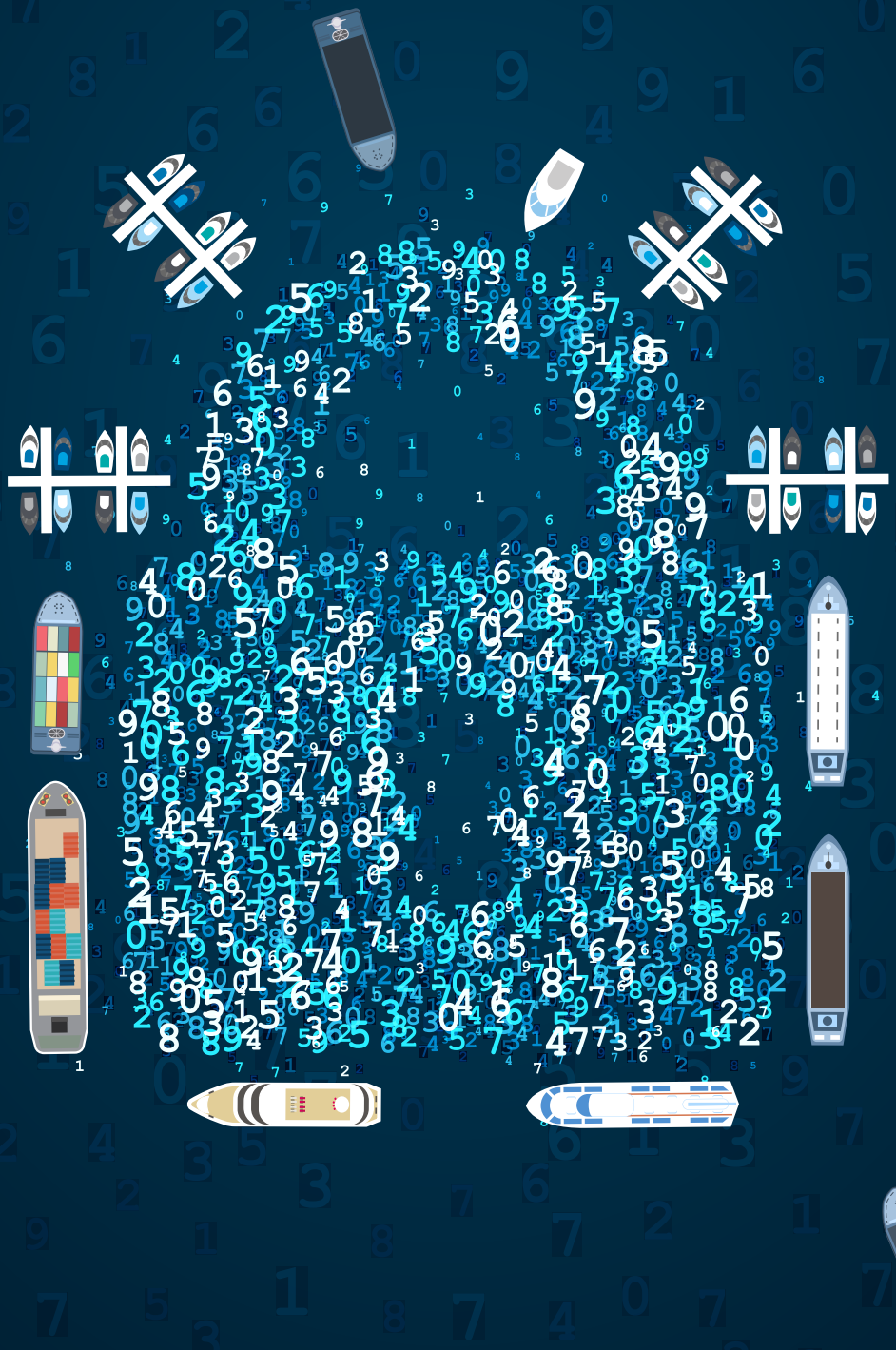
Leidraad good practices

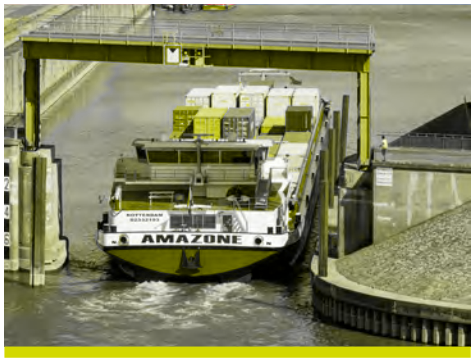
Cybersecurity binnenvaart

Zwaartepunt havens



Inhoudsopgave

Deel 3



Inleiding

Context

Leidraad opgesteld op initiatief van het Europees Comité voor de opstelling van standaarden voor de binnenvaart (CESNI)

Het Europees Comité voor de opstelling van standaarden voor de binnenvaart heeft onder andere de volgende taken:

- goedkeuring van technische standaarden op diverse gebieden, vooral met betrekking tot de schepen, informatietechnologie en bemanningen, waarnaar de respectieve regelgevingen op Europees en internationaal niveau, met inbegrip van die van de Europese Unie en de Centrale Commissie voor de Rijnvaart , kunnen verwijzen voor hun toepassing;
- overleg over onderwerpen die prioritair zijn voor de veiligheid van de scheepvaart, de bescherming van het milieu en andere belangrijke binnenvaartaspecten.

De Verklaring van Mannheim[1], die werd aangenomen door de ministers van verkeer van de lidstaten van de Centrale Commissie voor de Rijnvaart (CCR), en het NAIADES-actieprogramma[2] van de Europese Commissie noemen beide de digitalisering als een onderwerp dat van strategisch belang is voor de toekomst van de binnenvaart. Deze digitalisering gaat echter gepaard met diverse uitdagingen en nieuwe risico's zoals de cybersecurity.

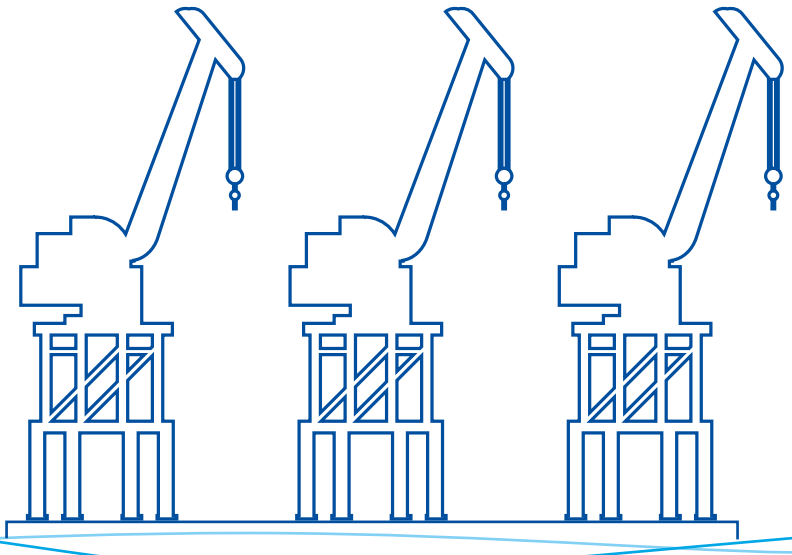
CESNI heeft derhalve besloten om samen met de Europese Federatie van binnenhavens (EFIP) good practices op het gebied van de cybersecurity bijeen te brengen en deze in de vorm van een leidraad aan de binnenhavens ter beschikking te stellen.

Relevantie voor de binnenhavens

Nu de wereld steeds meer onderling verbonden raakt en steeds meer aangewezen is op digitale diensten, neemt ook het aantal cyberaanvallen continu toe. In de afgelopen jaren werden meerdere havens getroffen door cyberaanvallen, waaruit blijkt dat deze sector geen uitzondering op de regel vormt.

In juni 2017 werd bijvoorbeeld de terminal van de onderneming APM op de Rotterdamse Maasvlakte slachtoffer van ransomware. De haven van Rotterdam werd verregaand lamgelegd door het virus en voor de havenactiviteiten kwam dit neer op een uitval van meerdere dagen. De kranen konden niets meer doen en de overslag van containers kwam stil te liggen. De gevolgen van deze cyberaanval waren in het hele ecosysteem van de haven merkbaar, met inbegrip van de maritieme activiteiten; dit was een bevestiging van wat al verregaand bekend was, namelijk dat alle sectoren gevoelig zijn voor cyberbedreigingen en dus niet meer alleen sectoren die volledig afhankelijk zijn van IT.

Nu in havens zoals Rotterdam inderdaad steeds meer via internet en digitaal gedaan wordt en men steeds sterker afhangt van geavanceerde IT-systemen, worden de havens ook gevoeliger voor cyberaanvallen zoals hierboven beschreven.[3]



[1] https://www.ccr-zkr.org/files/documents/dmannheim/Mannheimer_Erklaerung_nl.pdf
[2] https://transport.ec.europa.eu/transport-modes/inland-waterways/promotion-inland-waterway-transport/naiades-iii-action-plan_en
[3] https://www.dutchnews.nl/news/2017/06/smart-port-in-rotterdam-confounded-by-cyber-attack/

Om deze bedreigingen aan te kunnen pakken, zal men een beter begrip moeten krijgen van de cyberrisico's die zich binnen het havensysteem kunnen voordoen. Er zijn natuurlijk ook binnenhavens die voor hun dagelijkse activiteiten werken met computers die niet allemaal via internet met elkaar verbonden zijn. Zij voelen zich wellicht niet meteen aangesproken als het om cybersecurity gaat, maar ook deze havens zullen met verloop van tijd onvermijdelijk steeds meer online met elkaar in verbinding komen te staan. Dan zullen er grotere investeringen nodig zijn om kwetsbare systemen tegen cyberaanvallen te beschermen, zoals complexe software voor havenlogistiek, geïntegreerde camera- en gate-operatingsystemen, softwareprogramma's voor op afstand bestuurde schepen, containermanagementapplicaties en andere 'slimme' technologieën die bedoeld zijn om de efficiëntie van havenactiviteiten te verhogen. Een betere cyberbeveiliging is daarom niet alleen een kwestie van het verbeteren van de beveiliging van computer- en IT-systemen van binnenhavens. Alle partijen die betrokken zijn bij de havenactiviteiten zullen zich sterker bewust moeten zijn van de security-problemen die samenhangen met de diverse, aan elkaar gekoppelde middelen waarmee zij de verschillende havengerelateerde diensten verlenen.

Dit is de ruimere context van deze leidraad, die bedoeld is als een handig vertrekpunt voor good practices met betrekking tot de cybersecurity voor de afhandeling in de binnenhavens[4].

Scope van deze leidraad en enkele adviezen voor het gebruik

In het algemeen zijn er vijf manieren om op een cyberbeveiligingsrisico te reageren:

1. het risico aanvaarden, met andere woorden niets doen en daarvan de gevolgen dragen;
2. het risico vermijden, met andere woorden het volledig wegnemen door drastische maatregelen, bijvoorbeeld een sluis buiten werking stellen, het sluiten van de haven voor de scheepvaart of het verbieden van bepaalde schepen die een bepaald risico kunnen opleveren;
3. het risico overdragen, bijvoorbeeld door een verzekering af te sluiten of door een derde in te schakelen die de gevolgen ervan op zich neemt;
4. het risico delen, met andere woorden een overeenkomst sluiten met derden om de kosten of de gevolgen te delen indien het risico zich daadwerkelijk voordoet;
5. het risico beperken, met andere woorden diverse maatregelen nemen om de kans dat het risico zich voordoet te verkleinen of de gevolgen ervan te beperken.

Deze leidraad gaat in de eerste plaats over **risicobeperking**. Er zijn enige elementen van overdracht of deling van risico's, maar deze zijn slechts in geringe mate aanwezig. Er zij op gewezen dat niets doen op het gebied van cyberbeveiliging de facto neerkomt op het aanvaarden van alle al dan niet geïdentificeerde risico's.

De bedoeling van deze leidraad is om een overzicht te bieden van de risico's, bedreigingen en mitigerende maatregelen op het gebied van de cybersecurity, waarbij de nadruk vooral ligt op de binnenhavens. Het doel is om het doelpubliek (zie hieronder) in staat te stellen te begrijpen wie er schuilgaat achter de cyberaanvallen, wat hun motieven zijn, en welke bedrijfsmiddelen in de havens onder de loep genomen moeten worden om de bedreigingen en risico's op het gebied van de cybersecurity in kaart te kunnen brengen. Deze leidraad biedt tevens een overzicht van good practices voor de tenuitvoerlegging van maatregelen om de risico's op het gebied van de cybersecurity aan te pakken.

[4] https://www.dutchnews.nl/news/2017/06/smart-port-in-rotterdam-confounded-by-cyber-attack/

Om een beter beeld te kunnen geven van het haven-ecosysteem, worden in deze leidraad ook ICT-middelen behandeld die van belang zijn voor de binnenvaartschepen.

Deze leidraad bestaat uit drie delen:

1. het cyberdreigingslandschap voor de binnenhavens: een beschrijving van het hele scala aan bedreigingen voor de havens, met inbegrip van de cyberaanvallers, de ICT-componenten in de havens, een bedreigingsclassificatie en aanvalsscenario's;
2. mitigerende maatregelen tegen cyberrisico's in de binnenhavens: een gedetailleerde beschrijving van de uiteenlopende mitigerende maatregelen die genomen moeten worden om de cyberbeveiligingsrisico's voor havens te beperken;
3. tips voor de implementatie van mitigerende maatregelen: een overzicht van gerichte voorzorgsmaatregelen op het gebied van de cybersecurity, die om te beginnen getroffen kunnen worden door iedereen die bij de IT betrokken is, maar ook andere gebieden omvatten.

Deze leidraad is bedoeld als referentiedocument voor alle bij de havenactiviteiten betrokken partijen, maar vormt geen vervanging voor de bestaande methoden voor de evaluatie van cyberbeveiligingsrisico's. Hij moet alle bij de havenactiviteiten betrokken partijen in staat stellen de meest geschikte maatregelen vast te stellen voor de beoordeling en aanpak van cyberrisico's.

Voor wie is deze leidraad bestemd?

Deze leidraad is in de eerste plaats bedoeld voor havenactoren, namelijk:

- de havenautoriteiten of onderaannemers;
- de terminalexploitanten of onderaannemers;
- de logistiekondernemingen die samenwerken met de havenbedrijven of terminalexploitanten.

Een breder publiek zou echter ook geïnteresseerd kunnen zijn in het lezen van deze leidraad aangezien deze hen indirect aangaat:

- de nationale vaarwegautoriteiten;
- de scheepvaartondernemingen;
- de overheidsinstanties met regelgevende bevoegdheden voor de binnenwateren;
- de scheepsexploitanten;
- de schippers;
- de bemanningsleden;
- de fabrikanten van producten voor de binnenvaart.

Binnen deze grote kring maakt deze leidraad een onderscheid tussen drie doelgroepen die nauw betrokken moeten worden bij de tenuitvoerlegging van de good practices die hier voorgesteld worden:

IT-teams

Operationeel verantwoordelijken

Uitvoerend management

Verwijzingen naar internationale normen en standaarden

Deze leidraad is niet bedoeld ter vervanging van internationale normen en standaarden op het gebied van cyberbeveiliging, of zelfs van bestaande literatuur over dit onderwerp. Doel ervan is onderwerpen op het gebied van cyberbeveiliging onder de aandacht te brengen in een context die specifiek is voor binnenhavens.

Ter concretisering wordt een reeks maatregelen voorgesteld in de vorm van aanbevelingen en good practices die op de markt zijn waargenomen en die aansluiten op de normalisatiebeginselen van ISO/IEC 27001.

De toepassing van deze leidraad vormt op zich geen nalevingsprocedure van standaarden die tot certificering kan leiden. Deze leidraad biedt echter wel een eerste aanzet tot een proces en een bewustwording van cyberbeveiligingskwesties die vervolgens een meer formeel cyberbeveiligingscertificeringsproces (bv. ISO/IEC 27001) aanzienlijk kunnen vergemakkelijken.

Zo is het opzetten van een Information Security Management System (ISMS) een belangrijk punt voor de implementatie van ISO/IEC 27001. Deze norm omvat eisen voor de definitie, documentatie, implementatie, bewaking, onderhoud en voortdurende verbetering van een ISMS. Deze leidraad gaat niet zo uitvoerig op deze punten in, maar biedt wel stappen ter voorbereiding en vergemakkelijking van de invoering van een ISMS, mocht de organisatie of onderneming daartoe besluiten.

Verwijzingen naar nationale voorschriften

Net zomin als deze leidraad bedoeld is ter vervanging van internationale normen en standaarden op het gebied van cyberbeveiliging, vervangt hij evenmin de bestaande regelgeving, met name op nationaal niveau, die zo nodig met voorrang op deze richtsnoeren moet worden toegepast.

Bestaande lokale regelgeving of aanbevelingen van nationale instanties of internationale organen kunnen (of moeten) worden gebruikt om het niveau van cyberbeveiliging in havens te verhogen.

Hoe deze leidraad het beste te gebruiken

Als u deze leidraad leest om een **algemeen beeld te krijgen van de manier waarop de cybersecurity wordt bedreigd in de binnenhavens**, wordt aangeraden dat u eerst Deel 1 van de leidraad leest.

Deel 2 bevat alle maatregelen die voorgesteld worden voor binnenhavens om de risico's die samenhangen met de cybersecurity te verminderen. Zij vormen de kern van deze leidraad, met ongeveer hondertwintig maatregelen die specifiek gericht zijn op de context van binnenhavens en zijn onderverdeeld in drie categorieën:

1. maatregelen die vallen onder beleidsmatige en organisatorische procedures (OPP);
2. beleidsmatige maatregelen die samenhangen met IT en operationele technologieën (ITOT), en tot slot;
3. Technische maatregelen met betrekking tot de cybersecurity (TSM).

Deze maatregelen worden uitgelegd en zijn afgestemd op het maturiteitsniveau ten aanzien van de cybersecurity in elke haven.

Als u deze leidraad leest omdat u meer informatie wilt **over specifieke beveiligingsmaatregelen die u kunt nemen, of om een idee te krijgen hoe de beveiliging in uw organisatie ervoor staat ('cybermaturiteit')**, wordt aangeraden te beginnen met Deel 3 dat erop gericht is de toepassing van de in Deel 2 voorgestelde mitigerende maatregelen te vergemakkelijken. Dit derde deel kan los van de andere delen worden gebruikt als een checklist waarmee u snel kunt zien of uw onderneming of instantie de nodige maatregelen heeft genomen in functie van haar doelstellingen op het gebied van cybersecurity. Het zijn adviezen die toegankelijk en nuttig zijn voor de diverse doelgroepen.

Dit Deel 3 bevat een 'toepasbaarheidstabel', een schema waarmee de in Deel 2 beschreven mitigerende maatregelen gekoppeld kunnen worden aan de cybersecurity-doelstellingen die de haven heeft vastgelegd, en degenen waar de maatregelen voor bedoeld zijn (IT-teams, operationeel verantwoordelijken of algemeen management).

Als u deze leidraad leest als introductie op cybersecurity voor binnenhavens, krijgt u een goed overzicht over dit onderwerp door de leidraad van het begin tot het einde te lezen.

Izmail, Oekraine - Donau

Enkele begrippen die in deze leidraad gebruikt worden

Om deze leidraad goed leesbaar te maken, zijn een aantal begrippen vereenvoudigd.

Havens

Tenzij expliciet vermeld, wordt met 'havens' een binnenvaarthaven bedoeld. Ook gemengde havens vallen onder dit begrip, dat wil zeggen, een haven die zowel zee- als binnenhaven is, tenzij de context zodanig is dat er een onderscheid gemaakt moet worden tussen een haven die uitsluitend binnenhaven is en een gemengde haven.

ICT-middelen

In het kader van deze leidraad worden met 'ICT-middelen' digitale bedrijfsmiddelen bedoeld. Digitale bedrijfsmiddelen kunnen gedefinieerd worden als het geheel van digitale gegevens waarvan het eigendom of het gebruiksrecht deel uitmaakt van het bedrijfsvermogen van een binnenhaven. Deze (digitale) bedrijfsmiddelen of ICT-middelen zijn dus immaterieel. Het kan daarbij bijvoorbeeld gaan om gegevens of software (het begrip 'gegeven' wordt hier in de ruime zin van het woord gebruikt). Er moet op gewezen worden dat ICT-middelen nauw verbonden kunnen zijn met materiële 'klassieke' bedrijfsmiddelen, die - om goed te kunnen werken - daarvan afhangen. Een sluis is bijvoorbeeld een materieel bedrijfsmiddel, maar om te kunnen functioneren is er software nodig en een grote hoeveelheid specifieke gegevens. Elk materieel gedeelte van de sluis, de wanden, de deuren, maar ook de sensoren, de computers, informaticakabels of camera's zijn geen 'bedrijfsmiddelen' zoals bedoeld in deze leidraad. Alle softwareapplicaties (en de parameters daarvan) die door een van deze materiële bedrijfsmiddelen worden gebruikt, zijn digitale bedrijfsmiddelen en dus 'ICT-middelen' zoals bedoeld in deze leidraad.

IT/OT-systemen

In bepaalde delen van deze leidraad wordt er verwezen naar IT/OT-systemen. In deze context heeft de term 'IT' (informatietechnologie) betrekking op het deel van het systeem dat de informatie (de gegevens) verwerkt en in hoge mate programmeerbaar en aanpasbaar is. De term 'OT' (operationele technologie) duidt op het deel van het systeem dat de apparatuur bedient of fysieke processen uitvoert. Het OT-deel is doorgaans zeer autonoom en wordt zodanig geprogrammeerd dat het een specifieke taak kan verrichten (bijvoorbeeld de temperatuur regelen of ventileren). Eenvoudig gezegd: de IT verwerkt de gegevens, terwijl de OT de fysieke objecten bedient. Deze twee systeemtypes kunnen natuurlijk onderling met elkaar communiceren en het is met name in die gevallen dat de term 'IT/OT-systemen' wordt gebruikt.

Cybersecurity: deze term wordt uitgebreid gebruikt in deze leidraad, te beginnen met de titel. In de context van deze leidraad moet de term ‘cybersecurity’ in zeer ruime zin worden opgevat. Het gaat om de toepassing van een reeks technieken, praktijken, middelen en tools om informatiesystemen en hun gegevens te beschermen. Deze bescherming moet ook in de ruimste zin worden opgevat, van preventie tot herstel, via opsporing en reactie op gebeurtenissen. Deze bescherming wordt uitgeoefend tegen cyberdreigingen, die ook verschillende vormen kunnen aannemen. Dit kunnen computeraanvallen zijn, maar ook nalatigheid, ongelukken, natuurrampen of menselijke fouten. Bij ‘cybersecurity’ wordt rekening gehouden met computerbedreigingen, maar ook met bedreigingen die verband houden met fysieke en organisatorische aspecten. Er bestaan andere termen met verschillende betekenissen in verschillende landen en culturen, zoals ‘gegevensbeveiliging’ of ‘beveiliging van informatiesystemen’ of ‘computerbeveiliging’.

Deel 1

Cyberdreigingslandschap van havens

Algemene trends op het gebied van cybersecurity en gevolgen daarvan voor de havens

ENISA, het Agentschap van de Europese Unie voor cyberbeveiliging (European Union Agency for Cybersecurity), heeft in 2020 een rapport over het dreigingslandschap voor zeehavens uitgebracht. Het bevat de volgende conclusies, die met name van belang zijn voor de havensector:

VASTGESTELDE TREND	CONSEQUENTIES VOOR HAVENS
Voor het merendeel van de cyberaanvallen is en blijft financieel gewin de voornaamste drijfveer.	Als hubs voor economische transacties en handelsactiviteiten met mogelijk waardevolle vracht kunnen havens een doelwit worden voor criminelen die uit zijn op financieel gewin.
Doelgerichte en aanhoudende aanvallen op waardevolle gegevens, zoals intellectueel eigendom en staatsgeheimen, worden zorgvuldig gepland en uitgevoerd, vaak door hackers die door een staat worden gesteund.	Als kritieke handelscentra waar onontbeerlijke goederen aankomen, kunnen havens als doelwit worden gekozen om specifieke gegevens te verzamelen over landen die zij beleveren.
Ransomware blijft wijdverbreid en de schade die erdoor wordt berokkend, leidt wereldwijd tot zeer hoge kosten voor tal van organisaties en ondernemingen.	Een ransomware-aanval vormt een reële bedreiging voor de partijen in de operationele keten die vaak afhankelijk zijn van de beschikbaarheid van de systemen binnen de omgeving van havens.
Bij iedere nieuwe fase van digitale transformatie neemt de lijst met mogelijke kwetsbaarheden in een virtuele of fysieke omgeving toe (aangezien de diversificatie in de technologie zal worden voortgezet).	Havens behoren tot de industriële omgevingen die verstrekkende digitale veranderingen ondergaan, met name op het gebied van IT-/OT-convergente technologieën. Naarmate deze veranderingen plaatsvinden, moeten cyberveiligheidsrisico's goed geëvalueerd en ingeperkt worden.

Dit zijn de conclusies die van toepassing zijn op de havencontext en zij wijzen erop dat de problematiek die samenhangt met de cyberbeveiliging beschouwd moet worden als een echt risico voor de kritieke vervoers- en economische activiteiten van de havens. Maatregelen om dit risico tegen te gaan, dringen zich dus op.

De cybersecurity van havens, de belangrijkste ICT-middelen van havens en binnenvaartschepen

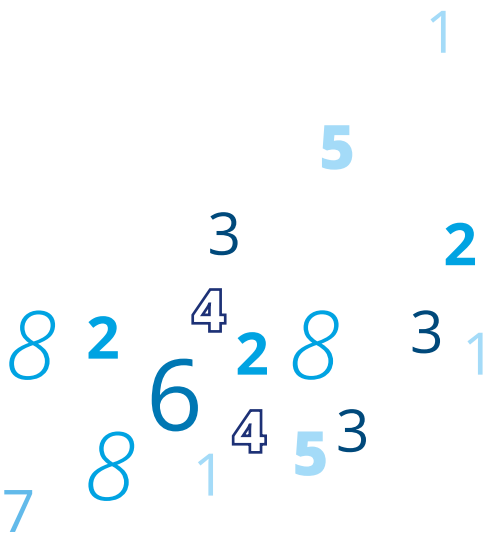
Voordat een onderneming of instantie de mogelijke bedreigingen voor de veiligheid en de manieren waarop de onderneming of instantie zichzelf hiertegen kan beschermen, gaat onderzoeken, moet eerst in kaart worden gebracht wat precies beschermd moet worden. Hiervoor is het nuttig om eerst een overzicht op te stellen met alle ICT-middelen die door een cyberaanval kunnen worden getroffen.

Om deze taak te vergemakkelijken, biedt deze leidraad een kader voor de beoordeling van ICT-middelen van havens en schepen. Hoewel niet al deze ICT-middelen een rol spelen bij of relevant zijn voor de activiteiten van alle lezers, kan de onderstaande lijst toch als benchmark worden gebruikt voor de beoordeling van de ICT-middelen in uw omgeving. Tegelijkertijd is het belangrijk erop te wijzen dat de kwetsbaarheid van de ICT-middelen van bedrijf tot bedrijf kan verschillen. Zo kan bijvoorbeeld voor de ene haven, die gespecialiseerd is in vrachtvervoer, het managementsysteem voor de containerterminal het meest cruciale ICT-onderdeel zijn, terwijl voor een andere haven het centrale managementsysteem van een sluis meer van belang is. Voor havens die voornamelijk actief zijn in de passagiersvaart, kunnen juist die activiteiten als kritiek worden beschouwd. Daarom is het uitvoeren van een algehele scan van de ICT-middelen de eerste stap die gezet moet worden om het begrip van de beveiligingsrisico's te vergroten en tegenmaatregelen te nemen. Het doel is dus de ICT-middelen die kritiek zijn voor uw organisatie, te identificeren en op te nemen in een lijst van '**kroonjuwelen**' (ICT-middelen waarvoor het hoogst mogelijke beveiligingsniveau moet worden gewaarborgd).

Wat de havens betreft kan vastgesteld worden dat er in sommige gevallen steeds meer industriële controlesystemen (Industrial Control Systems - ICS) ingezet worden, waaronder de SCADA-systemen (Supervisory Control and Data Acquisition - SCADA) waarin industriële systemen en apparatuur verbonden zijn met netwerken om beheer op afstand of vanaf de wal mogelijk te maken. Hoewel mechanische bedrijfsmiddelen zelf niet rechtstreeks door cyberaanvallen worden bedreigd, zijn zij wel toegankelijk via het netwerk en maken zij gebruik van verouderde systemen (die niet meer door de leveranciers worden geüpdatet). Bovendien kunnen ICS worden gebruikt om toegang te krijgen tot andere ICT-middelen, die het werkelijke doelwit zijn. Daarom mogen deze bedrijfsmiddelen niet ontbreken op de lijst met kritieke ICT-middelen.

Parijs, Frankrijk - Seine

De lijst hieronder beschrijft de belangrijkste ICT-middelen van havens, alsook enkele ICT-middelen aan boord van schepen, met name die middelen die op een bepaald moment verbonden kunnen worden met de systemen van de havens.



Belangrijkste ICT-middelen in havens

Havens binnenvaren en aanleggen van schepen
Dit betreft het binnenvaren en aanleggen van het schip in de haven. Dit omvat onder andere rivier-infrastructuursystemen zoals bedieningssystemen van bruggen en sluizen (Lock Bridge Management - LBM), aangesloten sensoren en mechanismen van bruggen en sluizen en verkeersplanningsystemen.

Systemen voor passagiersschepen en toerisme
Webapplicaties voor het boeken van toegangsbewijzen voor passagiersschepen zijn kritisch voor havens met veel toerisme en zijn bijzonder kwetsbaar omdat deze applicaties toegankelijk zijn voor het publiek. Zonder toegang tot deze systemen zouden de toeristische activiteiten worden verstoord of stil komen te liggen, met alle significante economische gevolgen van dien voor de partijen of partners van de havens.

Ligplaatsen voor schepen
Tools en processen waarmee schepen die de haven aandoen brandstof kunnen innemen, voedselvoorraden kunnen aanvullen en drinkwater tanken, reparaties aan het schip kunnen laten uitvoeren, enz.

Energievoorziening
Beheertools en IT-applicaties voor de monitoring en bediening van stroomkabels, apparatuur, centrales en stroomnetwerken, oftewel alle installaties die vereist zijn voor de levering van stroom aan de havens en de haveninfrastructuur.

Beveiliging en veiligheid
Alle tools die bijdragen tot de fysieke beveiliging van de havengebieden zoals aangesloten gates, CCTV/ camerasystemen, aangesloten deuren en doorgangen, badge-systemen, aangesloten alarmsystemen, wachtposten.

IT-systemen die een rol spelen bij de verkeersplanning, zoals verkeersbegeleiding voor de scheepvaart (Vessel Traffic Service - VTS)
De VTS-controlecentra in de havens vormen een centraal onderdeel van de havenactiviteiten en maken vaak gebruik van een internet- of VHF-verbinding, met als gevolg dat ze een mogelijk doelwit van cyberaanvallen worden.

Automatic Identification System (AIS)
Een systeem voor de automatische uitwisseling van berichten tussen schepen via VHF-radiotransmissie waarmee schepen en verkeersbegeleidingssystemen de identiteit, status, positie en route van schepen in het vaargebied kunnen zien.

Containeropslag en het stapelen van containers
Vrachtbeheer (Cargo and fleet management - CFM), tools voor het lossen en de opslag van containers zoals software voor het verplaatsen, opslaan en afhandeling van containers, tools voor het verwerken en sorteren van bulkmateriaal, koelcontaineropslag- en monitoring-tools, enz.

Autoriteiten en douanediensten
Tools voor de aangifte van goederen en de berekening van de hoogte van de te betalen douanerechten, de verkrijging van toestemmingen van de douaneautoriteiten, het verstrekken en indienen van aangifteformulieren, het stellen van vragen aan de bevoegde instanties en regelingen rond de beantwoording daarvan.

Supportservice
IT-hardware, -software, -applicaties van de haven, communicatiesystemen van het havenpersoneel, applicaties voor het beheer van vastgoed en bedrijfsmiddelen, software voor het beheer van gevaarlijke goederen en koelinstallaties. ICT-middelen van een supportservice omvatten ook de `systemen voor passagiersschepen en toerisme' (zie specifieke definitie).

Distributiediensten
Aangesloten tools die zorgen voor de overslag van containers of bulkgoederen naar rangeerstations, systemen voor het vervoersknooppunt ter aanvulling op de distributie zoals containercontrolesystemen en communicatieplatforms voor de distributie. Dit omvat tevens tools die hiermee verbonden zijn, zoals bij spoorwegstations en wagons voor het vervoer van containers.

ICT-middelen aan boord van schepen

Opmerking

Met uitzondering van de ICT-middelen voor de communicatie tussen het schip en de haven en andere plaatsen aan de wal, wordt de ICT aan boord van het schip zelf niet in deze leidraad behandeld.

River Information Services (RIS)
Tracking en tracing van schepen in de binnenvaart (Inland AIS), systeem voor elektronische weergave van binnenvaartkaarten en de daaraan verbonden informatie (Inland Electronic Chart Display and Information System - Inland ECDIS), berichten aan de scheepvaart (Notices to Skippers for Inland Navigation - NtS), elektronisch melden van schepen in de binnenvaart (Electronic Ship Reporting in Inland Navigation - ERI).

Installaties
Elektronische en IT-installaties van schepen waaronder de voortstuwings- en machine-installaties, stroommanagementsystemen, systemen in het stuurhuis, alsook brandstof-, batterij- en ladingcontrolesystemen.

Operationele ICT-middelen
ICT-middelen die ervoor zorgen dat de apparatuur die nodig is voor de havenactiviteiten, waaronder pc's, laptops, tablets en de bijbehorende bedrijfsapplicaties, aan boord en elders kan functioneren.

Communicatietechnologie en communicatiemiddelen van de bemanning
Apparatuur voor radio- en satellietcommunicatie en andere aangesloten apparaten die de verbinding tussen het schip en de wal vergemakkelijken; mobiele telefoons, computers en tablets die door de bemanning zowel aan boord als aan land worden gebruikt.

Lading
Tools die gebruikt worden om informatie over de status van de lading aan boord te verstrekken en om met de wal te communiceren als het gaat om het lossen, de inhoud en het soort vracht.

Bedreigingsclassificatie voor havens

Zodra men een overzicht heeft opgesteld van kritieke ICT-middelen van een haven, of systemen die beschadigd kunnen raken door een cyberaanval, kan onderzocht worden voor welke soort bedreigingen deze componenten en systemen kwetsbaar zijn.

Een cyberbedreiging is elke omstandigheid of gebeurtenis die een negatief effect kan hebben op bedrijfsactiviteiten, organisatorische ICT-middelen, personen, andere bedrijven of het openbaar belang. Het kan bijvoorbeeld gaan om niet-geautoriseerde toegang, het vernietigen, vrijgeven of wijzigen van gegevens en/of denial of service. Een bedreiging kan worden vastgesteld door de kwetsbaarheid van een haven te correleren met de beweegredenen van cybercriminelen.

Daarom moet men, om de bedreigingen te kunnen beoordelen, beginnen met een nauwkeurige omschrijving van de cybersecurity-kenmerken waar een ICT-middel over moet beschikken. De basiskenmerken van cybersecurity-beveiliging zijn beschikbaarheid (availability), integriteit (integrity) en vertrouwelijkheid (confidentiality), beter bekend als de CIA Triad of 'BIV-classificatie'.

Voor de havens en schepen is het begrip **controle (possession)**[5] als beveiligingskenmerk toegevoegd. In de onderstaande tabel worden de vier belangrijkste kenmerken van cyberbeveiliging beschreven die een rol spelen in het ecosysteem van een haven.

Cyberbeveiligingskenmerken

Vertrouwelijkheid

De informatie en gegevens die door de ICT-middelen in de haven worden verzonden, blijven indien nodig vertrouwelijk. Onbevoegde gebruikers kunnen geen toegang krijgen tot de gegevens en kunnen deze niet downloaden of doorsturen.

Controle

Alleen bevoegd personeel heeft operationele controle over de ICT-middelen van havens en schepen. Het is van cruciaal belang voor de havens en schepen dat zij de controle behouden over de schepen, installaties en andere aangesloten apparatuur. Wanneer iemand de controle over een systeem aan boord van het schip of een operationele uitrusting overneemt die van fundamenteel belang is, is dat net zo goed een zorgwekkend bedreigingsscenario als de elders beschreven scenario's.

Controle verschilt van integriteit, omdat het hier gaat om een fysieke (en niet een virtuele) controle. Het is namelijk zo dat, vergeleken met andere omgevingen waar uitsluitend wordt gewerkt met digitale componenten, de havens informatietechnologie (IT) met operationele technologie (OT) combineren om zowel fysieke als digitale diensten te kunnen aanbieden. Misbruik van deze fysieke diensten kan verstrekkende gevolgen hebben die niet alleen financieel van aard kunnen zijn, maar ook afbreuk kunnen doen aan de reputatie van een haven; bovendien kunnen er zelfs gewonden of doden vallen.

Beschikbaarheid

De nodige informatie, applicaties, tools of apparatuur voor de activiteiten van havens en schepen zijn beschikbaar. Het moet gewaarborgd zijn dat zij goed functioneren op de (bij voorbaat vastgelegde) momenten waarop er een beroep op wordt gedaan. In het kader van beschikbaarheid wordt ook de weerbaarheid gemeten, dat wil zeggen de tijd die nodig is om een systeem of dienst na een incident weer in werking te stellen (in nominale of gedegradeerde modus).

Integriteit

De informatie die via applicaties, tools of apparatuur voor de activiteiten van havens en schepen wordt verstrekt, is nauwkeurig en juist: tussen het verzenden en ontvangen van de gegevens is er niets gewijzigd in de inhoud. Integriteit omvat tevens dat gewaarborgd is dat de informatie onweerlegbaar is, dat wil zeggen dat er een niet te vervalsen bewijs is dat de informatie wel degelijk is geproduceerd of gevalideerd door een specifieke entiteit.

[5] Het begrip 'controle' is toegevoegd op basis van de richtsnoeren voor good practices "Cyber Security for Ports and Port Systems (2020)" van het Institution of Engineering and Technology.

Mogelijke dreigingsactoren

Cyberdreigingsactoren kunnen opzettelijk of onopzettelijk schade veroorzaken aan digitale systemen of netwerken.
In deze leidraad worden de mogelijke dreigingsactoren beschreven en onderverdeeld in zeven categorieën:

Type actor	Activiteit	Voorbeelden van de toepassing ervan binnen de binnenvaart
Medewerker met kwade bedoelingen of slecht getrainde of niet-gesensibiliseerde medewerker	Deze 'aanvaller' houdt zich (bewust of onbewust) niet aan elementaire cyberhygiëne en heeft al dan niet kwaad in de zin. Hoe het ook zij, door zijn handelingen wordt de onderneming in gevaar gebracht, of dit nu doelbewust is of door nalatigheid.	Door te klikken op een onveilige link in een e-mail die door een cyberaanvaller is verstuurd, worden schadelijke bestanden automatisch op de IT-systemen van de haven gedownload.
Cybercrimineel	Gedreven door financieel gewin gaat deze actor over tot diefstal, smokkel van mensen en goederen, belastingontduiking, vernieling.	Communicatie onderscheppen om containers te stelen of te smokkelen zonder douanerechten te betalen, het ontvreemden van lading op een schip, of het plegen van een ransomware-aanval waarbij IT-middelen van de haven worden geblokkeerd tot er losgeld is betaald.
Concurrenten	Gemotiveerd door de wens bedrijfs- of marktinformatie te verkrijgen, proberen deze hackers informatie te onderscheppen om zich een economisch voordeel te verschaffen ten opzichte van de concurrentie.	Het verkrijgen van vertrouwelijke informatie over havenmanagementprocessen voor eigen bedrijfsdoeleinden.
Activist of 'hacktivist'	Een vorm van burgerlijke ongehoorzaamheid waarbij de (h)activist gebruik maakt van het internet om uit ideologische motieven aanvallen te plegen of aandacht te vragen voor een specifiek doel.	Als uiting van protest wordt een schip zo bestuurd dat het de ingang van een haven blokkeert. Een kunstwerk op de waterweg (brug, sluis, enz.) wordt gemanipuleerd om het systeem te verstoren.
Nationale staat	Deze actoren opereren namens een nationale staat of een andere soevereine regeringsstructuur en willen een vorm van oorlog voeren (al dan niet openlijk) door activiteiten te verstoren of stil te leggen.	Het uitvoeren van denial-of-serviceaanvallen op ICT-middelen van havens om de toegang tot een rivier of een deel van de vaarweg, zoals een schutsluis, te blokkeren.
Terrorist	Het gebruik van internet om angst te zaaien of een zekere economische chaos of materiële schade te veroorzaken.	De controle over een schip bemachtigen om een haven schade te berokkenen of slachtoffers te maken. Onderscheppen van informatie over de aankomst van gevaarlijke goederen om daarmee een chaotische situatie te veroorzaken.
Spionage	Via aangesloten apparatuur worden vertrouwelijke of gevoelige gegevens buitgemaakt voor doorverkoop of om in het geheim informatie te leveren aan anderen. Het kan hier gaan om spionage door andere staten of concurrenten.	Een andere staat verzamelt informatie over een gevoelige lading die op weg is naar de haven (bijvoorbeeld vaccins en medische apparatuur). Het bespioneren van activiteiten in de haven voor concurrentiedoeleinden.

Sommige voorbeelden in de bovenstaande tabel, zoals de terroristische dreiging, zijn externe bedreigingen die buiten de scope van deze leidraad vallen, aangezien de havens op hun niveau geen gerichte maatregelen kunnen treffen om dit soort risico's tegen te gaan. In het kader van de coördinatie op het gebied van de cybersecurity tussen de havens en de andere bij de binnenvaart betrokken partijen, moet er echter wel rekening worden gehouden met deze dreigingen.

Een laatste belangrijke opmerking is dat de beweegredenen, financiële middelen en vastberadenheid van de bovengenoemde dreigingsactoren sterk kunnen verschillen. Hackers met sterke banden met staten die warfare- en spionagecampagnes uitvoeren, kunnen over omvangrijke financiële middelen beschikken. Een recente studie van ENISA, waarin een overzicht wordt gegeven van de trends op het gebied van cyberspionage[6], toont aan dat het aantal door een staat gesteunde hacks sterk toeneemt. Uit deze studie van 2020 blijkt dat circa 38% van de kwaadwillende aanvallers in opdracht van staten handelt en 11,2% van de cyberincidenten het gevolg was van cyberspionage.

[6] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage

In deze studie worden de risico's voor de platforms voor grondstoffenvervoer onder de aandacht gebracht. De binnenhavens worden niet uitdrukkelijk genoemd, maar beantwoorden aan de beschrijving en zijn vaak van cruciaal belang voor de economische activiteit in een land. Tegen die achtergrond benadrukt de studie dat de staatsgesponsorde aanvallen toenemen, met name in de sector openbare diensten, de aardgas- en oliesector en de industrie. Dit soort bedreigingen, die worden gesteund door landen, mogen niet worden onderschat, want het zijn goed gefinancierde campagnes waarbij hooggeschoold personeel meedogenloos te werk gaat en het doel heeft zeer veel schade aan te richten.

Bedreigingsclassificatie

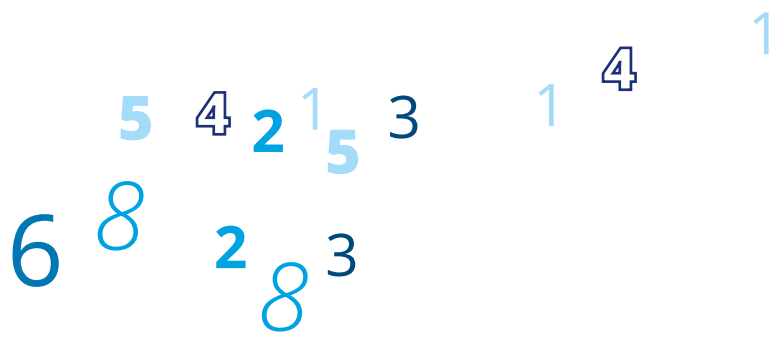
Aan de hand van de hierboven beschreven informatiebeveiligingskenmerken en cyberaanvallers kunnen een aantal bedreigingsscenario's worden vastgesteld. Op basis van die scenario's kan een bedreigingsclassificatie voor de haven worden opgesteld of een lijst van bedreigingen waarvoor een haven het meest kwetsbaar is en dat in functie van de kenmerken van de haven. Een bedreigingsclassificatie geeft een overzicht van de soorten cybersecurity-voorvallen die tot mogelijke schadelijke gevolgen zouden kunnen leiden. De volgende soorten bedreigingen zijn vastgesteld aan de hand van een uitgebreid literatuuronderzoek waarin is gekeken naar de bestaande bedreigingen voor schepen en zeehavens. De onderstaande bedreigingsclassificatie houdt echter rekening met het ecosysteem van een haven.

Toegepast op havens	Voorbeeld
Systeemuitval, storingen Apparatuur of systemen die nodig zijn voor de havenactiviteiten worden aangetast en kunnen niet meer optimaal werken.	Het besturingssysteem van sluizen of bruggen wordt door een 'denial-of-service'-aanval aangetast, waardoor niets meer kan bewegen en alle sluis- en brugactiviteiten stil komen te liggen.
Aanvallen op fysieke bestanddelen Een cyberaanval die ook gericht is op een operationeel technologiesysteem (OT), waardoor de fysieke controle over de machine in handen van de cybercriminelen komt om de machine voor fraude, sabotage, vandalisme, diefstal, terrorisme, hacktivisme of onbevoegde toegang te misbruiken.	Door een geavanceerde en aanhoudende cyberaanval (Advanced Persistent Threat - APT) wordt de controle over het voortstuwingssysteem van een schip overgenomen en het schip gebruikt om een haven in te varen voor terroristische doeleinden.
Afluisteren, onderscheppen, sessiehijacking Kwaadaardige activiteiten in het netwerk die gericht zijn op het onderscheppen van gevoelige gegevens of netwerkverkeer of de hijacking van een gebruikerssessie.	De gegevens die zijn opgeslagen in de applicatie voor het containerbeheer, met informatie over containers met gevaarlijke goederen, worden door terroristen onderschept om deze goederen te stelen.
Spoofing en jamming van informatie Vervalsen van een bericht of gegevensbron (verzender van een SMS, GPS-positie) om het erop te laten lijken alsof de informatie van een bekende, vertrouwde bron afkomstig is, terwijl het in feite gaat om informatie die gemanipuleerd of verzonnen is door de aanvaller.	GPS-informatie wordt gespooft om een verkeerde locatie weer te geven, waardoor het scheepsvervoer in gevaar komt.
Ramp Schade aan het ecosysteem van de haven veroorzaakt door milieu- of natuurrampen als gevolg van het misbruik van geïntegreerde ICT-middelen van de haven.	Een hacker knoeit met de applicatiegegevens van het containermanagementsysteem waardoor de overslag van containers met gevaarlijke goederen niet volgens de voorschriften verloopt. Dit kan op zijn beurt leiden tot een brand in de haven waarbij ernstige materiële schade aan de infrastructuur van de haven kan ontstaan.
Onderbrekingen of wegvallen van bedrijfsmiddelen Leveringen en dienstverleningen aan havens die nodig zijn voor de uitvoering van activiteiten worden onderbroken. Het gaat daarbij onder meer om netwerken, personeel, brandstof, water en elektriciteit.	Een grootschalige aanval op een aangesloten stroomnet leidt tot een grote stroomuitval en een onderbreking van de havenactiviteiten waardoor het vervoer van goederen vertraging oploopt.
Onopzettelijke schade Beschadiging van gegevens, systemen of fysieke infrastructuur van de haven als gevolg van onbewuste manipulaties van binnenuit.	Een medewerker downloadt een bestand met ransomware waardoor het gehele IT-systeem van de haven wordt gegijzeld. Op het bevroren scherm wordt gevraagd om losgeld.

Mogelijke gevolgen

Cyberbedreigingen worden als 'dreigend' ervaren, omdat er daadwerkelijk schade kan ontstaan als een onderneming of instantie wordt getroffen door een cyberaanval. Indien de hierboven beschreven cyberbeveiligingsprincipes niet worden nageleefd, kan dit zeer uiteenlopende gevolgen hebben voor de haven of de betrokken ondernemingen of instanties. Hieronder volgt een overzicht van de soorten gevolgen die cyberaanvallen met zich mee kunnen brengen.

Welke gevolgen	Details
Reputatieschade	Door een data-inbreuk of cyberincident kunnen de naam en het merk van een onderneming of instantie blijvend imagoschade oplopen. Reputatieschade is moeilijk in te schatten, omdat het vaak om immateriële schade gaat, maar het brengt wel verschillende indirecte gevolgen met zich mee zoals uitgaven om het vertrouwen van de klant terug te winnen, meer opgelegde beveiligingsmaatregelen en derving van inkomsten.
Financiële schade	De onderneming of instantie kan na een cyberincident voor aanzienlijke kosten komen te staan, waaronder de uitgaven voor het herstel van de beschadigde systemen en de kosten voor het uitgevoerde crisismanagement, advocatenkosten, hogere verzekeringspremies, verlies van goederen en kosten als gevolg van vertraging bij de uitvoering van de havendiensten.
Sanctievoorschriften	Als gevolg van een cyberincident kunnen sancties worden opgelegd zoals geldboetes en maatregelen voor een grotere aansprakelijkheid van de onderneming in kwestie.
Vernieling van eigendommen	Als gevolg van een aanval op de IT-systemen van een haven kan digitaal eigendom vernietigd worden zoals gegevens en informatie als er geen goede back-up is gemaakt. Daarnaast kan een cyberaanval ook leiden tot de vernietiging van fysiek eigendom zoals IT-hardware en SCADA-systemen, alsook vaartuigen van de haven, operationele installaties in de havens, containers en de inhoud van containers.
Gewonden of doden	In het geval van een cyberaanval met een terroristisch oogmerk kunnen mensen gewond raken of zelfs de dood vinden. Er kan een overstroming worden veroorzaakt als gevolg van een storing bij de sluizen. Gevaarlijke stoffen kunnen tot ontploffing worden gebracht.
Criminele activiteiten: fraude, illegale handel	Cybercriminelen kunnen gebruik maken van verschillende aanvalstechnieken zoals het onderscheppen van netwerkverkeer om informatie te verkrijgen en illegale activiteiten te ondernemen zoals illegale handel in verboden middelen of goederen in containers of mensensmokkel.
Diefstal van eigendommen	Criminelen kunnen aanvalstechnieken gebruiken als middel om in de haven een diefstal te plegen: containers, inhoud van containers, goederen of materiaal (machines, voertuigen, onderdelen…).
Milieuramp	Als door een cyberaanval verkeerd wordt omgaan met gevaarlijke goederen of brandstof, kan dat een milieuramp in de binnenwateren tot gevolg hebben.



Voorbeelden van aanvalsscenario's voor havens

Dit deel beschrijft een drietal praktijkvoorbeelden van aanvalsscenario's voor een aantal van de hierboven genoemde bedreigingen, met voor elk voorbeeld diverse beweegredenen en mogelijke cyberaanvallers. De bedoeling van dit overzicht is concrete voorbeelden te geven van de verschillende situaties waarin de veiligheid van de hierboven beschreven ICT-middeleninfrastructuur in het geding kan zijn. Elk aanvalsscenario is gebaseerd op een echte aanval die een aantal jaren geleden heeft plaatsgevonden en is aangepast aan de situatie in een haven.

Lyon, Frankrijk - Saône

Wijk bij Duurstede, Nederland - Amsterdam-Rijnkanaal

Scenario 1

Het infiltreren van het besturingssysteem van machines

Twee hackers konden in 2013 binnendringen in het systeem voor de bediening van een kleine dam in de staat New York.[7] De dam die gebruikt wordt om een stormvloed tegen te houden, werd bediend door een SCADA-systeem dat via een mobiele modem rechtstreeks met het internet was verbonden. Het systeem gebruikte deze internetlink om status- en operationele gegevens te verstrekken (waterstanden, enz.). Zo kon het personeel de sluissystemen op afstand bedienen, waarmee de waterstanden alsook de waterafvoersnelheid worden geregeld. Het lukte de hackers echter niet om de sluizen effectief te bedienen, omdat deze op dat moment toevallig wegens onderhoudswerkzaamheden niet met het systeem verbonden waren. Dit aanvalsscenario waarin installaties voor kritieke havenactiviteiten, zoals het sluismechanisme, worden verstoord of overgenomen, is een typisch voorbeeld van een scenario dat ook havens kan treffen. Een dergelijke aanval zou grote gevolgen kunnen hebben voor de veiligheid van de scheepvaart, alsook aanzienlijke economische gevolgen.

Dit aanvalsscenario zou zo door cyberaanvallers kunnen worden overgenomen en toegepast om voorzieningen van havens aan te vallen, zoals bijvoorbeeld stroomnetwerken, waterzuiveringsinstallaties, het besturingssysteem van een sluis, enz..

[7] https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

Hieronder worden de belangrijkste stappen beschreven van een malware-infectie van een industrieel controlesysteem, zoals bij de hierboven beschreven mogelijke aanval, en voor andere aanvalsscenario's voor industriële controlesystemen (Industrial Control Systems - ICS).

Stap 1 – Infiltratie

Een kwaadwillende slaagt erin de aangesloten systemen te infecteren. Hiervoor gebruikt de hacker een extern apparaat zoals een USB-stick, een link waarop geklikt kan worden, een downloadbaar bestand of simpelweg een externe internetpagina. In het geval van een USB-stick wordt deze in een computer geplugd, zodat het stukje programmatuur in de stick zich kan verspreiden door het hele computernetwerk.

Stap 2 – Spionage

De malware nestelt zich in de systemen van de onderneming, bespioneert de netwerkcommunicatie en zoekt wegen om zich te kunnen vermenigvuldigen en te verspreiden.

Stap 3 – Sabotage van de beveiligingsprocessen

De malware identificeert zwakke plekken of achterdeurtjes in de software, zodat mechanismen om indringpogingen en mogelijke bedreigingen te detecteren, kunnen worden omzeild. De malware blijft ongemerkt dankzij aanvallen die zorgen voor een geleidelijke aantasting van de besturingssystemen en, bij een stroomnetwerk van een haven, de programmeerbare logische eenheden (programmable logic controllers - PLCs) die in de operationele technologiesystemen zitten. Door de infiltratie van het systeem wordt het wellicht mogelijk operationele functies aan te sturen, zoals sensoren die de waterdruk controleren of zelfs ventielen te openen of te sluiten.

Stap 4 – Controle uitoefenen

De malware kaapt de functies die de PLC zou moeten uitvoeren, bijvoorbeeld door de binnenkomende gegevens of de interne programmatuur te manipuleren. In het geval van een sluis tussen twee havendokken zou de PLC bijvoorbeeld de opdracht kunnen geven om de sluisdeuren te openen op basis van onjuiste gegevens over de waterstanden aan weerszijden, wat tot een gevaarlijke situatie zou leiden. Als de malware de functies openen en sluiten zou omkeren voor een van beide deuren, zouden beide sluisdeuren gelijktijdig kunnen openen.

Stap 5 – Concrete handelingen

De hacker misbruikt het systeem om een bepaalde handeling uit te voeren en wil daarmee een bepaald doel bereiken. In het hierboven beschreven geval wordt bijvoorbeeld, in plaats van de sluisdeur stroomopwaarts te sluiten, de sluisdeur stroomafwaarts opengezet op het moment dat er zich in de sluiskolk een groot samenstel bevindt. Hierdoor zou het samenstel met grote kracht stroomafwaarts worden meegevoerd door het water, met gewonde of dode bemanningsleden tot gevolg. Daarnaast zou er door de grote kracht van het water ook materiële schade kunnen worden berokkend aan de schepen in het samenstel, alsmede schade voor of achter de sluis.

Stap 6 – Vermenigvuldiging

De malware vermenigvuldigt zich om andere apparatuur of systemen aan te vallen. Bij het voorbeeld van de sluis tussen twee stroomgebieden richt de malware zich ook op andere PLC-systemen in de buurt.

Scenario 2

Het manipuleren van gegevens om drugssmokkel te vergemakkelijken

Belgische en Nederlandse autoriteiten hebben in 2013 een tiental verdachten opgepakt die geprobeerd hadden meer dan duizend kilo cocaïne en duizend kilo heroïne in containers te smokkelen.[8] Met ondersteuning van hackers werden de computersystemen van het havenbedrijf gekraakt, zodat de criminelen toegang kregen tot de computers van de containerterminal en zelf de containers met hun verdovende middelen konden identificeren en volgen. Hun aanpak, die binnen de context van een haven goed denkbaar is, was als volgt:

Namen, België - Maas

Stap 1 - Digitale inbraak

De crimineel stuurt e-mails naar medewerkers van de containerterminal met kwaadaardige bijlagen waar downloadbare software in zit, zodat de crimineel spyware op de computers van de medewerkers kan installeren.

Stap 2 - Controle

De crimineel neemt de controle over geïnfecteerde computers over en krijgt zo toegang tot de managementsystemen en/of databanken voor de containers.

Stap 3 - Monitoring

De containers die worden gebruikt voor de smokkel van drugs, worden in het systeem geïdentificeerd en getagd om de verplaatsingen te kunnen volgen. Zo kunnen de criminelen hun smokkelwaar in de gaten houden en weten ze wanneer er controles gepland zijn (scans, röntgenfoto's, controles, enz.).

Stap 4 - Ophalen

De criminelen gebruiken hun toegang tot het containermanagementsysteem om een containerterminal uit te zoeken en een tijdstip te bepalen van de levering. Zo kunnen de criminelen eerder bij de container zijn dan het havenpersoneel en dus hun illegale drugspartij op tijd ophalen.

De belangrijkste conclusie die uit deze benadering getrokken kan worden, is dat de controle over de applicaties van het containersysteem door een onbewuste fout van een medewerker begon. Alle studies zijn het erover eens dat social engineering, en meer in het algemeen de 'menselijke factor', de belangrijkste risicofactor vormt als het gaat om cybersecurity en dat deze factor doorgaans wordt onderschat. De cijfers lopen uiteen, maar de menselijke factor zou in minstens één op twee gevallen de hoofdfactor zijn.

Deze casestudy laat zien hoe door het downloaden van een schadelijk bestand medewerkers hun onderneming en werkgever in gevaar brengen door criminele activiteiten in de hand te werken. Alleen opleidingen en een regelmatige sensibilisering van de medewerkers kunnen ervoor zorgen dat de invloed van de 'menselijke factor' in een onderneming steeds minder een risico vormt.

[8] https://www.europol.europa.eu/sites/default/files/documents/cyberbits_04_ocean13.pdf

Scenario 3

Het jammen van AIS-apparatuur

Een Inland AIS-apparaat wordt gebruikt om de positie van een schip met behulp van VHF te verzenden naar andere schepen in de omgeving. Bovendien wordt de verzonden informatie opgepikt door de vaste antennes die langs de waterwegen zijn geplaatst, en doorgestuurd naar de verkeersposten op de wal, die deze informatie gebruiken om een beeld te krijgen van het scheepvaartverkeer en de positie van elk schip. Aangezien deze via VHF verstuurde informatie niet versleuteld is en hiervoor geen authenticatie is vereist, is dit systeem zeer kwetsbaar voor acties van cyberaanvallers.

In 2017 hebben ten minste twintig schepen op de Zwarte Zee gemeld dat volgens hun AIS-apparaat hun positie dertig kilometer landinwaarts lag.[9] Aangezien de AIS-transceiver belangrijk is voor de veiligheid van de scheepvaart, bracht dit cyberincident (dat berustte op het gebruik van 'spoofing') de veiligheid van het schip en zijn bemanning rechtstreeks in gevaar. De beweegredenen kunnen zeer uiteenlopend zijn en gaan van terrorisme tot hacktivisme of criminele activiteiten. Hieronder volgt een beschrijving van de verschillende fasen van een dergelijke spoofing-aanval:

Boedapest, Hongarije - Donau

Stap 1 - Digitale verkenning (Reconnaissance)

Schepen die hun AIS-apparaat hebben aanstaan, zijn via een antenne of een externe verbinding verbonden met een bedrijf om berichten op basis van geo-lokalisatie te verzenden. Toegang tot dit positiebepalingsapparaat is mogelijk door de verbinding of het bericht met informatie over de positie te onderscheppen.

Stap 2 - Onderschepping

Een kwaadwillende vangt de AIS-signalen aan wal op door de positie van het schip te volgen met behulp van de gegevens die online beschikbaar zijn. De cyberaanvaller kan vervolgens radiosignalen versturen met een andere positie van het schip om de ontvangers te verwarren of simpelweg het signaal jammen/ blokkeren.

Stap 3 - Actie

De radiosignalen kunnen worden geblokkeerd door personen die kwade bedoelingen hebben: cyberaanvallers kunnen bijvoorbeeld de verkeerde locatie naar het AIS-apparaat verzenden waardoor de positie van een schip verkeerd wordt weergegeven of het schip geen correcte positie-informatie meer verstuurt. Dit houdt een risico in voor de scheepvaart.

Dit bedreigingsscenario is met name van belang voor havens, omdat het havenpersoneel de door het AIS-apparaat verstuurde informatie over de positie vertrouwt om het scheepsverkeer in de haven in goede banen te leiden. De havenautoriteiten verzenden via het AIS-apparaat ook specifieke berichten. Als de betrouwbaarheid van deze systemen wordt ondermijnd, kan dit niet alleen financiële gevolgen hebben en de reputatie schaden, maar ook de veiligheid ondermijnen en zelfs het leven van mensen in gevaar brengen.

[9] https://www.ship-technology.com/features/ship-navigation-risks/

Casestudy
Social-engineeringcampagnes

De bovenstaande voorbeelden laten zien dat in zeer uiteenlopende aanvalsscenario's op een gegeven moment misbruik kunnen maken van de 'menselijke factor'. Cybercriminelen weten dit maar al te goed en maken bijna systematisch misbruik van deze kwetsbaarheid om hun doel te bereiken.

Cybercriminelen en kwaadwillenden die van plan zijn een netwerk binnen te dringen, gebruiken vaak social-engineeringtechnieken om informatie te verzamelen en de eerste stappen van hun cyberaanval uit te voeren. Kort gezegd is **social engineering** de methode die gevolgd wordt om iemand te verleiden informatie prijs te geven door een weldoordachte interactie. In het kader van deze interactie passen cybercriminelen vaak psychologische trucs toe om een gebruiker te manipuleren. Soms speelt social engineering zich niet alleen af in de virtuele wereld, maar ook in de 'echte' wereld. Een persoon kan bijvoorbeeld proberen toegang te krijgen tot een fysieke locatie door middel van bedrog (vervalsing, oneerlijkheid…). Het doel van social engineering is erop gericht een slachtoffer te misleiden in de hoop dat hij op een malafide link klikt en zo vertrouwelijke informatie verstrekt zoals bv. codes, wachtwoorden of vertrouwelijke data.

Eén van de belangrijkste aanvalsvormen van social engineering is **phishing**, een methode waarbij een bericht met daarin een valstrik (via e-mail, telefoon, sms…) wordt verzonden naar een (zeer) groot aantal personen in de hoop dat minstens enkelen van hen in de val lopen. De aanvaller hoopt in dat geval financieel gewin te verkrijgen of bepaalde persoonlijke of vertrouwelijke informatie te ontfutselen die hij vervolgens kan misbruiken voor kwade doeleinden. Wanneer de doelgroep kleiner is (soms zelfs maar één persoon) wordt er gesproken van **spear phishing**; in dat geval is de valstrik doorgaans op het doelwit afgestemd en veel zorgvuldiger uitgewerkt, waardoor deze overtuigend is.

In deze casestudy zoomen we in op de vijf meest voorkomende phishing-vormen die berusten op social engineering: het manipuleren van een link, smishing, vishing, het vervalsen van een website en pop-ups.

Link-manipulatie is een methode waarbij de cyberaanvaller de gebruiker ertoe verleidt op een link te klikken die het slachtoffer naar een valse website stuurt. Dit kan gedaan worden door middel van een e-mail, een sms-bericht, een post op social media of via een ander type platform voor het delen van berichten. De website in kwestie ziet eruit als een bekende of betrouwbare bron, maar is in werkelijkheid gemanipuleerd door cybercriminelen om hun criminele activiteiten uit te kunnen voeren.

Smishing is een vorm van phishing waarbij iemand probeert via een sms-bericht een slachtoffer over te halen zijn of haar privé-gegevens door te geven. De meest voorkomende vorm van smishing is een tekstberichtje met malware die automatisch wordt gedownload wanneer gebruikers op de link klikken. Een geïnstalleerd bestand met malware kan persoonlijke gegevens stelen zoals bank- en inloggegevens, lokalisatiegegevens of telefoonnummers uit het adressenbestand, zodat het virus zich kan verspreiden, in de hoop vele anderen te kunnen infecteren. Bij een andere smishing-tactiek wordt gedaan alsof de berichten van een bevoegde en bekende instantie afkomstig zijn om zo persoonlijke informatie van slachtoffers te bemachtigen.

Vishing is een vorm van telefoonzwendel, oftewel een vorm van phishing waarbij het slachtoffer gebeld wordt door een persoon die informatie probeert te ontfutselen zoals bv. persoonlijke of privé-informatie, wachtwoorden of andere persoonlijke gegevens. De beller kan zich voordoen als een medewerker van een officiële organisatie zoals een bank of overheidsinstantie, als een medewerker van de IT- of HR-afdeling van het bedrijf (of het hoofdkantoor) of als een hiërarchisch meerdere om op deze manier het vertrouwen van het slachtoffer te winnen en de gewenste informatie te verkrijgen.

Website-vervalsing is een techniek waarbij de bezoekers op een valse website belanden, die qua opmaak een kopie is van de echte website: het gevolg is dat de bezoekers hun gevoelige en vertrouwelijke informatie afstaan zoals bankgegevens, wachtwoorden of kredietkaartnummers.

Pop-upberichten zijn een opdringerige manier om naar gegevens te hengelen, waarbij er rechtstreeks naar het scherm van het slachtoffer een pop-up wordt gestuurd met een dringend verzoek om gegevens te verstrekken. Wanneer een pop-up op zijn scherm opduikt, is het slachtoffer vaak snel geneigd informatie te verstrekken die vervolgens bij cybercriminelen terechtkomt.

De social-engineeringmethoden die hierboven zijn beschreven, zijn vaak gebaseerd op de volgende beginselen:

1. misleidende informatie: URL's zien er vaak net een beetje anders uit en e-mails/sms-berichten kunnen spelfouten bevatten, omdat deze meestal zijn opgesteld door leken of door buitenlanders die automatische vertaalprogramma's gebruiken;
2. het gebruik van dreigende of spoed vereisende formuleringen: cybercriminelen maken gebruik van angst en paniek om slachtoffers over te halen gegevens door te geven die zij normaliter niet zomaar zouden delen;
3. de kans van je leven: aanbiedingen zoals de belofte van hoge geldbedragen of andere geschenken om slachtoffers in de val te lokken;
4. verzoeken om vertrouwelijke informatie: verzoeken om persoonlijke gegevens, iets wat bijna nooit wordt gedaan door officiële instanties, vormen de basis van veel phishing-berichten;
5. verdachte bijlagen: in het geval van link-manipulatie of pop-ups kunnen criminelen slachtoffers vragen kwaadaardige bestanden op hun apparaat te downloaden.

Als u een phishingmail of -mededeling ontvangt die er verdacht uit ziet, kunt u het beste het volgende doen:

1. klik niet op de links of download geen bestanden in de e-mail;
2. markeer het bericht als spam of ongewenst;
3. indien van toepassing: stuur een kopie van de e-mail of een screenshot van het adres ter informatie naar de persoon die in uw onderneming verantwoordelijk is voor de cybersecurity, zodat deze op de hoogte is en eventueel maatregelen kan treffen om erger kwaad te voorkomen.

Wat de cyberbedreigingen voor de haven betreft, is het belangrijk dat men begrijpt dat de meeste cyberaanvallen erop rekenen dat zij op een bepaald moment misbruik kunnen maken van de menselijke factor. Daarom wordt er zo vaak gebruik gemaakt van social-engineeringtechnieken en in het bijzonder van de hierboven beschreven phishing-methoden. Zij moeten dan ook wel degelijk au sérieux worden genomen. Soms volstaat het namelijk dat één enkele medewerker zich laat misleiden om de hele onderneming of instantie in gevaar te brengen.

De positieve conclusie van deze casestudy is dat een goede bewustmaking van de havenmedewerkers, het management, de leveranciers en andere stakeholders die bij de haven betrokken zijn, 'volstaat' om zich zeer doeltreffend te wapenen tegen tal van cyberdreigingen. Alle medewerkers regelmatig informeren over dit soort social-engineeringaanvallen en ze aanmoedigen van hun kant alert en waakzaam te blijven en bij te dragen aan de cybersecurity, is een eenvoudige maatregel die niet veel kost en zeer doeltreffend is.

Deel 2

Maatregelen ter beperking van de cyberrisico's in havens

Wenen, Oostenrijk - Donau

Overzicht van voor de havens relevante regelgeving en beleid

Momenteel zijn er voor havens geen specifieke, gemeenschappelijke en verplichte werkwijzen vastgelegd om cyberrisico's te beperken. Dit is een gevolg van het grote aantal regelgevende instanties in de sector van de binnenhavens. Bovendien is de bestaande regelgeving voor het overgrote deel gericht op zeehavens en bevat deze regelgeving geen specifieke bepalingen voor binnenhavens. Tegen deze achtergrond biedt de onderhavige leidraad een kader voor maatregelen om cyberrisico's te beperken en vult hij de leemten in de huidige versnipperde literatuur en regelgeving op.

Dat gezegd zijnde, moet erop gewezen worden – met name voor de lidstaten van de Europese Unie – dat de EU voorziet in een rechtskader, beter bekend als de NIB-richtlijn, om het algemeen niveau van cyberbeveiliging in de EU te verhogen (Richtlijn 2016/1148 van het Europees Parlement en de Raad). Deze richtlijn is in werking getreden in augustus 2016 en omvat specifieke bepalingen voor specifieke actoren die als 'aanbieders van essentiële diensten' worden geïdentificeerd. Aanbieders van binnenvaartdiensten worden expliciet vermeld in de richtlijn, ook al moet elke lidstaat zelf bepalen wie de aanbieders van essentiële diensten zijn. Aanbevolen wordt dat lezers van deze leidraad die in een EU-lidstaat gevestigd zijn en op zoek zijn naar aanvullende informatie over hoe aan de maatregelen en voorschriften kan worden voldaan, de delen van de NIB-richtlijn die betrekking hebben op aanbieders van essentiële diensten, erop naslaan, met name als de desbetreffende binnenhavens door hun land als essentiële diensten worden beschouwd.

Daarnaast zijn er ook verschillende nationale autoriteiten die informatie publiceren over hoe binnenvaartactoren cyberrisico's kunnen beperken. Lezers wordt daarom aanbevolen niet alleen de onderhavige leidraad te raadplegen, maar ook de technische regelgeving en de maatregelen inzake conformiteit die in hun land gelden.

Volgorde van de mitigerende maatregelen in deze leidraad

In deze leidraad zijn de mitigerende maatregelen om de hierboven beschreven mogelijke cyberrisico's te beperken, onderverdeeld in drie delen:

1. **Organisatorische beleidsmaatregelen en procedures (OPP, Organisation Policies and Procedures)**
   Dit deel omvat aanbevelingen met betrekking tot de organisatiestructuur, de taken en verantwoordelijkheden, de governance-maatregelen en de organisatorische beleidsmaatregelen die kunnen worden getroffen om de maturiteit van een haven op het gebied van cybersecurity te verhogen.
2. **Beleidsmaatregelen met betrekking tot de informatietechnologie/operationele technologie**
   In dit deel worden de maatregelen besproken die kunnen worden uitgevoerd om de ICT-middelen die in Deel 1 werden geïdentificeerd, te beveiligen.
3. **Technische cybersecurity-maatregelen voor havens (TSM, Technical Security Measures)**
   In dit deel wordt een algemeen overzicht gegeven van de basismaatregelen die het IT-personeel van havens kan nemen om de IT-infrastructuur te beveiligen.

In elk van deze delen wordt een algemeen overzicht gegeven van de mitigerende maatregelen die een haven in overweging kan nemen, maar deze vervangen in geen geval de cybersecurity-maatregelen die worden vereist in het kader van een audit of in regelgeving die is vastgesteld door certificeringsinstellingen, individuele landen of andere regelgevende instanties.

De voorgestelde mitigerende maatregelen zijn gerangschikt volgens hun maturiteitsniveau op het gebied van cybersecurity, van laag naar hoog. De maatregelen die hieronder bij het begin van elke tabel uiteengezet worden, zouden bij een cybersecurity-benadering eerst moeten worden uitgevoerd. Naarmate deze maatregelen worden toegepast en de cybersecurity-maturiteit toeneemt, kunnen vervolgens stap voor stap de volgende maatregelen worden uitgevoerd. Aan de hand van kleuren wordt het maturiteitsniveau van elke maatregel weergegeven:

- Maturiteitsniveau : **laag**
- Maturiteitsniveau : **middelhoog**
- Maturiteitsniveau : **hoog**

Meer informatie over deze rangschikking vindt u in het schema voor de beoordeling van de maturiteit in Deel 3.


Meppel, Nederland - Meppelerdiep

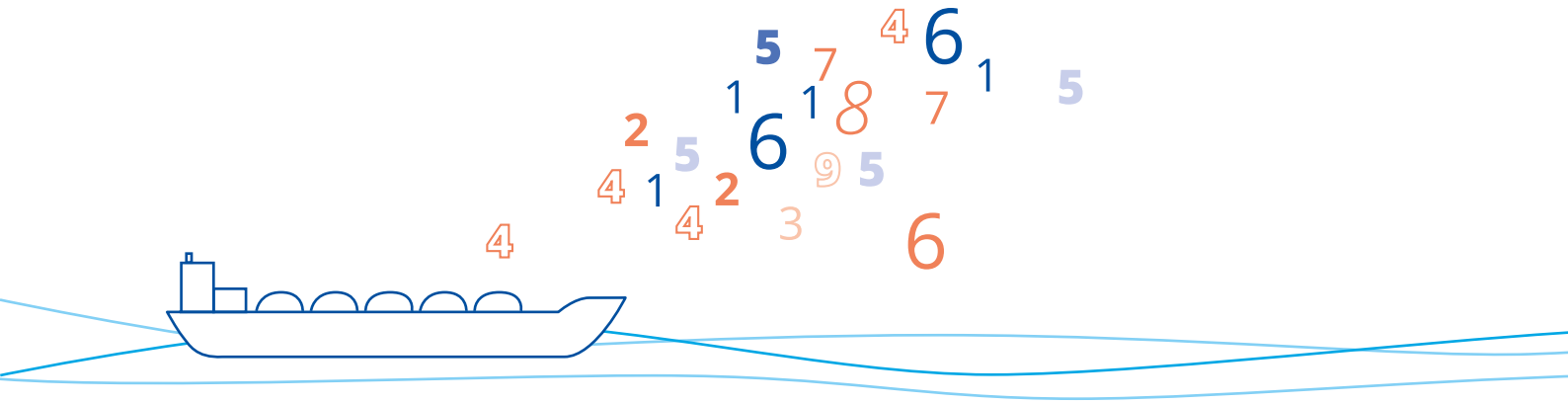
Organisatorische beleidsmaatregelen en procedures

In dit deel wordt een overzicht gegeven van de organisatorische beleidsmaatregelen en procedures die kunnen worden uitgevoerd voor een 'mature' cybersecurity. Deze maatregelen kunnen worden uitgevoerd door het hoofd informatiebeveiliging van de haven of, in het geval van een kleinere haven, door een manager of andere leidinggevende. Deze maatregelen zijn algemeen toepasbaar, maar de omvang, reikwijdte en werkingssfeer ervan kunnen verschillen in functie van de middelen die een haven ter beschikking staan.

Taken en verantwoordelijkheden

Duidelijke taken en verantwoordelijkheden toewijzen is de eerste stap om een cultuur van verantwoording tot stand te brengen en de cybersecurity-maturiteit van een organisatie te verhogen. In dit verband dienen havens de volgende maatregelen te nemen.

	Nummer	Maatregel
●	[OPP] 1.1	Het management moet de cybersecurity-aspecten opnemen in de prioriteiten en adequate middelen en ressources ter beschikking stellen om passende maatregelen te kunnen treffen, bijvoorbeeld maatregelen zoals voorgesteld in deze leidraad. Het management moet beginnen met het aanwijzen van een contactpersoon voor alle cybersecurity-maatregelen en er moet bij alle medewerkers en onderaannemers uitgebreid worden gecommuniceerd over de rol van deze persoon en zijn contactgegevens.
●●	[OPP] 1.2	Er moet een algemeen cybersecurity-handvest worden opgesteld waarin duidelijk wordt beschreven wat er wordt verwacht van alle medewerkers, en dit handvest moet worden ondertekend door de medewerkers en door de stakeholders in de haven.
●●●	[OPP] 1.3	Er moet een algemene cybersecurity-strategie of een beleid voor de beveiliging van informatiesystemen worden vastgelegd en goedgekeurd door het management.
●●●	[OPP] 1.4	In de cybersecurity-strategie moeten de taken van de verschillende stakeholders in de haven (havenautoriteit, terminalexploitanten, dienstverleners, leveranciers, enz.) duidelijk worden beschreven.
●●●	[OPP] 1.5	Alle beveiligingsaspecten in het kader van nauwe samenwerking met derden moeten worden vastgelegd en gedocumenteerd, met name voor door derden verstrekte kritieke systemen.
●●●	[OPP] 1.6	De cybersecurity-strategie moet regelmatig worden geëvalueerd en bijgestuurd, met name na risicobeoordelingen, aanpassingen in de organisatie of cybersecurity-incidenten.



Organisatorische procedures

Nadat de taken en verantwoordelijkheden zijn vastgelegd, moeten in een tweede fase de procedures en vereisten worden gedocumenteerd om de continuïteit van de dienstverlening te garanderen, te voldoen aan bepaalde veiligheidsvoorschriften en ervoor te zorgen dat de informatie correct wordt doorgegeven in geval van een reorganisatie van de havendiensten.

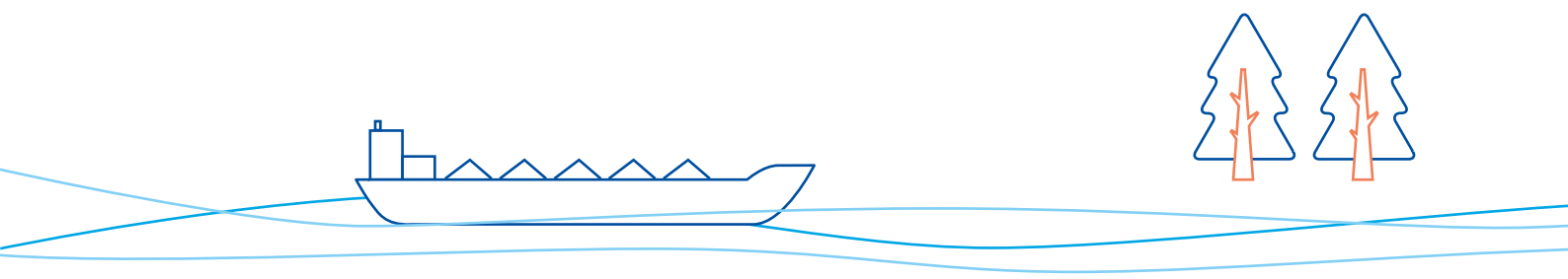
	Nummer	Maatregel
●	[OPP] 2.1	De haven moet aan een grondige beoordeling worden onderworpen, zodat de belangrijkste ICT-middelen in kaart kunnen worden gebracht en gerangschikt in functie van hun kritieke belang.
●	[OPP] 2.2	De basisvereisten met betrekking tot cybersecurity voor relevante leveranciers moeten worden vastgelegd en aan de leveranciers worden meegedeeld. Er kunnen bijvoorbeeld standaard contractuele clausules met betrekking tot cybersecurity opgesteld worden en vervolgens gebruikt worden in alle contracten met leveranciers. Er moet worden toegezien op de naleving van deze vereisten door competente havenmedewerkers of door een vertrouwde derde die dit als enige taak heeft.
●	[OPP] 2.3	De antecedenten van personen in belangrijke leidinggevende functies of IT-functies (systeembeheerders, personen die de IT/OT bedienen) moeten worden onderzocht voor zij in dienst worden genomen. Bewijs van dit onderzoek moet in het dossier worden bewaard met het oog op een eventuele controle door de regelgevende instanties.
●●	[OPP] 2.4	Ook de onderlinge afhankelijkheid van en de informatiestromen tussen de verschillende ICT-middelen moeten in kaart worden gebracht.
●●	[OPP] 2.5	Voor elk ICT-middel moet er een risicobeoordeling worden verricht om de mogelijke cyberrisico's te identificeren. Het management moet erop toezien dat er voor elk nieuw project of initiatief een beoordeling van de cybersecurity-risico's wordt verricht, met name wanneer er in het kader daarvan nieuwe technologieën worden gebruikt.
●●●	[OPP] 2.6	Er moeten regelmatig interne en externe cybersecurity-audits plaatsvinden en er moet regelmatig worden gecontroleerd of de ICT-middelen van de haven aan de voorschriften voldoen. Het management bepaalt hoe vaak deze audits en conformiteitsbeoordelingen plaatsvinden, alsook de aard ervan (intern/extern). De haven zou kunnen overwegen sommige technische audits te automatiseren indien mogelijk. Voor havens die specifieke software hebben ontwikkeld, kan bijvoorbeeld worden voorzien in een regelmatige analyse van de broncode met gespecialiseerde tools om te zoeken naar bekende kwetsbaarheden of veiligheidsgebreken.
●●●	[OPP] 2.7	De vastgelegde en toegepaste cybersecurity-procedures moeten worden gedocumenteerd, goedgekeurd en regelmatig herzien. Mogelijke onderwerpen waarvoor een beleid op schrift kan worden gezet, zijn (deze lijst is niet volledig): • cybersecurity-maatregelen om webportalen en -services te beveiligen; • cybersecurity-maatregelen voor netwerk- of communicatieverbindingen (met inbegrip van draadloze communicatietechnologie); • cybersecurity-maatregelen voor softwareconfiguratie; • vereisten en regels voor het koppelen van apparaten aan de IT-omgeving (met inbegrip van de verbinding met persoonlijke apparaten); • maatregelen voor software-updates en change-management-taken (wanneer ITIL wordt uitgevoerd); • regels met betrekking tot het gebruik van persoonlijke mobiele radiozendapparatuur; • regels met betrekking tot het correcte gebruik van de IT-infrastructuur door het personeel overeenkomstig het algemene cybersecurity-handvest; • configuratie en beheer van de rechten van gebruikers- en systeemaccounts, met inbegrip van de accounts van personeelsleden van derden met toegang tot de systemen van de haven (zoals voor stroom, verwarming, elektriciteit, enz.); • procedure voor het aanpakken van cybersecurity-crisissen en -incidenten.

Fysieke beveiliging

In de context van cybersecurity wordt er gesproken van 'fysieke beveiliging' wanneer het nuttig of noodzakelijk is IT-apparatuur fysiek te beschermen. Vaak wordt er een onderscheid gemaakt tussen 'fysieke beveiliging' en 'logische beveiliging', die bestaat in het beschermen van IT-apparatuur tegen toegang via software of het netwerk. Fysieke beveiliging is een volwaardig onderdeel van cybersecurity, aangezien deze een belangrijke rol kan spelen in tal van aanvalsscenario's. Toegang tot een aan/uit-knop kan volstaan om een server buiten werking te stellen en toegang tot een USB-poort maakt het mogelijk de netwerkbeveiliging te omzeilen en malware te introduceren. Onder fysieke beveiliging vallen eveneens brandveiligheid en beveiliging tegen overspanning of stroomonderbreking.

Bij de opstelling van een cybersecurity-plan moeten ook vereisten met betrekking tot de fysieke beveiliging in aanmerking worden genomen. Kritieke IT-infrastructuur kan kwetsbaar zijn als deze vrij toegankelijk is voor externe personen met mogelijk kwaadwillige bedoelingen. Cybersecurity-plannen moeten daarom rekening houden met de risico's die gepaard gaan met inbreuken op de fysieke beveiliging.

	Nummer	Maatregel
●	[OPP] 3.1	Het management van de haven moet duidelijke regels vastleggen voor de fysieke beveiliging en moet maatregelen nemen voor de controle op fysieke toegang om toegang tot en diefstal of beschadiging van de gevoelige systemen van de haven te voorkomen. De lijst van deze gevoelige systemen moet vooraf worden opgesteld en goedgekeurd door het management.
●	[OPP] 3.2	De haven moet niet alleen de gevoelige systemen beschermen, maar moet door middel van controlepunten voor fysieke toegang of vergrendelde deuren ook verhinderen dat onbevoegden toegang hebben tot nutsvoorzieningen (zoals systemen voor verwarming, ventilatie of koeling).
●	[OPP] 3.3	Elke toegestane fysieke toegang tot de haven moet worden geregistreerd en minstens een keer per jaar worden gecontroleerd.
●●	[OPP] 3.4	Er moet een procedure worden vastgelegd en onder de aandacht worden gebracht met betrekking tot de aanpak van fysieke inbraken en de beschikbaarheid van en reactie door het havenpersoneel en externe agentschappen in zulke gevallen.
●●	[OPP] 3.5	De mate waarin bepaalde zones van de haven toegankelijk zijn voor derden of het publiek, moet worden gedocumenteerd en beoordeeld met het oog op een aanvaardbaar risiconiveau.
●●	[OPP] 3.6	Er moet een beleid worden uitgewerkt voor de controle op fysieke toegang waarin procedures voor handelingen die voor de beveiliging van kritiek belang zijn, zoals het inzamelen van badges van vertrekkende werknemers, het updaten van alarmcodes, het beheer van videobewakingsbeelden, enz., stap voor stap worden beschreven.



Reactie op incidenten en crisismanagement

Er moeten duidelijke beleidsmaatregelen en procedures worden vastgelegd en uitgevoerd voor cybersecurity-incidenten of -crisissen. In deze leidraad wordt een onderscheid gemaakt tussen cybersecurity-incidenten (situaties die kunnen worden opgelost door het IT-/veiligheidspersoneel zonder escalatie of overleg) en cybersecurity-crisissen (situaties met grotere omvang die de werking van de haven verstoren en de betrokkenheid vereisen van het management).

	Nummer	Maatregel
○	[OPP] 4.1	De haven moet beschikken over een plan voor incidentmanagement dat goedgekeurd is door het management en gebaseerd is op een goed inzicht in de cybersecurity-problemen die de goede werking kunnen verstoren, de essentiële systemen die zijn opgenomen in de lijst van kritieke ICT-middelen, en de middelen en vaardigheden die de haven ter beschikking staan.
●●	[OPP] 4.2	De haven moet beschikken over een plan voor crisismanagement dat is goedgekeurd door het management. Daarin moeten de besluitvormers worden aangewezen en moet worden beschreven hoe de communicatie moet verlopen in geval van een incident en wanneer een incident escaleert tot een crisis.
●●	[OPP] 4.3	In het plan voor crisismanagement moet worden ingegaan op rapportage aan en overleg met de nationale autoriteiten, indien van toepassing.
●●	[OPP] 4.4	Het plan voor crisismanagement moet een procedure omvatten voor de communicatie met getroffen partijen en slachtoffers van cyberincidenten, wanneer nodig.
●●	[OPP] 4.5	De medewerkers die binnen de haven verantwoordelijk zijn voor incidentmanagement, moeten het nieuws in de sector volgen, zodat zij op de hoogte blijven van mogelijke cybersecurity-incidenten bij vergelijkbare instanties of bedrijven in hun sector, en er moet een procedure worden vastgelegd voor het verzamelen van relevante informatie over bedreigingen voor de beveiliging van havens.
●●	[OPP] 4.6	In het plan voor incidentmanagement moet in detail worden gedefinieerd wat een cybersecurity-incident precies inhoudt, wat de taken en verantwoordelijkheden zijn bij het aanpakken van een incident en wanneer een incident escaleert tot een crisis.
●●●	[OPP] 4.7	Er moet een plan voor bedrijfscontinuïteit worden vastgelegd om ervoor te zorgen dat de havenactiviteiten niet stil komen te liggen in geval van een crisis of incident. Dit plan moet duidelijke doelen omvatten. Het bevat belangrijke parameters voor de bedrijfscontinuïteit in de haven, zoals de beoogde hersteltijd (RTO, recovery time objective), het beoogde herstelpunt (RPO, recovery point objective), de maximaal aanvaardbare uitvalsduur (MTO, maximum tolerable outage) en de beoogde minimale bedrijfscontinuïteit (MBCO, minimum business continuity objective).
●●●	[OPP] 4.8	Het plan voor crisismanagement voorziet in een analyse na afloop van het incident om de oorzaak van het incident te bepalen.
●●●	[OPP] 4.9	De procedures die zijn vastgelegd om een incident of crisis aan te pakken, moeten regelmatig worden geëvalueerd en getest, eventueel door een crisis te simuleren of door potentiële scenario's te doorlopen ('tabletop-oefening'). Daarbij moeten zo veel mogelijk stakeholders worden betrokken, zodat alle schakels in de keten goed voorbereid zijn.
●●●	[OPP] 4.10	Na een significant cybersecurity-incident (een buitengewoon incident of een incident met operationele gevolgen) moet het management erop toezien dat informatie over relevante cybersecurity-incidenten wordt gerapporteerd en gedeeld, zodat de sector daaruit kan leren.
●●●	[OPP] 4.11	De haven kan overwegen een operationeel cyberbeveiligingscentrum (SOC, Cybersecurity Operations Centre) op te richten om de beveiliging te bevorderen en om te kunnen gaan met cyberincidenten.

Cybersecurity-plannen: in de bovenstaande maatregelen komen verschillende cybersecurity-documenten aan bod. Deze kunnen los van elkaar worden beschouwd, maar uiteindelijk vormen zij één coherent geheel. Deze documenten zijn:

- het plan voor incidentmanagement;
- het plan voor crisismanagement;
- het plan voor bedrijfscontinuïteit;

Het 'beveiligingsbeleid' is een ander document (dat aan bod komt bij de hogere maturiteitsniveaus van de hierboven beschreven maatregelen met betrekking tot 'taken en verantwoordelijkheden'). In een deel daarvan wordt beschreven hoe de verschillende plannen moeten worden uitgevoerd, herzien en getest.

Opleiding en bewustmaking

Opleidings- en bewustmakingsactiviteiten die tot alle stakeholders zijn gericht, zijn van cruciaal belang om good practices voor cybersecurity te verspreiden. Zoals in het eerste deel van deze leidraad wordt uitgelegd, is het in de praktijk bij het merendeel van de aanvalsscenario's namelijk zo dat inspelen op de 'menselijke factor' door de cybercrimineel een cruciale rol speelt. De onderstaande maatregelen kunnen helpen het risico van de 'menselijke factor' te reduceren door medewerkers bewust te maken van de cruciale rol die zij vervullen bij het garanderen van de cybersecurity.

	Nummer	Maatregel
○	[OPP] 5.1	De medewerkers moeten worden aangespoord om voorzichtig te zijn met e-mails. Daarbij moet worden benadrukt dat zij: • de identiteit van de afzender moeten controleren; • geen bijlagen mogen openen of op internetlinks mogen klikken die afkomstig zijn van verdachte of onbekende afzenders.
○	[OPP] 5.2	De haven zou een 'beleid inzake wachtwoordbeheer' moeten vaststellen. Dit beleid moet een educatieve dimensie omvatten om het personeel bewust te maken van het gebruik van sterke wachtwoorden. Ook moeten de regels voor het vernieuwen van wachtwoorden worden vastgesteld. Het beleid moet een onderscheid maken tussen individuele gebruikerswachtwoorden en wachtwoorden die gekoppeld zijn aan systeem- of beheerdersaccounts die gedeeld kunnen worden voor servicedoeleinden, of gebruikt kunnen worden door programma's.
○	[OPP] 5.3	Medewerkers moeten bewust worden gemaakt van een gepast gebruik van sociale netwerken, fora, formulieren, enz., vooral wanneer het gaat om havengerelateerde informatie.
○	[OPP] 5.4	Medewerkers moeten bewust worden gemaakt van de regels voor de installatie van programma's en software. Er moet worden gecommuniceerd over hoe ze toestemming kunnen krijgen van de netwerkbeheerder van de haven om software te downloaden.
○	[OPP] 5.5	Medewerkers moeten worden geïnformeerd over het gebruik van wifi, 4G/5G en veilige netwerken: medewerkers moeten voorzichtig zijn met het gebruik van openbare wifi-netwerken wanneer zij voor hun werk op pad zijn.
○	[OPP] 5.6	Er moet een beleid voor medewerkers worden uitgewerkt en onder de aandacht worden gebracht over het scheiden van persoonlijk en professioneel gebruik en het werken op privétoestellen (BYOD).
○	[OPP] 5.7	De haven moet een programma ontwikkelen om alle medewerkers regelmatig bewust te maken van cybersecurity waarin dieper wordt ingegaan op algemene basisregels voor een goede 'cyberhygiëne'.
●●●	**[OPP] 5.8**	De haven moet een programma voor cybersecurity-opleidingen ontwikkelen om het IT-personeel en de medewerkers die gebruik maken van IT/OT-middelen, in staat te stellen hun cybersecurity-vaardigheden te verbeteren.
●●●	**[OPP] 5.9**	Alle medewerkers die gebruik maken van verbonden apparatuur, moeten een basisopleiding over veilig gebruik van IT/OT volgen.

Wat is een 'sterk wachtwoord'?

Een sterk wachtwoord is een wachtwoord dat moeilijk kan worden geraden door een mens of een computer. Maar opgelet: mensen programmeren computers op zo'n manier dat deze per seconde duizenden wachtwoorden kunnen uitproberen. Hoe kan je dat dan het beste aanpakken? De meeste systemen stellen 'complexiteitsregels' voor wachtwoorden voor (minimumaantal tekens, letters, cijfers, speciale tekens, enz.). Dat is een goed begin, maar het is niet voldoende, omdat het nog steeds mogelijk is dat je een zwak wachtwoord maakt, hoewel je alle regels gevolgd hebt. Bijvoorbeeld: 'P@ssw0rd'. Het is onder andere good practice om een wachtwoord te kiezen dat lang genoeg is (minstens 8 of zelfs 10 tekens) en het wachtwoord mag niet, zelfs niet in geringe mate, gebaseerd zijn op een woord uit het woordenboek. Het mag ook geen rechtstreeks verband hebben met de positie van de toetsen op het toetsenbord ('qwerty', 'azerty', '123456' enz.) of met de gebruiker (geboortedatum, voornaam van de kinderen, enz.). Vandaag de dag wordt het steeds meer als good practice gezien om gebruik te maken van een authenticatie in meerdere stappen, dat wil zeggen dat er naast het wachtwoord nog een ander authenticatiemiddel nodig is (bijvoorbeeld een eenmalige code die per SMS, e-mail of naar een app op een smartphone gestuurd wordt). Het beleid ten aanzien van het beheer van wachtwoorden dat genoemd wordt in regel [OPP] 5.2 moet gedetailleerde regels en aanbevelingen omvatten die hiervoor in acht genomen zouden moeten worden.

Casestudy
Bewustmakingsprogramma's voor medewerkers

In deze leidraad wordt benadrukt dat alle medewerkers, leveranciers en andere stakeholders een belangrijke rol spelen bij de cybersecurity van havens. Zoals in Deel 1 van deze leidraad wordt beschreven in de scenario's voor cyberaanvallen, is een groot deel van de cybersecurity-incidenten het gevolg van een menselijke fout. De organisatie van een bewustmakingsprogramma voor medewerkers is dan ook een belangrijke mitigerende maatregel die snel resultaat oplevert ('quick-win') en die de havens kunnen uitvoeren om hun cybersecurity-houding te verbeteren. Om ze hierbij te helpen, wordt in deze casestudy een overzicht gegeven van de stappen voor het starten van een bewustmakingsprogramma, de verschillende soorten modules die in dit programma kunnen worden opgenomen, en enkele factoren die cruciaal zijn om van het programma een succes te maken.

Overzicht van de stappen

Stap 1

Bepalen in hoeverre de havenmedewerkers zich momenteel bewust zijn van het belang van cybersecurity (benchmark). Door het huidige maturiteitsniveau van de haven te beoordelen, krijgt het management een beeld van het vertrekpunt voor het bewustmakingsprogramma en de onderwerpen die in het kader daarvan bijzondere aandacht moeten krijgen, en kan worden geëvalueerd welke vorderingen er na de bewustmakingssessies zijn gemaakt. Deze beoordeling kan worden gemaakt aan de hand van een vragenlijst voor havenmedewerkers of een andere informele onderzoeksmethode.

Stap 2

Een strategie opstellen om de havenmedewerkers bewust te maken van cybersecurity. Elementen die in deze strategie aan bod moeten komen, zijn: tastbare doelstellingen, een realistisch tijdschema, de verdeling van taken en verantwoordelijkheden en de vereiste financiële middelen. Om de doeltreffende uitvoering van een programma te garanderen, is het belangrijk dat het management zich betrokken voelt, wat kan worden bewerkstelligd door middel van een presentatie van de strategie.

Stap 3

De vorm van de bewustmakingsmodules bepalen. Een bewustmakingscampagne kan bestaan uit een verplichte cursus, webinars, verschillende soorten oefeningen zoals phishing-oefeningen, enz. De vorm van de bewustmakingsmodule moet worden gekozen in functie van de vastgelegde strategie, met name de financiële middelen die de haven ter beschikking heeft, en het beoogde tijdschema. Als de haven zelf niet de nodige vaardigheden heeft om een bewustmakingsprogramma te ontwikkelen, kan hiervoor worden samengewerkt met externe deskundigen. Dit kan ook van belang zijn voor het privégebruik van IT door de werknemers thuis.

Stap 4

Het bewustmakingsprogramma uitrollen.

Stap 5

De resultaten registreren. Om te voldoen aan de regelgeving of met het oog op de groei van de haven moet na het bewustmakingsprogramma de feedback van de deelnemers worden verzameld. Er moet een overzicht worden opgesteld en bewaard van de bewustmakingsdoelstellingen die met dit programma werden beoogd en gehaald. Omdat organisaties moeten proberen het bewustmakingsprogramma steeds beter te maken, dienen zij bovendien nota te nemen van de goede punten en de punten die voor verbetering vatbaar zijn.

Stap 6

Een volgende editie plannen. Bewustmakingsprogramma's kunnen pas doeltreffend zijn als zij regelmatig worden bijgewerkt en opnieuw worden georganiseerd naarmate de haven evolueert. De streefdatum voor de tweede fase moet in overleg met het management worden vastgelegd.

Soorten modules die in het bewustmakingsprogramma kunnen worden opgenomen

Bewustmakingsprogramma's en -initiatieven kunnen verschillende vormen aannemen en kunnen op de behoeften van de haven worden afgestemd. Hieronder is een overzicht opgenomen van de belangrijkste soorten bewustmakingsmodules.

Soort bewustmakings-module	Korte beschrijving	Belangrijkste voorde(e)l(en)	Belangrijkste nade(e)l(en)
Offline of online cursus	Bij bewustmakings-cursussen vinden de lessen plaats in realtime, met een instructeur.	• Een gespecialiseerde instructeur checkt of de materie is begrepen en beantwoordt vragen. • Controle op aanwezigheid en aandacht voor het lesmateriaal.	• Vergt veel tijd en middelen; neemt tijd in beslag tijdens werkuren. • Hoge kosten.
E-learning	Cursussen worden digitaal gegeven via een onlineplatform, doorgaans in videoformaat.	• Er is een groot aanbod aan online bewustmakings-cursussen; sommige zijn zelfs gratis. • Stakeholders kunnen de e-learning volgen.	• Controle op aanwezigheid en aandacht van deelnemers is moeilijk.
Ernstige spelletjes	Stakeholders 'spelen' een online of mobiel spel dat bedoeld is om hen meer bewust te maken van het belang van cybersecurity; achteraf worden de belangrijkste conclusies en lessen besproken.	• Door informatie op een leuke en andere manier over te brengen, trekt u de aandacht van de stakeholders en blijft de ervaring hun beter bij. • Dit soort bewustmakings-opleiding vereist een minder grote betrokkenheid van de deelnemers.	• Vereist een zorgvuldige planning: selectie van een adequaat spel; aanpassing van het spel aan de behoeften van de organisatie; uitvoering van het spel. • Moeilijk te garanderen dat deelnemers aandachtig blijven en het 'spel' uitspelen.
Phishing-oefeningen	Simulatie-oefening waarbij er een phishing e-mail wordt verzonden naar havenmedewerkers; personen die niet slagen voor de oefening, worden opgespoord en doorgaans doorverwezen naar een opleidingsmodule.	• Tastbare ervaring die personen die niet slagen voor de oefening, niet snel vergeten. • Documentatie en statistische informatie over de aard van de stakeholders die niet slagen voor de phishing-oefening.	• Behandelt slechts een onderdeel van cybersecurity: phishing. • Zorgt niet voor een grotere bewustwording bij zij die slagen voor de test; geen garantie dat personen die slagen, niet gewoon de e-mail gemist hebben.
Simulatie van een malware-campagne	Bewustmakings-campagne over malware aanpassen om te evalueren in hoeverre de medewerkers zich bewust zijn van het risico met betrekking tot het gebruik van externe apparaten en verbindingen. Deze campagnes hebben dezelfde kenmerken als de phishing-campagnes maar verspreiden malware. Malware-scripts zijn niet blijvend van aard. Ze 'vangen' alleen de realtime gegevens van het slachtoffer en het systeem.	• Tastbare ervaring die de deelnemers niet snel vergeten. • Zelfde effect als een brandoefening: er wordt een crisis gesimuleerd zodat de organisatie beter zal presteren in geval van een echte crisis.	• Plannen en uitvoeren van de simulatie is tijds- en arbeidsintensief. Mogelijk hulp nodig van een extern bedrijf. • Mogelijk nadelig voor de vertrouwensband met medewerkers die het slachtoffer worden van deze test.
Informatie-materiaal	Maandelijkse editie met verhalen over echte aanvallen op organisaties, vastgestelde beveiligingsproblemen, de gevolgen van deze aanvallen, de toegepaste oplossingen en de lessen die werden getrokken. Kan ook gaan over actuele beveiligings-onderwerpen in de sector.	• Ontwikkeling en verspreiding zijn redelijk eenvoudig: een gewone e-mail volstaat. • Regelmatige informatie-verstrekking zodat stakeholders op de hoogte blijven.	• Succes van deze informatie-verstrekking monitoren is moeilijk: sommige stakeholders zullen de informatie gewoon negeren/omzeilen.
Evenement	Specifiek evenement (infosessie tijdens ontbijt of lunch ('lunch and learn'), enz.) om een gesprek op gang te brengen of een demo te geven over een cybersecurity-onderwerp.	• Brengt de stakeholders van de organisatie bijeen in een sessie en maakt informatie-uitwisseling en gesprekken mogelijk. • Organisatie en uitvoering zijn redelijk eenvoudig.	•Interactie van korte duur • Moeilijker om na te gaan welke lessen de deelnemers hebben geleerd en of dit ene evenement het besef heeft vergroot.

Factoren die bepalend zijn voor het succes van het bewustmakingsprogramma

1. **Het bewustmakingsprogramma afstemmen op de operationele problemen en uitdagingen.**
   Door het bewustmakingsprogramma af te stemmen op de operationele problemen van de haven zal het een grotere impact en dus meer succes hebben. Het bewustmakingsprogramma moet in het bijzonder aandacht besteden aan de kritieke havensystemen en aan de mogelijke gevolgen van cybersecurity-voorvallen.
2. **Zo veel mogelijk stakeholders betrekken**
   Door zo veel mogelijk stakeholders, alsook derden en leveranciers, bij het programma te betrekken, zullen actoren in de hele keten de nodige kennis opdoen en zich bewust worden van het probleem. Dit is zeer belangrijk voor havens, omdat een groot aantal derden betrokken zijn bij de havenactiviteiten.
3. **Impact en vooruitgang meten**
   De doeltreffendheid van een bewustmakingscampagne kan het best worden geëvalueerd door aan het einde van de module een soort kennistest of evaluatie te organiseren. Dit kan bijvoorbeeld aan de hand van een korte vragenlijst of quiz voor de deelnemers.

Koblenz, Duitsland - Rijn

Casestudy
Uitwerking van een cyberrisicobeoordeling

Vóór verschillende van de bovengenoemde mitigerende maatregelen kunnen worden uitgevoerd - zoals het uitvoeren van een cybersecurity-strategie, moeten de te beschermen ICT-middelen in kaart worden gebracht. Om deze in kaart te kunnen brengen, moeten de havens op een bepaald moment de cyberrisico's beoordelen. Een degelijke risicobeoordeling vormt de basis voor een robuuste cybersecurity-strategie. In de huidige good practices wordt namelijk de voorkeur gegeven aan een aanpak die is afgestemd op de behoeften, waarbij kennis van de procedures en het in kaart brengen van de kritieke ICT-middelen centraal staan, in plaats van de naleving van gemeenschappelijke normen die kenmerkend was voor de vroegere benaderingen. In de onderstaande casestudy wordt een overzicht gegeven van de algemene stappen voor een grondige beoordeling van het cyberrisico voor een haven en wordt er dieper ingegaan op enkele factoren die bepalend zijn voor het succes van de risicobeoordeling.

Overzicht van de stappen

Stap 1

De ICT-middelen van de haven en de mogelijke gevolgen van een cybersecurity-voorval voor deze ICT-middelen in kaart brengen

- De belangrijkste activiteiten van de haven en de ICT-middelen die daarvoor nodig zijn, moeten in kaart worden gebracht. Daarbij moet rekening worden gehouden met een breed spectrum aan ICT-middelen, zoals controlesystemen, technische managementsystemen voor schepen, controleruimten, videobewaking (CCTV)/alarmen, navigatiesystemen die communiceren met schepen, bekabelingsroutes, havensystemen voor het plannen en in ontvangst nemen van lading en de door havens verzamelde en opgeslagen gegevens.
- Aan de hand van de volgende vragen moet worden bepaald hoe belangrijk de verschillende ICT-middelen precies zijn: welke activiteiten zijn het belangrijkst? Welke ICT-middelen zijn nodig voor de uitvoering van deze activiteiten? Worden sommige van deze ICT-middelen gebruikt voor verschillende operationele processen, waardoor zij cruciaal zijn voor het goede functioneren van de haven?
- Er moet een overzicht worden gemaakt van de systemen die de ICT-middelen van de haven ondersteunen. Daarbij moet worden genoteerd of deze systemen zijn verbonden met het internet en of ze afhankelijk zijn van een specifieke energiebron.
- Voor bepaalde ICT- middelen moet worden onderzocht wat de gevolgen voor de activiteiten kunnen zijn als de integriteit of beschikbaarheid ervan in het gedrang komt.
- **Belangrijkste eindproduct:** een lijst van alle ICT-middelen in de haven. Voor elk middel: vastleggen hoe groot het potentiële gevolg is voor de activiteiten in geval van een aanval. Dit eindproduct bevat gevoelige informatie en moet dus worden beveiligd en strikt vertrouwelijk blijven.

Stap 2

Een gedetailleerd overzicht opstellen van de bedrijfsprocessen in de haven

- De bedrijfsprocessen en de ICT-middelen die daarvoor nodig zijn, moeten in kaart worden gebracht.
- Er moet een overzicht worden gemaakt van de informatiestromen en gegevensuitwisseling die nodig zijn om deze processen uit te voeren. Op die manier krijgt men zicht op de soorten interacties die cruciaal zijn voor de activiteiten en deze ernstig kunnen verstoren als ze worden onderbroken.
- **Belangrijkste eindproduct:** een schematische voorstelling van de gegevens- en informatiestromen voor de drie hoofdactiviteiten van de haven. Ook dit eindproduct moet worden beveiligd en strikt vertrouwelijk blijven.

Stap 3

Cybersecurity-bedreigingen in kaart brengen

- Er moet een overzicht worden gemaakt van de potentiële bedreigingen voor de in stap 1 in kaart gebrachte ICT-middelen. Deze informatie kan worden gehaald uit bestaand onderzoek naar voor de haven relevante cybersecurity-bedreigingen (zoals eerder in deze leidraad beschreven) of kan worden verkregen door middel van een uitgebreider dreigingsonderzoek. Dit proces hoeft niet zeer gesofisticeerd te zijn: er kan een standaardlijst van bedreigingen worden opgesteld en deze bedreigingen kunnen in verband worden gebracht met de ICT-middelen van de haven om zo een volledig overzicht van de voor de haven relevante bedreigingen te krijgen.
- **Belangrijkste eindproduct:** een informatierapport over de belangrijkste bedreigingen voor de haven.

Stap 4

Evalueren of deze bedreigingen kunnen worden uitgevoerd en hoe waarschijnlijk dat is

- Voor elke bedreiging moet worden ingeschat hoe haalbaar die is. Dat kan door verschillende gegevens te beoordelen, zoals de voorafgaande kennis van de systemen die nodig is om deze bedreiging in praktijk te brengen, de noodzaak om fysieke toegang te hebben tot het systeem of de gebruikersrechten die nodig zijn om bepaalde handelingen uit te voeren, het niveau van gebruikersinteractie dat nodig is om rechten te verkrijgen, de technische complexiteit van de vereiste handeling en het vermogen van de haven om deze bedreiging af te slaan dankzij robuuste werkingsmodi (eventueel in gedegradeerde modus).
- Voor elke bedreiging moet er een aanvallersprofiel worden opgesteld om te beoordelen hoe waarschijnlijk het is dat de bedreiging wordt uitgevoerd. Bij het opstellen van de aanvallersprofielen moeten verschillende factoren in aanmerking worden genomen, zoals de vaardigheden die de aanvaller nodig heeft om de bedreiging uit te voeren, de motivatie/beloning en de middelen/kennis/informatie die nodig zijn voor de uitvoering ervan.
- Voor elke bedreiging moet het aanvallersprofiel worden gecombineerd met de haalbaarheidsinformatie om te bepalen hoe waarschijnlijk het is dat de bedreiging wordt uitgevoerd (waarschijnlijkheidsscore).
- **Belangrijkste eindproduct**: een lijst van de belangrijke bedreigingen met bijbehorende haalbaarheids- en waarschijnlijkheidsscore.

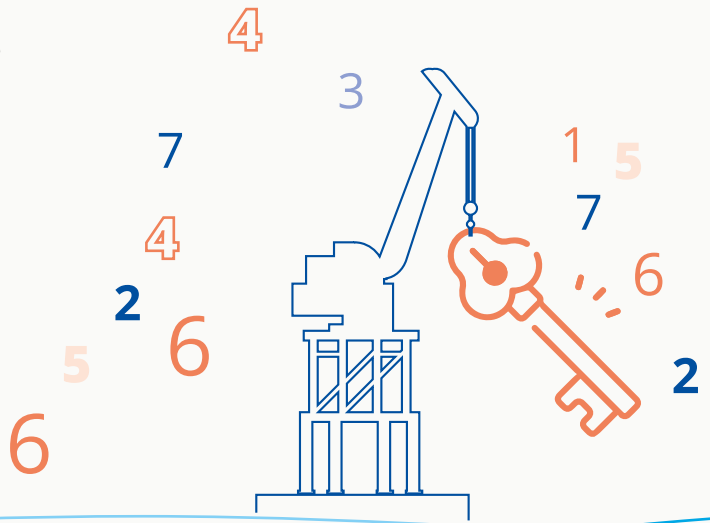
Stap 5

Voor elke bedreiging de informatie over de waarschijnlijkheid ervan en over de gevolgen voor de kwetsbare ICT-middelen combineren

- Aan de hand van een tabel kan de informatie over de gevolgen van een aanval op het ICT-middel voor de activiteiten worden gecombineerd met de informatie over de waarschijnlijkheid van de aanval. Op deze manier kunnen kritieke risico's (risico's met grote gevolgen en hoge waarschijnlijkheid) worden geïdentificeerd.
- Als de risicobeoordeling afgerond is, zou het management van de haven een duidelijk beeld moeten hebben van de belangrijkste cyberrisico's waarmee de haven op dat moment te kampen heeft. Op basis van deze risico's kan worden bepaald in welke volgorde de beveiligingsmaatregelen moeten worden uitgevoerd of kan een algemene cybersecurity-strategie voor de hele organisatie worden ontwikkeld.
- **Belangrijkste eindproduct:** tweedimensionale tabel (haalbaarheid/waarschijnlijkheid) met daarin de verschillende bedreigingen op basis waarvan in een volgende fase kan worden bepaald welke maatregelen er moeten worden getroffen.

Factoren die bepalend zijn voor het succes van de risicobeoordeling

- **Relevantie van de bedreigingen voor de bedrijfsprocessen**
  De bedreigingen die bij de risicobeoordeling worden onderzocht, moeten relevant zijn in de context van de havenactiviteiten. Om ervoor te zorgen dat hun dreigingsanalyse relevant is, moeten de havens zich toespitsen op de bedreigingen waarmee hun sector momenteel te maken krijgt; deze informatie is te vinden in gespecialiseerde informatierapporten over de bedreigingen in hun sector of kan verkregen worden door informatie-uitwisseling met andere havens of door deel te nemen aan cybersecurity-werkgroepen in de sector.
- **Onafhankelijke en objectieve beoordeling van potentiële gevolgen**
  Bij het uitvoeren van een zelfbeoordeling is het moeilijk de overtuigingen over de eigen capaciteiten en organisatorische aspecten opzij te schuiven om een objectief oordeel te vellen over de potentiële gevolgen van een cyberaanval. Men moet voor ogen houden dat een effectbeoordeling op basis van argumenten en feitelijke informatie moet weergeven welke potentiële gevolgen een cyberincident kan hebben voor een ICT-middel. Het is niet de bedoeling een opiniepeiling te houden over de gevolgen die waarschijnlijk worden geacht. Als er maatregelen worden genomen om waarschijnlijk geachte gevolgen te beperken, bestaat het risico dat er uitgebreide werkzaamheden met hoge kosten worden uitgevoerd die desalniettemin nutteloos zijn omdat ze berusten op ongegronde of foutief ingeschatte veronderstellingen.



Beleidsmaatregelen met betrekking tot de informatietechnologie (IT) en operationele technologie (OT) in havens

In dit deel, dat van toepassing is op havens en hun leveranciers, worden enkele algemene good practices voor de beveiliging van IT/OT-systemen uiteengezet. Pro memorie: de term 'IT/OT' wordt gedefinieerd in de Inleiding van deze leidraad. Eenvoudig gezegd, heeft de term 'IT' betrekking op de systemen voor gegevensverwerking, terwijl de term 'OT' betrekking heeft op systemen die zorgen voor de interactie met fysieke objecten. Deze twee systeemtypes kunnen natuurlijk onderling met elkaar communiceren en het is met name in die gevallen dat de term 'IT/OT-systemen' wordt gebruikt.

Dit deel is dus gericht tot de stakeholders die werken met de operationele systemen en werktuigen die in de havens aanwezig zijn. De IT/OT-systemen kunnen verschillen van haven tot haven, maar doorgaans gaat het om systemen die operationele of fysieke taken verrichten en worden bediend met een computer of via een verbonden gateway. In de context van de haven gaat het onder meer om:

- systemen voor verkeersmanagement in de haven (tools voor monitoring van het scheepvaartverkeer, ligplaatsmanagement, weermonitoring);
- navigatieapparatuur die communiceert met havennetwerken (AIS, GNSS);
- systemen voor terminalmanagement (operationele werktuigen, systemen voor overslag en opslag, TOS (terminal operating systems));
- veiligheids- en beveiligingssystemen: toegangscontrole, detectie van indringers, bewakingssystemen en andere alarmsystemen.

IT/OT-systemen spelen een belangrijke rol bij de cyberbeveiliging van een haven, omdat ze steeds vaker met het internet zijn verbonden, met name door het toenemende gebruik van IoT-apparaten. IT/OT-systemen zijn bijzonder kwetsbaar omdat er bij hun ontwerp doorgaans geen rekening is gehouden met de cybersecurity-configuraties die moderne IT-software wel bevat. Bovendien draaien ze vaak op oude systemen die niet of amper kunnen worden geüpdatet, en worden ze bij cybersecurity-projecten en onderhoudsplannen dikwijls buiten beschouwing gelaten.

Algemene verantwoordelijkheden met betrekking tot informatietechnologie (IT)/operationele technologie (OT)

Naast het vastleggen van de hierboven beschreven algemene taken en verantwoordelijkheden moet het management of zijn vertegenwoordiger ook verantwoordelijkheden toewijzen die specifiek verband houden met de IT/OT-systemen. De groep die met deze systemen werkt, is mogelijk niet dezelfde als de groep die zich bezighoudt met het management van de havenactiviteiten en IT-systemen. Daarom mag niet worden vergeten dat de personen die de werktuigen en systemen bedienen die cruciaal zijn voor de havenactiviteiten, belangrijk zijn voor de cybersecurity. Deze operationele systemen moeten in aanmerking worden genomen bij de beoordeling van de cyberrisico's van de havens.

	Nummer	Maatregel
●●	[ITOT] 1.1	Er moet een lijst worden opgesteld van alle IT/OT-middelen die bij havenactiviteiten worden gebruikt. Deze IT/OT-middelen moeten vervolgens worden gerangschikt in functie van het kritieke belang van het systeem.
●●	[ITOT] 1.2	De verantwoordelijkheden met betrekking tot cybersecurity moeten duidelijk worden vastgelegd en gecommuniceerd voor elke stakeholder die met een van de IT/OT-middelen op de lijst werkt, ongeacht wat dat werk precies inhoudt (bijvoorbeeld ontwikkeling, integratie, bediening, onderhoud).
●●●	[ITOT] 1.3	Voor een nieuw IoT-apparaat of -systeem in gebruik wordt genomen, moet een beoordeling worden gemaakt van de cyberrisico's die daarmee gepaard gaan.
●●●	[ITOT] 1.4	De meest kritieke IT/OT-middelen moeten worden onderworpen aan een cyberrisicobeoordeling.

Identiteits- en toegangsbeheer (IAM, identity and access management)

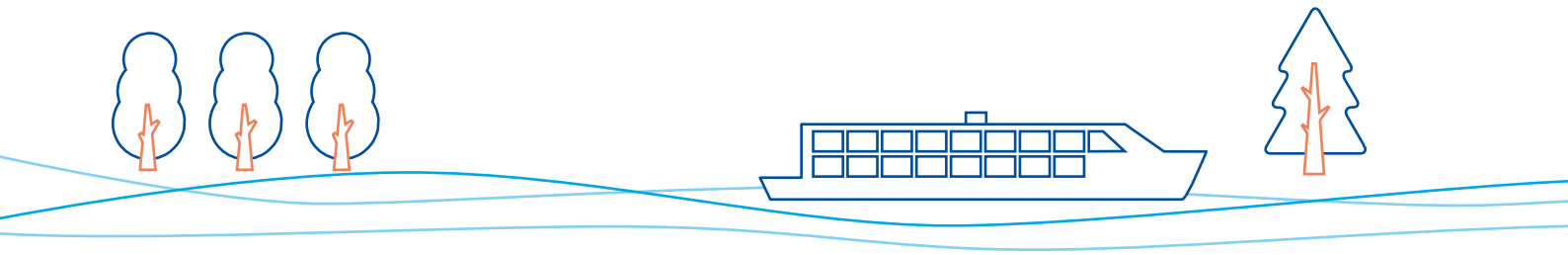
De havens moeten een duidelijk beleid hebben voor de toegang tot en het gebruik van industriële systemen, verbonden werktuigen en andere operationele systemen die voor de havenactiviteiten worden gebruikt. Onderstaande maatregelen kunnen worden getroffen om de gebruikers en de toegangsrechten te beheren.

	Nummer	Maatregel
●	[ITOT] 2.1	Indien mogelijk moet ervoor worden gezorgd dat toegang tot werktuigen en systemen alleen mogelijk is met een gebruikersnaam en wachtwoord. Wachtwoorden moeten robuust zijn.
●	[ITOT] 2.2	Standaardwachtwoorden voor operationele systemen moeten worden gewijzigd en er moet een procedure worden vastgelegd om deze wachtwoorden regelmatig te veranderen overeenkomstig het hiervoor door het bedrijf of de organisatie vastgelegde beleid.
●	[ITOT] 2.3	Als authenticatie niet mogelijk is (met name door operationele beperkingen), moeten er aanvullende maatregelen in overweging worden genomen, met inbegrip van controles op de fysieke toegang, beperking van de beschikbare functies in het systeem, authenticatie door middel van een badge, enz.
●●	[ITOT] 2.4	Havens moeten registreren welke stakeholders toegang hebben en tot welke kritieke systemen zij toegang hebben. Deze lijst moet regelmatig worden bijgewerkt.
●●	[ITOT] 2.5	Als authenticatie mislukt, wordt de gebruiker bij voorkeur niet van het systeem uitgesloten, maar moet hij enige tijd wachten voor een nieuwe poging kan worden ondernomen.
●●	[ITOT] 2.6	Voor bijzonder gevoelige systemen moet er in een authenticatie in meerdere stappen (bijvoorbeeld met een PIN-code en smartcard) voor bijzonder gevoelige systemen worden voorzien.

Fysieke beveiliging

Omdat operationele systemen, industriële systemen en andere werktuigen doorgaans direct fysiek toegankelijk zijn (in tegenstelling tot andere bedrijfsmiddelen zoals gegevens, IT-componenten, software, IT-applicaties, enz.), moeten er voor deze systemen specifieke fysieke beveiligingsmaatregelen worden vastgelegd en uitgevoerd. De fysieke beveiligingsmaatregelen die hieronder worden beschreven, zijn enkele best practices voor de fysieke bescherming van deze bedrijfsmiddelen tegen cyberrisico's.

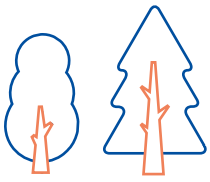
	Nummer	Maatregel
●	[ITOT] 3.1	Toegangspunten voor industriële controlesystemen (ICS) en andere operationele apparatuur mogen niet toegankelijk zijn voor onbevoegden. Dit geldt met name voor havens waar veel voorbijgangers of toeristen komen.
●	[ITOT] 3.2	Centrale eenheden voor werkstations, industriële netwerkapparatuur en programmeerbare logische besturingseenheden (PLC, Programmable Logic Controller) moeten in afgesloten kasten of ruimten worden geplaatst.
●	[ITOT] 3.3	In de haven gehoste IT- en OT-systemen moeten worden beschermd volgens beproefde best practices op het gebied van veiligheid (branddetectie, airconditioning, enz.) en beveiliging (toegangscontrole, videobewaking, enz.).



Onderhoud en bediening van IT/OT-systemen

Zoals hierboven al werd aangegeven, zijn IT/OT-systemen vaak kwetsbaar voor cyberaanvallen omdat ze in veel gevallen draaien op oudere systemen en de gebruikelijke cybersecurity-maatregelen, zoals systeemupdates en patching, vaak niet bij deze systemen worden doorgevoerd. Bovendien is het onderhoud van IT/OT-systemen zuiver routinematig. Een best practice met betrekking tot cybersecurity bestaat uit de integratie van enkele basisbeginselen voor beveiliging in het onderhoudsproces van IT/OT-systemen. Bij het buiten bedrijf stellen en verwijderen van IT/OT-systemen moet er ook rekening worden gehouden met beveiligingsoverwegingen.

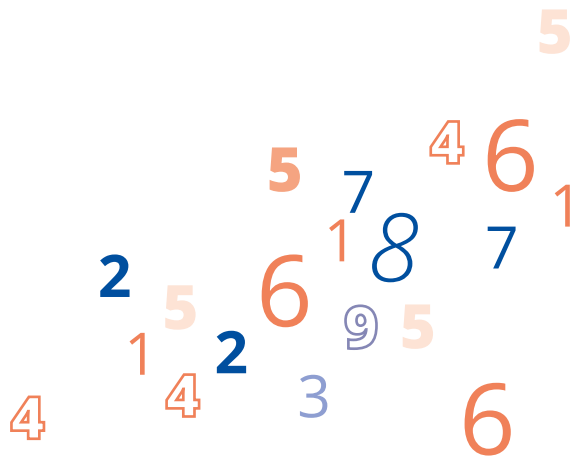
	Nummer	Maatregel
●●	[ITOT] 4.1	Er moet een procedure worden vastgesteld voor het updaten en onderhouden van operationele systemen. In deze procedure moeten de regelmaat van de updates en de taken en verantwoordelijkheden van de met de updates belaste personen worden vastgelegd. De systeemupdates moeten nader worden beschreven in de onderhoudscontracten met de leverancier.
●●	[ITOT] 4.2	Er moeten tools en procedures voorhanden zijn om na te gaan in hoeverre de huidige versie verschilt van de versie die in het kader van een systeemupdate moet worden geïnstalleerd.
●●	[ITOT] 4.3	Alle onderhoudswerkzaamheden moeten worden goedgekeurd. Er moet een goedkeuringsprocedure worden opgesteld en deze moet worden meegedeeld aan de medewerkers die met de operationele systemen werken.
●●	[ITOT] 4.4	Er moet een procedure voor het buiten bedrijf stellen van operationele systemen worden gevolgd. In deze procedure moet worden vastgelegd op welke datum het systeem buiten bedrijf wordt gesteld, wie daarbij betrokken zijn, en hoe de apparatuur correct moet worden verwijderd en verwerkt.
●●●	[ITOT] 4.5	Wanneer er interventies of updates plaatsvinden, moet de volgende informatie worden geregistreerd: • de persoon die de werkzaamheden uitvoert en de partij die daartoe de opdracht geeft, • de datum en het tijdstip van de interventie, • waar de werkzaamheden betrekking op hebben, • de uitgevoerde werkzaamheden, • de lijst van apparaten die worden verwijderd of vervangen (met inbegrip van het identificatienummer, indien beschikbaar), • de aangebrachte wijzigingen en de impact daarvan.
●●●	[ITOT] 4.6	Er moeten regelmatig audits plaatsvinden (opstelling van een auditplan, frequentie van de audits te bepalen door de haven) om na te gaan of aan de updateprocedure is voldaan. Na de audits moet worden gecontroleerd of de bij de audit gedane aanbevelingen worden opgevolgd.



Technische beveiligingsmaatregelen voor IT/OT-systemen

De havenmedewerkers die verantwoordelijk zijn voor de netwerkconfiguratie, het opzetten en configureren van operationele systemen en het algemeen technisch onderhoud van deze systemen, moeten overwegen de onderstaande technische beveiligingsmaatregelen toe te passen. In het algemeen moet worden getracht om, zo mogelijk, de kritieke systemen te isoleren van de algemeen beschikbare netwerken en van de overige IT-infrastructuur.

	Nummer	Maatregel
●	[ITOT] 5.1	Toegang tot het internet vanaf kritieke industriële systemen (zoals managementsystemen voor sluizen of bruggen, elektriciteitscentrales, drinkwaterinstallaties) moet tot een minimum worden beperkt.
●	[ITOT] 5.2	Ontwikkelingstools mogen niet worden geïnstalleerd op machines die actief en in gebruik zijn. Op IT/OT-apparatuur mogen alleen de runtime-systemen actief zijn.
●	[ITOT] 5.3	Voor de operationele systemen moeten onbeveiligde protocollen (bijvoorbeeld HTTP, Telnet, FTP) worden uitgeschakeld en moet de voorkeur worden gegeven aan beveiligde protocollen (bijvoorbeeld HTTPS, SSH, SFTP).
●●	[ITOT] 5.4	Er moeten gescheiden netwerkzones worden voorzien voor de verbinding van operationele systemen, voor alle IoT-apparatuur, voor wifi voor professioneel gebruik en voor openbare wifi.
●●	[ITOT] 5.5	Industriële controlesystemen (ICS) moeten worden opgesplitst in consistente functionele of technische zones. Deze zones moeten losstaan van elkaar.
●●	[ITOT] 5.6	Tussen verschillende zones en bij administratieve gateways moeten filters worden toegepast overeenkomstig een vastgelegd strikt protocol (met name een protocol voor datastromen, registratie van activiteiten, registratie van IP-adressen, enz.).
●●	[ITOT] 5.7	Waar mogelijk moet op gateways een VPN worden toegepast, zodat extern verkeer geen toegang krijgt tot operationele systeemzones.
●●	[ITOT] 5.8	Werkstations die gemachtigd zijn om verbinding te maken met netwerkelementen met een hoge bevoegdheid (beheerder) moeten, waar mogelijk, worden gescheiden van het hoofdnetwerk. Deze werkstations moeten worden gecontroleerd en mogen niet voor andere doeleinden worden gebruikt. Ze moeten regelmatig worden geüpdatet en versterkt door middel van een 'verhardingsbeleid' (system hardening).
●●●	[ITOT] 5.9	Wanneer operationele systemen op afstand moeten worden bediend, moeten de verbindingen daarvoor worden gecertificeerd, moeten de wachtwoorden voor verbinding worden beheerd in het kader van een door de organisatie vastgesteld wachtwoordenbeleid, moeten de gegevens worden geregistreerd, moeten er beveiligde communicatieprotocollen worden gebruikt en moet de verbinding op afstand automatisch worden verbroken na een bepaalde tijdspanne van inactiviteit.
●●●	[ITOT] 5.10	Er moeten mechanismen worden geïntegreerd om de data-uitwisseling tussen verschillende apparaten (machine-to-machine) te beveiligen (onder meer voor de EDI-berichten en API die doorgaans worden gebruikt met externe stakeholders) en om wederzijdse authenticatie, integriteit en vertrouwelijkheid met de havensystemen mogelijk te maken, vooral wanneer de uitwisseling plaatsvindt via het internet (voorbeelden van deze mechanismen zijn versleuteling, PKI of digitale certificaten, integriteitscontroles, digitale handtekeningen en tijdstempels).



IT/OT-systemen monitoren

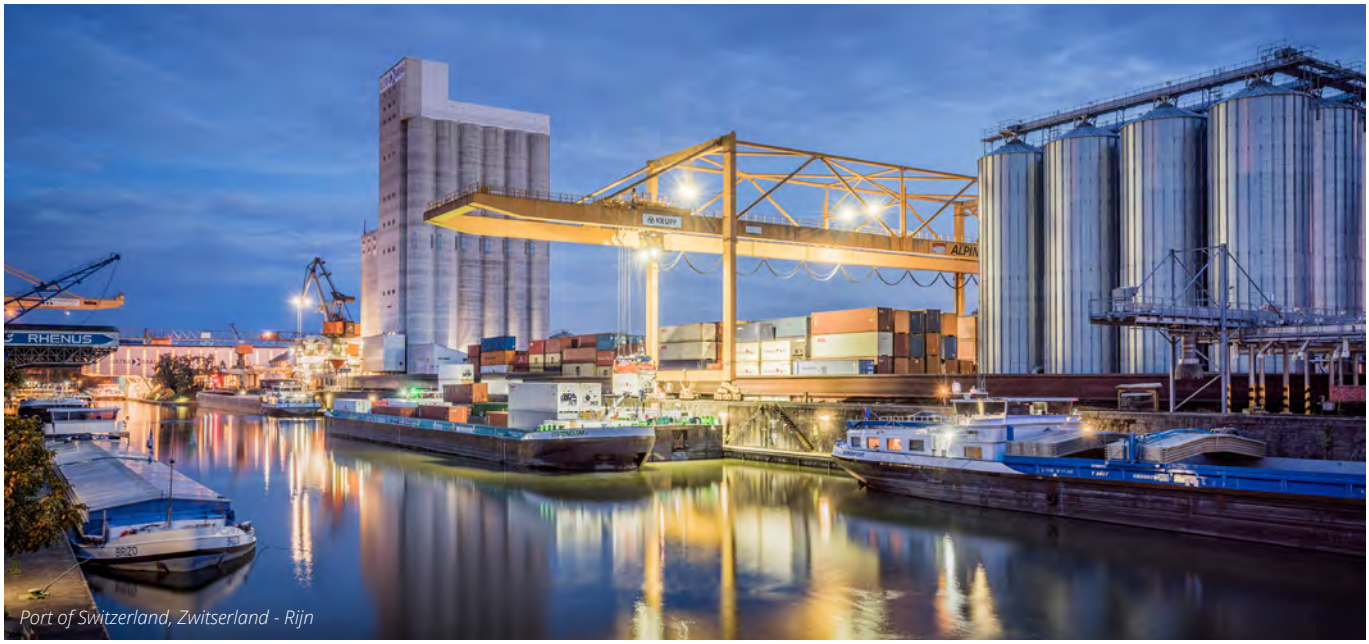
Monitoring van operationele systemen is mogelijk niet haalbaar voor havens met een klein aantal operationele assets of beperkte middelen/capaciteit. Het management moet deze maatregelen in overweging nemen als hun operationele systemen cruciaal zijn voor de havenactiviteiten en als een van hun strategische prioriteiten op het gebied van cyberbeveiliging bestaat in het detecteren van en anticiperen op cybersecurity-bedreigingen voor hun systemen.

	Nummer	Maatregel
●●	[ITOT] 6.1	Wijzigingen in de parameters van kritieke operationele systemen moeten worden gevolgd en geregistreerd.
●●	[ITOT] 6.2	Kritieke systemen moeten worden voorzien van functies om activiteiten en voorvallen op operationele systemen te traceren.
●●●	[ITOT] 6.3	Systeemeigenaren moeten een procedure hanteren voor het beheer van cybersecurity-voorvallen op operationele systemen. In deze procedure moet worden vastgelegd hoe het voorval wordt geregistreerd (als er een register wordt bijgehouden, hoe wordt dat opgeslagen en beveiligd en hoe wordt er een back-up van gemaakt), moet in grote lijnen worden toegelicht wat afwijkende systeemactiviteit inhoudt, en moeten de voorwaarden worden vastgelegd op basis waarvan wordt bepaald of en wanneer een voorval een cybersecurity-incident wordt.
●●●	[ITOT] 6.4	De haven moet overwegen om voor de cybersecurity-monitoring van operationele systemen commerciële tools te gebruiken.

Reactie op incidenten en crisismanagement voor IT/OT-systemen

Deze maatregelen vormen een aanvulling op de maatregelen met betrekking tot de reactie op incidenten en crisismanagement die zijn uiteengezet in de 'organisatorische beleidsmaatregelen en procedures', en zijn in het bijzonder gericht op stakeholders die werken met IT/OT-systemen.

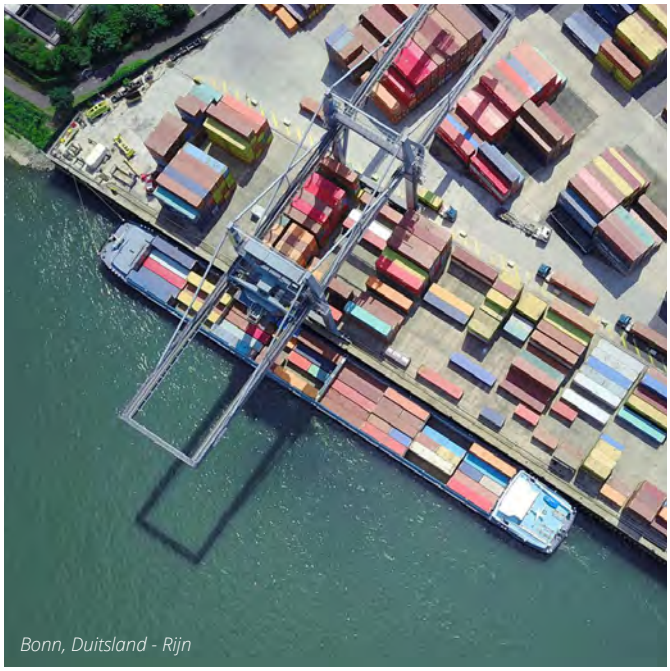
	Nummer	Maatregel
●●	[ITOT] 7.1	Er moet een specifiek, op de IT/OT-systemen gericht plan voor incidentmanagement worden opgesteld. Dit plan moet gedetailleerde informatie bevatten over de back-up van de gegevens die nodig zijn voor de werking van de IT/OT-systemen, over interventieprocedures en over de activering van de noodmodus van IT/OT-systemen en moet voorzien in maatregelen om de handelingen die tijdens het beheer van een incident worden gesteld, te traceren.
●●	[ITOT] 7.2	Operationele systemen moeten voorzien zijn van een modus voor bedrijfsstoring, zodat zij in geval van een incident worden stilgelegd of in handmatige modus kunnen worden gebruikt.



Port of Switzerland, Zwitserland - Rijn

Beveiliging van navigatiesystemen

In dit deel worden enkele mitigerende maatregelen voorgesteld die kunnen worden toegepast op de IT/OT-navigatiesystemen die de haven verbinden met de schepen. Alleen de systemen die relevant zijn voor de havens, zijn in deze leidraad opgenomen. Systemen die alleen relevant zijn voor de bemanning of het schip, komen niet aan bod in deze leidraad. Met deze mitigerende maatregelen kunnen de risico's worden aangepakt die eerder in deze leidraad zijn beschreven in de specifieke aanvalsscenario's voor havens.



Bonn, Duitsland - Rijn

	Nummer	Maatregel
●●	[ITOT] 8.1	Er moet een handleiding voor noodsituaties worden verspreid waarin wordt beschreven hoe de automatische programmering van apparaten voor communicatie op afstand kan worden opgeheven; daarnaast moeten de medewerkers in de haven worden gewezen op de cruciale rol die zij kunnen spelen bij het detecteren van afwijkend of abnormaal gedrag van deze systemen.
●●	[ITOT] 8.2	Havenexploitanten moeten bijzondere voorzorgsmaatregelen nemen voor de monitoring van de beveiliging van netwerken die toegang hebben tot systemen voor de elektronische weergave van binnenvaartkaarten en -informatie (ECDIS), en erop toezien dat deze zijn beschermd tegen externe internettoegang. Software-updates en patches voor ECDIS-systemen moeten systematisch worden geïnstalleerd.
●●●	**[ITOT] 8.3**	Havens die GNSS- en GPS-signalen verzenden en ontvangen, moeten overwegen mitigerende maatregelen te nemen om zich te beschermen tegen het risico op signaalspoofing. Zo zou men tools of technieken kunnen gebruiken die helpen om anomalieën in ontvangen signalen op te sporen, zoals technieken voor de monitoring van de autonome integriteit van ontvangers (RAIM, Receiver Autonomous Integrity Monitoring) die satellietsignalen controleren op onregelmatigheden.
●●●	**[ITOT] 8.4**	Havens die AIS-gegevens van schepen ontvangen, moeten overwegen mitigerende maatregelen te nemen om potentieel abnormaal gedrag op te sporen. Door middel van datamonitoring kunnen onverwachte wijzigingen in de trajecten van vaartuigen of de statische informatie worden gedetecteerd die kunnen wijzen op mogelijk kwade bedoelingen.

Casestudy
Bescherming van containerterminals

De containerterminals die in sommige havens aanwezig zijn, hebben voor hun werkzaamheden uitgebreide IT/OT-apparatuur nodig, waardoor de containerterminal een interessante casestudy vormt voor de toepassing van maatregelen om het cyberrisico voor IT/OT te beperken. Omdat deze terminals door veel havens als kritiek zijn aangemerkt, wordt in deze casestudy dieper ingegaan op de belangrijkste diensten en ICTmiddelen van een containerterminal en de mogelijke cyberrisico's die daarmee gepaard gaan.

Diensten en ICT-middelen van containerterminals

De dienst die containerterminals verlenen aan klanten bestaat in het overladen van containers van schepen naar vrachtwagens of treinen en vice versa in de haven. Containerterminals maken doorgaans gebruik van een systeem voor terminalmanagement of **Terminal Operating System** (TOS) om te communiceren met klanten – transporteurs – en om hun interne werkzaamheden te regelen. Omdat het met andere apparatuur is verbonden, kan dit systeem worden gebruikt voor de volgende diensten:

Aanvragen van klanten managen
Klanten hebben toegang tot een **online applicatie-platform** waar ze informatie kunnen verstrekken over de te vervoeren containers en eventuele vereisten waaraan voor deze containers moet worden voldaan (soort goederen, gewicht, afmetingen, stapelvereisten, enz.). Dat platform maakt gebruik van de informatie die is opgeslagen in het TOS.

Onderhoud van containers
Het TOS centraliseert informatie over schade aan containers en de staat van ontvangen en verzonden containers en **stuurt** in geval van schade een **raming** voor het herstellen of reinigen van de container naar de klant.

Plaatsing van containers
Op basis van de informatie die in het TOS is opgeslagen (afmetingen, locatie, stapelvereisten en type van de containers, maar ook de faciliteiten die beschikbaar zijn voor containeropslag), kan het TOS informatie versturen naar de **stuwadoors/kranen** die vervolgens de containers heffen, verplaatsen en op elkaar stapelen voor opslag of transport.

Operationeel personeelsbeheer
Het TOS stuurt informatie over opdrachten, uit te voeren onderhoud en andere werkzaamheden naar havenarbeiders via **tablets of draagbare toestellen**.

Opstellen van facturen en financieel beheer
Via het systeem worden de facturen voor verleende diensten rechtstreeks **verstuurd** naar de klant en worden bevestigingen van betaling ontvangen en geregistreerd.

Beheer van derden/leveranciers
Derden die bij het containervervoer zijn betrokken, zoals vrachtwagenchauffeurs, hebben toegang tot een **applicatie** waarmee kan worden bevestigd dat zij een container hebben opgehaald of afgeleverd, en die hun informatie verstrekt over het tijdstip waarop en de plaats waar zij een container moeten ophalen of afleveren.

Cyberrisico's voor het TOS van containerterminals

Op basis van de hierboven in kaart gebrachte ICT-middelen en diensten zijn twee belangrijke cyberrisico's geïdentificeerd door de informatie over de waarschijnlijkheid ervan te combineren met de informatie over de mogelijke gevolgen voor het TOS van de containerterminal. Deze risico's zijn:

- Een **aanval met ransomware** op de systemen die door de containerterminal worden gebruikt, met name op het TOS, waardoor de activiteiten in de containerterminal stilvallen. Deze aanval zou tot gevolg kunnen hebben dat het TOS niet correct kan werken en zou daarom enkele of alle bovengenoemde diensten kunnen aantasten. Opgemerkt dient te worden dat als met name de kranen die de containers op elkaar stapelen, niet kunnen werken zonder de input van het TOS, de operationele werkzaamheden in dergelijk geval verstoord zullen worden of zelfs volledig zullen stilvallen.
- Een indringer met kwade bedoelingen die **kritieke gegevens** over de data waarop containers worden opgehaald en afgeleverd, of de locatie of de inhoud van de containers **onderschept**, zou strafbare feiten kunnen plegen (diefstal, smokkel of ophalen van illegale goederen). Hoewel het voor een indringer niet gemakkelijk is een fysieke container daadwerkelijk te stelen, gelet op de afmetingen van de container en de logistieke handelingen die nodig zijn om deze te verplaatsen, kan de indringer de havensystemen wel in de gaten houden om informatie te verkrijgen over de locatie en verplaatsingen van een welbepaalde container, zoals hierboven werd beschreven in een van de scenario's. Dit kan leiden tot zware imagoschade voor de haven en bovendien kan de beveiliging van de haven worden aangetast en kan de haven aansprakelijk worden gesteld voor de gevolgen van de onderschepte gegevens.

Technische cybersecurity-maatregelen voor havens

De onderstaande technische cybersecurity-maatregelen zijn bedoeld voor de IT-afdeling of de afdeling informatiebeveiliging van een haven of een organisatie die samenwerkt met een haven. De hieronder aanbevolen maatregelen zijn aangepast aan de context van de haven, maar zijn algemene IT-beveiligingsmaatregelen die door alle organisaties met een gedegen beleid voor informatiebeveiliging worden genomen. Daarbij wordt opgemerkt dat misschien niet alle maatregelen relevant of haalbaar zijn voor havens met beperkte (personele) middelen, zoals havens zonder specifieke IT-afdeling. Toch wordt aangeraden deze maatregelen te bekijken, omdat ze een goede referentie kunnen bieden voor de fundamentele verwachtingen op het gebied van beveiliging die in aanmerking moeten worden genomen naarmate de 'IT-maturiteit' van een organisatie toeneemt.

Identiteits- en toegangsbeheer (IAM)

In dit deel worden beveiligingsmaatregelen voorgesteld met betrekking tot de regelingen rond de gebruikers van de IT-systemen en -apparatuur van de haven. In deze leidraad wordt een onderscheid gemaakt tussen de IAM-maatregelen voor algemene IT-systemen enerzijds en die voor technische operationele systemen anderzijds. Meer informatie over de IAM-maatregelen voor IT/OT-systemen, is te vinden in punt [ITOT] 4. In de praktijk kunnen beide onderwerpen evenwel samen worden aangepakt.

	Nummer	Maatregel
●	[TSM] 1.1	De persoon die verantwoordelijk is voor de beveiliging van IT-systemen, moet erop toezien dat de authenticatieopties worden geactiveerd op alle pc's, tablets, software en applicaties, en dat standaardwachtwoorden worden gewijzigd. Waar mogelijk moeten er regels en principes worden vastgelegd met betrekking tot de complexiteit van wachtwoorden.
●	[TSM] 1.2	Alle gebruikers van het IT-systeem moeten worden geïdentificeerd en moeten een individueel account op hun naam gebruiken.
●	[TSM] 1.3	Derden en leveranciers mogen alleen toegang krijgen tot de IT-systemen of databases van de haven gedurende een bepaalde periode en voor een specifiek doel.
●	[TSM] 1.4	Er moet een onderscheid worden gemaakt tussen gebruikersaccounts (user accounts) en beheerdersaccounts (admin accounts). Beheerdersaccounts mogen alleen worden toegekend aan de personen die een dergelijk account echt nodig hebben. De rechten van gebruikersaccounts moeten tot het strikt noodzakelijke worden beperkt. Rechten moeten worden verdeeld volgens het beginsel van de 'scheiding van taken', dat wil zeggen dat elke gebruiker uitsluitend toegang mag krijgen tot de gegevens die hij nodig heeft voor zijn taken, en alleen die.
●	[TSM] 1.5	Beheerdersaccounts mogen alleen worden gebruikt voor administratieve handelingen, zoals het beheer van gebruikersaccounts, het installeren of updaten van software en onderhoudswerkzaamheden. Het moet vermeden worden dat beheerdersaccounts worden gebruikt voor andere handelingen, zoals surfen of e-mails beantwoorden.
●	[TSM] 1.6	Anonieme of generieke accounts moeten uit de IT-systemen worden verwijderd.
●●	[TSM] 1.7	Er moet een procedure worden vastgelegd voor het toekennen en afnemen van gebruikersrechten.
●●	[TSM] 1.8	Er moet een procedure worden vastgelegd voor het beheer van de levenscyclus van gebruikersaccounts, met onder meer regels voor het aanmaken, wijzigen, updaten en verwijderen van een account en voor het maken van een back-up van de gegevens. Deze procedure moet ook gedetailleerde regels omvatten voor het toevoegen en verwijderen van gebruikersapparatuur.
●●	[TSM] 1.9	Er moet regelmatig worden nagegaan welke toegangsrechten aan een account zijn verbonden. Na deze controle moeten rechten die werden toegekend maar niet nodig zijn, worden ingetrokken. Oude gebruikersaccounts moeten waar mogelijk worden verwijderd of, wanneer dat niet mogelijk is, worden gedeactiveerd/gearchiveerd.
●●●	[TSM] 1.10	Afhankelijk van het aantal stakeholders dat bij de havenactiviteiten is betrokken, moeten de stakeholders van de haven overwegen een tool in te stellen voor het beheer van de accounts en de toegangsrechten voor de IT-middelen in de haven. Relevante stakeholders zijn onder meer de havenautoriteiten, de terminalexploitanten, de lokale overheden, derden, enz.
●●●	[TSM] 1.11	Voor de meest kritieke applicaties en databases, met name de databases met persoonsgegevens, gevoelige operationele gegevens zoals gedetailleerde scheepsinformatie, en informatie over gevaarlijke goederen of ladingen, moet multifactor-authenticatie (MFA, multi-factor authentication) worden toegepast (zie maatregel [ITOT] 2.6).
●●●	[TSM] 1.12	Er moet een procedure worden vastgelegd voor het beheer van geprivilegieerde accounts (PAM, Privileged Account Management), met inbegrip van de vereisten voor de beveiliging en het beheer van de levenscyclus van deze accounts. Vooral bij geprivilegieerde accounts van derden moet worden toegezien op de naleving van deze procedure.

Beveiliging van de systemen

In dit deel worden enkele maatregelen met betrekking tot IT-systemen en -middelen uiteengezet die moeten worden getroffen om de algemene beveiliging te verbeteren. Omdat ze een specifieke configuratie van de IT-middelen vereisen, zullen deze taken hoogstwaarschijnlijk moeten worden uitgevoerd door een IT-expert of een expert in IT-beveiliging.

	Nummer	Maatregel
●	[TSM] 2.1	IT-teams moeten erop toezien dat er op alle havensystemen, met inbegrip van desktops en servers, antimalware-, antispam- en antivirussoftware is geïnstalleerd en dat deze up-to-date is. Bij deze updates moet voorrang worden gegeven aan de gevoeligste en kwetsbaarste IT-apparatuur.
●●	[TSM] 2.2	Er moet een volledige lijst worden bijgehouden van alle IT-middelen, met inbegrip van hardware, apparatuur, software, systemen, servers, netwerken en netwerkcomponenten, en deze lijst moet regelmatig worden bijgewerkt.
●●	[TSM] 2.3	Aan de hand van de lijst van IT-middelen moet er een beleid voor het uitvoeren van updates worden opgesteld, waarin wordt vastgelegd hoe vaak en hoe deze updates worden uitgevoerd en wie daarvoor verantwoordelijk is, en waarin mogelijk ook wordt voorzien in een goedkeuringsproces. In dit beleid moet worden vastgelegd dat er voor het verkrijgen van de updates alleen een beroep mag worden gedaan op betrouwbare bronnen, zoals de officiële website van de uitgever.
●●	[TSM] 2.4	IT-teams moeten erop toezien dat verbindingen op afstand goed beveiligd zijn door middel van technieken zoals VPN met hoge niveaus van versleuteling. De wachtwoorden waarmee gebruikers op afstand toegang krijgen tot middelen, moeten versterkt worden of gebruikt worden in combinatie met aanvullende voorzieningen (multifactor authenticatie, op de pc geïnstalleerd certificaat, wachtwoord voor eenmalig gebruik, enz.), zodat er geen zwak punt in het systeem ontstaat waarvan misbruik kan worden gemaakt. Er moet ook worden onderzocht of toegang op afstand moet worden beperkt tot specifieke gebruikers of systemen.
●●	[TSM] 2.5	Er moet een beleid worden uitgewerkt voor het gebruik van verwijderbare media (bij voorkeur verboden), met inbegrip van USB-sticks, cd-roms, externe harde schijven, diskettes, enz.
●●●	[TSM] 2.6	Er moet een procedure voor verandermanagement (*change management*) (zoals bedoeld in ITIL) worden vastgelegd met regels voor de integratie van nieuwe apparatuur in havensystemen.
●●●	[TSM] 2.7	Er moet een lijst worden opgesteld van goedgekeurde apparatuur en software en deze moet regelmatig worden bijgewerkt (met voor elke software vermelding van de specifieke toegestane versies).
●●●	[TSM] 2.8	IT-teams moeten een strategie voor de beveiliging van eindpunten (pc, tablet, telefoon en alle andere apparatuur die met het netwerk is verbonden en waartoe gebruikers rechtstreeks toegang hebben) ontwikkelen om op poorten aangesloten eindapparatuur te monitoren en beter te beveiligen door middel van beveiligingstools en -mechanismen, zoals antivirussoftware, versleuteling, beheer van mobiele apparaten (MDM, mobile device management) en 'verharding' (verhoging van de beveiliging door alle applicaties en softwareprogramma's die standaard geïnstalleerd zijn, maar voor het beoogde gebruik niet nodig zijn, te verwijderen).
●●●	[TSM] 2.9	IT-teams moeten een beleid en regels uitwerken met betrekking tot de installatie en configuratie; daarbij is het zo dat er met het oog op de beveiliging a priori alleen diensten en functies die echt nodig zijn, mogen worden geïnstalleerd en dat er alleen toestemming wordt gegeven voor apparatuur die cruciaal is voor de beveiliging en de werking van de havensystemen.
●●●	[TSM] 2.10	IT-teams moeten software-updates en servers regelmatig aan een audit onderwerpen.

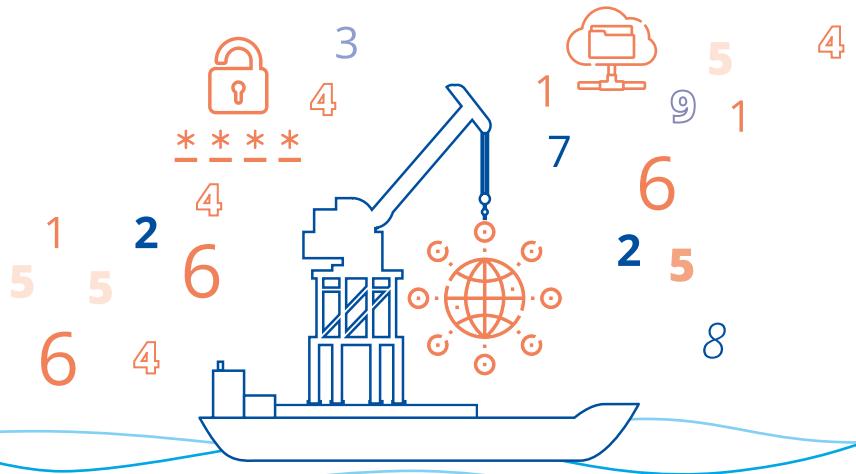
Netwerkbeveiliging

In dit deel worden enkele maatregelen uiteengezet voor de beveiliging van de netwerken die door de havens worden gebruikt. Net als bij het vorige deel is het zeer waarschijnlijk dat er bij de uitvoering van deze maatregelen medewerkers van de afdeling IT(-beveiliging) moeten worden betrokken. Als een haven geen personeel voor IT-beveiliging heeft, kan worden overwogen een beroep te doen op een externe aanbieder van IT-beveiliging.

	Nummer	Maatregel
●	[TSM] 3.1	IT-teams moeten erop toezien dat het wifiwachtwoord complex is en regelmatig wordt gewijzigd.
●	[TSM] 3.2	De wifinetwerken die door de IT-teams van de havens worden gebruikt, moeten zo worden geconfigureerd dat er met het versleutelingsprotocol 'WPA2-enterprise' of 'WPA3-enterprise' kan worden gewerkt. Als dat niet mogelijk is, moet WPA2-(PSK-)AES of WPA3 (Persoonlijk of Overgangsmodus) worden gebruikt.
●●	[TSM] 3.3	Er moeten gepaste regels voor netwerkfiltering (bijvoorbeeld met betrekking tot IP-adressen of geautoriseerd verkeer) worden toegepast.
●●	[TSM] 3.4	Er moet een onderscheid worden gemaakt tussen een professioneel wifinetwerk (typisch voor professioneel gebruik door terdege geauthentiseerde medewerkers) en een openbaar wifinetwerk (typisch voor gasten/ bezoekers of voor persoonlijk gebruik door de medewerkers) en deze moeten van elkaar worden gescheiden. Er moet een beleid voor netwerkscheiding worden uitgevoerd om te vermijden dat aanvallen zich verspreiden binnen de havensystemen en om het risico op toegang via het internet te beperken.
●●	[TSM] 3.5	De IT-teams moeten de toegangspunten tot het netwerk in kaart brengen. Deze lijst moet regelmatig worden bijgewerkt. Ongebruikte toegangspunten tot het netwerk moeten worden uitgeschakeld.
●●	[TSM] 3.6	IT-teams moeten een beleid met betrekking tot de toegestane apparatuur en software uitwerken en uitvoeren om ervoor te zorgen dat alleen betrouwbare componenten in het netwerk worden geïntegreerd.
●●●	[TSM] 3.7	De netwerkregels moeten regelmatig gecheckt worden en zo nodig worden aangepast. De netwerken moeten regelmatig worden gescand om ongeoorloofde netwerkactiviteiten op te sporen.
●●●	[TSM] 3.8	Er moet een beleid worden uitgewerkt voor het melden en aanpakken van abnormale netwerkactiviteit overeenkomstig de in maatregel [OPP] 4.3 beschreven procedures voor incidentmanagement.
●●●	[TSM] 3.9	Er moet een strategie worden vastgelegd voor het monitoren van de netwerkactiviteit. Deze strategie kan verschillende tools en technologieën voor netwerkmonitoring omvatten. In de strategie moet evenwel ook worden voorzien dat deze tools worden gebruikt, geconfigureerd en regelmatig gecontroleerd door opgeleide en competente medewerkers.

Gegevensbescherming

Dit deel heeft betrekking op het beheer van de gegevens die worden vergaard, verwerkt en gebruikt door de stakeholders in de haven. Er wordt op gewezen dat de havens in de Europese Unie vallen onder het toepassingsgebied van de Algemene Verordening Gegevensbescherming (AVG) uit 2016. Indien de AVG van toepassing is, dient u eerst deze wetgeving erop na te slaan met het oog op de correcte verwerking van gegevens en informatie.



	Nummer	Maatregel
●	[TSM] 4.1	De relevante havenmedewerkers moeten een goed begrip hebben van reglementaire en wettelijke vereisten (zoals de AVG) met betrekking tot het verzamelen en bewaren van gegevens die op hen van toepassing zijn. Er moet een beleid voor gegevensbeheer worden gevoerd dat in overeenstemming is met deze reglementaire en wettelijke vereisten en dat eventueel nadere toelichting of aanvullende bepalingen omvat.
●●	[TSM] 4.2	Er moet een beleid voor het bewaren van gegevens worden vastgelegd met daarin duidelijke regels over classificatie en verwijdering van gegevens. Identificeerbare persoonsgegevens en andere bijzonder gevoelige gegevens moeten worden versleuteld of beveiligd daar waar ze worden opgeslagen, maar ook wanneer ze op het interne netwerk circuleren.
●●	[TSM] 4.3	Er moet een beleid worden vastgelegd en uitgevoerd voor het maken van back-ups van gegevens. Er moet regelmatig worden getest of deze back-ups van gegevens goed functioneren en of er voorrang wordt gegeven aan de back-ups van kritieke systemen en gegevens.
●●	[TSM] 4.4	Er moet een datarecuperatieplan (DRP, Data Recovery Plan) worden opgesteld met daarin een gedetailleerde beschrijving van het protocol dat in geval van een cybersecurity-incident of een ander voorval dat tot gegevensverlies kan leiden, moet worden toegepast.
●●●	[TSM] 4.5	Er moet een analyse van de gegevens (data assets) worden uitgevoerd met daarin gedetailleerde informatie over: • het soort gegevens dat de haven moet kunnen raadplegen om de vereiste minimumactiviteiten te kunnen uitvoeren; • de herkomst van de door de haven verwerkte gegevens en gegevensstromen; • de opslag van de verzamelde en verwerkte gegevens; • de interne stakeholders en derden die momenteel toegang hebben tot de databases; • de levenscyclus van gegevens en de behoeften op het gebied van gegevensbewaring.
●●●	[TSM] 4.6	Voor het geval er zich een cybersecurity-incident voordoet, moeten er reserve-harddisks beschikbaar zijn en een online gegevensopslag.
●●●	[TSM] 4.7	Servers voor netwerkopslag moeten regelmatig worden gecontroleerd om eventuele defecten van de opslagruimte, de gegevens of de schijven vroegtijdig op te sporen.

Kwetsbaarheidsbeheer en systeemmonitoring

Maatregelen voor kwetsbaarheidsbeheer zijn bedoeld om informatie te verkrijgen aan de hand waarvan bestaande zwakke punten beter kunnen worden aangepakt. Monitoringactiviteiten kunnen helpen bij het opsporen van kwaadwillig cybergedrag binnen de systemen van de haven.

	Nummer	Maatregel
●●	[TSM] 5.1	Havens moeten een procedure voor cybersecurity-monitoring opstellen zodat ze op de hoogte blijven van de nieuwe kwetsbaarheden die worden vastgesteld en gemeld (door medewerkers, verkopers, derden, sectorgenoten) en ze snel de nodige mitigerende maatregelen kunnen nemen. Deze procedure moet worden afgestemd op de procedures voor de IT/OT-systemen en de procedures van hun eigenaren (zie [ITOT] 6.1).
●●	[TSM] 5.2	IT-teams moeten een procedure voor kwetsbaarheidsbeheer opstellen om de zwakke punten van de ICT-middelen in kaart te brengen (bijvoorbeeld door middel van een kwetsbaarheidsscan), alsook een procedure om deze zwakke punten weg te werken.
●●	[TSM] 5.3	Er moet een logsysteem worden ingesteld om activiteiten en voorvallen te registreren, vooral als het gaat om gebruikersauthenticatie, beheer van accounts en toegangsrechten, wijzigingen van de beveiligingsregels, en alle aanpassingen of veranderingen in de werking van de systemen.
●●	[TSM] 5.4	Voor elk vastgesteld zwak punt moeten er mitigerende maatregelen worden vastgelegd en uitgevoerd. Als er geen mitigerende maatregelen mogelijk zijn of worden vastgelegd, moet de reden daarvoor worden toegelicht en in het dossier worden bewaard.
●●●	[TSM] 5.5	IT-teams moeten de nodige tools of procedures voorzien om de beschikbaarheid van de systemen en apparatuur in de haven in realtime te monitoren. Hierbij moet voorrang worden gegeven aan kritieke systemen (admin-stations, communicatie- en navigatieapparatuur).
●●●	[TSM] 5.6	De havens moeten systemen instellen voor de correlatie en analyse van logs die voorvallen kunnen detecteren en kunnen helpen bij het opsporen van cybersecurity-incidenten.

Deel 3

Tips voor de uitvoering van de mitigerende maatregelen

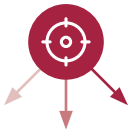
In dit deel worden enkele instrumenten voorgesteld om de uitvoering van de hierboven beschreven mitigerende maatregelen te vergemakkelijken. Omdat de voorgestelde maatregelen sterk verschillen qua inhoud en complexiteit, moeten de havens de volgorde waarin ze maatregelen uitvoeren, bepalen in functie van de beschikbare middelen, het beoogde maturiteitsniveau en hun cybersecurity-behoeften.

In de tabel hieronder is aan de hand van twee criteria, namelijk het maturiteitsniveau op het gebied van cybersecurity van de haven enerzijds en de betrokken stakeholders anderzijds, weergegeven met welke maatregelen het beste kan worden begonnen.

Dit maturiteitsniveau kan op een specifiek moment worden bepaald, bijvoorbeeld aan de hand van het hieronder voorgestelde evaluatieschema. Zodra het niveau bekend is, kan het worden versterkt of verhoogd, of in deze vorm worden behouden. Voor elk van deze opties zullen inspanningen moeten worden geleverd en dus kosten moeten worden gemaakt. Bij de keuze van het beoogde maturiteitsniveau moet het management rekening houden met meerdere criteria, zoals de omvang, de blootstelling en de technologische afhankelijkheid van de haven, het aantal leveranciers en onderaannemers, de technische en financiële middelen van de haven, alsook de ervaring en de cybersecurity-uitdagingen van de haven.

Bij wijze van voorbeeld worden hieronder enkele criteria weergegeven die kunnen helpen bij het vastleggen van het beoogde cybersecurity-maturiteitsniveau. Deze criteria zijn louter indicatief of dienen uitsluitend als bron van inspiratie voor het management, dat in ieder geval moet beslissen welke criteria er worden vastgelegd.

Beoogde maturiteitsniveau



Laag	Middelhoog	Hoog
Mogelijke criteria • De binnenhaven is geen belangrijke hub voor het transport of de handel in de regio. • De IT-teams zijn zeer klein of de IT wordt verzorgd door externe stakeholders. • Er is bijna geen digitale infrastructuur vereist voor de havenactiviteiten.	**Mogelijke criteria** • De binnenhaven heeft belangrijke infrastructuur, maar is niet de belangrijkste handelshub in de regio. • Aanbieders van IT-diensten zijn aanwezig en worden regelmatig ingezet, of de organisatie beschikt over een eigen IT-team (in welke vorm dan ook). • Voor sommige havenactiviteiten is digitale infrastructuur nodig.	**Mogelijke criteria** • De haven is een belangrijke handelshub voor de regio. Er bevindt zich een belangrijke overslag/containerhub of een belangrijke transitzone. • Er is een intern IT-team, met bijbehorende besluitvormers. • De havenactiviteiten zijn sterk afhankelijk van digitale infrastructuur en er worden zelfs enkele 'SmartPort'-technologieën gebruikt.

De verschillende stakeholders zijn de actoren die de respectieve maatregelen moeten uitvoeren. Sommige van de hierboven voorgestelde maatregelen kunnen namelijk alleen worden uitgevoerd door IT-deskundigen of security experts, terwijl andere maatregelen de betrokkenheid vereisen van leidinggevenden of het management van de haven.

Het maturiteitsniveau kan per definitie niet snel evolueren. Een haven die bij de beoordeling vaststelt dat het maturiteitsniveau 'laag' is, kan ernaar streven binnen enkele jaren door de nodige inspanningen een 'middelhoog' niveau te bereiken, maar kan binnen dezelfde termijn niet onmiddellijk streven naar een 'hoog' niveau, zelfs niet wanneer daarvoor aanzienlijke financiële middelen worden uitgetrokken. Cybersecurity-maturiteit is namelijk ook een kwestie van ervaring, cultuur en praktijk en deze vergen nu eenmaal tijd.

Het maturiteitsniveau moet bovendien coherent en zo homogeen mogelijk zijn. Bijvoorbeeld: een haven mag geen genoegen nemen met een 'laag' maturiteitsniveau voor 'organisatorische beleidsmaatregelen en procedures' en streven naar een 'middelhoog' of 'hoog' niveau voor 'netwerkbeveiliging'. Tevens is het nutteloos of zelfs contraproductief en in ieder geval duur om een maatregel van het maturiteitsniveau 'hoog' te willen uitvoeren, als een overgrote meerderheid van de maatregelen van het niveau 'laag' of 'middelhoog' nog niet zijn uitgevoerd (of er zelfs nog geen enkele van deze maatregelen is uitgevoerd). Het uitvoeren van cybersecurity-maatregelen wordt vaak vergeleken met het bouwen van een fort en het spreekt vanzelf dat het geen zin heeft de ene zijde te versterken als de andere zijde volledig blootgesteld is. Cybersecurity-incidenten en aanvallen vinden zeer vaak plaats daar waar de cybersecurity het minst sterk is. Een goede strategie houdt dus in dat de cybersecurity wordt versterkt daar waar deze het zwakst is.

Desalniettemin is het mogelijk, zonder al het overige te verwaarlozen, om op specifieke punten 'een stapje verder te gaan' als deze als bijzonder kritiek zijn geïdentificeerd.

Schema voor de beoordeling van de maturiteit

In deze leidraad wordt het volgende schema geboden om het huidige maturiteitsniveau van een haven te beoordelen.

Het betreft een methode voor zelfbeoordeling waarbij voor elke, in Deel 2 uiteengezette maatregel een score van 1 tot 5 wordt toegekend. Idealiter wordt deze zelfbeoordeling verricht door een klein multidisciplinair team met minstens één vertegenwoordiger per stakeholder, dat wil zeggen:

- een lid van het management, bij voorkeur de persoon die verantwoordelijk is voor cybersecurity;
- een lid van het IT-team dat een goed overzicht heeft over de infrastructuur en de applicaties;
- een operationeel verantwoordelijke met een goede kennis van de bedrijfsprocessen (of meerdere verantwoordelijken als één persoon niet alle bedrijfsprocessen kan afdekken).

Elk teamlid moet elke maatregel los van de andere leden beoordelen. Bij voorkeur beoordeelt elk teamlid elke maatregel op basis van zijn vakkennis en aandachtspunten, maar in ieder geval beoordeelt hij minstens alle maatregelen in zijn kolom van de toepasbaarheidstabel, zelfs als hij voor bepaalde punten een beroep moet doen op zijn collega's.

In een tweede fase komen de leden dan bijeen om hun beoordelingen te bespreken. Als er verschillen worden vastgesteld, wisselen de leden van gedachten en verklaren zij waarom ze een bepaalde score hebben toegekend. Na dit overleg beslist het lid dat de voor de maatregel verantwoordelijke stakeholder vertegenwoordigt, wat de uiteindelijke score is; daarbij houdt hij rekening met de opmerkingen van de andere teamleden.

Om een score van 1 tot 5 toe te kennen, kan de volgende schaal worden gehanteerd:

Punten	Beschrijving
1	Voor deze maatregel vindt er geen coördinatie plaats en zijn er geen medewerkers aangewezen; er is geen formeel programma voorzien of er worden geen specifieke controles uitgevoerd.
2	Bij deze maatregel is er sprake van informele communicatie of een informeel proces, maar er staat niets op papier en er is geen officiële procedure.
3	Sommige taken en verantwoordelijkheden met betrekking tot deze maatregel hebben een formeel karakter en er zijn procedures voor vastgelegd, maar de uitvoering ervan wordt niet systematisch gecontroleerd.
4	De taken en verantwoordelijkheden zijn duidelijk vastgelegd en er zijn formele stappen voorzien voor het controleproces om ervoor te zorgen dat de maatregel consequent wordt uitgevoerd.
5	Men tracht voortdurend de uitvoering van deze maatregel te verbeteren en er vindt een kwantitatieve monitoring plaats van de achterliggende processen om zo inzicht te krijgen in de situatie en deze te verbeteren.

Zodra deze zelfbeoordeling is afgerond, wordt voor elk van de drie rijen van de onderstaande toepasbaarheidstabel het gemiddelde berekend van de scores van de respectieve maatregelen. Zo krijgt men dus voor elk van de maturiteitsniveaus ('laag', 'middelhoog' en 'hoog') een gemiddelde score van 1 tot 5 (3 gemiddelde scores in totaal).

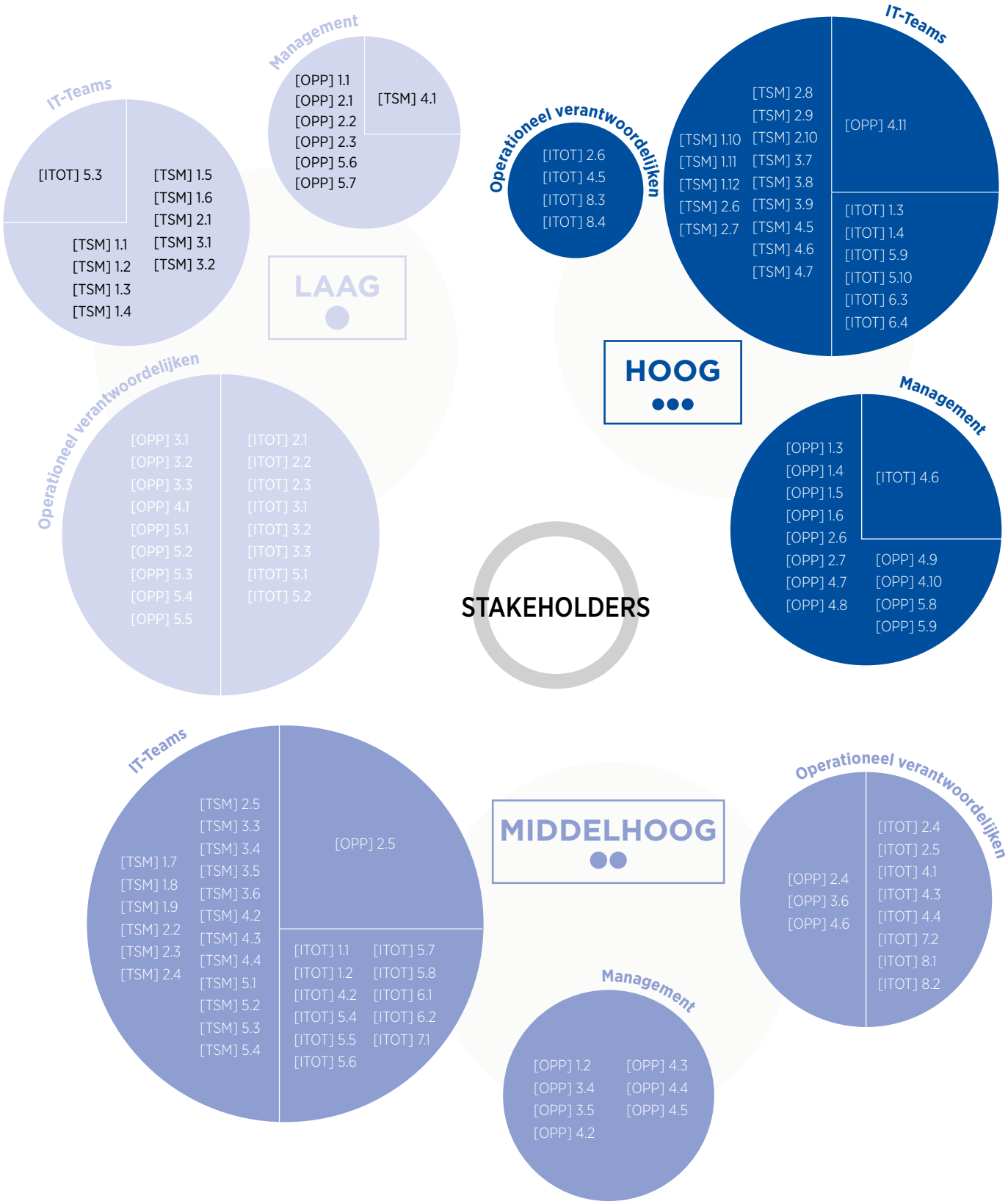
Een maturiteitsniveau wordt geacht te zijn behaald als:

1. de gemiddelde score van de maatregelen van het beoogde niveau minstens 2,5 is;
2. de gemiddelde score van de maatregelen van het niveau onder het beoogde niveau van 3,5 ligt;
3. de gemiddelde score van de maatregelen van het niveau daaronder 4 bedraagt.

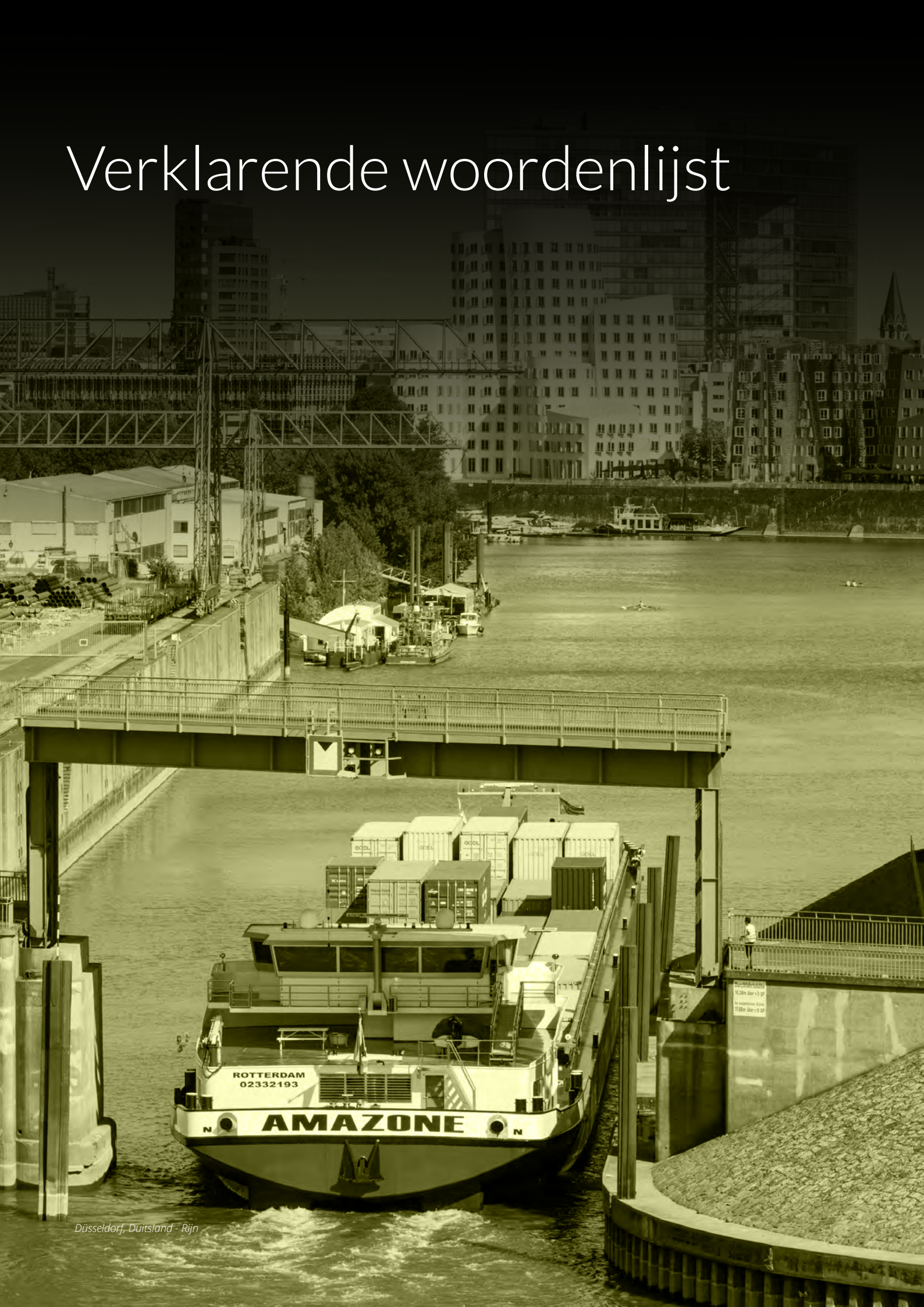
Bijvoorbeeld: om het niveau 'middelhoog' te halen, moet de gemiddelde score van de maatregelen van het niveau 'middelhoog' minstens 2,5 bedragen en moet de gemiddelde score van de maatregelen van het niveau 'laag' minstens bij 3,5 liggen. Om het niveau 'hoog' te halen, moet de gemiddelde score van de maatregelen van het niveau 'hoog' minstens 2,5 bedragen, van het niveau 'middelhoog' minstens 3,5 en van het niveau 'laag' minstens 4.

Toepasbaarheidstabel voor maatregelen

In de onderstaande tabel worden maatregelen voorgesteld die de stakeholders kunnen uitvoeren in functie van het door het management beoogde maturiteitsniveau.



Verklarende woordenlijst



Düsseldorf, Duitsland - Rijn

Achterdeur (back door)

In software is een achterdeur een eigenschap waarvan de legitieme gebruiker niet op de hoogte is en die geheime toegang tot de software verleent.

Bedreiging

Een bedreiging is een actor, een omstandigheid of een gebeurtenis die mogelijk een negatieve impact heeft op een organisatie (haar activiteiten, ICT-middelen, imago, of de met de organisatie verbonden personen) of, via de organisatie, op andere organisaties die met haar verbonden zijn. Om deze impact te hebben, moet de bedreiging misbruik maken van een of meerdere zwakke punten volgens een bepaald scenario. Hoe waarschijnlijker het scenario is, des te belangrijker de zwakke punten zijn en hoe talrijker de bedreigingen zijn, des te waarschijnlijker het is dat een cybersecurity-incident zich voordoet. In dat geval is er sprake van een verhoogde dreiging. Bijvoorbeeld: het dreigingsniveau van een server die is blootgesteld op het internet, is hoger dan dat van een server die alleen is blootgesteld op een intern netwerk, omdat er in het eerste geval mogelijk meer personen zijn die kunnen proberen de server te hacken. Om het dreigingsniveau te verlagen, worden zeer vaak de zwakke punten aangepakt, hetzij door ze weg te werken (of minder talrijk te maken), of door misbruik ervan te bemoeilijken (bijvoorbeeld door bescherming te voorzien). Soms is het mogelijk het aantal actoren, omstandigheden of gebeurtenissen die een negatieve impact kunnen hebben, rechtstreeks aan te pakken. Bij de beoordeling van de bedreiging wordt nooit rekening gehouden met de impact (zie definitie).

BYOD

Staat voor 'Bring Your Own Device' (breng je eigen apparaat mee). In een bedrijfscontext is BYOD een werkwijze die soms wordt aangemoedigd en soms wordt ingeperkt waarbij de werknemers bepaalde persoonlijke apparaten gebruiken voor hun werk. Een typisch voorbeeld hiervan is de smartphone en soms ook de laptop van de medewerker. Voor de medewerkers gaat het erom dat het aangenaam is een apparaat te kunnen gebruiken dat ze goed kennen en graag gebruiken. Voor het bedrijf kan deze werkwijze een besparing betekenen. Op het gebied van cybersecurity kunnen de persoonlijke apparaten een uitdaging vormen, omdat het vaak onmogelijk is ze goed te beveiligen en omdat de risico's toenemen door de grote verscheidenheid aan merken en modellen.

CFM

Cargo and Fleet Management (vrachtbeheer).

Cybersecurity incident

Algemene term die wordt gebruikt om te verwijzen naar een gebeurtenis met negatieve gevolgen op het gebied van cybersecurity. Dit incident kan worden veroorzaakt door defecte apparatuur (een defecte harde schijf), een crash (een server die reboot), sabotage (bewuste introductie van een computervirus), een menselijke fout (klikken op een link in een bedrieglijke e-mail) of zelfs een nalatigheid (een medewerker die zijn Pincode op de achterkant van zijn smart card noteert). Als de gevolgen van dit incident tijdig worden aangepakt, is het incident afgehandeld. Zo niet, kan het incident uitmonden in een crisis met een impact die zich verspreidt en gevolgen die met het verstrijken van de tijd, al dan niet snel, ernstiger worden.

Hacktivisme

Computerhacking (door infiltratie en verstoring van een netwerk of website) om de doelstellingen van politiek of maatschappelijk activisme te bevorderen.[10]

Impact/gevolgen

Met deze term wordt verwezen naar de impact of gevolgen van een cybersecurity-incident wanneer dat zich voordoet (ongeacht de waarschijnlijkheid ervan). De cruciale vraag is dus: Als een dergelijk cybersecurity-incident zich voordoet, wat zal er dan – in het slechtste geval – gebeuren? De impact kan van meet af aan aanzienlijk zijn of niet. Bijvoorbeeld: de impact van een server die wordt vernietigd (cybersecurity-incident) kan zeer uiteenlopend zijn al naargelang het gaat om een ontwikkelingsserver of een kritieke operationele server. De impact kan echter worden beperkt door strategieën te ontwikkelen om eventuele problemen te omzeilen en door het systeem weerbaarder te maken, bijvoorbeeld door noodprocedures te voorzien. In het geval van een kritieke server kan een tweede server worden voorzien die het kan overnemen wanneer de eerste niet meer functioneert. Er kan een back-up worden voorzien voor het geval er gegevens verloren gaan, enz. Bij de beoordeling van de impact wordt nooit rekening gehouden met de bedreiging (zie definitie).

ITIL

(Information Technology Infrastructure Library) is een verzameling van good practices voor het verlenen van digitale diensten. De norm ISO-20000 is gebaseerd op de door ITIL beschreven good practices.

Kroonjuweel

kroonjuwelen (*Crown Juwels*) zijn de cyber-assets die cruciaal zijn voor de werkzaamheden van het bedrijf of de iinstantie. Een analyse is nodig om te bepalen welke van de cyber-assets kroonjuwelen zijn.[11]

[10] https://www.merriam-webster.com/dictionary/hacktivism

[11] https://www.mitre.org/our-impact/intellectual-property/crown-jewels-analysis

Kwetsbaarheid

Zwakke plek in een informatiesysteem, procedure voor systeembeveiliging, interne controle of uitvoering die kan worden misbruikt of geactiveerd door een dreigingsbron.

LBM

`Lock and Bridge Management' (sluis- en brugbediening). Bruggen en sluizen worden aangestuurd door machines; denk aan bijvoorbeeld beweegbare bruggen en installaties waarmee de waterstand kan worden aangepast, zoals sluizen en sluiskolken; dit zijn bijzonder kritieke systemen, aangezien er in het geval van een cyberaanval sprake is van een grootschalig overstromingsrisico.

Operationeel beveiligingscentrum (SOC, Security Operations Center)

Een operationeel beveiligingscentrum is een dienst binnen een bedrijf of instantie waar alles wat verband houdt met IT-beveiliging wordt gecentraliseerd. Deze afdeling kan actie ondernemen met betrekking tot medewerkers van de organisatie, processen en technologie om de beveiligingshouding van de organisatie voortdurend te monitoren en te verbeteren en tegelijkertijd cybersecurity-incidenten te voorkomen, op te sporen, te analyseren en erop te reageren.[12]

Phishing

Bedrog waarbij een internetgebruiker (door middel van een misleidend e-mailbericht) wordt overgehaald persoonlijke of vertrouwelijke informatie te onthullen die de oplichter kan misbruiken voor illegale doeleinden.[13]

Programmeerbare logische besturingseenheid (PLC, Programmable Logic Controller)

Programmeerbaar digitaal elektronisch apparaat dat bedoeld is om industriële processen aan te sturen door middel van sequentiële verwerking. Het apparaat stuurt orders naar (pre) actuatoren op basis van inputgegevens (sensoren), instructies en/of een computerprogramma. In bijna alle industriële processen wordt er uitgebreid gebruikgemaakt van PLC's. Voor complexe processen wordt doorgaans een SCADA voorzien voor de coördinatie tussen de verschillende PLC's en hun integratie in een grootschaliger netwerk.[14]

Risico

In de context van cybersecurity wordt deze term formeel gebruikt voor de beoordeling van een reeks bedreigingen voor een systeem die in meer of mindere mate waarschijnlijk zijn en waarvan de gevolgen in meer of mindere mate ernstig kunnen zijn. Er is sprake van een hoog risico als de waarschijnlijkheid en de impact van een bedreiging groot zijn en van een laag risico als deze beperkt zijn. Bij een risicobeoordeling worden de waarschijnlijkheid en de impact van de verschillende bedreigingen los van elkaar beoordeeld en worden op basis daarvan algemene conclusies geformuleerd. Ter illustratie: het 'risico op overstroming' wordt beoordeeld in functie van de waarschijnlijkheid van een overstroming (overstromingsgevoelige gebieden), maar ook in functie van de kenmerken van het desbetreffende gebied, bijvoorbeeld of het dichtbevolkt is of niet. Het risico op overstroming wordt aldus ongeveer even groot geacht in een overstromingsgevoelig gebied met een zeer lage bevolkingsdichtheid als in een niet-overstromingsgevoelig gebied dat zeer dichtbevolkt is (niet-overstromingsgevoelig gebied moet worden opgevat als een gebied waar de kans op overstroming gering is, maar niet onbestaand). Het risico kan worden verlaagd door de impact te beperken of door de waarschijnlijkheid te verlagen. In het geval van het overstromingsrisico kunnen enerzijds de waterlopen worden gekanaliseerd en kunnen er dammen en opvangbekkens worden gebouwd (om de waarschijnlijkheid te verlagen); anderzijds kunnen er dijken worden aangelegd om de huizen te beschermen, kan de voorkeur worden gegeven aan paalwoningen en kan worden vermeden dat de bevolking te sterk toeneemt in overstromingsgevoelige gebieden (om de impact te beperken).[15]

SCADA

Supervisory Control And Data Acquisition (systeem voor het controleren en verwerven van gegevens). Een SCADA-systeem is een systeem voor grootschalig beheer op afstand dat het mogelijk maakt om in realtime een groot aantal maatregelen op afstand te verwerken en op afstand technische installaties te bedienen. Het is industriële instrumentatietechnologie. SCADA-systemen vormen een hele uitdaging voor de cybersecurity, omdat deze apparaten verbonden zijn met een netwerk en de persoon die erin slaagt de controle erover te verkrijgen, in staat stellen de onderliggende technische installaties te bedienen.

[12] https://www.trellix.com/en-us/security-awareness/operations/what-is-soc.html

[13] https://www.merriam-webster.com/dictionary/phishing

[14] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[15] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Social engineering

Social engineering verwijst naar alle technieken die worden gehanteerd om een doelwit ertoe te brengen specifieke informatie te onthullen of een specifieke handeling te stellen voor illegale doeleinden.[16]

Spoofing

In een cybersecurity-context is spoofing het geheel aan methoden die bedoeld zijn om een doelwit te misleiden over de werkelijke herkomst van de informatie die hij of zij ontvangt. Voorbeelden van methoden die worden gebruikt, zijn zich uitgeven voor iemand anders, zich voordoen als iets anders, nabootsen, enz.

Verharding (hardening)

Beveiliging van een systeem door componenten die het systeem (bijvoorbeeld een pc of een server) niet nodig heeft om te kunnen functioneren, te verwijderen. Verharding houdt in dat het 'aanvalsoppervlak' van een systeem wordt verkleind, dat wil zeggen dat alle onnodige componenten die standaard geïnstalleerd zijn en die (eventueel) zwakke punten kunnen bevatten (applicaties, softwarebibliotheken, optionele modules, enz.), worden verwijderd. Het wordt algemeen erkend dat het aantal zwakke punten in een systeem die vatbaar zijn voor misbruik, ongeveer evenredig is aan het aantal programmatuurregels dat het systeem bevat. Door de niet-noodzakelijke componenten te verwijderen, daalt dus het aantal zwakke punten waarvan een aanvaller misbruik kan maken.

WEP/WPA/WPA2/WPA3

Deze acroniemen verwijzen naar beveiligingsprotocollen voor toegang tot een draadloos netwerk (wifi). WEP (Wired Equivalent Privacy) verscheen in 1999. WEP bood slechts een zeer beperkte beveiliging en werd daarom in 2003 vervangen door het WPA-protocol (Wi-Fi- Protected Access). WPA is van meet af aan ontworpen als een overgangsprotocol. In 2004 werd het namelijk vervangen door WPA2, dat gebaseerd is op de norm 802.11i van het Institute of Electrical and Electronics Engineers (IEEE). WPA3 werd gepubliceerd in 2017, maar is slechts een verder uitgewerkte versie van WPA2, dat (nog) niet achterhaald is en in 2023 nog steeds zeer vaak wordt gebruikt. WPA2 bestaat in twee versies. Enerzijds is er de 'persoonlijke' versie van WPA2 (die ook wel WPA2-PSK wordt genoemd waarbij PSK staat voor 'Pre-shared Key'), die gebaseerd is op een gedeelde sleutel en bedoeld is voor gebruik thuis, in familieverband of in een zeer klein gebouw. Anderzijds is er WPA2 'Enterprise', dat is gebaseerd op RADIUS-authenticatie (meerdere gebruikers met verschillende accounts) en bedoeld is voor gebruik in een bedrijf. Er wordt op gewezen dat WPA2-PSK met twee versleutelingsalgoritmen kan worden gebruikt: AES en TKIP. Het algoritme AES is beter beveiligd.

[16] https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

Foto credits

Beeldmateriaal, courtesy Europese Federatie van Binnenhavens (EFIP)
p. 28 : © Steve Haider
p. 45 : © Patrik Walde, patrikwalde.com
p. 46 : © AZS Group Bonn
p. 58 : © Haven Düsseldorf

Shutterstock
Adobe stock

Art direction & design : dot. Deloitte Agency Frankrijk

Europees Comité voor de opstelling van standaarden voor de binnenvaart (CESNI)
Secretariaat van de Centrale Commissie voor de Rijnvaart (CCR)
2 Place de la République – CS10023
F-67082 Strasbourg cedex
Frankrijk
comite_cesni@cesni.eu
https://www.cesni.eu

In samenwerking met de Europese Federatie van binnenhavens (EFIP)
The European Port House
Treurenberg 6
B-1000 Brussel
België