Europese Commissie

# Toolkit voor de cyberbeveiliging van de vervoerssector

# Inleiding

Het directoraat-generaal Mobiliteit en Vervoer (DG MOVE) van de Europese Commissie heeft opdracht gegeven voor het opstellen van deze toolkit om belanghebbenden beter bewust te maken van en voor te bereiden op cyberdreigingen. De toolkit verschaft inzicht in cyberdreigingen en hoe de gevolgen daarvan kunnen worden beperkt. Deze toolkit biedt twee alternatieve bewustmakingstrajecten die overeenstemmen met twee verschillende profielen:

- vervoerspersoneel (met algemene informatie en richtsnoeren);
- besluitvormers op het gebied van cyberbeveiliging.

Hyperlinks verbinden de verschillende onderdelen van de toolkit en ondersteunen het navigeren.

**De in deze toolkit vermelde methoden zijn uitsluitend bedoeld als adviezen. De aanbevelingen in deze toolkit zijn niet bindend of verplicht. Bovendien geeft deze toolkit niet de officiële standpunten van de Europese Commissie weer en is de toolkit niet bedoeld als middel om bestaande of toekomstige EU-wetgeving na te leven.**

# Bewustmakingsprofielen op het gebied van cyberbeveiliging

**Profiel I: Vervoerspersoneel.** Het eerste traject is gericht op alle werknemers in vervoersorganisaties. Het biedt informatie om een beter inzicht te verwerven in de meest voorkomende cyberdreigingen voor vervoer. Daarnaast biedt het inzicht in de aanpak van potentiële cyberdreigingen, met inbegrip van het identificeren, rapporteren en beperken ervan door goede praktijken op het gebied van cyberbeveiliging.

**Profiel II: Besluitvormers op het gebied van cyberbeveiliging in de vervoerssector.** Het tweede traject is gericht op de besluitvormers op het gebied van cyberbeveiliging in vervoersorganisaties. Dit traject vestigt de aandacht op goede praktijken voor de verschillende vervoerswijzen. Er worden goede praktijken voorgesteld om opkomende cyberdreigingen tegen vervoersorganisaties te identificeren, te detecteren, erop te reageren en de organisatie te beschermen.

Europese Commissie

# Toolkit voor de cyberbeveiliging van de vervoerssector

## Dreigingslandschap in de vervoerssector

Opkomende cyberdreigingen voor de verschillende vervoerswijzen


## Bewustmakingsprofielen op het gebied van cyberbeveiliging

Alternatieve bewustmakingstrajecten op het gebied van cyberbeveiliging voor verschillende vervoersprofielen

Europese Commissie

# Dreigings-landschap in de vervoerssector

Het digitale dreigingslandschap is dynamisch en evolueert voortdurend. Niettemin kunnen we een aantal cyberdreigingen in kaart brengen waar alle vervoerswijzen mee worden geconfronteerd.

Europese Commissie

## Dreigingsactoren

Personen of organisaties die de veiligheid en beveiliging van vervoersdiensten en -systemen mogelijk kunnen beïnvloeden.

## Opkomende cyberdreigingen

Geselecteerde cyberdreigingen die een impact kunnen hebben op de veiligheid en beveiliging van vervoersdiensten en -systemen.

Europese Commissie

# Dreigingsactoren

Personen of organisaties kunnen opzettelijk of onopzettelijk zwakke punten prijsgeven, waarvan gebruik kan worden gemaakt. Dat kan leiden tot incidenten die schadelijke gevolgen kunnen hebben voor vervoersdiensten, m.i.v. de veiligheid, beveiliging, bedrijfsvoering, financiën en reputatie van die diensten.

De belangrijkste kwaadwillige actoren die vervoersorganisaties in het vizier nemen, zijn **cybercriminelen**, **insiders**, **natiestaten** en **door staten gesteunde groepen**.
Tegenstanders zoals **cybercriminelen** voeren grootschalige aanvalscampagnes uit en zijn vaak uit op geld.

**Insiders** kennen de bijzondere kenmerken van de organisaties waarvoor ze werken en zijn vaak goed op de hoogte van de subtiele zwakke punten in de beveiliging.

Insiders kunnen bijvoorbeeld ontevreden werknemers, leveranciers en individuele aannemers zijn.
Naarmate de wereldwijde geopolitieke spanningen toenemen, **richten natiestaten** en **door staten gesteunde groepen** zich op strategische langetermijndoelstellingen. Vaak proberen zij zichzelf tot diep binnen de systemen van de organisatie te infiltreren en gevoelige informatie te verzamelen. Zodra zij voet aan de grond krijgen in de systemen, proberen door staten gesteunde aanvallers een positie te verwerven waarin zij de grootst mogelijke schade kunnen berokkenen.

Niet-kwaadaardige dreigingsactoren zijn bijvoorbeeld **insiders** die onopzettelijk of per ongeluk handelingen uitvoeren die leiden tot cyberincidenten en, in de ergste gevallen, tot cyberincidenten.

Europese Commissie

# Opkomende cyberdreigingen

Verschillende cyberdreigingen focussen op vervoer: **DDoS-aanvallen (Distributed Denial of Service)**, **DoS-aanvallen (Denial of Service)**, gegevensdiefstal, **malwareverspreiding**, **phishing**, softwaremanipulatie, **ongeoorloofde toegang**, destructieve aanvallen, vervalsing of omzeilen van het beveiligingsproces van de exploitant, maskering van de identiteit, misbruik van toegangsrechten, **social engineering**, defacen van websites, afluisteren, misbruik van activa en manipulatie van hardware.

Op basis van uitgebreid literatuuronderzoek van openbaar beschikbare documentatie en interviews met deskundigen zijn de meest urgente opkomende cyberdreigingen voor de vervoerssector vastgesteld, namelijk: malware, (D) DoS-aanvallen, ongeoorloofde toegang en diefstal, en softwaremanipulatie.

Europese Commissie

## Dreiging #1: Malware

kwaadaardige software die schade kan berokkenen aan personen of organisaties in alle vervoerswijzen

## Dreiging #2: (D)DoS-aanval (Distributed) Denial of Service

cyberaanval waardoor personen or organisaties geen toegang krijgen tot vervoersdiensten en -middelen

## Dreiging #3: Ongeoorloofde toegang en diefstal

Ongeoorloofde toegang, toe-eigening en exploitatie van kritieke activa


## Dreiging #4: Software-manipulatie

Cyberaanvallen gericht op software om functies daarvan te manipuleren en specifieke aanvallen uit te voeren

Europese Commissie

# Dreiging #1: Malware

Malware bestaat uit kwaadaardige software die verschillende soorten softwaretoepassingen kan omvatten zoals virussen, Trojaanse paarden, wormen, ransomware, cryptocurrency-miners of andere software die schadelijke gevolgen kan hebben voor organisaties of personen in alle vervoerswijzen.

Een van de belangrijkste prioriteiten van cyberbeveiliging in alle vervoerswijzen is het beperken van de verspreiding van malware die ontworpen is om opzettelijk schade toe te brengen aan computers, servers, clients en/of netwerken. Een typische aanvalsvector kan bestaan uit phishingmails gericht aan werknemers. Andere aanvalsvectoren kunnen verschillende en geavanceerde social engineering-strategieën omvatten zoals het inpluggen van een USB in een vrije poort (bv. om een mobiele telefoon op te laden). Door in verdachte e-mails op een hyperlink te klikken of een bijlage te openen, kan de gebruiker onbewust malware installeren.

Zo heeft de cyberaanval met WannaCry-ransomware meer dan 150 landen getroffen en meer dan 230 000 systemen besmet. Het ging om ransomware die zich gewoonlijk verspreidt via phishingmails met geïnfecteerde bijlagen of hyperlinks. Met dit soort aanvallen wordt social engineering op kwaadaardige wijze uitgebuit om systeemgebruikers te misleiden om specifieke malware te installeren (of te activeren).

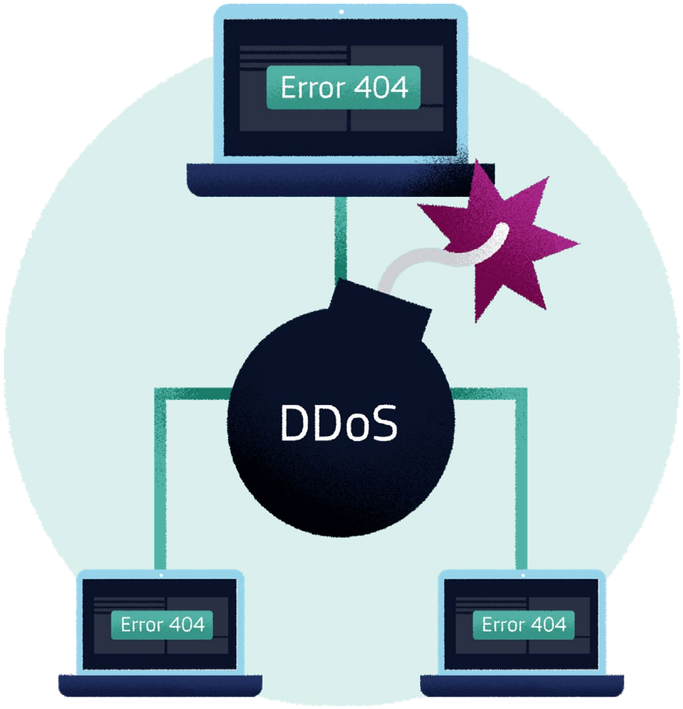
Europese Commissie

# Dreiging #2: (D)DoS-aanvallen — (Distributed) Denial of Service

DDoS-aanvallen (Distributed Denial of Service) en DoS-aanvallen (Denial of Service) vormen een bedreiging voor de beschikbaarheid en toegankelijkheid van gegevens, diensten, systemen en andere middelen. Dit soort aanvallen kunnen qua duur uiteenlopen en kunnen op meer dan één dienst of systeem tegelijk gericht zijn. DDoS-aanvallen maken gebruik van meerdere systemen (of aanvalskanalen) om diensten of systemen te overbelasten met verzoeken. Bij succesvolle aanvallen zijn diensten en systemen niet meer in staat om te reageren op het onverwachte volume aan verzoeken. Dit heeft tot gevolg dat de toegang tot diensten en bronnen wordt geweigerd.

Diensten en systemen die deel uitmaken van vervoersorganisaties kunnen ook gebruikt worden voor DDoS- en DoS-aanvallen om specifieke operationele systemen of andere organisaties te treffen.

Zo kunnen bedrijfsinformatiesystemen (zoals pc's en apparaten) het doelwit zijn om toegang te krijgen tot operationele technologieën, die voor de overdracht van operationele gegevens verbonden kan zijn met het internet of netwerken. Verbindingen tussen verschillende systemen en netwerken (zoals bedrijfsnetwerken, operationele technologieën en toegang op afstand voor onderhoud) kunnen kwetsbaarheden vormen die benut kunnen worden voor DDoS- of DoS-aanvallen op kritieke vervoersdiensten en -systemen. Zo kunnen DDoS- of DoS-aanvallen gemeenschappelijke netwerken en communicatieprotocollen zoals Web Services Dynamic Discovery (WS-Discovery) benutten, die IoT-apparaten gebruiken om automatisch alle knooppunten in LAN's (Local Area Network) bloot te leggen. Als IoT-apparaten kwetsbaarheden vertonen, kunnen aanvallers deze benutten om andere gekoppelde apparaten op te sporen en DDoS- of DoS-aanvallen uit te voeren.



Europese Commissie

# Dreiging #3: Ongeoorloofde toegang en diefstal

Dreigingsactoren kunnen zonder toestemming logische of fysieke toegang proberen te verkrijgen tot een netwerk, systeem, toepassing, gegevens, of een andere bron om kwaadaardige activiteiten uit te voeren, met inbegrip van diefstal van gevoelige gegevens of middelen (waaronder fysieke middelen). Dreigingen zoals ongeoorloofde toegang en diefstal richten zich op vertrouwelijke en gevoelige activa (met inbegrip van persoonsgegevens, toegangsgegevens van bevoorrechte accounts, systemen en andere soorten vertrouwelijke en door eigendomsrechten beschermde informatie). Bij deze dreigingen kan misbruik worden gemaakt van kwetsbaarheden in systemen en van personen die onbewust gevoelige gegevens openbaar maken, zoals toegangsgegevens (bv. login, wachtwoord, enz.) of persoonlijke gegevens (bv. e-mail, persoonlijk identificatienummer enz.).

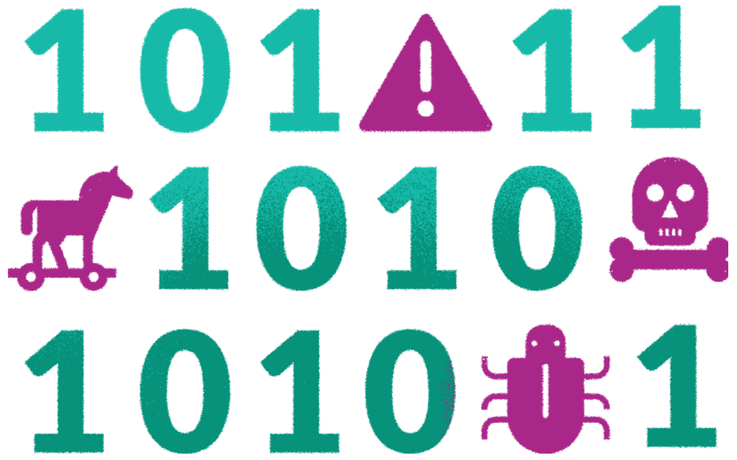
Wat ongeoorloofde toegang betreft, is identiteitsdiefstal het onwettige gebruik van persoonsgegevens of unieke identificatiecodes om zich voor te doen als een andere persoon of andere dienst of systeem om toegang te krijgen tot persoonlijke of door eigendomsrechten beschermde middelen (bv. inclusief financiële en fysieke middelen). Dergelijke cyberdreigingen kunnen zich ook richten op fysieke activa in alle vervoerswijzen.

Europese Commissie

# Dreiging #4: Softwaremanipulatie

Onjuiste configuratie en manipulatie van software en daarmee verbonden systemen of onderdelen kunnen een rechtstreekse impact hebben op de beveiligingspositie van vervoersdiensten en -systemen.
Cyberaanvallen die gebruik maken van softwaremanipulatie wijzigen software-instellingen of beïnvloeden de integriteit van gegevens om het gedrag van systemen en diensten te veranderen. Aanvallers kunnen opzettelijk software (of een gedeelte ervan) manipuleren om voordelen te behalen (bv. het verkrijgen van ongeoorloofde toegang, legitieme personen of systemen de toegang tot noodzakelijke middelen ontzeggen, het verzamelen van gevoelige informatie, het veranderen van functioneel gedrag enz.) ten aanzien van gevoelige activa.

Aanvallen kunnen bijvoorbeeld gericht zijn op communicatiekanalen van fabrikanten om schadelijke software-updates te uploaden naar diensten en systemen (met inbegrip van operationele technologieën). Een dreigingsactor maakt gebruik van gecompromitteerde inloggegevens om toegang te krijgen tot een beveiligd onderhoudsnetwerk op afstand om gemanipuleerde software te installeren en compromitteert zo andere toegankelijke diensten en systemen. De dreigingsactor installeert gemanipuleerde software die specifieke diensten en systemen verder compromitteert of voert een aanval uit op andere geconnecteerde diensten of systemen.



Europese Commissie

# Bewustmakingsprofielen op het gebied van cyberbeveiliging

Europese Commissie

1

## Profiel I: Vervoerspersoneel

Het eerste traject is gericht op alle medewerkers van vervoersorganisaties, van operationeel tot administratief personeel. Dit traject biedt richtsnoeren voor een beter begrip en bewustzijn van de meest voorkomende cyberdreigingen. Het biedt ook inzicht in de aanpak van potentiële cyberdreigingen, met inbegrip van het identificeren, rapporteren en beperken daarvan. Dit traject is relevant voor alle vervoerswijzen.

2

## Profiel II: Besluitvormers op het gebied van cyberbeveiliging in de vervoerssector

Het tweede traject is gericht op besluitvormers op het gebied van beveiliging of cyberbeveiliging in vervoersorganisaties. In dit traject worden goede praktijken voorgeteld op de verschillende vervoerswijzen zijn afgestemd. Het biedt met name goede praktijken om opkomende cyberdreigingen tegen vervoersorganisaties te identificeren, op te sporen en erop te reageren en organisaties daartegen te beschermen.

Europese Commissie

# Profiel I: Al het vervoerspersoneel

Dit deel is gericht op alle medewerkers van vervoersorganisaties, van operationeel tot administratief personeel. Het biedt richtsnoeren voor een beter begrip en bewustzijn van de meest voorkomende cyberdreigingen. Het biedt ook inzicht in de aanpak van potentiële cyberdreigingen, met inbegrip van het identificeren, rapporteren en beperken daarvan.
Er worden aanbevolen praktijken en nuttige tips aangereikt die relevant zijn **voor alle vervoerswijzen**.

# Goede praktijken tegen malware

U kunt uw organisatie helpen beschermen door goede praktijken te volgen om **de verspreiding van malware te identificeren en te voorkomen**, zoals:

- ***Volg het beveiligingsbeleid*** *en andere richtsnoeren, zoals opslagmedia en bestanden scannen op virussen, bepaalde bestandstypes niet openen of mailen (bv. uitvoerbare bestanden zoals .exe, .bat, .com enz.), alleen toegestane software installeren, ervoor zorgen dat de software (met inbegrip van het antivirusprogramma) up-to-date is en goed functioneert.*

- ***Maak regelmatig een back-up van uw gegevens*** *op beveiligde (en toegelaten) gegevensopslagapparaten en -diensten, die encryptie zouden moeten ondersteunen om gegevens in rust te beschermen en beschikbaar moeten zijn voor gegevensherstelprocedures.*

- *Bescherm alle systemen, ook mobiele en eindapparaten, met geschikte* ***beveiligingsmaatregelen*** *(bv. wachtwoord, versleuteling enz.) en zorg ervoor dat alle systemen veilig vergrendeld zijn (fysiek en digitaal) als ze onbeheerd zijn.*

- *Open geen bijlagen of klik niet op links in onverwachte e-mails en verdachte pop-upvensters in webbrowsers met een vreemd uitziende tekst of van onbekende afzenders en internetdomeinen.*

- *Sluit geen* ***onbetrouwbare of onbekende verwijderbare apparaten****, zoals USB-sticks, harde schijven en andere opslagapparaten, op uw computer aan.*

- *Schakel software ter bescherming tegen malware niet uit (bv. antivirussoftware, software voor contentcontrole, firewall enz.).*

- ***Update geïnstalleerde software*** *regelmatig naar de laatst beschikbare versies (die informatiebeveiligingsfunctionarissen of systeembeheerders met regelmatige updates uitbrengen).*

- *Vermijd het gebruik van bevoorrechte accounts (bv. op beheerdersniveau) en inloggegevens voor regelmatige activiteiten en operationele taken.*

- *Meld elke verdachte mail of elk onverwacht systeemgedrag aan de informatiebeveiligingsverantwoordelijken of systeembeheerders.*

- *Besteed bij dagelijkse routinewerkzaamheden aandacht aan informatiebeveiliging om IT-beveiligingsproblemen te onderkennen en er adequaat op te reageren.*

Europese Commissie

# Goede praktijken tegen (D)DoS-aanvallen - (Distributed) Denial of Service

U kunt uw organisatie helpen beschermen door het identificeren van **DDoS-aanvallen (Distributed Denial of Service)** en **DoS-aanvallen (Denial of Service)**. Neem onmiddellijk contact op met uw beveiligings- en IT-teams als u een van de volgende indicatoren ontdekt of ervaart van mogelijke DDoS- en DoS-aanvallen op uw diensten of systemen:

- *toename van het aantal verzoeken die capaciteit van het netwerk vergen (merkbaar aan de tragere werking en respons) en de dienst of het systeem overspoelen met meer verzoeken dan deze of dit aankan;*

- *toenemende vraag naar geheugencapaciteit zonder duidelijke reden;*

- ***onverwacht gedrag van diensten of systemen**, frequente crashes en vreemde foutmeldingen als gevolg van kwaadwillig gebruik van IT-hulpmiddelen of netwerkverbindingen;*

- ***gestoorde prestaties** van apparaten, vertraging bij de uitvoering van triviale taken en merkbare activiteiten (bv. lawaaierige ventilator terwijl apparatuur traag werkt);*

- ***onverwachte internetverbindingen of verlies van verbindingen** op diensten en systemen;*

- *subtiele veranderingen in de bedieningsinstellingen of operationele technologieën die tot fysieke schade leiden;*

- *geweigerde toegang tot bevoorrechte of beheerdersaccounts waardoor responsprocedures bij incidenten zich niet kunnen herstellen.*

# Goede praktijken tegen ongeoorloofde toegang en diefstal

Om aanvallen met ongeoorloofde toegang en diefstal te voorkomen, moeten beginselen zoals *"need-to-know"* en *"security and privacy by default"* worden gevolgd, die benadrukken dat gevoelige en vertrouwelijke activa (inclusief persoonlijke en gevoelige gegevens, vervoerssystemen, enz.) uitsluitend toegankelijk mogen zijn voor personen met rechtmatige toegang voor het uitvoeren van hun taken.
U kunt uw organisatie helpen beschermen door goede praktijken te volgen voor het voorkomen van ongeoorloofde toegang en diefstal, zoals:

- *Volg de veiligheidsrichtlijnen van de organisatie.*

- *Vermijd het delen en online publiceren van inlog- en persoonlijke gegevens, ook van foto's die dergelijke informatie kunnen bevatten.*

- *Vermijd het gebruik of de doorgifte van inlog- en persoonsgegevens (en andere gevoelige gegevens) op onbetrouwbare en onbeveiligde netwerken, apparaten of webdiensten (bv. websites die onbeveiligde protocollen of adressen gebruiken zoals http:// in plaats van beveiligde https://).*

- ***Deel nooit uw toegangsgegevens met iemand*** *(bv. login en wachtwoord), ook niet via e-mail of telefoon.*

- *Bescherm gevoelige gegevens die op toetsenborden worden getypt of op schermen worden weergegeven (met inbegrip van mobiele apparaten) tegen onbevoegde personen, installeer privacyschermen, werk niet op openbare plaatsen met eigen apparaten, en voorkom dat apparaten onvergrendeld en onbewaakt blijven.*

- ***Gebruik complexe wachtwoorden*** *(bv. een voldoende lang wachtwoord dat alfanumerieke en speciale karakters combineert) die voldoen aan de beveiligingsrichtlijnen van de organisatie om ongeoorloofde toegang te voorkomen.*

- ***Wijzig de standaardwachtwoorden*** *van aangesloten systemen en apparaten (bv. printers, routers, camera's, smart locks enz.).*

- *Vermijd het gebruik van dezelfde toegangsgegevens (bv. login en wachtwoord) voor meerdere diensten en systemen, en vermijd het gebruik van dezelfde toegangsgegevens voor diensten en systemen waarvoor bevoorrechte accounts vereist zijn.*

- *Stuur wachtwoorden en sleutels voor overgedragen beschermde bestanden (bv. zip-bestanden) alleen via een afzonderlijk communicatiekanaal (bv. een sms via gsm en telefoongesprek) en nooit via e-mail.*

- ***Activeer de tweefactorauthenticatie (2FA)*** *of multifactorauthenticatie (MFA), indien mogelijk.*

Europese Commissie

# Goede praktijken tegen softwaremanipulatie

U kunt uw organisatie helpen beschermen door goede praktijken te volgen voor het identificeren en voorkomen van softwaremanipulatie, zoals:

- *Installeer geen onbetrouwbare software op systemen en apparaten (met inbegrip van pc's, servers, randapparatuur, netwerkapparaten, smartphones enz.).*
- *Installeer alleen software en updates van officiële bronnen en websites (bv. producenten, bedrijfsrepository's enz.).*
- *Vermijd het downloaden van software en toepassingen (en bestanden) van illegale bronnen.*
- *Verwijder niet-noodzakelijke of niet recent gebruikte software en schakel niet-noodzakelijke verbindingen uit (bv. netwerkprotocollen en -diensten) met inbegrip van toegang tot diensten op afstand (bv. cloudopslagdiensten).*
- *Scan alle software of opslagapparaten met een betrouwbare en geactualiseerde antivirussoftware.*
- *Download veilige industriële software (bv. updates, patches, nieuwe producten enz.) van vertrouwde leveranciers die het "white station"-beginsel hanteren.*
- *Update alle geïnstalleerde software in overeenstemming met de richtlijnen en praktijken van de organisatie.*

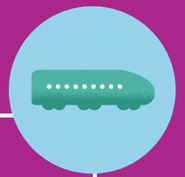
Europese Commissie

# Profiel II: Besluitvormers op het gebied van cyberbeveiliging in de vervoerssector

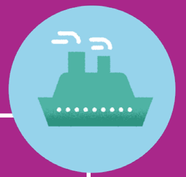
Dit traject is gericht op besluitvormers op het gebied van beveiliging of cyberbeveiliging in vervoersorganisaties. Dit traject legt de nadruk op goede praktijken die zijn afgestemd op de verschillende vervoerswijzen. Het biedt met name goede praktijken om opkomende cyberdreigingen te identificeren, op te sporen, erop te reageren en de organisatie te beschermen.

Europese Commissie

## Goede cyberbeveiligings-praktijken voor de luchtvaart



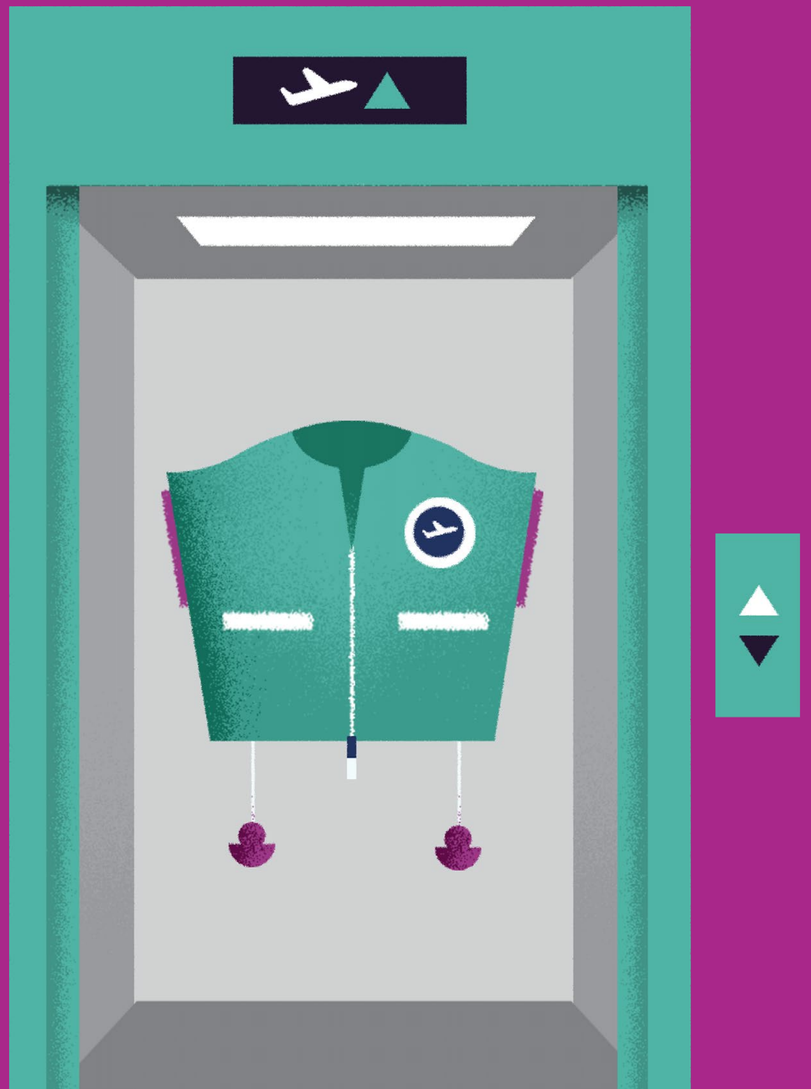
## Goede cyberbeveiligings-praktijken voor het vervoer over land



## Goede cyberbeveiligings-praktijken voor vervoer over zee

Europese Commissie

# Goede praktijken en beveiligingsmaatregelen voor de luchtvaart



# Governance

Luchtvaartorganisaties hebben behoefte aan duidelijke afspraken over opkomende dreigingen voor het vaststellen van hun managementbeleid en -processen voor een betere cyberbeveiliging van hun operationele diensten en systemen, met inbegrip van informatietechnologie (IT) en operationele technologie (OT).

Ongeachte de omvang van de organisaties, zijn dit een aantal goede praktijken:

- ervoor zorgen dat hogere leidinggevenden punten van zorg op het gebied van cyberbeveiliging melden aan de bedrijfstop en bestuurders, die met kennis van zaken beslissingen kunnen nemen over de toewijzing van middelen.

- aanstelling van een hogere leidinggevende, verantwoordelijk voor de cyber- en de fysieke beveiliging, met algemene managementverantwoordelijkheden voor de beveiliging van IT en operationele technologie (OT). Om belangenconflicten te vermijden mag die persoon niet bij de operationele activiteiten betrokken zijn;

- duidelijke omschrijving van functies, verantwoordelijkheden, competenties en machtigingen in verband met cyberbeveiliging en deze communiceren aan en overeenkomen met het relevante personeel, met name voor leden van de computercrisisteams (CERT's - Computer Emergency Response Teams);

- de cyberbeveiligingsgovernance waarborgen in de hele toeleveringsketen op het gebied van beveiliging, met inbegrip van fysieke en digitale interfaces, van technologiefabrikanten en installateurs tot beveiligingsdiensten;

- overeenstemming bereiken over activiteiten en controles, met inbegrip van gedeelde verantwoordelijkheden, om cyberbeveiligingsrisico's te beheren en ervoor te zorgen dat deze verantwoordelijkheden tijdens de levenscyclus van beveiligingsoplossingen en -diensten (bv. serviceovereenkomsten) worden gehandhaafd;

- governancemechanismen vaststellen (bv. beleidsmaatregelen) om te voldoen aan de verplichtingen van de EU-regelgeving zoals Verordening (EU) 2018/1139 inzake gemeenschappelijke regels op het gebied van burgerluchtvaart en Uitvoeringsverordening (EU) 2017/373 van de Commissie tot vaststelling van gemeenschappelijke eisen voor verleners van luchtverkeersbeheers-/luchtvaartnavigatiediensten en andere netwerkfuncties voor luchtverkeersbeheer en het toezicht daarop, en de NIS-richtlijn (Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen).

Europese Commissie

**Voorbeelden van diensten en systemen in de luchtvaart:**
Voorbeelden van IT die toegankelijk is voor werknemers (bv. pc's, mobiele telefoons, randapparatuur op kantoor enz.) en voor passagiers (bv. openbare wifi-routers en verbindingen enz.). Voorbeelden van OT zijn SCADA-systemen (Supervisory Controls and Data Acquisition), HVAC-systemen (verwarming, ventilatie en koeling), veiligheidscontrolepunten voor cabinebagage, bagageafhandelingssystemen, toegangscontrole, monitoring, toezicht, alarmopvolging, screeningtechnologie, controlesysteem voor vliegveldverlichting, radarsystemen en sensoren, gps-systemen, systemen voor luchtverkeersbeheer (ATM), communicatie-, navigatie- en plaatsbepalingsdiensten (CNS), aëronautische informatiesystemen, meteorologische systemen, systemen van operationele beveiligingscentra, boordsystemen van luchtvaartmaatschappijen, en andere.

Europese Commissie

# Cyberdreigingen identificeren

**Risicobeheer:** Luchtvaartorganisaties moeten passende maatregelen nemen om cyberbeveiligingsrisico's voor de netwerk- en informatiesystemen die de werking van essentiële functies ondersteunen, in kaart te brengen, te beoordelen en te begrijpen.

Dit vereist een algemene organisatorische aanpak van risicobeheer die het volgende omvat:

- *zorgen voor een duidelijk overzicht van de verschillende hardware- en softwaresystemen die ingezet worden voor het leveren van verschillende diensten. In de luchtvaart maken dergelijke systemen gebruik van IT en operationele technologieën (OT).*

- *het uitvoeren van **risicobeoordelingen inzake cyberbeveiliging**, waarbij rekening wordt gehouden met opkomende dreigingen, gekende kwetsbaarheden en operationele gegevens met betrekking tot de relevante systemen. Organisaties zoals het Europese computercrisisteam voor luchtverkeersbeheer (EATM-CERT) en het centrum voor informatie-uitwisseling en analyse in de luchtvaartsector (A-ISAC) kunnen inzicht verschaffen in bedreigingen voor de luchtvaart.*

- *ervoor zorgen dat de risicobeoordelingen ook betrekking hebben op de risico's in verband met dagelijkse activiteiten van het personeel (bv. gebruik van sociale media, van persoonlijke apparatuur, gegevensverwerking, informatie-uitwisseling enz.).*

- *vaststellen en uitvoeren van risicobehandelingsmaatregelen en -plannen voor het beperken van cyberbeveiligingsrisico's.*

- *implementatie van een alomvattend **beheerssysteem voor informatiebeveiliging** (ISMS) en een **beheerssysteem voor vertrouwelijke informatie** (PIMS) die afgestemd zijn op andere beheerssystemen. Dergelijke beheerssystemen (d.w.z. ISMS en PIMS) omvatten het uitvoeren van beveiligingscontroles (evenals gegevensbeschermings- en privacycontroles) om opkomende dreigingen voor de beveiliging van luchtvaartdiensten en -systemen (met inbegrip van hun data) te beperken en te voorkomen.*

- *rekening houden met eventuele beperkingen in verband met **het activabeheer en de planning van middelen** (d.w.z. beperkingen die van invloed kunnen zijn op de levering, het onderhoud en de ondersteuning van kritieke systemen voor de werking van essentiële functies in de luchtvaart).*

Europese Commissie

**Voorbeelden van risicobeheerskaders:** Verschillende kaders (bv. normen in de ISO/IEC 27000-familie, NIST-cyberbeveiligingskader, MITRE ATT&CK-kader, BSI IT-Grundschutz enz.) kunnen informatief en ondersteunend zijn voor een specifieke aanpak van risicobeheer voor de luchtvaart. Internationale organisaties zoals IATA en ICAO bieden richtsnoeren voor risicobeoordelingen inzake cyberbeveiliging. Enisa, EASA, Eurocontrol en Airports Council International (ACI) bieden een overzicht van goede praktijken voor de beveiliging van luchthavens, dienstverleners op het gebied van luchtverkeersbeheer en andere luchtvaartorganisaties. De Gemeenschappelijke Onderneming SESAR coördineert en concentreert alle onderzoeks- en ontwikkelingsactiviteiten van de EU op het gebied van luchtverkeersbeheer, met inbegrip van veiligheids- en beveiligingsaspecten.

Europese Commissie

# Beschermen tegen cyberdreigingen

Organisaties in het luchtvervoer moeten passende en evenredige beveiligingsmaatregelen treffen om hun netwerken en informatiesystemen tegen cyberaanvallen te beschermen – met inbegrip van IT en OT, zoals:

- ***beveiligingsbeleid en -processen:*** *vaststellen, uitvoeren, communiceren en handhaven van passende beleidslijnen en processen die een algemene aanpak inhouden voor het beveiligen van systemen en gegevens die de werking van essentiële functies in de luchtvaart ondersteunen. Dergelijk beveiligingsbeleid (bv. wachtwoord- en opslagbeleid) en -procedures moeten ook patch- en kwetsbaarhedenbeheer van hardware- en softwaresystemen (met inbegrip van IT en OT), incidentbeheer, systeem- en netwerkbescherming omvatten.*

- ***identiteits- en toegangsbeheer:*** *begrijpen, documenteren en beheren van de toegang tot netwerken en informatiesystemen (met inbegrip van IT en OT) die de werking van essentiële functies in de luchtvaart ondersteunen. Gebruikers (of geautomatiseerde functies) die toegang hebben tot gegevens of systemen zijn adequaat geverifieerd, geauthenticeerd en gemachtigd. Hierbij moet ook rekening worden gehouden met de verschillende functies en verantwoordelijkheden voor reguliere en bevoorrechte accounts.*

- ***gegevens- en systeembeveiliging:*** *bescherming van (opgeslagen en elektronisch overgedragen) gegevens, kritieke netwerken en informatiesystemen (met inbegrip van IT en OT) tegen cyberaanvallen. Rekening houdend met een risicogestuurde aanpak moeten organisaties beveiligingsmaatregelen treffen waardoor aanvallers effectief minder mogelijkheden hebben om gegevens, netwerken en systemen te compromitteren. Deze beveiligingsmaatregelen moeten ook het gebruik van versleuteling en beveiligde communicatieprotocollen omvatten om gegevens in rust en in overdracht te beschermen tegen cyberdreigingen die resulteren in tussenpersoonaanvallen. Bovendien moeten dergelijke maatregelen worden gecombineerd met fysieke beveiligingsmaatregelen om de toegang tot systemen te beschermen (systemen moeten zich bijvoorbeeld in gesloten ruimten bevinden met beperkte toegang).*

- ***veerkracht van netwerken en systemen:*** *veerkracht van netwerken en systemen opbouwen (met inbegrip van IT en OT) door deze (en hun operationele procedures) zo te ontwerpen en uit te voeren dat ze de impact van cyberaanvallen kunnen weerstaan en beperken. Voorbeelden van ontwerp- en uitvoeringsoplossingen voor een grotere veerkracht zijn: formeel geverifieerde kritieke functies, redundantie van systemen en netwerken, scheiding van netwerken (met name scheiding van IT en OT), meerlagige beveiligingsmaatregelen, en vele andere. Vanuit het oogpunt van informatiebeveiliging kunnen beveiligingsdomeinen die netwerk- en systeemscheiding toepassen, geschikte beveiligingsoplossingen bieden. Voor de operationele vereisten (bv. onderhoudswerkzaamheden, gegevensoverdracht enz.) van systemen kan het echter nodig zijn om verschillende beveiligingsdomeinen (bv. gescheiden systemen en netwerken) te omzeilen of te verbinden, met inbegrip van het verbinden van IT en OT.*

Europese Commissie

# Cyberdreigingen detecteren

Organisaties moeten ervoor zorgen dat beveiligingsmaatregelen doeltreffend blijven en alle cyberbeveiligingsvoorvallen detecteren die van invloed zijn of kunnen zijn op beveiligingscontroles en op essentiële diensten en systemen. Relevante beveiligingsmaatregelen voor het detecteren van cyberdreigingen zijn:

■ ***beveiligingsmonitoring:*** *toezicht houden op de beveiligingsstatus van netwerken en informatiesystemen — met inbegrip van IT en OT — die de werking van essentiële functies in luchtvervoersdiensten ondersteunen. Ter ondersteuning van de beveiligingsmonitoring worden bijvoorbeeld de volgende gegevens gebruikt:*

- *beveiligingslogbestanden;*
- *virusdetectielogbestanden;*
- *inbraakdetectielogbestanden;*
- *logbestanden voor identificatie, authenticatie en machtiging;*
- *systeem- en servicelogbestanden;*
- *netwerkverkeerlogbestanden;*
- *gegevensverwerkingslogbestanden;*

■ ***ontdekking van een beveiligingsvoorval:*** *detecteren van kwaadaardige activiteiten (oftewel beveiligingsvoorvallen) die van invloed zijn of kunnen zijn op de beveiliging van netwerken en informatiesystemen (met inbegrip van IT en OT) die de werking van essentiële functies in luchtvervoersdiensten ondersteunen.*

Voor deze maatregelen kan het vereist zijn om specifieke technologieën (bv. het beheer van beveiligingsinformatie en beveiligingsvoorvallen, een inbraakdetectiesysteem, een inbraakpreventiesysteem enz.) te gebruiken en een operationeel beveiligingscentrum (SOC) of het equivalent daarvan op te zetten. Dat vergt middelen om ter plekke cyberaanvallen te detecteren, te analyseren, erop te reageren en ervan te herstellen.

Nationale CSIRT's (Computer Security Incident Response Teams), sectorale CERT's (bv. het European Air Traffic Management Computer Emergency Response Team (EATM-CERT) of Eurocontrol, commerciële CERT's van luchtvaartmaatschappijen en het centrum voor informatie-uitwisseling en -analyse in de luchtvaartsector (A-ISAC) kunnen met Cyber Threat Intelligence (CTI) informatie verschaffen voor de beveiligingsmonitoring en de ontdekking van een voorval.

Europese Commissie

# Respons- en herstelplanning

Organisaties moeten procedures voor incidentbeheer vaststellen, implementeren en testen, die de bedrijfscontinuïteit van diensten en systemen in geval van cyberbeveiligingsincidenten moeten waarborgen. Beperkende maatregelen voor het beheersen of beperken van de impact van cyberbeveiligingsincidenten.

Respons- en herstelplanning moet rekening houden met maatregelen voor de accountbeveiliging en de impact van specifieke cyberaanvallen beperken, zoals:

- *coördinatie en samenwerking met nationale CSIRT's, (publieke en commerciële) CERT's en ISAC's tijdens cyberbeveiligingsincidenten, coördinatie van incidenten en crises op pan-Europees niveau;*

- *informatie delen met andere organisaties, met inbegrip van dienstverleners in de toeleveringsketen van luchtvaartdiensten;*

- *uitvoeren van periodieke **cyberaanval-oefeningen** (theoretische en technische coördinatie) voor het beoordelen van beveiligingsmaatregelen en -procedures evenals de veerkracht van organisaties om met cyberincidenten om te gaan;*

- *toegang tot opslaglocaties voor gearchiveerde of back-upgegevens indien de integriteit of de beschikbaarheid van opgeslagen gegevens is aangetast;*

- ***beveiligingsplaybooks** met gedetailleerde procedures voor het beheren van cyberincidenten en het herstellen van de normale werking van diensten en systemen;*

- *omleiding van het netwerkverkeer naar redundante diensten tijdens DoS-aanvallen;*

- *manuele procedures om diensten en systemen in werking te stellen bij gedegradeerde operationele omstandigheden;*

- *procedures vaststellen voor het aanpakken van gegevensinbreuken, met inbegrip van procedures voor het aanpakken van inbreuken op persoonsgegevens in overeenstemming met de Algemene verordening gegevensbescherming (AVG) en elke andere relevante sectorale verordening of richtlijn;*

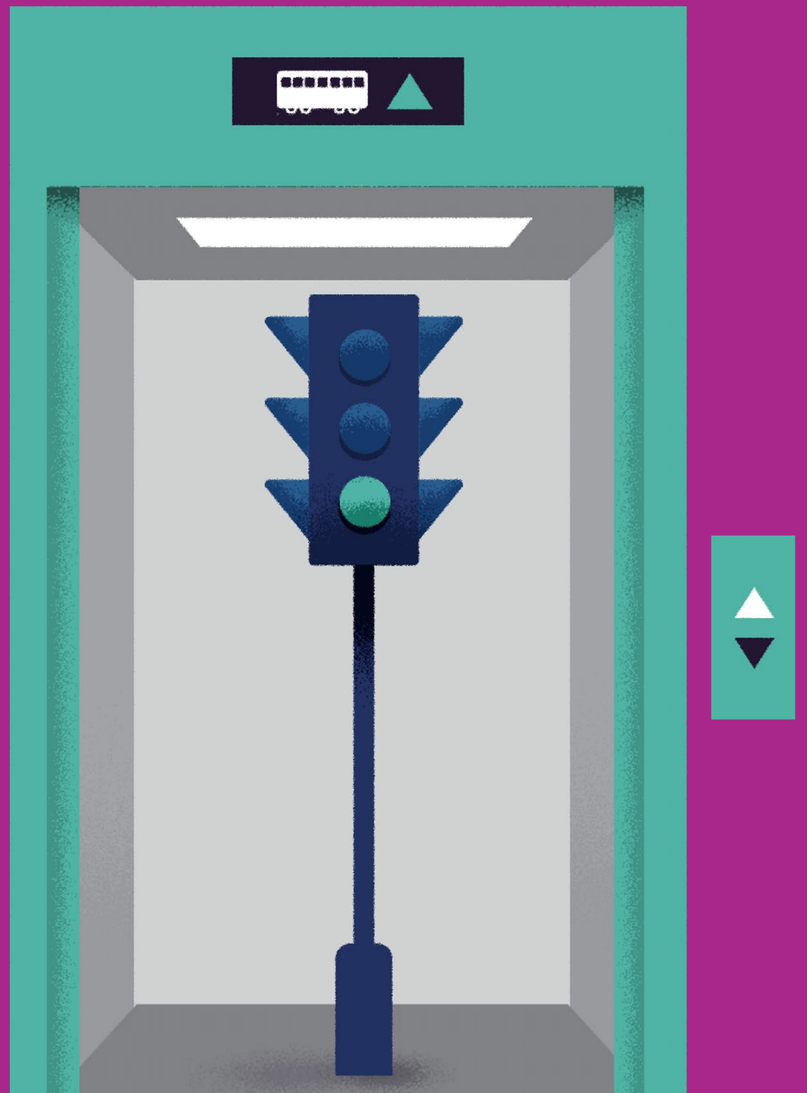
- *afsluiten van een **cyberverzekering** om het risico in verband met ernstige cyberincidenten deels op te vangen;*

- *afsluiten van een incidentresponscontract met een of meer gespecialiseerde firma's voor extra capaciteit en expertise;*

- *procedures vaststellen voor het **delen van informatie over cyberbeveiligingsincidenten** met relevante belanghebbenden, met inbegrip van procedures voor de melding van incidenten overeenkomstig de NIS-richtlijn (Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie).*

Europese Commissie

# Goede praktijken en beveiligingsmaatregelen voor het vervoer over land



# Governance

Organisaties op het gebied van vervoer over land (per spoor en over de weg) hebben behoefte aan duidelijke afspraken over opkomende dreigingen voor het vaststellen van hun managementsbeleid en -processen voor een betere cyberbeveiliging van hun operationele diensten en systemen, met inbegrip van informatietechnologie (IT) en operationele technologie (OT).

Ongeachte de omvang van de organisaties, zijn dit een aantal goede praktijken:

- *ervoor zorgen dat hogere leidinggevenden punten van zorg op het gebied van cyberbeveiliging melden aan de bedrijfstop en bestuurders, die met kennis van zaken beslissingen kunnen nemen over de toewijzing van middelen;*

- *aanstelling van een hogere leidinggevende, verantwoordelijk voor de cyber- en de fysieke beveiliging, met algemene managementverantwoordelijkheden voor de beveiliging van IT en operationele technologie (OT). Om belangenconflicten te vermijden mag die persoon niet bij de operationele activiteiten betrokken zijn;*

- *duidelijk definiëren van functies, verantwoordelijkheden, competenties en machtigingen in verband met cyberbeveiliging en deze communiceren aan en overeenkomen met het relevante personeel. Dit is met name nodig voor leden van de computercrisisteams (CERT's - Computer Emergency Response Teams);*

- *de cyberbeveiligingsgovernance waarborgen in de hele toeleveringsketen op het gebied van beveiliging, met inbegrip van fysieke en digitale interfaces, van technologiefabrikanten en installateurs tot beveiligingsdiensten;*

- *overeenstemming bereiken over activiteiten en controles, met inbegrip van gedeelde verantwoordelijkheden, om cyberbeveiligingsrisico's te beheren en ervoor te zorgen dat deze verantwoordelijkheden tijdens de levenscyclus van beveiligingsoplossingen en -diensten (bv. serviceovereenkomsten) worden gehandhaafd;*

- *vaststellen van governancemechanismen (bv. beleid) om te voldoen aan de verplichtingen die voortvloeien uit relevante verordeningen en richtlijnen. Dit omvat een breed scala aan beleidsmaatregelen die betrekking hebben op de specifieke vervoerswijzen en verschillende soorten belanghebbenden (zoals fabrikanten van voertuigen en spoorwegsystemen) en de NIS-richtlijn (Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie).*

Europese Commissie

**Voorbeelden van diensten en systemen in vervoer over land:** Voorbeelden van IT die toegankelijk is voor werknemers (bv. pc's, mobiele telefoons, randapparatuur op kantoor enz.) en voor passagiers (bv. openbare wifi-routers en verbindingen enz.). Voorbeelden van OT zijn SCADA-systemen (Supervisory Controls and Data Acquisition), HVAC-systemen (verwarming, ventilatie en koeling), gps-systemen, toegangscontrole, monitoring, toezicht, alarmopvolging en screeningtechnologie. Specifieke systemen voor spoorvervoer zijn bijvoorbeeld: operationele systemen voor besturing en seingeving, het Europees beheerssysteem voor het spoorverkeer (ERTMS), boordsystemen in treinen, onderhoudssystemen, en andere.

# Cyberdreigingen identificeren

**Risicobeheer:** Organisaties voor vervoer over land moeten passende maatregelen nemen om cyberbeveiligingsrisico's voor de netwerk- en informatiesystemen die de werking van essentiële functies ondersteunen, in kaart te brengen, te beoordelen en te begrijpen. Dit vereist een algemene organisatorische aanpak van risicobeheer die het volgende omvat:

- *zorgen voor een duidelijk overzicht van de verschillende hardware- en softwaresystemen die ingezet worden voor het leveren van verschillende diensten. In het kader van het vervoer over land maken dergelijke systemen gebruik van IT en OT.*

- *uitvoeren van **risicobeoordelingen inzake cyberbeveiliging**, waarbij rekening wordt gehouden met opkomende dreigingen, gekende kwetsbaarheden en operationele gegevens met betrekking tot de relevante systemen. Voorbeelden van systemen in het vervoer over land zijn: betalingssystemen, netwerk- en communicatiesystemen (bv. internet, radiocommunicatie, wifi enz.), boordapparatuur, operationele controlecentra, systemen voor identiteitsbeheer, veiligheidssystemen, en andere. Voor spoorweginfrastructuur zijn voorbeelden van systemen: subsystemen rollend materieel, exploitatie en verkeersleiding, trein- en baansystemen besturing en seingeving, en andere.*

- *ervoor zorgen dat risicobeoordelingen ook betrekking hebben op de risico's in verband met dagelijkse activiteiten van het personeel (bv. gebruik van sociale media, van persoonlijke apparatuur, gegevensverwerking, informatie-uitwisseling enz.).*

- *vaststellen en uitvoeren van risicobehandelingsmaatregelen en -plannen voor het beperken van cyberbeveiligingsrisico's, zoals de invoering van een uitgebreid **beheerssysteem voor informatiebeveiliging** (ISMS) en een **beheerssysteem voor vertrouwelijke informatie** (PIMS) die afgestemd zijn op andere beheerssystemen. Dergelijke beheerssystemen (d.w.z. ISMS en PIMS) omvatten het uitvoeren van beveiligingscontroles (evenals gegevensbeschermings- en privacycontroles) om opkomende dreigingen voor diensten en systemen op het gebied van vervoer over land (met inbegrip van hun data) te beperken en te voorkomen;*

- *rekening houden met eventuele beperkingen in verband met **het activabeheer en de planning van middelen** (d.w.z. beperkingen die van invloed kunnen zijn op de levering, het onderhoud en de ondersteuning van kritieke systemen voor de werking van essentiële functies in het vervoer over land).*

Europese Commissie

**Voorbeelden van risicobeheerskaders:** Verschillende kaders (bv. normen in de ISO/IEC 27000-familie, NIST-cyberbeveiligingskader, MITRE ATT&CK-kader, BSI IT-Grundschutz enz.) kunnen informatief en ondersteunend zijn voor een specifieke aanpak van risicobeheer voor het weg- en spoorvervoer. Organisaties zoals Enisa definiëren goede praktijken voor de cyberbeveiliging van slimme auto's en intelligent openbaar vervoer ten behoeve van fabrikanten en verenigingen (bv. de European Automobile Manufacturers' Association — ACEA). In het spoorvervoer stelt het Spoorwegbureau van de Europese Unie (ERA) technische specificaties voor interoperabiliteit (TSI's) vast waaraan elk subsysteem of onderdeel van een subsysteem moet voldoen om aan de essentiële eisen te beantwoorden en de interoperabiliteit van het spoorwegsysteem van de Europese Unie te waarborgen. De Gemeenschappelijke Onderneming Shift2Rail stimuleert ook innovatie-initiatieven en projecten voor het spoorvervoer (met inbegrip van cyberbeveiliging).

# Beschermen tegen cyberdreigingen

Organisaties in het vervoer over land moeten passende en evenredige beveiligingsmaatregelen treffen om hun netwerken en informatiesystemen tegen cyberaanvallen te beschermen — met inbegrip van IT en OT, zoals:

- ***beveiligingsbeleid en -processen:*** *vaststellen, uitvoeren, communiceren en handhaven van passende beleidsmaatregelen en processen, die een algemene aanpak bieden voor het beveiligen van systemen en gegevens die de werking van essentiële functies in het vervoer over land ondersteunen. Dergelijk beveiligingsbeleid (bv. wachtwoord- en opslagbeleid) en -procedures moeten ook patch- en kwetsbaarhedenbeheer van hardware- en softwaresystemen (met inbegrip van IT en OT), incidentbeheer, systeem- en netwerkbescherming omvatten;*

- ***identiteits- en toegangsbeheer:*** *begrijpen, documenteren en beheren van de toegang tot netwerken en informatiesystemen (met inbegrip van IT en OT) die de werking van essentiële functies in het vervoer over land ondersteunen. Gebruikers (of geautomatiseerde functies) die toegang hebben tot gegevens of systemen worden adequaat geverifieerd, geauthenticeerd en gemachtigd. Hierbij moet ook rekening worden gehouden met de verschillende functies en verantwoordelijkheden voor reguliere en bevoorrechte accounts;*

- ***gegevens- en systeembeveiliging:*** *bescherming van (opgeslagen en elektronisch overgedragen) gegevens, kritieke netwerken en informatiesystemen (met inbegrip van IT en OT) tegen cyberaanvallen. Rekening houdend met een risicogestuurde aanpak moeten organisaties beveiligingsmaatregelen treffen waardoor aanvallers effectief minder mogelijkheden hebben om gegevens, netwerken en systemen te compromitteren. Deze beveiligingsmaatregelen moeten ook het gebruik van versleuteling en beveiligde communicatieprotocollen omvatten om gegevens in rust en in overdracht te beschermen tegen cyberdreigingen die resulteren in tussenpersoonaanvallen. Bovendien moeten dergelijke maatregelen worden gecombineerd met fysieke beveiligingsmaatregelen om de toegang tot systemen te beschermen (systemen moeten zich bijvoorbeeld bevinden in een gesloten ruimte met een toegangsbeperking). Dit is van groot belang voor systemen die van invloed kunnen zijn op de veiligheid van mensenlevens;*

- ***veerkracht van netwerken en systemen:*** *veerkracht van netwerken en systemen opbouwen (met inbegrip van IT en OT) door deze (en hun operationele procedures) zo te ontwerpen en uit te voeren dat ze de impact van cyberaanvallen kunnen weerstaan en beperken. Voorbeelden van ontwerp- en uitvoeringsoplossingen voor een grotere veerkracht zijn: formeel geverifieerde kritieke functies, redundantie van systemen en netwerken, scheiding van netwerken (met name scheiding van IT en OT), meerlagige beveiligingsmaatregelen en vele andere. Vanuit het oogpunt van informatiebeveiliging kunnen beveiligingsdomeinen die netwerk- en systeemscheiding toepassen, geschikte beveiligingsoplossingen bieden. Voor de operationele vereisten (bv. onderhoudswerkzaamheden, gegevensoverdracht enz.) van systemen kan het echter nodig zijn om verschillende beveiligingsdomeinen (bv. gescheiden systemen en netwerken) te omzeilen of te verbinden, met inbegrip van het verbinden van IT en OT.*

Europese Commissie

# Cyberdreigingen detecteren

Organisaties moeten ervoor zorgen dat beveiligingsmaatregelen doeltreffend blijven en alle cyberbeveiligingsvoorvallen detecteren die van invloed zijn of kunnen zijn op beveiligingscontroles en op essentiële diensten en systemen. Relevante beveiligingsmaatregelen voor het detecteren van cyberdreigingen zijn:

- ***beveiligingsmonitoring:*** *toezicht houden op de beveiligingsstatus van netwerken en informatiesystemen — met inbegrip van IT en OT — die de werking van de essentiële functies in vervoerswijzen over land ondersteunen. Dit is noodzakelijk om potentiële bedreigingen te detecteren en de blijvende doeltreffendheid van beschermende beveiligingsmaatregelen te volgen. Ter ondersteuning van de beveiligingsmonitoring worden bijvoorbeeld de volgende gegevens gebruikt:*

  - *beveiligingslogbestanden;*
  - *virusdetectielogbestanden;*
  - *inbraakdetectielogbestanden;*
  - *logbestanden voor identificatie, authenticatie en machtiging;*
  - *systeem- en servicelogbestanden;*
  - *netwerkverkeerlogbestanden;*
  - *gegevensverwerkingslogbestanden;*

- ***ontdekking van een beveiligingsvoorval:*** *detecteren van kwaadaardige activiteiten (oftewel beveiligingsvoorvallen) die van invloed zijn of kunnen zijn op de beveiliging van netwerken en informatiesystemen (met inbegrip van IT en OT) die de werking van essentiële functies ondersteunen.*

*Voor deze maatregelen kan het vereist zijn om specifieke technologieën (bv. het beheer van beveiligingsinformatie en beveiligingsvoorvallen, een inbraakdetectiesysteem, een inbraakpreventiesysteem enz.) te gebruiken en een operationeel beveiligingscentrum (SOC) of het equivalent daarvan op te zetten. Dat vergt middelen om ter plekke cyberaanvallen te detecteren, te analyseren, erop te reageren en ervan te herstellen.*
*Nationale CSIRT's (Computer Security Incident Response Teams), sectorale en commerciële CERT's of weg- en spoorwegexploitanten, en het Europese centrum voor informatie-uitwisseling en -analyse in de spoorwegsector (ER-ISAC) kunnen met Cyber Threat Intelligence (CTI) informatie verschaffen voor de beveiligingsmonitoring en de ontdekking van een voorval.*

Europese Commissie

# Respons- en herstelplanning

Organisaties moeten procedures voor incidentbeheer vaststellen, implementeren en testen, die tot doel hebben de bedrijfscontinuïteit van diensten en systemen in geval van cyberbeveiligingsincidenten te waarborgen.

Respons- en herstelplanning moet rekening houden met maatregelen voor de accountbeveiliging en de impact van specifieke cyberaanvallen beperken zoals:

- *coördinatie en samenwerking met nationale CSIRT's, (publieke en commerciële) CERT's en ISAC's tijdens cyberbeveiligingsincidenten, coördinatie van incidenten en crises op pan-Europees niveau;*

- *informatie-uitwisseling met andere organisaties, met inbegrip van aanbieders in de toeleveringsketen van vervoerdiensten over land;*

- *uitvoeren van periodieke **cyberaanval-oefeningen** (theoretische en technische coördinatie) voor het beoordelen van beveiligingsmaatregelen en -procedures evenals de veerkracht van organisaties om met cyberincidenten om te gaan;*

- *toegang tot opslaglocaties voor gearchiveerde of back-upgegevens indien de integriteit of de beschikbaarheid van opgeslagen gegevens is aangetast;*

- ***beveiligingsplaybooks** met gedetailleerde procedures voor het beheren van cyberincidenten en het herstellen van de normale werking van diensten en systemen;*

- *omleiding van het netwerkverkeer naar redundante diensten tijdens DoS-aanvallen;*

- *manuele procedures om diensten en systemen in werking te stellen in geval van gestoord bedrijf;*

- *procedures vaststellen voor het aanpakken van gegevensinbreuken, met inbegrip van procedures om de schending van persoonsgegevens aan te pakken conform de Algemene verordening gegevensbescherming (AVG) en alle andere relevante sectorale verordeningen of richtlijnen;*

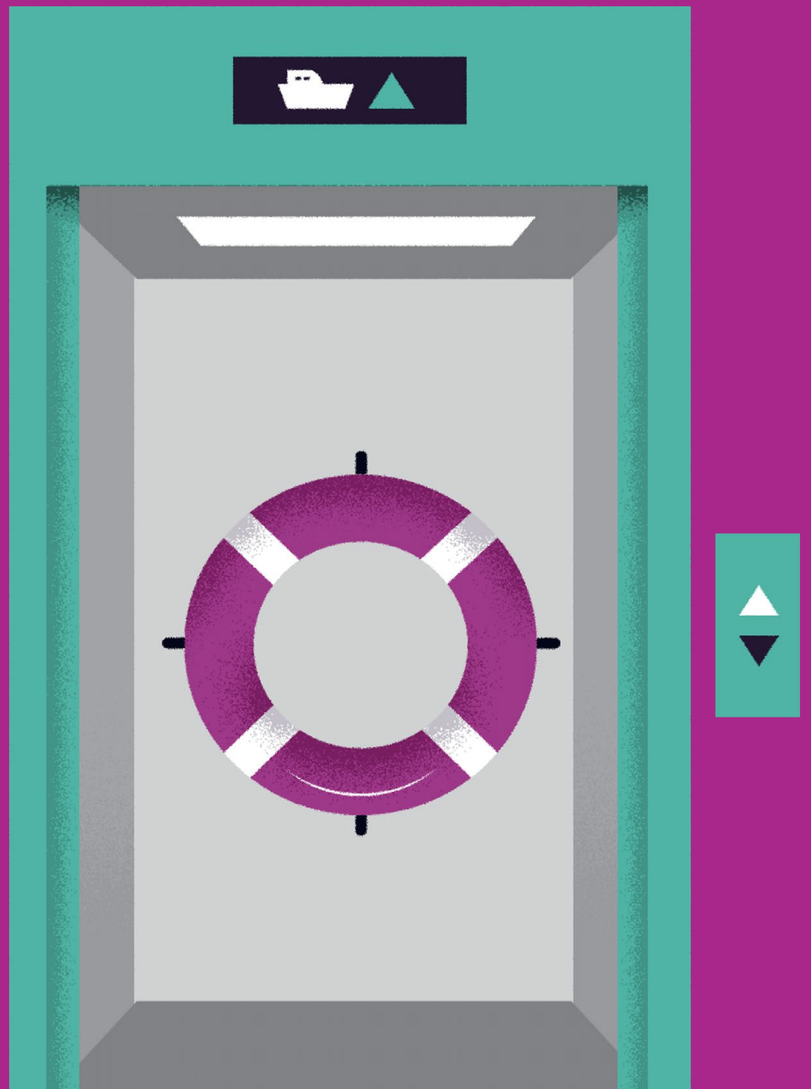
- *afsluiten van een **cyberverzekering** om het risico in verband met ernstige cyberincidenten deels op te vangen;*

- *afsluiten van een incidentresponscontract met een of meer gespecialiseerde firma's voor extra capaciteit en expertise;*

- *procedures vaststellen voor het delen van informatie over cyberbeveiligingsincidenten met relevante belanghebbenden, met inbegrip van procedures voor de melding van incidenten overeenkomstig de NIS-richtlijn (Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie).*

Europese Commissie

# Goede praktijken en beveiligingsmaatregelen voor het vervoer over zee



Europese Commissie

# Governance

Organisaties op het gebied van vervoer over zee hebben behoefte aan duidelijke afspraken over opkomende dreigingen voor het vaststellen van hun managementsbeleid en -processen voor een betere cyberbeveiliging van hun operationele diensten en systemen, met inbegrip van informatietechnologie (IT) en operationele technologie (OT).

Ongeacht de omvang van de organisatie, zijn dit een aantal goede praktijken:

- *ervoor zorgen dat hogere leidinggevenden punten van zorg op het gebied van cyberbeveiliging melden aan de bedrijfstop en bestuurders, die met kennis van zaken beslissingen kunnen nemen over de toewijzing van middelen;*

- *aanstelling van een hogere leidinggevende met algemene managementverantwoordelijkheden voor de beveiliging van IT en OT. In deze functie moet men zowel voor de cyberbeveiliging als voor de fysieke beveiliging verantwoordelijk zijn.*

- *duidelijk omschrijven van functies, verantwoordelijkheden, competenties en machtigingen in verband met cyberbeveiliging, definiëren van gezagsniveaus en communicatiekanalen tussen wal- en boordpersoneel en tussen personeelsleden onderling, en deze overeenkomen met het relevante personeel. Dit is met name nodig voor leden van de computercrisisteams (CERT's — Computer Emergency Response Teams). Personeelsleden met functies in verband met de EU-wetgeving inzake maritieme beveiliging en veiligheid, zoals veiligheidsbeambten van de havenfaciliteit, havenveiligheidsbeambten of veiligheidsbeambten van de maatschappij of de aangewezen persoon aan wal (DPA) en de kapitein aan boord, moeten ten minste vertrouwd zijn met de door de organisatie genomen cyberbeveiligingsmaatregelen.*

- *de cyberbeveiligingsgovernance waarborgen in de hele toeleveringsketen op het gebied van beveiliging, met inbegrip van fysieke en digitale interfaces, van technologiefabrikanten en installateurs tot beveiligingsdiensten;*

- *overeenstemming bereiken over activiteiten en controles, met inbegrip van gedeelde verantwoordelijkheden, om cyberbeveiligingsrisico's te beheren en ervoor te zorgen dat deze verantwoordelijkheden tijdens de levenscyclus van beveiligingsoplossingen en -diensten (bv. serviceovereenkomsten) worden gehandhaafd.*

- *governancemechanismen (bv. beleidsmaatregelen) vaststellen om te voldoen aan de verplichtingen die voortvloeien uit de EU-regelgeving, zoals Verordening (EU) 2019/1239 tot instelling van een Europees maritiem éénloketsysteem (EMSWe), Verordening (EG) Nr. 725/2004 betreffende de verbetering van de beveiliging van schepen en havenfaciliteiten, Richtlijn 2005/65/EG betreffende het verhogen van de veiligheid van havens, en Verordening (EG) Nr. 336/2006 inzake de implementatie van de internationale veiligheidsmanagementcode (ISM), en Resolutie A.741(18) ter goedkeuring van de internationale veiligheidscode voor de scheepvaart en ter voorkoming van verontreiniging. In dit verband moet ook melding worden gemaakt van de gemeenschappelijke gegevensuitwisselingsstructuur (Common Information Sharing Environment – CISE) te noemen, een EU-initiatief dat tot doel heeft de Europese en nationale surveillancesystemen van de EU interoperabel te maken zodat alle betrokken overheden toegang hebben tot gerubriceerde en niet-gerubriceerde informatie die zij nodig hebben om missies op zee uit te voeren.*

Europese Commissie

**Voorbeelden van diensten en systemen in het vervoer over zee:** Voorbeelden van IT die toegankelijk is voor werknemers (bv. pc's, mobiele telefoons, randapparatuur op kantoor enz.) en voor passagiers (bv. openbare wifi-routers en verbindingen enz.). Voorbeelden van OT zijn SCADA-systemen (Supervisory Controls and Data Acquisition), HVAC-systemen (verwarming, ventilatie en koeling), gps-systemen, toegangscontrole, monitoring, toezicht, alarmopvolging en screeningtechnologie, boordnavigatiesystemen, SafeSeaNet, brugsystemen, vrachtafhandelings- en beheerssystemen, aandrijf- en machinebeheer en besturingssystemen, systemen voor toegangscontrole, systemen voor passagiersafhandeling en passagiersbeheer, openbare netwerken voor passagiers, systemen voor de administratie en sociale voorzieningen voor de bemanning, communicatiesystemen, en andere.

Europese Commissie

# Cyberdreigingen identificeren

**Risicobeheer:** Maritieme organisaties moeten passende maatregelen nemen om cyberbeveiligingsrisico's in kaart te brengen, te analyseren, te beoordelen en te communiceren en deze tot een aanvaardbaar niveau accepteren, vermijden, overdragen of beperken. Dit vereist een algemene organisatorische aanpak van risicobeheer die het volgende omvat:

- *zorgen voor een duidelijk overzicht van de verschillende hardware- en softwaresystemen die ingezet worden voor het leveren van verschillende diensten. In het kader van vervoer over zee omvatten dergelijke systemen IT) en OT, en een overzicht over de verbinding en integratie van deze systemen met de wal, met inbegrip van openbare instanties, terminals en stuwadoors;*

- *vaststellen en beoordelen van de kernactiviteiten aan boord die kwetsbaar zijn voor cyberaanvallen, en uitvoeren van risicobeoordelingen inzake cyberbeveiliging (met inbegrip van het beoordelen van mogelijke operationele gevolgen en de waarschijnlijkheid dat deze zich voordoen), rekening houdend met opkomende dreigingen, gekende kwetsbaarheden en operationele gegevens met betrekking tot de relevante systemen. In voorkomend geval het verband leggen met uitgevoerde beoordelingen van de veiligheid van schepen, havenfaciliteiten en havens, zoals bepaald in de EU-wetgeving inzake maritieme beveiliging. Hierin worden mogelijke bedreigingen vastgesteld voor de haveninfrastructuur en veiligheidslacunes. Daarnaast kunnen maritieme organisaties zoals de Internationale Maritieme Organisatie (IMO) en maritieme ISAC's inzicht verschaffen over bedreigingen die gericht zijn op het vervoer over zee;*

- *ervoor zorgen dat risicobeoordelingen ook betrekking hebben op de risico's in verband met dagelijkse activiteiten van het personeel (bv. gebruik van sociale media, van persoonlijke apparatuur, gegevensverwerking, informatie-uitwisseling enz.);*

- *vaststellen en uitvoeren van risicobehandelingsmaatregelen en -plannen voor het beperken van cyberbeveiligingsrisico's. Bijvoorbeeld het implementeren van een uitgebreid beheerssysteem voor informatiebeveiliging (ISMS) en een beheerssysteem voor vertrouwelijke informatie (PIMS), afgestemd op andere beheerssystemen zoals veiligheidsbeheersystemen (SMS) in overeenstemming met de internationale veiligheidsmanagementcode (ISM). Dergelijke beheerssystemen (d.w.z. ISMS en PIMS) omvatten het uitvoeren van beveiligingscontroles (evenals gegevensbeschermings- en privacycontroles) om opkomende bedreigingen voor de zeevervoersdiensten en -systemen (met inbegrip van hun data) te beperken en te voorkomen;*

- *rekening houden met eventuele beperkingen in verband met **het activabeheer en de planning van middelen** (d.w.z. beperkingen die van invloed kunnen zijn op de levering, het onderhoud en de ondersteuning van kritieke systemen voor de werking van essentiële functies in het vervoer over zee). Wat beoordelingen betreft, kan in voorkomend geval verwezen worden naar de eisen van de ISM-code, veiligheidsbeheersystemen (SMS) en de veiligheidsplannen die uitgevoerd zijn in overeenstemming met de EU-wetgeving inzake maritieme veiligheid en beveiliging.*

**Voorbeelden van risicobeheerskaders:** Verschillende kaders (bv. de ISM-code of normen in de ISO/IEC 27000-familie, NIST-cyberbeveiligingskader, MITRE ATT&CK-kader, BSI IT-Grundschutz enz.) kunnen informatief en ondersteunend zijn voor een specifieke aanpak van risicobeheer voor het vervoer over zee. Het NIST-cyberbeveiligingskader is ook afgestemd op de cyberbeveiliging van de overdracht van maritieme bulkvloeistoffen (MBLT), offshore-operaties en activiteiten met passagiersschepen. Evenzo heeft de BIMCO (Baltic and International Maritime Council) *"The Guidelines on Cyber Security Onboard Ships"* gepubliceerd en de Internationale Maritieme Organisatie (IMO) heeft specifieke richtsnoeren uitgebracht, namelijk *"Guidelines on maritime cyber risk management"* (MSC-FAL.1/Circ.3). Het Enisa heeft verschillende studies uitgevoerd die betrekking hebben op goede praktijken op het gebied van maritieme cyberbeveiliging, met name op het gebied van cyberbeveiliging in havens. Het EMSA verleent diensten aan de maritieme gemeenschap, waaronder bewustmakingstrainingen op het gebied van cyberbeveiliging. In normen (bv. IEC 61162-460:2018 betreffende de veiligheid en beveiliging van maritieme navigatie en radiocommunicatieapparatuur en -systemen, ISO 16425:2013 betreffende schepen en mariene technologie, IEC 62443-4-1:2018 betreffende de beveiliging voor industriële automatisering en controlesystemen enz.) worden ook specifieke beveiligings- en veiligheidseisen voor systemen en netwerken in het vervoer over zee vastgesteld.

# Beschermen tegen cyberdreigingen

[TEXT A] Organisaties in het vervoer over zee moeten passende en evenredige beveiligingsmaatregelen treffen om hun netwerken en informatiesystemen te beschermen — met inbegrip van informatietechnologie (IT) en operationele technologie (OT), zoals:

- ***beveiligingsbeleid en -processen:*** *vaststellen, uitvoeren, communiceren en handhaven van passende beleidslijnen en processen die een algemene aanpak inhouden voor het beveiligen van systemen en gegevens die de werking van essentiële functies in het vervoer over zee ondersteunen. Beveiligingsmaatregelen (met inbegrip van cyber- en fysieke beveiligingsmaatregelen) moeten worden opgenomen in relevante plannen zoals het veiligheidsbeheersysteem (SMS) en in het scheepsveiligheidsplan (SSP). Dergelijk beveiligingsbeleid (bv. wachtwoord- en opslagbeleid) en -procedures moeten ook patch- en kwetsbaarhedenbeheer van hardware- en softwaresystemen (met inbegrip van IT en OT), incidentbeheer, systeem- en netwerkbescherming omvatten;*

- ***identiteits- en toegangsbeheer:*** *begrijpen, documenteren en beheren van de toegang tot netwerken en informatiesystemen (met inbegrip van IT en OT) die de werking van essentiële functies in het vervoer over zee ondersteunen. Gebruikers (of geautomatiseerde functies) die toegang hebben tot gegevens of systemen worden adequaat geverifieerd, geauthenticeerd en gemachtigd. Hierbij moet ook rekening worden gehouden met de verschillende functies en verantwoordelijkheden voor reguliere en bevoorrechte accounts;*

- ***gegevens- en systeembeveiliging:*** *bescherming van (opgeslagen en elektronisch overgedragen) gegevens, kritieke netwerken en informatiesystemen (met inbegrip van IT en OT) tegen cyberaanvallen. Rekening houdend met een risicogestuurde aanpak moeten organisaties beveiligingsmaatregelen treffen waardoor aanvallers effectief minder mogelijkheden hebben om gegevens, netwerken en systemen te compromitteren. Deze beveiligingsmaatregelen moeten ook het gebruik van versleuteling en beveiligde communicatieprotocollen omvatten om gegevens in rust en in overdracht te beschermen tegen cyberdreigingen die resulteren in tussenpersoonaanvallen. Bovendien moeten dergelijke maatregelen worden gecombineerd met fysieke beveiligingsmaatregelen om de toegang tot systemen te beschermen (systemen moeten zich bijvoorbeeld bevinden in een gesloten ruimte met een toegangsbeperking). Dit is van groot belang voor systemen die van invloed kunnen zijn op de veiligheid van mensenlevens (bv. navigatie- en radiocommunicatiesystemen van categorie II en III);*

- ***veerkracht van netwerken en systemen:*** *veerkracht van netwerken en systemen opbouwen (met inbegrip van IT en OT) door deze (en hun operationele procedures) zo te ontwerpen en uit te voeren dat ze de impact van cyberaanvallen kunnen weerstaan en beperken. Voorbeelden van ontwerp- en uitvoeringsoplossingen voor een grotere veerkracht zijn: formeel geverifieerde kritieke functies, redundantie van systemen en netwerken, scheiding van netwerken (met name scheiding van IT en OT), meerlagige beveiligingsmaatregelen en vele andere. Vanuit het oogpunt van informatiebeveiliging kunnen beveiligingsdomeinen die netwerk- en systeemscheiding toepassen, geschikte beveiligingsoplossingen bieden. Voor de operationele vereisten (bv. onderhoudswerkzaamheden, gegevensoverdracht enz.) van systemen (bv. maritieme autonome oppervlakteschepen — MASS) kan het echter nodig zijn om verschillende beveiligingsdomeinen (bv. gescheiden systemen en netwerken) te omzeilen of te verbinden, met inbegrip van het verbinden van IT en OT.*

Europese Commissie

# Cyberdreigingen detecteren

Organisaties moeten ervoor zorgen dat beveiligingsmaatregelen doeltreffend blijven en alle cyberbeveiligingsvoorvallen detecteren die van invloed zijn of kunnen zijn op beveiligingscontroles en op essentiële diensten en systemen. Relevante beveiligingsmaatregelen voor het detecteren van cyberdreigingen zijn:

- ***beveiligingsmonitoring:*** *toezicht houden op de beveiligingsstatus van netwerken en informatiesystemen – met inbegrip van IT en OT – die de werking van essentiële functies in zeevervoerdiensten ondersteunen. Dit is noodzakelijk om potentiële bedreigingen te detecteren en de blijvende doeltreffendheid van beschermende beveiligingsmaatregelen te volgen. Ter ondersteuning van de beveiligingsmonitoring worden bijvoorbeeld de volgende gegevens gebruikt:*
  - *beveiligingslogbestanden;*
  - *virusdetectielogbestanden;*
  - *inbraakdetectielogbestanden;*
  - *logbestanden voor identificatie, authenticatie en machtiging;*
  - *systeem- en servicelogbestanden;*
  - *netwerkverkeerlogbestanden;*
  - *gegevensverwerkingslogbestanden;*
- ***ontdekking van een beveiligingsvoorval:*** *detecteren van kwaadaardige activiteiten (oftewel beveiligingsvoorvallen) die van invloed zijn of kunnen zijn op de beveiliging van netwerken en informatiesystemen (met inbegrip van IT en OT) die de werking van essentiële functies in zeevervoerdiensten ondersteunen.*

Voor deze maatregelen kan het vereist zijn om specifieke technologieën (bv. het beheer van beveiligingsinformatie en beveiligingsvoorvallen, een inbraakdetectiesysteem, een inbraakpreventiesysteem enz.) te gebruiken en een operationeel beveiligingscentrum (SOC) of het equivalent daarvan op te zetten. Dat vergt middelen om ter plekke cyberaanvallen te detecteren, analyseren, erop te reageren en ervan te herstellen.

Nationale CSIRT's (Computer Security Incident Response Teams), sectorale en commerciële CERT's van maritieme vervoerders, en het Europese centrum voor informatie-uitwisseling en -analyse in de spoorwegsector (ER-ISAC) kunnen met Cyber Threat Intelligence (CTI) informatie verschaffen voor de beveiligingsmonitoring en de ontdekking van een voorval.

Europese Commissie

# Respons- en herstelplanning

Organisaties moeten procedures voor incidentbeheer vaststellen, implementeren en testen, die tot doel hebben de bedrijfscontinuïteit van diensten en systemen in geval van cyberbeveiligingsincidenten te waarborgen.
Respons- en herstelplanning moet rekening houden met maatregelen voor de accountbeveiliging en de impact van specifieke cyberaanvallen beperken zoals:

- *omleiding van het netwerkverkeer naar redundante diensten tijdens DoS-aanvallen;*
- *manuele procedures om diensten en systemen in werking te stellen in geval van gestoord bedrijf;*
- *programma's opstellen voor oefeningen (bv. theoretische coördinatie, technische coördinatie en responsoefeningen) om te kunnen reageren op cyberaanvallen en noodsituaties en voor het beoordelen van beveiligingsmaatregelen, procedures en de organisatorische veerkracht om met cyberincidenten om te gaan;*
- *toegang tot opslaglocaties voor gearchiveerde of back-upgegevens indien de integriteit of de beschikbaarheid van opgeslagen gegevens is aangetast;*
- *coördinatie en samenwerking met nationale CSIRT's, (publieke en commerciële) CERT's en ISAC's tijdens cyberbeveiligingsincidenten, coördinatie van incidenten en crises op pan-Europees niveau;*
- *informatie delen met andere organisaties, met inbegrip van dienstverleners in de toeleveringsketen van het vervoer over zee;*
- *beveiligingsplaybooks met gedetailleerde procedures voor het beheren van cyberincidenten en het herstellen van de normale werking van diensten en systemen;*
- *procedures vaststellen voor het aanpakken van gegevensinbreuken, met inbegrip van procedures om de schending van persoonsgegevens aan te pakken conform de Algemene verordening gegevensbescherming (AVG) en alle andere relevante sectorale verordeningen of richtlijnen;*
- *afsluiten van een cyberverzekering om het risico in verband met ernstige cyberincidenten deels op te vangen;*
- *afsluiten van een incidentresponscontract met een of meer gespecialiseerde firma's voor extra capaciteit en expertise;*
- *procedures vaststellen voor het delen van informatie over cyberbeveiligingsincidenten (met inbegrip van inbreuken, ongevallen en gevaarlijke situaties) met relevante belanghebbenden, met inbegrip van procedures voor de melding van incidenten overeenkomstig de NIS-richtlijn (Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie).*

Luxemburg: Bureau voor publicaties van de Europese Unie, 2021



Print ISBN 978-92-76-40502-3 doi:10.2832/549165 MI-05-21-230-NL-C
PDF ISBN 978-92-76-40496-5 doi:10.2832/254328 MI-05-21-230-NL-N

Bureau voor publicaties
van de Europese Unie