastructuur en Waterstaat
Postbus 20901 | 2500 EX Den Haag
T 070 456 00 00

Mei 2024