Europeiska kommissionen

Verktygslåda för cybersäkerhet inom transport

Inledning

Kommissionens generaldirektorat för transport och rörlighet (GD Transport och rörlighet) har låtit ta fram denna verktygslåda för att öka medvetenheten om och beredskapen inför cyberhot bland berörda parter inom transportsektorn. Den ger insikter om cyberhot och hur man begränsar deras inverkan på transporttjänster, -system och -verksamhet. Verktygslådan innehåller alternativa vägar för att öka medvetenheten med tanke på olika transportprofiler:

- all transportpersonal (allmän information och vägledning),
- beslutsfattare för cybersäkerhet inom olika transportsätt.

Hyperlänkar ansluter de olika delarna som bildar verktygslådan för att underlätta navigeringen av medvetenhetsvägarna, som har anpassats till dessa specifika transportprofiler.

Den praxis som anges i denna verktygslåda är endast rådgivande. Eventuella rekommendationer är varken bindande eller tvingande. Verktygslådan utgör heller inte Europeiska kommissionens formella åsikter och är inte avsedd att tillhandahålla sätt att efterleva befintlig eller framtida EU-lagstiftning.

Profiler för cybersäkerhetsmedvetenhet

Profil I: All transportpersonal. Den första vägen är avsedd för all personal i transportorganisationer, från personal som tillhandahåller transporttjänster till administrativ personal. Den vägleder dem mot ökad förståelse och medvetenhet om de vanligaste cyberhoten riktade mot transporttjänster och -system. Dessutom ger den insikter om hur man hanterar potentiella cyberhot, inklusive att identifiera, rapportera och begränsa dem genom god cybersäkerhetspraxis.

Profil II: Beslutsfattare på området cybersäker transport. Den andra vägen är avsedd för personal som har beslutsfattande ansvar för cybersäkerhet i transportorganisationer. Denna väg belyser god praxis anpassad till de olika transportsätten för att förbättra transportorganisationernas cybersäkerhetsställning. I synnerhet ger den god praxis för att identifiera, skydda mot, upptäcka och svara på nya cyberhot som riktas mot transportorganisationer.

Europeiska kommissionen

Verktygslåda för cybersäkerhet inom transport

Hotbilder för transport

Framväxande cybersäkerhetshot som påverkar olika transportsätt

Profiler för cyber-säkerhetsmedvetenhet

Alternativa vägar för öka medvetenheten om cybersäkerhet riktade till olika transportprofiler

Europeiska kommissionen

Hotbilder för transport

Cyberhotbilderna är dynamiska och utvecklas kontinuerligt. Ändå är det möjligt att identifiera cyberhot som alla transportsätt möter inom verksamheten, inklusive systemdrift.

Europeiska kommissionen

Fientliga aktörer

Individer eller organisationer som potentiellt kan påverka säkerheten i transporttjänster och -system

Framväxande cyberhot

Utvalda cyberhot som potentiellt kan utgöra attackvektorer som påverkar säkerheten i transporttjänster och -system

Europeiska kommissionen

Fientliga aktörer

Individer eller organisationer kan avsiktligt eller oavsiktligt avslöja och utnyttja sårbarheter som kan orsaka incidenter och påverka transporttjänster, inklusive säkerhet, företag, ekonomi och rykte. Fientliga aktörer är bland annat statligt sponsrade grupper, cyberbrottslingar, cyberterrorister, hacktivister, hackare (inklusive skriptknattar) och insider (inklusive privilegierade insider).

De viktigaste fientliga aktörerna som avsiktligt riktar in sig på transportorganisationer är **cyberbrottslingar**, **insider**, **nationalstater** och **statsunderstödda grupper**.
Motståndare som **cyberbrottslingar** genomför massiva attackkampanjer och verkar ofta för monetär ersättning.

Insider känner till särdragen hos de organisationer de arbetar för och är ofta väl medvetna om subtila säkerhetsproblem. Insiderhotsaktörer kan vara missnöjda anställda, leverantörer och enskilda entreprenörer.
I takt med att de globala geopolitiska spänningarna ökas riktar sig **nationalstater** och **statsunderstödda grupper** in på strategiska långsiktiga mål. De försöker ofta dölja sig i djupet av organisationers system och samlar in känslig information. När statsunderstödda angripare väl har fått fotfäste i system letar de efter möjligheter att göra så mycket skada som möjligt. De kan till exempel rikta in sig på andra organisations system genom att utnyttja organisationernas nätverksanslutningar.

Andra fientliga aktörer är **insider**, som oavsiktligt eller av misstag kan utföra åtgärder som resulterar i cybersäkerhetstillbud och i värsta fall cyberincidenter som påverkar säkerheten för transporttjänster.

Europeiska kommissionen

Framväxande cyberhot

Det finns ett stort antal cyberhot som riktas mot transportområdet: **samordnad överbelastning**, **överbelastning**, datastöld, spridning av **sabotageprogram**, **nätfiske**, manipulering av programvara, **obehörig åtkomst**, skadliga attacker, förfalskning eller kringgående av säkerhetsoperatörers beslutsprocess, uppträdande under falsk identitet, missbruk av åtkomsträttigheter, **social manipulering**, hackning, tjuvlyssning, missbruk av tillgångar och manipulering av maskinvara.

Baserat på omfattande litteraturforskning av offentligt tillgängliga dokumentationer och intervjuer med experter är de mest akuta framväxande cyberhot som påverkar transporter sabotageprogram, (samordnad) överbelastning, obehörig åtkomst och stöld samt manipulering av programvara.

Europeiska kommissionen

Hot nr 1: Sabotage-program

Skadlig programvara som potentiellt kan påverka individer eller organisationer inom olika transportsätt

Hot nr 2: (Samordnad) Överbelastning

Cybersäkerhetsattacker som förhindrar att individer eller organisationer får åtkomst till relevanta transporttjänster och -resurser

Hot nr 3: Obehörig åtkomst och stöld

Obehörig åtkomst, personintrång och utnyttjande av kritiska tillgångar

Hot nr 4: Manipulering av programvara

Cybersäkerhetsattacker som riktar in sig på programvara för att ändra dess beteende och genomföra specifika attacker

Hot nr 1: Sabotageprogram

Sabotageprogram består av skadlig programvara, som kan innehålla olika typer av program, till exempel virus, trojaner, maskar, utpressningsprogram, program för skadlig utvinning av kryptovaluta eller annan programvara som kan ha en negativ inverkan på organisationer eller individer inom olika transportsätt.

En av de viktigaste prioriteringarna för cybersäkerhet för alla transportsätt är att begränsa spridningen av sabotageprogram som är avsedda för att avsiktligt skada datorer, servrar, klienter, nätverk eller alla av de nämnda. En typisk attackvektor kan innebära nätfiskemeddelanden riktade till anställda. Andra attackvektorer kan omfatta olika och sofistikerade strategier för social manipulering som att ansluta en USB-nyckel till en ledig port (t.ex. laddning av mobiltelefon). Genom att klicka på hyperlänkar i misstänksamma e-postmeddelanden eller öppna filbilagor kan användaren omedvetet installera programvara eller medvetet äventyra transporttjänster och -resurser.

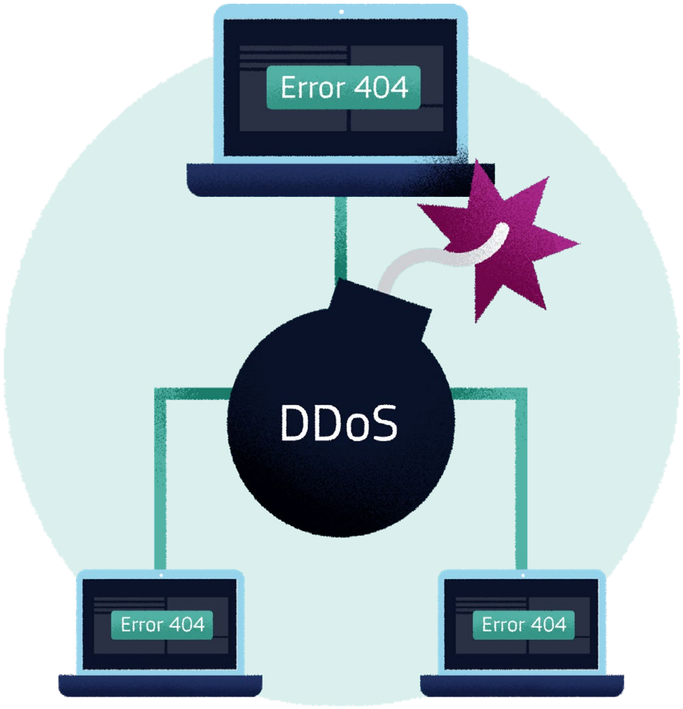
Till exempel attacken med WannaCry-utpressningsprogrammet drabbade mer än 150 länder och infekterade över 230 000 system. Det var ett utpressningsprogram som vanligtvis sprids via nätfiskemeddelanden som innehåller skadliga bilagor eller hyperlänkar. Den här typen av attacker utnyttjar social manipulering med illvilja för att vilseleda systemanvändare att installera (eller aktivera) specifika sabotageprogram.

Hot nr 2: (Samordnad) Överbelastning

Samordnade överbelastningsattacker (DDoS) och överbelastningsattacker påverkar tillgänglighet och åtkomst av data, tjänster, system och andra resurser. Dessa typer av attacker kan variera i varaktighet och kan rikta in sig på mer än en tjänst eller ett system i taget. Samordnade överbelastningsattacker använder flera system (eller attackkanaler) för att överbelasta måltjänster eller -system med förfrågningar. Framgångsrika attacker påverkar kapaciteten hos tjänster och system att hantera oväntade volymförfrågningar. Detta resulterar i att man nekar åtkomst till tjänster och resurser.

Observera att berörda tjänster och system som tillhör transportorganisationer kan utnyttjas för att utföra (samordnade) överbelastningsattacker som riktar in sig på specifika system i verksamheter eller även andra organisationer.

Till exempel kan informationssystem för företag (t.ex. persondatorer och enheter) attackeras för att komma åt driftsteknik som kan vara ansluten till internet eller för att få åtkomst till nätverk för att överföra driftdata. Anslutningar mellan olika system och nätverk (såsom företagsnätverk, driftsteknik och fjärrunderhållsåtkomster) kan utgöra exploaterbara sårbarheter för att utföra (samordnade) överbelastningsattacker mot kritiska transporttjänster och -system. Till exempel kan (samordnade) överbelastningsattacker utnyttja vanliga nätverks- och kommunikationsprotokoll, till exempel Web Services Dynamic Discovery (WS-Discovery), som enheter inom sakernas internet kan använda för att automatiskt upptäcka varje nod i lokala nätverk (LAN). Om enheter inom sakernas internet uppvisar sårbarheter kan angripare utnyttja dem för att upptäcka andra anslutna enheter och genomföra (samordnade) överbelastningsattacker.



Europeiska kommissionen

Hot nr 3: Obehörig åtkomst och stöld

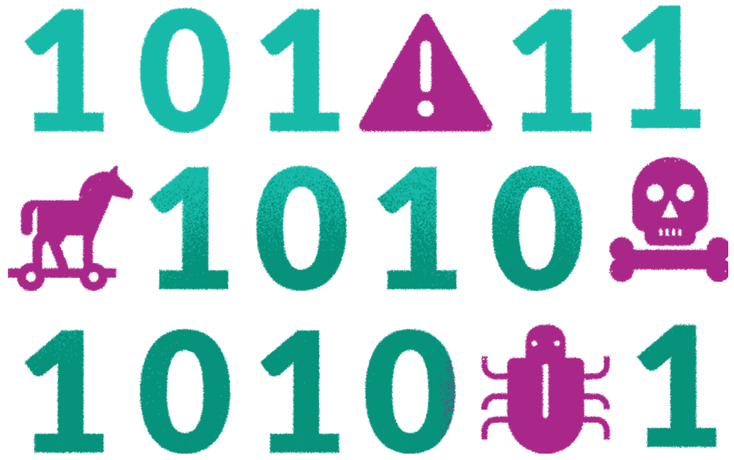
Fientliga aktörer kanske vill få logisk eller fysisk åtkomst utan tillstånd till nätverk, system, applikationer, uppgifter eller andra resurser för att utföra skadliga aktiviteter, inklusive stöld av känsliga uppgifter eller resurser (inklusive fysiska resurser). Åtkomst- och stöldhot riktas mot konfidentiella och äganderättsliga tillgångar (inklusive personlig identitet, identifieringsinformation för privilegierade konton, system och andra typer av konfidentiell och äganderättslig information). Utöver systemsårbarheter kan dessa hot utnyttja omedvetna individer som avslöjar känsliga uppgifter, såsom identifieringsinformation (t.ex. inloggningsuppgifter, lösenord etc.) eller personuppgifter (t.ex. e-post, personligt identifieringsnummer etc.).

När det gäller obehörig åtkomst är identitetsstöld olaglig användning av personuppgifter eller unika identifierare för att efterlikna personer eller tjänster och system för att få åtkomst till privata eller äganderättsliga resurser (t.ex. ekonomiska och fysiska resurser). Sådana cybersäkerhetshot kan också riktas mot fysiska tillgångar inom alla transportsätt.

Hot nr 4: Manipulering av programvara

Felkonfigurationer och manipuleringar av programvara och relaterade system eller komponenter kan ha en direkt inverkan på säkerhetsställningen för transporttjänster och system.
Cybersäkerhetsattacker som utnyttjar manipulering av programvara ändrar programvaruinställningar eller påverkar dataintegriteten för att ändra beteenden hos system och tjänster. Angripare kan avsiktligt manipulera programvara (eller en del av den) för att dra nytta av känsliga tillgångar (t.ex. för att få obehörig åtkomst, förhindra att legitima individer eller system får åtkomst till nödvändiga resurser, samla in känsliga uppgifter, ändra funktionellt beteende etc.).

Till exempel kan angripare rikta in sig på tillverkares kommunikationskanaler för att ladda upp skadliga programuppdateringar av tjänster och system (inklusive driftsteknik) i verksamheter. En fientlig aktör använder komprometterad identifieringsinformation för att få åtkomst till ett säkert nätgränssnitt för fjärrunderhåll för att installera manipulerad programvara och ytterligare kompromettera andra tillgängliga tjänster och system. Den fientliga aktören installerar manipulerad programvara som ytterligare komprometterar måltjänster och -system eller attackerar andra anslutna tjänster eller system.



Europeiska kommissionen

Profiler för cyber-säkerhetsmedvetenhet

Europeiska kommissionen

1

Profil I: All transportpersonal

Den första vägen är avsedd för all personal i transportorganisationer, från operativ till administrativ personal. Den ger vägledning i riktning mot ökad förståelse och medvetenhet om de vanligaste cybersäkerhetshoten som riktas mot transporttjänster. Den ger också insikter om hur man hanterar potentiella cybersäkerhetshot, liksom även att identifiera, anmäla och begränsa dem med hjälp av praxis för cybersäkerhet. Denna väg är gemensam för alla transportsätt.

2

Profil II: Beslutsfattare på området cybersäker transport

Den andra vägen är avsedd för personal som har beslutsfattande ansvar för säkerhet eller cybersäkerhet i transportorganisationer. Denna väg ger god praxis som är anpassad till de olika transportsätten. Den ger god praxis för att identifiera, skydda mot, upptäcka och svara på nya cybersäkerhetshot som riktas mot transportorganisationer.

Europeiska kommissionen

Profil I: All transport-personal

Denna del riktar sig till all personal i transportorganisationer, från operativ till administrativ personal. Den ger vägledning mot ökad förståelse och medvetenhet om de vanligaste cybersäkerhetshoten riktade mot transporttjänster. Den ger också insikter om hur man hanterar potentiella cybersäkerhetshot, liksom även att identifiera, anmäla och begränsa dem med hjälp av praxis för cybersäkerhet. Denna del ger rekommenderad praxis och användbara tips, som är relevanta **för alla transportsätt**.

Europeiska kommissionen

God praxis mot sabotageprogram

Du kan hjälpa till att skydda din organisation genom att följa god praxis för att **identifiera och förhindra spridning av sabotageprogram**, bland annat följande:

- ***Följ säkerhetspolicyer*** *som att skanna lagringsmedier och -filer efter virus, undvika att öppna och skicka specifika filtyper via e-post (t.ex. körbara filer såsom .exe, .bat, .com etc.), endast installera auktoriserad programvara och säkerställa att programvara (inklusive antivirusprogram) är uppdaterad och fungerar korrekt samt andra policyer*

- ***Säkerhetskopiera dina data*** *regelbundet till säkra (och auktoriserade) datalagringsenheter eller -tjänster, som bör stödja krypteringsmekanismer för att skydda vilande data och erbjuda möjlighet att återställa data*

- *Använd lämpliga **säkerhetsåtgärder** (t.ex. lösenord, kryptering etc.) för att skydda alla system inklusive mobila enheter och slutpunktsenheter och kom ihåg att säkert låsa (fysiskt och digitalt) alla system om de är utan uppsikt*

- *Undvik att öppna bilagor eller klicka på hyperlänkar i oväntade e-postmeddelanden och misstänkta popupfönster i webbläsaren om de har en konstig brödtext eller härstammar från okända avsändare eller internetdomäner*

- *Undvik att koppla **otillförlitliga eller okända flyttbara enheter** till din dator, såsom USB-minnen, hårddiskar och andra lagringsenheter*

- *Undvik att inaktivera säkerhetsåtgärder för sabotageprogram (t.ex. antivirusprogram, program för innehållsfiltrering, brandvägg etc.)*

- ***Uppdatera installerad programvara*** *regelbundet till de senaste tillgängliga versionerna (som säkerhetsansvariga för informationssystem eller systemadministratörer kan släppa med regelbundna uppdateringar)*

- *Undvik att använda konton och identifieringsinformation med privilegierad åtkomst (t.ex. på administratörsnivå) för vanliga aktiviteter och operationer*

- *Rapportera misstänkta e-postmeddelanden eller oväntade systembeteenden till säkerhetsansvariga för informationssystem eller systemadministratörer*

- *Fokusera på informationssäkerhet i det dagliga rutinarbetet för att känna igen it-säkerhetsproblem och reagera därefter.*

Europeiska kommissionen

God praxis mot (samordnad) överbelastning

Du kan hjälpa till att skydda din organisation genom att identifiera **samordnade överbelastningsattacker (DDoS)** och **överbelastningsattacker**. Du bör omedelbart kontakta din säkerhets- och it-personal om du upptäcker eller upplever någon av följande indikatorer på potentiellt pågående (samordnade) överbelastningsattacker på dina tjänster eller system:

- *Ökade förfrågningar som förbrukar nätverkskapaciteten (som uppfattas som långsamma tjänster och svar) vilket resulterar i service- eller systemfel på grund av överbelastning.*

- *Ökande efterfrågan på användning av minnesresurser utan en uppenbar anledning.*

- ***Oväntade beteenden hos tjänster och system**, frekventa kraschar och konstiga felmeddelanden till följd av skadlig förbrukning av dataresurser eller nätverksanslutningar.*

- ***Försämrad prestanda** av enheter, långa körningar för triviala uppgifter och märkbara aktiviteter (t.ex. bullriga fläktar medan enheter har en långsam prestanda).*

- ***Oväntade internetanslutningar eller förlust av anslutningar** till tjänster och system.*

- *Subtila beteendeförändringar i driftskontroller eller teknik som leder till fysiska skador.*

- *Nekad åtkomst till privilegierade eller administrativa konton för att blockera incidenthanteringsprocesser från att återhämta sig.*

Europeiska kommissionen

God praxis mot obehörig åtkomst och stöld

För att förhindra attacker som innebär obehörig åtkomst och stöld är det nödvändigt att följa principer som *”behovsenlig behörighet”* och *”säkerhet och integritetsskydd som standard”*, som betonar att känsliga och konfidentiella tillgångar (inklusive personliga och känsliga uppgifter, transportsystem etc.) endast bör vara tillgängliga för den som har rätt att få tillgång till dem för att utföra sina uppgifter. Du kan hjälpa till att skydda din organisation genom att följa god praxis för att identifiera och förhindra obehörig åtkomst och stöld, till exempel följande:

- *Följ säkerhetsorganisatoriska policyer.*
- *Undvik att dela och publicera identifieringsinformation och personuppgifter online, inklusive bilder som kan innehålla sådan information.*
- *Undvik att använda eller överföra identifieringsinformation och personuppgifter (och andra känsliga uppgifter) till otillförlitliga och osäkra nätverk, enheter eller webbtjänster (t.ex. webbplatser som använder osäkra protokoll eller adresser [http://] och inte säkra [https://])*
- ***Avslöja aldrig för någon din identifieringsinformation*** *(t.ex. inloggningsuppgifter och lösenord), inte ens via e-post eller telefon.*
- *Skydda känsliga uppgifter som skrivs på tangentbord eller visas på skärmar (inklusive på mobila enheter) från obehöriga, installera sekretesskärmar samt undvik att arbeta på offentliga platser med privata enheter och att lämna någon enhet olåst och utan uppsikt.*
- ***Använd komplexa lösenord*** *(t.ex. tillräckligt långt lösenord med både alfanumeriska tecken och specialtecken) i enlighet med relevanta organisatoriska säkerhetspolicyer för att förhindra obehörig åtkomst.*
- ***Ändra standardlösenord*** *för anslutna system och enheter (t.ex. skrivare, routrar, kameror, smartlås etc.).*
- *Undvik att använda samma identifieringsinformation (t.ex. inloggningsuppgifter och lösenord) för flera tjänster och system, och undvik att använda samma identifieringsinformation för tjänster och system som kräver privilegierade konton.*
- *Skicka endast lösenord och nycklar för överförda skyddade filer (t.ex. zip-filer) via en kanal utanför bandet (t.ex. sms via GSM och telefonsamtal) och aldrig via e-post.*
- ***Aktivera tvåfaktorsautentisering*** *eller flerfaktorsautentisering, om möjligt.*

Europeiska kommissionen

God praxis mot manipulering av programvara

Du kan hjälpa till att skydda din organisation genom att följa god praxis för att identifiera och förhindra manipulering av programvara, till exempel följande:

- *Undvik att installera opålitlig programvara på system och enheter (inklusive persondatorer, servrar, kringutrustning, nätverksenheter, smarttelefoner etc.).*
- *Installera alltid programvara och uppdateringar från officiella källor och webbplatser (t.ex. producenter, företagsdatabassystem etc.).*
- *Undvik att ladda ner programvara och applikationer (och eventuella filer) från olagliga källor.*
- *Avinstallera onödig programvara och programvara som inte använts nyligen samt inaktivera onödiga anslutningar (t.ex. nätverksprotokoll och tjänster) inklusive åtkomst till fjärrtjänster (t.ex. molntjänster).*
- *Skanna all programvara och alla lagringsenheter med ett pålitligt och uppdaterat antivirusprogram.*
- *Ladda ner säker industriell programvara (t.ex. uppdateringar, patchar, nya produkter etc.) från betrodda leverantörer med hjälp av white station-principen.*
- *Uppdatera all installerad programvara i enlighet med organisationens policyer och praxis.*

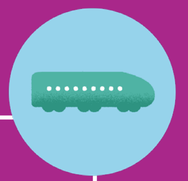
Europeiska kommissionen

Profil II: Beslutsfattare på området cybersäker transport

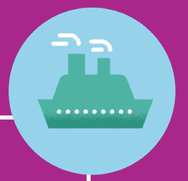
Den här delen riktar sig till personal som har beslutsfattande ansvar för säkerhet eller cybersäkerhet i transportorganisationer. Denna väg framhåller god praxis som är anpassad till de olika transportsätten. I synnerhet ger den god praxis för att identifiera, skydda mot, upptäcka och svara på nya cyberhot.

Europeiska kommissionen

God praxis för cybersäkerhet anpassad för luftfart



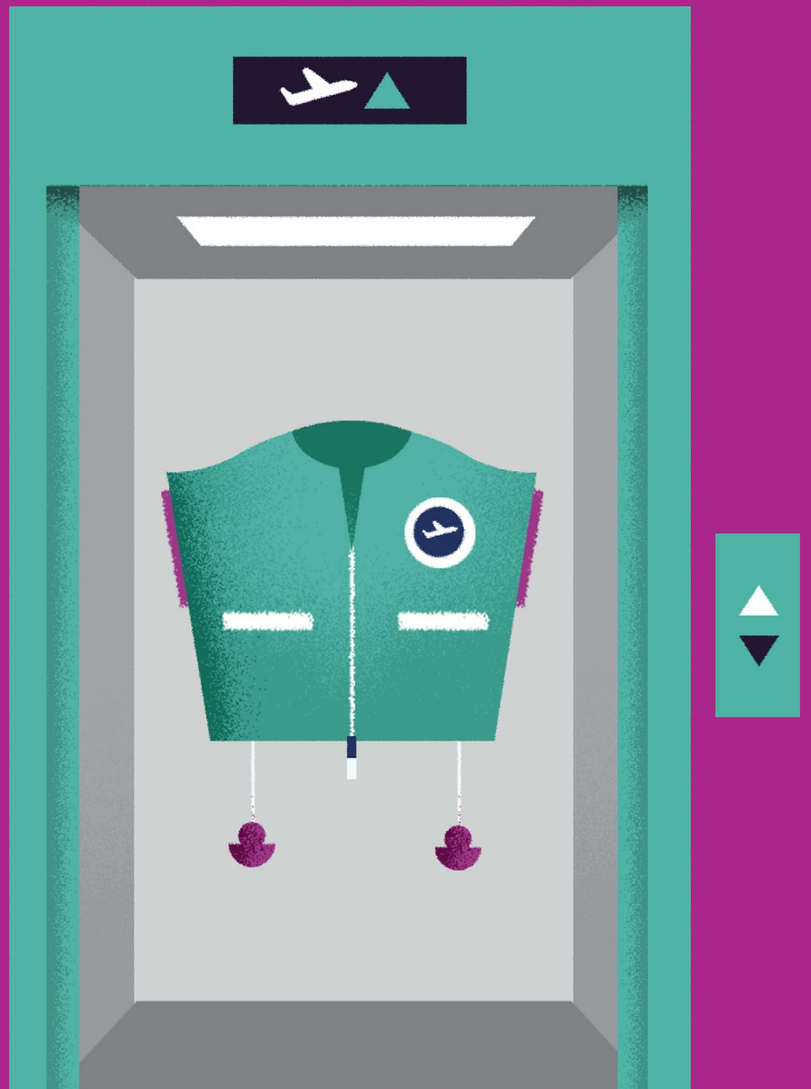
God praxis för cybersäkerhet anpassad för landtransport



God praxis för cybersäkerhet anpassad för sjöfart

Europeiska kommissionen

God praxis och säkerhetsåtgärder anpassade för luftfart



Styrning

Luftfartsorganisationer behöver tydlig förståelse om nya hot för att definiera hanteringspolicyer och -rutiner för att styra deras strategi för att förbättra cybersäkerheten för tjänster och system i verksamheten, inklusive informationsteknik (it) och driftteknik (dt).

God praxis för organisationer av alla storlekar inbegriper följande:

- Säkerställa att ledningsnivåer rapporterar cybersäkerhetsfrågor till chefer och styrelser, som kan fatta välgrundade beslut om resursfördelningar.

- Inrätta en ledande befattning, som ansvarar för cybersäkerhet såväl som fysisk säkerhet, med övergripande ledningsansvar för säkerheten för informationsteknik och driftteknik, men utan inblandning i verksamheten för att undvika intressekonflikter.

- Definiera tydligt roller, ansvar, kompetenser och godkännanden som rör cybersäkerhet samt kommunicera och kom överens om dem med relevant personal, särskilt för medarbetare i it-incidenthanteringsorganisationer.

- Säkerställa styrning av cybersäkerhet genom hela säkerhetskedjan, inklusive både fysiska och digitala gränssnitt, från tekniktillverkare och installatörer till säkerhetsleverantörer.

- Komma överens om aktiviteter och kontroller, inklusive gemensamt ansvar, för att hantera cybersäkerhetsrisker och se till att detta ansvar upprätthålls under hela löptiden (t.ex. genom serviceavtal) för säkerhetslösningar och tjänster.

- Definiera styrningsmekanismer (t.ex. policyer) för att uppfylla skyldigheter från relevanta förordningar och direktiv, till exempel förordning 2018/1139 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och kommissionens genomförandeförordning 2017/373 om gemensamma krav för leverantörer av flygledningstjänst/flygtrafiktjänster och övriga nätverksfunktioner för flygledningstjänst och om tillsyn över dessa leverantörer samt NIS-direktivet (EU-direktiv 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem).

Exempel på tjänster och system inom luftfart: Exempel på it (informationsteknik) är sådana som är tillgängliga för anställda (t.ex. persondatorer, mobiltelefoner, kontorsutrustning etc.) samt passagerare (t.ex. offentliga wifi-routrar och anslutningar etc.). Exempel på dt (driftteknik) är avancerade styrsystem (Scada-system), luftkonditioneringssystem, säkerhetskontroller för kabinbagage, bagagehanteringssystem, åtkomstkontroll, bevakning och övervakning, larmsvar, säkerhetsteknik, kontrollsystem för flygfältsbelysning, radarsystem och sensorer, global positioning system (GPS), system för flygledningstjänst (ATM), kommunikations-, navigations- och övervakningssystem (CNS), system för flyginformation, meteorologiska system, system för säkerhetscentrum, flygbolags ombordssystem och övriga.

Europeiska kommissionen

Identifiera cybersäkerhetshot

Riskhantering: Luftfartsorganisationer måste vidta lämpliga åtgärder för att identifiera, bedöma och förstå cybersäkerhetsrisker för nätverks- och informationssystem som stöder driften av viktiga funktioner.

Detta kräver en övergripande organisatorisk strategi för riskhantering som omfattar följande:

- *Säkerställa en tydlig överblick över de olika maskin- och programvarusystem som används för att leverera olika tjänster. I luftfartssammanhang omfattar sådana system informationsteknik (it) samt driftteknik (dt).*

- *Utföra **cybersäkerhetsriskbedömningar** som tar hänsyn till nya hot, kända sårbarheter och driftsdata i förhållande till de system som omfattas. Organisationer som den europeiska flygledningstjänstens it-incidenthanteringsorganisation (Eatm-Cert) och luftfartens informations- och analyscentral (A-Isac) kan ge insikter om hot som riktas mot luftfarten.*

- *Säkerställa att riskbedömningarna också omfattar riskerna i samband med personalens dagliga aktiviteter (t.ex. användning av sociala medier, användning av personliga enheter, databehandling, informationsutbyte etc.).*

- *Identifiera och genomföra riskhanteringsåtgärder och planer för att minska cybersäkerhetsrisker.*

- *Införa ett omfattande **ledningssystem för informationssäkerhet** och ett **informationshanteringssystem för integritetsskydd** anpassade till andra hanteringssystem. Sådana system (dvs. ledningssystem för informationssäkerhet och informationshanteringssystem för integritetsskydd) innebär införande av säkerhetskontroller (liksom data- och integritetsskydd) för att begränsa och förhindra nya hot som påverkar säkerheten för luftfartstjänster och -system (inklusive deras data)*

- *Ta hänsyn till alla begränsningar som rör **förvaltning av tillgångar och resursplanering** (det vill säga begränsningar som kan påverka leverans, underhåll och support av kritiska system för drift av viktiga funktioner inom luftfart).*

Europeiska kommissionen

Exempel på riskhanteringsramar: Olika ramar (t.ex. standarder i ISO/IEC 27000-familjen, NIST-cybersäkerhetsramverket, MITER ATT&CK-ramverket, BSI IT-Grundschutz etc.) kan informera och stödja en anpassad strategi för riskhantering för luftfart. Internationella organisationer som Iata och Icao ger vägledning för riskbedömningar för cybersäkerhet. Bland annat Enisa, Easa, Eurocontrol och Airports Council International (ACI) lyfter fram god praxis för att säkra flygplatser, leverantörer av flygtrafikledning och andra luftfartsorganisationer. Det gemensamma företaget Sesar samordnar och koncentrerar all EU:s forskning och utveckling (FoU) inom flygtrafikledning som även omfattar aspekter av skydd såväl som säkerhet.

Skydda mot cybersäkerhetshot

Organisationer inom luftfart bör genomföra lämpliga och proportionella säkerhetsåtgärder för att skydda sina nätverks- och informationssystem – inklusive informationsteknik (it) och driftteknik (dt) mot cyberattacker. Säkerhetsåtgärder inkluderar följande:

- ***Säkerhetspolicyer och -förfaranden:*** *definiera, genomföra, kommunicera och tillämpa lämpliga policyer och rutiner, som definierar en övergripande strategi för att säkra system och uppgifter som stöder driften av väsentliga funktioner inom luftfarten. Sådana säkerhetspolicyer (t.ex. lösenord och lagringspolicyer) och -rutiner bör också omfatta patchar och sårbarhetshantering av maskin- och programvarusystem (inklusive it och dt), incidenthantering, system- och nätverksskydd.*

- ***Identitets- och åtkomsthantering:*** *förstå, dokumentera och hantera åtkomst till nätverk och informationssystem (inklusive it och dt) som stöder driften av viktiga funktioner inom luftfart. Användare (eller automatiska funktioner) som kan komma åt data eller system verifieras, autentiseras och auktoriseras på lämpligt sätt. Detta bör också ta hänsyn till olika roller och ansvar för vanliga och privilegierade konton.*

- ***Data- och systemsäkerhet:*** *skydda data (lagrade och elektroniskt överförda), kritiska nätverk och informationssystem (inklusive it och dt) mot cyberattacker. Med hänsyn till en strategi som bygger på risk bör organisationer genomföra säkerhetsåtgärder för att effektivt begränsa möjligheterna för angripare att kompromettera data, nätverk och system. Dessa säkerhetsåtgärder bör också inkludera antagandet av kryptering och säkra kommunikationsprotokoll för att skydda vilande data och data under överföring mot cybersäkerhetshot som leder till man-i-mitten-attacker. Dessutom är det nödvändigt att kombinera sådana åtgärder med fysiska säkerhetsåtgärder för att skydda åtkomsten till system (t.ex. bör system placeras i slutna rum med begränsad åtkomst).*

- ***Nätverks och systems motståndskraft:*** *bygga upp motståndskraft i nätverk och system (inklusive it och dt) genom att utforma och införa dem (och deras driftrutiner) för att motstå och minska effekterna av cyberattacker. Följande är exempel på lösningar för utformning och införande som ökar motståndskraften: formellt verifierade kritiska funktioner, redundans av system och nätverk, segregering av nätverk (särskilt segregering av it och dt), säkerhetsåtgärder i flera lager och många andra. Observera att från en informationssäkerhetssynpunkt kan säkerhetsdomäner som genomför nätverks- och systemsegregeringar tillhandahålla lämpliga säkerhetslösningar. Driftsbehov (t.ex. underhållsaktiviteter, dataöverföringar etc.) för system kan dock kräva att olika säkerhetsdomäner (t.ex. segregerade system och nätverk) kringgås eller kopplas in, inklusive anslutning av it och dt.*

Upptäcka cybersäkerhetshot

Organisationer bör se till att säkerhetsåtgärder förblir effektiva och upptäcker eventuella cybersäkerhetshändelser som påverkar eller kan påverka säkerhetskontroller samt viktiga tjänster och system. Följande säkerhetsåtgärder är relevanta för att upptäcka cybersäkerhetshot:

- ***Säkerhetsövervakning:*** *övervakning av säkerhetsstatus för nätverk och informationssystem – inklusive informationsteknik (it) och driftteknik (dt) – som stöder driften av viktiga funktioner inom luftfartstjänster. Till exempel följande typer av data bör beaktas för att stödja säkerhetsövervakning:*

  - *Säkerhetsloggar.*
  - *Virusskyddsloggar.*
  - *Intrångsskyddsloggar.*
  - *Loggar för identifiering, autentisering och auktorisering.*
  - *System- och tjänsteloggar.*
  - *Nätverkstrafiksloggar.*
  - *Databehandlingsloggar.*

- ***Upptäckt av säkerhetshändelser:*** *upptäckt av skadliga aktiviteter (dvs säkerhetshändelser) som påverkar eller har potential att påverka säkerheten för nätverk och informationssystem (inklusive it och dt) som stöder driften av viktiga funktioner inom lufttransporttjänster.*

Dessa åtgärder kan kräva antagande av specifik teknik (t.ex. säkerhetsinformation och händelsehantering, system för upptäckt av intrång, intrångsskydd etc.) och inrättande av ett SOC (säkerhetscentrum) eller motsvarande. Det vill säga utveckla medel för att lokalt upptäcka, analysera, svara på och återhämta sig från cyberattacker.

Nationella it-incidentcentrum (CSIRT), sektoriella it-incidenthanteringsorganisationer (t.ex. den europeiska flygledningstjänstens it-incidenthanteringsorganisation Eatm-Cert vid Eurocontrol), kommersiella it-incidenthanteringsorganisationer för flygbolag och luftfartens informations- och analyscentral (A-Isac) kan tillhandahålla underrättelser om cyberhot som informerar om säkerhetsövervakning och upptäckter.

Beredskaps- och återhämtningsplanering

Organisationer bör definiera, genomföra och testa förfaranden för incidenthantering som avser att säkerställa kontinuitet i tjänster och system i händelse av cybersäkerhetsincidenter. Riskreducerande åtgärder avser att begränsa effekterna av cybersäkerhetsincidenter.

Beredskaps- och återhämtningsplaneringen bör ta hänsyn till bland annat följande säkerhetsåtgärder för att minska effekterna av specifika cybersäkerhetsattacker:

- *Samordning och samarbete med nationella it-incidentcentrum, (offentliga och kommersiella) it-incidenthanteringsorganisationer och informations- och analyscentraler vid cybersäkerhetsincidenter samt samordning av incidenter och kriser på Europaomfattande nivå.*

- *Informationsutbyte med andra organisationer, inklusive leverantörer inom luftfartstjänsters leverantörskedja.*

- *Genomförande av regelbundna **cyberattackövningar** (skrivbordssamordning samt teknisk) för bedömning av säkerhetsåtgärder och -rutiner samt organisationens motståndskraft för att hantera cyberincidenter.*

- *Åtkomst till arkiverade eller säkerhetskopierade lagringsplatser vid komprometterad integritet och tillgänglighet för datalagring.*

- ***Säkerhetshandböcker** med detaljerade förfaranden för hantering av cybersäkerhetsincidenter och återställande av tjänster och system till normala driftsförhållanden*

- *Omdirigeringar av nätverkstrafik till redundanta tjänster vid överbelastningsattacker.*

- *Manuella förfaranden för drift med tjänster och system i försämrade driftslägen.*

- *Definition av förfaranden för att hantera dataintrång, inklusive förfaranden för hantering av dataintrång som påverkar personuppgifter i enlighet med den allmänna dataskyddsförordningen och andra relevanta sektorsföreskrifter eller direktiv.*

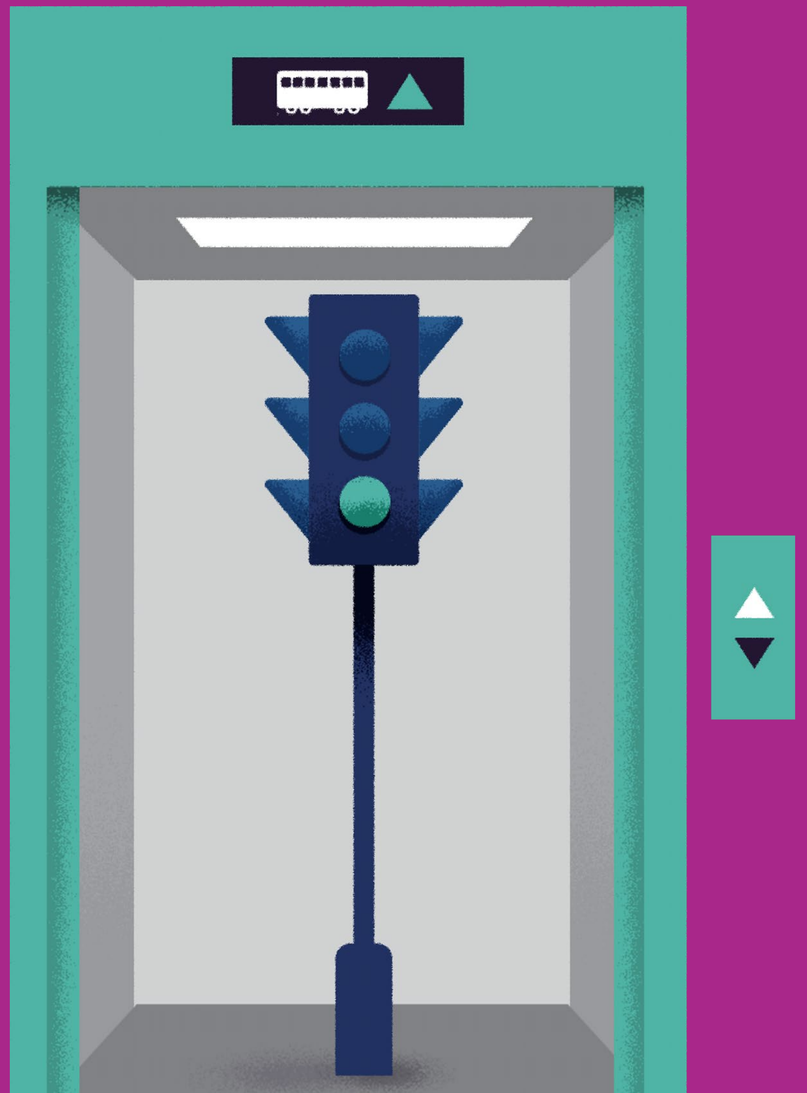
- *Anskaffning av **cyberförsäkring** för att delvis motverka risken i samband med allvarliga cyberincidenter.*

- *Ingående av avtal om ombudstjänst för incidentberedskap med ett eller flera specialiserade företag för extra kapacitet och expertis.*

- *Definition av förfaranden för **informationsutbyte om cybersäkerhetsincidenter** med relevanta intressenter, inklusive förfaranden för incidentanmälan i enlighet med NIS-direktivet (EU-direktiv 2016/1148 om åtgärder för en hög gemensam säkerhetsnivå i nätverks- och informationssystem i hela unionen).*

Europeiska kommissionen

God praxis och säkerhetsåtgärder anpassade till landtransport



Styrning

Organisationer inom landtransport (järn- och landsväg) behöver tydlig förståelse om nya hot för att definiera hanteringspolicyer och -rutiner för att styra deras strategi för att förbättra cybersäkerheten för tjänster och system i verksamheten, inklusive informationsteknik (it) och driftteknik (dt).

God praxis för organisationer av alla storlekar inbegriper följande:

- *Säkerställ att ledningsnivåer rapporterar cybersäkerhetsfrågor till chefer och styrelser, som kan fatta välgrundade beslut om resursfördelningar.*

- *Utnämna ledande roll, som ansvarar för cybersäkerhet såväl som fysisk säkerhet, med övergripande ledningsansvar för säkerheten för informationsteknik och driftteknik, men utan inblandning i verksamheten för att undvika intressekonflikter.*

- *Definiera roller, ansvar, kompetenser och godkännanden relaterade till cybersäkerhet tydligt och kommunicera med och kom överens med relevant personal. Detta är särskilt nödvändigt för medlemmar i it-incidenthanteringsorganisationer (CERT).*

- *Säkerställa styrning av cybersäkerhet genom hela säkerhetskedjan, inklusive både fysiska och digitala gränssnitt, från tekniktillverkare och installatörer till säkerhetsleverantörer.*

- *Komma överens om aktiviteter och kontroller, inklusive gemensamt ansvar, för att hantera cybersäkerhetsrisker och se till att detta ansvar upprätthålls under hela livstiden (t.ex. genom serviceavtal) för säkerhetslösningar och tjänster.*

- *Definiera styrningsmekanismer (t.ex. policyer) för att uppfylla skyldigheterna från relevanta förordningar och direktiv. Detta omfattar en bred uppsättning av policyer som omfattar de specifika transportsätten samt olika typer av intressenter (t.ex. tillverkare av fordon och järnvägssystem) samt NIS-direktivet (EU-direktiv 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem).*

Exempel på tjänster och system inom landtransport:
Exempel på it (informationsteknik) är sådana som är tillgängliga för anställda (t.ex. persondatorer, mobiltelefoner, kontorsutrustning etc.) samt passagerare (t.ex. offentliga wifi-routrar och anslutningar etc.).
Exempel på dt är avancerade styrsystem (Scada-system), luftkonditioneringssystem, global positioning system (GPS), åtkomstkontroll, bevakning och övervakning, larmsvar och säkerhetsteknik. Specifika system för järnvägstransporter är till exempel drift- (kontroll- och styrsystem) inklusive signalsystem, det europeiska trafikstyrningssystemet för tåg (ERTMS), fordonsbaserade system, underhållssystem och övriga.

Identifiera cybersäkerhetshot

Riskhantering: Organisationer inom landtransport måste vidta lämpliga åtgärder för att identifiera, bedöma och förstå cybersäkerhetsrisker för nätverks- och informationssystem som stöder driften av viktiga funktioner. Detta kräver en övergripande organisatorisk strategi för riskhantering som omfattar följande:

- *Säkerställa en tydlig överblick över de olika maskin- och programvarusystemen som används för att leverera olika tjänster. I landtransportssammanhang omfattar sådana system informationsteknik (it) samt driftteknik (dt).*

- *Utföra **cybersäkerhetsriskbedömningar**, som bör ta hänsyn till nya hot, kända sårbarheter och driftsdata i förhållande till de system som omfattas. Följande är exempel på system i landtransportsätten: betalningssystem, nätverks- och kommunikationssystem (t.ex. internet, radiokommunikation, wifi etc.), fordonsutrustning, driftscentraler, identitetshanteringssystem, säkerhetssystem och övriga system. Följande är exempel på system i järnvägsinfrastrukturer: rullande materiel, delsystem för drift och trafikledning, trafikstyrning och delsystem för signalering ombord och vid banan samt övriga system.*

- *Säkerställa att riskbedömningar också omfattar riskerna i samband med personalens dagliga aktiviteter (t.ex. användning av sociala medier, användning av personlig enhet, databehandling, informationsutbyte etc.).*

- *Identifiera och genomföra riskhanteringsåtgärder och planer för att minska cybersäkerhetsrisker. Detta kan till exempel innebära att införa ett omfattande **ledningssystem för informationssäkerhet** och ett **informationshanteringssystem för integritetsskydd** anpassade till andra hanteringssystem. Sådana system (dvs. ledningssystem för informationssäkerhet och informationshanteringssystem för integritetsskydd) innebär införande av säkerhetskontroller (liksom data- och integritetsskydd) för att begränsa och förhindra nya hot som påverkar säkerheten för landtransporttjänster och -system (inklusive deras data)*

- *Ta hänsyn till alla begränsningar som rör **förvaltning** av tillgångar **och resursplanering** (det vill säga begränsningar som kan påverka leverans, underhåll och support av kritiska system för drift av väsentliga funktioner inom landtransport).*

Exempel på riskhanteringsramar: Olika ramar (t.ex. standarder i ISO/IEC 27000-familjen, NIST-cybersäkerhetsramverket, MITER ATT&CK-ramverket, BSI IT-Grundschutz etc.) kan informera och stödja en anpassad strategi för riskhantering för väg- och järnvägstransport. Organisationer som Enisa definierar god praxis för cybersäkerhet för smarta bilar och intelligent kollektivtrafik, som informerar industritillverkare och föreningar (t.ex. den europeiska bilindustriföreningen ACEA). Inom järnvägstransporten definierar Europeiska unionens järnvägsbyrå (ERA) tekniska specifikationer för driftskompatibilitet (TSD:er), som måste uppfyllas av varje delsystem eller del av sådana för att uppfylla de väsentliga kraven och säkerställa driftskompatibiliteten hos EU:s järnvägssystem. Det gemensamma företaget Shift2Rail driver också innovationsinitiativ (inklusive cybersäkerhet) och projekt för järnvägstransporter.

Skydda mot cybersäkerhetshot

Organisationer inom landtransport bör genomföra lämpliga och proportionella säkerhetsåtgärder för att skydda sina nätverks- och informationssystem – inklusive informationsteknik (it) och driftteknik (dt) – mot cyberattacker. Säkerhetsåtgärder inkluderar följande:

- ***Säkerhetspolicyer och -förfaranden:*** *definiera, genomföra, kommunicera och tillämpa lämpliga policyer och rutiner, som definierar en övergripande strategi för att säkra system och uppgifter som stöder drift av väsentliga funktioner i landtransportsätt. Sådana säkerhetspolicyer (t.ex. lösenord och lagringspolicyer) och -rutiner bör också omfatta patchar och sårbarhetshantering av maskin- och programvarusystem (inklusive it och dt), incidenthantering, system- och nätverksskydd.*

- ***Identitets- och åtkomsthantering:*** *förstå, dokumentera och hantera åtkomst till nätverk och informationssystem (inklusive it och dt) som stöder driften av viktiga funktioner inom landtransportsätt. Användare (eller automatiska funktioner) som kan komma åt data eller system verifieras, autentiseras och auktoriseras på lämpligt sätt. Detta bör också ta hänsyn till olika roller och ansvar för vanliga och privilegierade konton.*

- ***Data- och systemsäkerhet:*** *skydda data (lagrade och elektroniskt överförda), kritiska nätverk och informationssystem (inklusive it och dt) mot cyberattacker. Med hänsyn till en strategi som bygger på risk bör organisationer genomföra säkerhetsåtgärder för att effektivt begränsa möjligheter för angripare att kompromettera data, nätverk och system. Dessa säkerhetsåtgärder bör också inkludera antagandet av kryptering och säkra kommunikationsprotokoll för att skydda vilande data och data under överföring mot cybersäkerhetshot som leder till man-i-mitten-attack. Dessutom är det nödvändigt att kombinera sådana åtgärder med fysiska säkerhetsåtgärder för att skydda åtkomsten till system (t.ex. bör system placeras i slutna rum med begränsad åtkomst). Detta är mycket viktigt för de system som kan påverka livssäkerheten.*

- ***Nätverks och systems motståndskraft:*** *bygga upp motståndskraft i nätverk och system (inklusive it och dt) genom att utforma och införa dem (och deras driftrutiner) för att motstå och minska effekterna av cyberattacker. Följande är exempel på lösningar för utformning och införande som ökar motståndskraften: formellt verifierade kritiska funktioner, redundans av system och nätverk, segregering av nätverk (särskilt segregering av it och dt), säkerhetsåtgärder i flera lager och många andra. Observera att från en informationssäkerhetssynpunkt kan säkerhetsdomäner som genomför nätverks- och systemsegregeringar tillhandahålla lämpliga säkerhetslösningar. Driftsbehov (t.ex. underhållsaktiviteter, dataöverföringar etc.) för system kan dock kräva att olika säkerhetsdomäner (t.ex. segregerade system och nätverk) kringgås eller kopplas in, inklusive anslutning av it och dt.*

Upptäcka cybersäkerhetshot

Organisationer bör se till att säkerhetsåtgärder förblir effektiva och upptäcker eventuella cybersäkerhetshändelser som påverkar eller kan påverka säkerhetskontroller samt viktiga tjänster och system. Följande säkerhetsåtgärder är relevanta för att upptäcka cybersäkerhetshot:

- ***Säkerhetsövervakning:*** *övervakning av säkerhetsstatus för nätverk och informationssystem – inklusive informationsteknik (it) och driftteknik (dt) – som stöder drift av viktiga funktioner inom landtransportsätt. Detta är nödvändigt för att upptäcka potentiella säkerhetshot och för att spåra den pågående effektiviteten av skyddande säkerhetsåtgärder. Till exempel följande typer av data bör beaktas för att stödja säkerhetsövervakning:*

  - *Säkerhetsloggar.*
  - *Virusskyddsloggar.*
  - *Intrångsskyddsloggar.*
  - *Loggar för identifiering, autentisering och auktorisering.*
  - *System- och tjänsteloggar.*
  - *Nätverkstrafiksloggar.*
  - *Databehandlingsloggar.*

- ***Upptäckt av säkerhetshändelser:*** *upptäcka skadliga aktiviteter (det vill säga säkerhetshändelser) som påverkar eller med potential att påverka säkerheten för nätverks- och informationssystem (inklusive it och dt) som stöder driften av viktiga funktioner.*

Dessa åtgärder kan kräva antagande av specifik teknik (t.ex. säkerhetsinformation och händelsehantering, system för upptäckt av intrång, intrångsskydd etc.) och inrättande av ett SOC (säkerhetscentrum) eller motsvarande. Det vill säga utveckla medel för att lokalt upptäcka, analysera, svara på och återhämta sig från cyberattacker.
Nationella it-incidentcentrum, sektoriella och kommersiella it-incidenthanteringsorganisationer eller väg- och järnvägsoperatörer och den europeiska järnvägsinformations- och analyscentralen (Er-Isac) kan tillhandahålla underrättelser om cyberhot som informerar om säkerhetsövervakning och upptäckter.

Europeiska kommissionen

Beredskaps- och återhämtningsplanering

Organisationer bör definiera, genomföra och testa förfaranden för incidenthantering som avser att säkerställa kontinuitet i tjänster och system i händelse av cybersäkerhetsincidenter.

Beredskaps- och återhämtningsplaneringen bör ta hänsyn till bland annat följande säkerhetsåtgärder för att minska effekterna av specifika cybersäkerhetsattacker:

- *Samordning och samarbete med nationella it-incidentcentrum, (offentliga och kommersiella) it-incidenthanteringsorganisationer och informations- och analyscentraler vid cybersäkerhetsincidenter samt samordning av incidenter och kriser på Europaomfattande nivå.*

- *Informationsutbyte med andra organisationer, inklusive leverantörer i landtransportkedjans leveranskedja.*

- *Genomförande av regelbundna **cyberattackövningar** (skrivbordssamordning såväl som teknisk) för bedömning av säkerhetsåtgärder och -rutiner samt organisationers motståndskraft att hantera cyberincidenter.*

- *Åtkomst till arkiverade eller säkerhetskopierade lagringsplatser vid komprometterad integritet och tillgänglighet för datalagring.*

- ***Säkerhetshandböcker** med detaljerade förfaranden för hantering av cybersäkerhetsincidenter och återställande av tjänster och system till normala driftsförhållanden.*

- *Omdirigeringar av nätverkstrafik till redundanta tjänster vid överbelastningsattacker.*

- *Manuella förfaranden för drift med tjänster och system i försämrade driftslägen.*

- *Definition av förfaranden för att hantera dataintrång, bl.a. förfaranden för hantering av dataintrång som påverkar personuppgifter i enlighet med den allmänna dataskyddsförordningen och andra relevanta sektorsföreskrifter eller direktiv.*

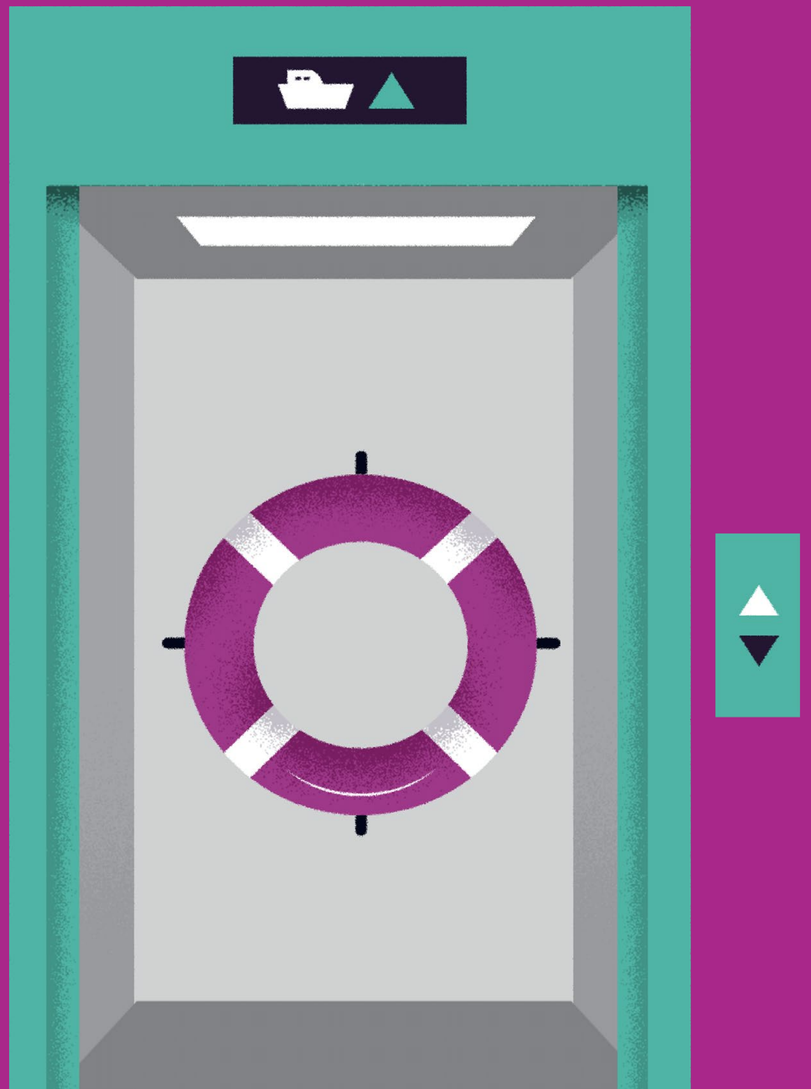
- *Anskaffning av **cyberförsäkring** för att delvis motverka risken i samband med allvarliga cyberincidenter.*

- *Ingående av avtal om ombudstjänst för incidentberedskap med ett eller flera specialiserade företag för extra kapacitet och expertis.*

- *Definition av förfaranden för informationsutbyte av cybersäkerhetsincidenter med relevanta intressenter, inklusive förfaranden för incidentanmälan i enlighet med NIS-direktivet (EU-direktiv 2016/1148 om åtgärder för en hög gemensam säkerhetsnivå i nätverks- och informationssystem i hela unionen).*

Europeiska kommissionen

God praxis och säkerhetsåtgärder anpassade till sjöfart



Styrning

Sjöfartsorganisationer behöver tydlig förståelse om nya hot för att definiera hanteringspolicyer och -rutiner för att styra deras strategi för att förbättra cybersäkerheten för tjänster och system i verksamheten, inklusive informationsteknik (it) och driftteknik (dt).

God praxis för organisationer av alla storlekar inkluderar följande:

- *Säkerställa att ledningsnivåer rapporterar cybersäkerhetsfrågor till chefer och styrelser, som kan fatta välgrundade beslut om resursfördelningar.*

- *Utnämna en ledande roll med övergripande ledningsansvar för säkerheten för informationsteknik och driftteknik. Denna tjänst bör ansvara för cybersäkerhet såväl som fysisk säkerhet.*

- *Definiera tydligt, roller, ansvar, kompetenser och godkännanden relaterade till cybersäkerhet, definiera auktoritetsnivåer och kommunikationslinjer mellan, och bland land- och fartygspersonal, och enas om dem med relevant personal. Detta är särskilt nödvändigt för medlemmar i it-incidenthanteringsorganisationer. Personal med roller avseende EU-lagstiftning för sjöfartssäkerhet och sjöfartsskydd, såsom sjöfartsskyddsansvariga vid hamnanläggningar, hamnskyddsansvariga eller säkerhetsansvariga vid företag eller ansvariga personer på land och ansvarsstyrmän ombord, bör åtminstone vara bekant med de cybersäkerhetsåtgärder som vidtagits av organisationen*

- *Säkerställa styrning av cybersäkerhet genom hela säkerhetskedjan, inklusive både fysiska och digitala gränssnitt, från tekniktillverkare och installatörer till säkerhetsleverantörer.*

- *Komma överens om aktiviteter och kontroller, inklusive gemensamt ansvar, för att hantera cybersäkerhetsrisker och se till att detta ansvar upprätthålls under hela livstiden (t.ex. genom serviceavtal) för säkerhetslösningar och tjänster.*

- *Definiera styrningsmekanismer (t.ex. policyer) för att uppfylla skyldigheterna från relevanta förordningar och direktiv, till exempel förordning 2019/1239 om inrättande av en europeisk kontaktpunkt för sjöfart (EMSWe), förordning 725/2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar, direktiv 2005/65/EG om ökat hamnskydd och förordning (EG) nr 336/2006 om genomförande av Internationella säkerhetsorganisationskoden (ISM) samt resolution A.741.18 om antagande av ISM-koden för säker drift av fartyg och förebyggande av föroreningar. I detta sammanhang är det också relevant att nämna den gemensamma miljön för informationsdelning (CISE), ett EU-initiativ som syftar till att göra europeiska och medlemsstaters övervakningssystem driftskompatibla för att ge alla berörda myndigheter tillgång till den sekretessbelagda och oklassificerade information de behöver för att utföra uppdrag till havs.*

Europeiska kommissionen

Exempel på tjänster och system inom sjöfart:
Exempel på it (informationsteknik) är sådana som är tillgängliga för anställda (t.ex. persondatorer, mobiltelefoner, kontorsutrustning etc.) samt passagerare (t.ex. offentliga wifi-routrar och anslutningar etc.). Exempel på dt (driftteknik) är avancerade styrsystem (Scada-system), luftkonditioneringssystem, global positioning system (GPS), åtkomstkontroll, bevakning och övervakning, larmsvar, säkerhetsteknik, navigationssystem ombord, SafeSeaNet, bryggsystem, system för godshantering och drift, system för framdrivning och maskinstyrning samt driftcentraler, system för åtkomstkontroll, system för passagerarservice och -hantering, offentliga nätverk för passagerare, administrativa system och system för besättningens välbefinnande, kommunikationssystem och övriga.

Identifiera cybersäkerhetshot

Riskhantering: Sjöfartsorganisationer måste vidta lämpliga åtgärder för att identifiera, analysera, bedöma och kommunicera cybersäkerhetsrisker och acceptera, undvika, överföra eller minska dem till en acceptabel nivå. Detta kräver en övergripande organisatorisk strategi för riskhantering som omfattar följande:

- *Säkerställa en tydlig överblick över de olika maskin- och programvarusystemen som används för att leverera olika tjänster. I sjöfartssammanhang omfattar sådana system informationsteknik (it) samt driftteknik (dt) och hur dessa system ansluter och integreras med landsidan, inklusive offentliga myndigheter, marina terminaler och stuvare*

- *Identifiera och utvärdera viktiga verksamheter ombord på skepp som är sårbara för cyberattacker, och utföra cybersäkerhetsriskbedömningar (inklusive bedömning av potentiella operativa effekter och sannolikhet för inträffande), som bör ta hänsyn till nya hot, kända sårbarheter och driftuppgifter i förhållande till de system som omfattas. I förekommande fall skapa en koppling mellan skyddsutredningar av fartyg, hamnanläggningar och hamnar enligt EU-lagstiftning om sjöfartsskydd. Dessa identifierar möjliga säkerhetshot mot hamninfrastruktur och säkerhetsbrister. Dessutom kan sjöfartsorganisationer som Internationella sjöfartsorganisationen (IMO) och sjöfartens informations- och analyscentraler ge insikter om hot som riktar sig mot sjöfartstransporter.*

- *Säkerställa att riskbedömningar också omfattar riskerna i samband med personalens dagliga aktiviteter (t.ex. användning av sociala medier, användning av personlig enhet, databehandling, informationsutbyte etc.).*

- *Identifiera och genomföra riskbehandlingsåtgärder och planer för att minska cybersäkerhetsrisker. Till exempel införa ett omfattande ledningssystem för informationssäkerhet och ett informationshanteringssystem för integritetsskydd anpassade till andra liknande system såsom säkerhetsstyrningssystem i enlighet med den internationella säkerhetsorganisationskoden (ISM-koden). Sådana system (dvs. ledningssystem för informationssäkerhet och informationshanteringssystem för integritetsskydd) innebär införande av säkerhetskontroller (liksom data- och integritetsskydd) för att begränsa och förhindra nya hot som påverkar säkerheten för sjöfartstjänster och -system (inklusive deras data)*

- *Ta hänsyn till alla begränsningar som rör **förvaltning av tillgångar och resursplanering** (det vill säga begränsningar som kan påverka leverans, underhåll och support av kritiska system för drift av viktiga funktioner inom sjöfart). När det gäller bedömningar, gör en korshänvisning där det är lämpligt till kraven i ISM-koden, säkerhetshanteringssystem och säkerhetsplaner som genomförs enligt EU-lagstiftning om sjösäkerhet och sjöfartsskydd.*

Exempel på riskhanteringsramar: Olika ramverk (t.ex. ISM-koden eller standarder i ISO/IEC 27000-familjen, NIST-cybersäkerhetsramverket, MITER ATT&CK-ramverket, BSI IT-Grundschutz etc.) kan informera och stödja en anpassad riskhanteringsstrategi för sjöfartstransporter. NIST-ramverket för cybersäkerhet har också anpassats för att ta itu med cybersäkerheten för sjötransport av vätskor i bulk, offshore-verksamheter och passagerarfartygsverksamheter. På samma sätt har Baltic and International Maritime Council (BIMCO) utfärdat *The Guidelines on Cyber Security Onboard Ships* (Riktlinjer för cybersäkerhet ombord på fartyg) och Internationella sjöfartsorganisationen (IMO) har utfärdat specifika riktlinjer för cyberriskhantering för sjöfart: *Guidelines on maritime cyber risk management* (MSC-FAL.1/Circ.3). Enisa har genomfört flera studier avseende god praxis för sjöfartscybersäkerhet, i synnerhet hamncybersäkerhet. Emsa tillhandahåller tjänster till sjöfartsnäringen, bl.a. utbildning om cybersäkerhet. Standarder (t.ex. IEC 61162-460:2018 om skydd och säkerhet för sjöfarts- och radiokommunikationsutrustning och -system, ISO 16425:2013 om fartyg och marinteknik, IEC 62443-4-1:2018 om säkerhet för industriell automatisering och styrsystem etc.) definierar också specifika säkerhetskrav för system och nätverk inom sjöfart.

Skydda mot cybersäkerhetshot

Organisationer inom sjöfart bör genomföra lämpliga och proportionella säkerhetsåtgärder för att skydda sina nätverks- och informationssystem – inklusive informationsteknik (it) och driftteknik (dt). Säkerhetsåtgärder inkluderar följande:

- ***Säkerhetspolicyer och -förfaranden:*** *definiera, genomföra, kommunicera och tillämpa lämpliga policyer och rutiner, som definierar en övergripande strategi för att säkra system och uppgifter som stöder drift av viktiga funktioner inom sjöfarten. Säkerhetsåtgärder (inklusive cybersäkerhetsåtgärder och fysiska säkerhetsåtgärder) bör ingå i relevanta planer, till exempel säkerhetsstyrningssystemet och skyddsplanen för fartyg. Sådana säkerhetspolicyer (t.ex. lösenord och lagringspolicyer) och -rutiner bör också omfatta patchar och sårbarhetshantering av maskin- och programvarusystem (inklusive it och dt), incidenthantering, system- och nätverksskydd.*

- ***Identitets- och åtkomsthantering:*** *förstå, dokumentera och hantera åtkomst till nätverk och informationssystem (inklusive it och dt) som stöder driften av viktiga funktioner inom sjöfart. Användare (eller automatiska funktioner) som kan komma åt data eller system verifieras, autentiseras och auktoriseras på lämpligt sätt. Detta bör också ta hänsyn till olika roller och ansvar för vanliga och privilegierade konton.*

- ***Data- och systemsäkerhet:*** *skydda data (lagrade och elektroniskt överförda), kritiska nätverk och informationssystem (inklusive it och dt) mot cyberattacker. Med hänsyn till en strategi som bygger på risk bör organisationer genomföra säkerhetsåtgärder för att effektivt begränsa möjligheter för angripare att kompromettera data, nätverk och system. Dessa säkerhetsåtgärder bör också inkludera antagandet av kryptering och säkra kommunikationsprotokoll för att skydda vilande data och data under överföring mot cybersäkerhetshot som leder till man-i-mitten-attack. Dessutom är det nödvändigt att kombinera sådana åtgärder med fysiska säkerhetsåtgärder för att skydda åtkomsten till system (t.ex. bör system placeras i slutna rum med begränsad åtkomst). Detta är mycket viktigt för de system som kan påverka livssäkerheten (t.ex. navigations- och radiokommunikationssystem i kategori II och III).*

- ***Nätverks och systems motståndskraft:*** *bygga upp motståndskraft i nätverk och system (inklusive it och dt) genom att utforma och införa dem (och deras driftrutiner) för att motstå och minska effekterna av cyberattacker. Följande är exempel på lösningar för utformning och införande som ökar motståndskraften: formellt verifierade kritiska funktioner, redundans av system och nätverk, segregering av nätverk (särskilt segregering av it och dt), säkerhetsåtgärder i flera lager och många andra. Observera att från en informationssäkerhetssynpunkt kan säkerhetsdomäner som genomför nätverks- och systemsegregeringar tillhandahålla lämpliga säkerhetslösningar. Behov (t.ex. underhåll, dataöverföringar etc.) för system (t.ex. Maritime Autonomous Surface Ships – MASS) kan dock kräva att man kringgår eller ansluter olika säkerhetsdomäner (t.ex. segregerade system och nätverk), inklusive anslutning av informationsteknik och driftteknik.*

Upptäcka cybersäkerhetshot

Organisationer bör se till att säkerhetsåtgärder förblir effektiva och upptäcker eventuella cybersäkerhetshändelser som påverkar eller kan påverka säkerhetskontroller samt viktiga tjänster och system. Följande säkerhetsåtgärder är relevanta för att upptäcka cybersäkerhetshot:

- ***Säkerhetsövervakning:*** *övervakning av säkerhetsstatus för nätverk och informationssystem - inklusive informationsteknik (it) och driftteknik (dt) - stöd för drift av viktiga funktioner inom sjöfartstjänster. Detta är nödvändigt för att upptäcka potentiella säkerhetshot och för att spåra den pågående effektiviteten av skyddande säkerhetsåtgärder. Till exempel följande typer av data bör beaktas för att stödja säkerhetsövervakning:*

  - *Säkerhetsloggar.*
  - *Virusskyddsloggar.*
  - *Intrångsskyddsloggar.*
  - *Loggar för identifiering, autentisering och auktorisering.*
  - *System- och tjänsteloggar.*
  - *Nätverkstrafiksloggar.*
  - *Databehandlingsloggar.*

- ***Upptäckt av säkerhetshändelser:*** *upptäckt av skadliga aktiviteter (det vill säga säkerhetshändelser) som påverkar eller har potential att påverka säkerheten för nätverk och informationssystem (inklusive it och dt) som stöder driften av viktiga funktioner inom sjöfartstjänster.*

Dessa åtgärder kan kräva antagande av specifik teknik (t.ex. säkerhetsinformation och händelsehantering, system för upptäckt av intrång, intrångsskydd etc.) och inrättande av ett SOC (säkerhetscentrum) eller motsvarande. Det vill säga utveckla medel för att lokalt upptäcka, analysera, svara på och återhämta sig från cyberattacker.

Nationella it-incidentcentrum, sektoriella it-incidenthanteringsorganisationer och kommersiella it-incidenthanteringsorganisationer för sjöfartsoperatörer samt sjöfartens informations- och analyscentraler kan tillhandahålla underrättelser om cyberhot som informerar om säkerhetsövervakning och upptäckter.

Beredskaps- och återhämtningsplanering

Organisationer bör definiera, genomföra och testa förfaranden för incidenthantering som avser att säkerställa kontinuitet i tjänster och system i händelse av cybersäkerhetsincidenter.
Beredskaps- och återhämtningsplaneringen bör ta hänsyn till bland annat följande säkerhetsåtgärder för att minska effekterna av specifika cybersäkerhetsattacker:

- *Omdirigeringar av nätverkstrafik till redundanta tjänster vid överbelastningsattacker.*

- *Manuella förfaranden för drift med tjänster och system i försämrade driftslägen.*

- *Upprättande av program för övningar (t.ex. skrivbordssamordning, tekniska övningar och svarsövningar) för att reagera på cyberattacker och nödsituationer samt för att bedöma säkerhetsåtgärder, rutiner och organisatorisk motståndskraft för att hantera cyberincidenter.*

- *Åtkomst till arkiverade eller säkerhetskopierade lagringsplatser vid komprometterad integritet och tillgänglighet för datalagring.*

- *Samordning och samarbete med nationella it-incidentcentrum, (offentliga och kommersiella) it-incidenthanteringsorganisationer och informations- och analyscentraler vid cybersäkerhetsincidenter samt samordning av incidenter och kriser på Europaomfattande nivå.*

- *Informationsutbyte med andra organisationer, inklusive leverantörer inom sjöfartstjänsters leverantörskedja.*

- *Säkerhetshandböcker med detaljerade förfaranden för hantering av cybersäkerhetsincidenter och återställande av tjänster och system till normala driftsförhållanden.*

- *Definition av förfaranden för att hantera dataintrång, inklusive förfaranden för hantering av dataintrång som påverkar personuppgifter i enlighet med den allmänna dataskyddsförordningen och andra relevanta sektorsföreskrifter eller direktiv.*

- *Anskaffning av cyberförsäkring för att delvis motverka risken i samband med allvarliga cyberincidenter.*

- *Ingående av avtal om ombudstjänst för incidentberedskap med ett eller flera specialiserade företag för extra kapacitet och expertis.*

- *Definition av förfaranden för informationsutbyte av cybersäkerhetsincidenter (inklusive avvikelser, olyckor och farliga situationer) med relevanta intressenter, inklusive förfaranden för incidentanmälan i enlighet med NIS-direktivet (EU-direktiv 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen).*

Luxemburg: Europeiska unionens publikationsbyrå, 2021

Print	ISBN 978-92-76-40470-5	doi:10.2832/03338	MI-05-21-230-SV-C
PDF	ISBN 978-92-76-40489-7	doi:10.2832/070979	MI-05-21-230-SV-N

Europeiska unionens publikationsbyrå