Euroopan komissio

# Liikenteen kyberturvallisuutta koskeva välineistö

# Johdanto

Euroopan komission liikenteen ja liikkumisen pääosasto (MOVE) on teettänyt tämän välineistön parantaakseen liikennealan sidosryhmien tietoisuutta kyberuhkista ja niihin varautumista. Välineistön avulla voidaan ymmärtää kyberuhkia ja lieventää niiden vaikutusta liikennepalveluihin, -järjestelmiin ja -toimiin. Välineistöön sisältyy vaihtoehtoiset tietoisuuden lisäämiseen tähtäävät polut, jotka on tarkoitettu liikennealan eri profiileille:

- kaikki liikennealan henkilöstö (yleiset tiedot ja ohjeet)
- eri liikennemuotojen kyberturvallisuuden alan päätöksentekijät.

Hyperlinkeistä pääsee välineistön eri osiin, jotta eri liikennealan profiileille räätälöidyillä oppimispoluilla on helppo kulkea.

**Tässä välineistössä luetellut käytännöt ovat luonteeltaan vain ohjeellisia. Esitetyt suositukset eivät ole sitovia tai pakollisia. Tämä välineistö ei myöskään edusta Euroopan komission virallisia näkemyksiä, eikä sen tarkoituksena ole tarjota keinoja EU:n nykyisen tai tulevan lainsäädännön noudattamiseksi.**

# Kyberturvallisuutta koskevan tietoisuuden profiilit

**Profiili I: Kaikki liikennealan henkilöstö.** Ensimmäinen polku on tarkoitettu kaikelle liikennealan organisaatioiden henkilöstölle liikennepalvelujen henkilöstöstä hallintohenkilöstöön. Siinä annetaan ohjeita ymmärryksen ja tietoisuuden lisäämiseksi yleisimmistä kyberuhkista, joita liikennepalveluihin ja -järjestelmiin kohdistuu. Lisäksi siinä annetaan tietoa siitä, miten mahdollisia kyberuhkia voidaan käsitellä (niiden tunnistaminen, niistä raportointi ja niiden lieventäminen) kyberturvallisuutta koskevien hyvien käytäntöjen avulla.

**Profiili II: Liikenteen kyberturvallisuuden alan päätöksentekijät.** Toinen polku on tarkoitettu henkilöstölle, joka vastaa liikennealan organisaatioiden kyberturvallisuuteen liittyvästä päätöksenteosta. Tällä polulla korostetaan eri liikennemuotoihin räätälöityjä hyviä käytäntöjä, joilla pyritään parantamaan liikennealan organisaatioiden kyberturvallisuutta. Siinä esitetään erityisesti hyviä käytäntöjä, joiden avulla voidaan tunnistaa liikennealan organisaatioihin kohdistuvia uusia kyberuhkia sekä suojautua niiltä, havaita niitä ja vastata niihin.

Euroopan komissio

# Liikenteen kyberturvallisuutta koskeva välineistö

## Liikennealan uhkaympäristö

Eri liikennemuotoihin kohdistuvat uudet kyberturvallisuusuhat


## Kyberturvallisuutta koskevan tietoisuuden profiilit

Liikennealan eri profiileille tarkoitetut vaihtoehtoiset polut kyberturvallisuuteen liittyvän tietoisuuden lisäämiseksi

Euroopan komissio

# Liikennealan uhkaympäristö

Kyberturvallisuuteen liittyvä uhkaympäristö on dynaaminen, ja se kehittyy jatkuvasti. On kuitenkin mahdollista tunnistaa kyberuhkia, joita kohdistuu kaikkien liikennemuotojen palveluihin ja järjestelmiin.

Euroopan komissio

## Uhkatoimijat

Henkilöt tai organisaatiot, jotka saattavat vaikuttaa liikennepalvelujen ja -järjestelmien turvallisuuteen

## Uudet kyberuhkat

Valitut kyberuhkat, jotka saattavat olla liikennepalvelujen ja -järjestelmien turvallisuuteen vaikuttavia uhkavektoreita

# Uhkatoimijat

Henkilöt tai organisaatiot voivat tahallisesti tai tahattomasti paljastaa ja hyödyntää haavoittuvuuksia, jotka voivat aiheuttaa häiriöitä ja vaikuttaa liikennepalveluihin sekä niiden turvallisuuteen, liiketoimintaan, talouteen ja maineeseen. Uhkatoimijoita ovat muun muassa valtion tukemat ryhmät, kyberrikolliset, kyberterroristit, haktivistit, hakkerit (myös script kiddies -hakkerit) sekä sisäpiiriläiset (myös etuoikeutetut sisäpiiriläiset).

Merkittävimpiä tarkoituksellisesti liikennealan organisaatioita kohtaan hyökkääviä toimijoita ovat **kyberrikolliset**, **sisäpiiriläiset**, **kansallisvaltiot** ja **valtion tukemat ryhmät**.
Viholliset, kuten **kyberrikolliset**, toteuttavat valtavia hyökkäyskampanjoita ja pyrkivät usein saamaan rahallista hyötyä.

**Sisäpiiriläiset** tuntevat niiden organisaatioiden erityispiirteet, joiden palveluksessa he työskentelevät, ja ovat usein hyvin tietoisia pienistä tietoturva-aukoista. Sisäpiirin uhkatoimijoita voivat olla tyytymättömät työntekijät, toimittajat ja yksittäiset toimeksisaajat.
Maailmanlaajuisten geopoliittisten jännitteiden voimistuessa **kansallisvaltiot** ja **valtion tukemat ryhmät** pyrkivät strategisiin pitkän aikavälin tavoitteisiin. Ne yrittävät usein piiloutua organisaatioiden järjestelmiin ja kerätä arkaluonteista tietoa. Kun valtion tukemat hyökkääjät ovat saaneet jalansijaa järjestelmissä, ne pyrkivät asemaan, josta ne pystyvät aiheuttamaan mahdollisimman suurta vahinkoa. Ne voivat esimerkiksi hyökätä organisaation järjestelmiin hyödyntämällä organisaatioiden verkkoyhteyksiä.

Muita uhkatoimijoita ovat **sisäpiiriläiset**, jotka voivat tahattomasti tai tahallisesti toteuttaa toimia, jotka johtavat kyberturvallisuustapahtumiin ja pahimmissa tapauksissa liikennepalvelujen turvallisuuteen ja turvaamiseen vaikuttaviin kyberturvallisuuden häiriöihin.

Euroopan komissio

# Uudet kyberuhkat

Liikenteeseen kohdistuu huomattava määrä kyberuhkia: **hajautettu palvelunesto**, **palvelunesto**, **tietovarkaus**, **haittaohjelmien** levittäminen, **verkkourkinta**, ohjelmistojen manipulointi, **luvaton käyttö**, tuhoisat hyökkäykset, turvallisuusalan toimijan päätöksentekoprosessin väärentäminen tai ohittaminen, henkilöllisyyden peittäminen, käyttöoikeuksien väärinkäyttö, **käyttäjien manipulointi**, turmeleminen, salakuuntelu, varojen väärinkäyttö ja laitteistojen manipulointi.
Julkisesti saatavilla olevia asiakirjoja koskevan kattavan kirjallisuustutkimuksen ja asiantuntijahaastattelujen perusteella merkittävimpiä liikennealaan vaikuttavia uusia kyberuhkia ovat haittaohjelmat, (hajautettu) palvelunesto, luvaton käyttö ja varkaus sekä ohjelmistojen manipulointi.

Euroopan komissio

## Uhka #1: haittaohjelmat

Haitalliset ohjelmistot, jotka voivat vaikuttaa henkilöihin tai organisaatioihin eri liikennemuodoissa

## Uhka #2: (hajautettu) palvelunesto

Kyberturvallisuushyökkäys, jolla estetään henkilöitä tai organisaatioita käyttämästä tiettyjä liikennepalveluja ja -resursseja

## Uhka #3: luvaton käyttö ja varkaus

Kriittisten resurssien luvaton käyttö, varastaminen ja hyödyntäminen


## Uhka #4: ohjelmistojen manipulointi

Kyberturvallisuushyökkäys, joka kohdistuu ohjelmistoihin ja jolla pyritään muokkaamaan ohjelmiston toimintaa ja toteuttamaan kohdistettuja hyökkäyksiä

# Uhka #1: haittaohjelmat

Haittaohjelmat ovat haitallisia ohjelmistoja, jotka voivat olla erityyppisiä ohjelmistosovelluksia, kuten viruksia, troijalaisia, matoja, kiristysohjelmia, kryptolouhijoita tai mitä tahansa ohjelmistoja, joilla voi olla haitallisia vaikutuksia organisaatioihin tai henkilöihin eri liikennemuodoissa.

Tietokoneita, palvelimia, asiakkaita, verkkoja tai kaikkia niitä tahallisesti vahingoittaviksi suunniteltujen haittaohjelmien leviämisen hillitseminen on yksi kyberturvallisuuden ensisijaisista tavoitteista kaikissa liikennemuodoissa. Tyypilliseen hyökkäysvektoriin liittyy työntekijöiden sähköpostien urkintaa. Muut hyökkäysvektorit voivat hyödyntää erilaisia ja pitkälle kehitettyjä strategioita, joilla tähdätään käyttäjien manipulointiin (esim. siihen, että käyttäjä kytkee USB-laitteen vapaaseen porttiin esimerkiksi matkapuhelimen lataamiseksi). Jos käyttäjä napsauttaa epäilyttävissä sähköpostiviesteissä olevia hyperlinkkejä tai avaa tiedostoliitteitä, hän voi tietämättään asentaa ohjelmistoja tai vaarantaa kuljetuspalvelut ja -resurssit tietoisesti.

Esimerkiksi kyberhyökkäys WannaCry-kiristysohjelmalla vaikutti yli 150 maahan, ja ohjelma saastutti yli 230 000 järjestelmää. Kyseessä oli kiristysohjelma, joka leviää yleensä haitallisia liitteitä tai hyperlinkkejä sisältävien urkintasähköpostiviestien välityksellä. Tämäntyyppisessä hyökkäyksessä käyttäjää pyritään vahingoittamistarkoituksessa manipuloimaan niin, että käyttäjä asentaa (tai aktivoi) erityisiä haittaohjelmia.

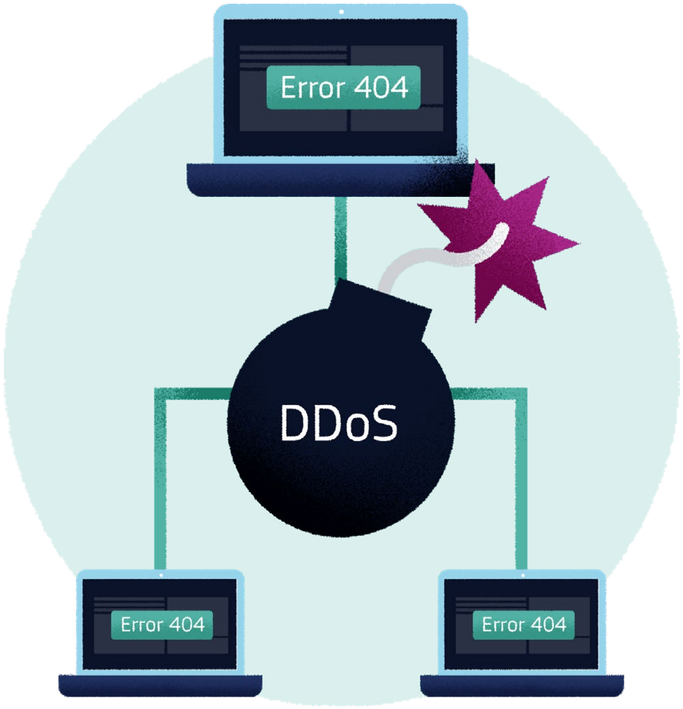
Euroopan komissio

# Uhka #2: (hajautettu) palvelunesto

Hajautettu palvelunesto (Distributed Denial of Service, DDoS) ja palvelunesto (Denial of Service, DoS) ovat hyökkäyksiä, jotka vaikuttavat tietojen, palvelujen, järjestelmien ja muiden resurssien saatavuuteen ja käytettävyyteen. Näiden hyökkäysten kesto voi vaihdella, ja ne voivat kohdistua useampaan kuin yhteen palveluun tai järjestelmään kerrallaan. DDoS-hyökkäyksissä hyödynnetään useita järjestelmiä (tai hyökkäyskanavia) kohteena olevien palvelujen tai järjestelmien ylikuormittamiseksi pyynnöillä. Onnistuneet hyökkäykset vaikuttavat palvelun ja järjestelmän valmiuksiin käsitellä odottamattomia pyyntömääriä. Tämä johtaa palvelujen ja resurssien käytön estymiseen.

On huomattava, että DDoS- ja DoS-hyökkäyksiin voidaan käyttää liikennealan organisaatioille kuuluvia palveluja ja järjestelmiä, jotta hyökkäykset voidaan kohdistaa tiettyihin käytössä oleviin järjestelmiin tai myös muihin organisaatioihin.

Hyökkäys voidaan kohdistaa esimerkiksi organisaation tietojärjestelmiin (kuten henkilökohtaisiin tietokoneisiin ja laitteisiin) pääsyn saamiseksi operatiivisiin teknologioihin, jotka voidaan yhdistää internetiin tai jotka voivat käyttää verkkoja operatiivisten tietojen siirtämiseksi. Eri järjestelmien ja verkkojen väliset yhteydet (kuten yritysverkot, operatiiviset teknologiat ja ylläpidon etäyhteydet) voivat olla haavoittuvuuksia, joita vastaan kriittisiin liikennepalveluihin ja -järjestelmiin kohdistuvia DDoS- tai DoS-hyökkäyksiä voidaan tehdä. Esimerkiksi DDoS- ja DoS-hyökkäyksissä voidaan hyödyntää yhteisiä verkko- ja viestintäprotokollia (esim. Web Services Dynamic Discovery eli WS-Discovery), joita esineiden internetin laitteet voivat käyttää kunkin solmun löytämiseen automaattisesti lähiverkoista. Jos esineiden internetin laitteissa on haavoittuvuuksia, hyökkääjät voivat hyödyntää niitä löytääkseen muita verkkoon liitettyjä laitteita ja tehdäkseen DDoS- tai DOS-hyökkäyksiä.



Euroopan komissio

# Uhka #3: luvaton käyttö ja varkaus

Uhkatoimijat saattavat pyrkiä saamaan luvattomasti loogisen tai fyysisen pääsyn verkkoon, järjestelmään, sovellukseen, tietoihin tai muuhun aineistoon toteuttaakseen haitallisia toimia, kuten varastaakseen arkaluontoisia tietoja tai resursseja (myös fyysisiä resursseja).
Luvattoman käytön ja varkauden uhka kohdistuu luottamuksellisiin ja omistusoikeuden alaisiin resursseihin (mukaan lukien henkilöllisyydet, etuoikeutettujen käyttäjätilien käyttöoikeudet, järjestelmät ja muuntyyppiset luottamukselliset ja omistusoikeuden alaiset tiedot). Näissä uhkissa voidaan hyödyntää järjestelmien haavoittuvuuksia sekä henkilöitä, jotka paljastavat tietämättään arkaluonteisia tietoja, kuten tunnuksia (esim. käyttäjätunnus tai salasana) tai henkilötietoja (esim. sähköposti tai henkilökohtainen tunnusluku).

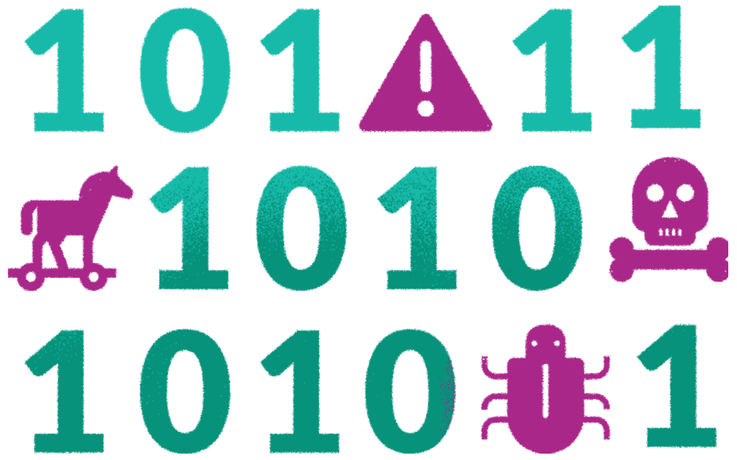
Luvattomassa käytössä identiteettivarkaus tarkoittaa henkilötietojen tai yksilöllisten tunnisteiden laitonta käyttöä henkilöiksi, palveluiksi tai järjestelmiksi tekeytymiseksi niin, että tavoitteena on saada käyttöön yksityisiä tai omistusoikeuden alaisia resursseja (esim. taloudellisia ja fyysisiä resursseja). Tällaiset kyberturvallisuusuhkat voivat kohdistua myös fyysisiin resursseihin kaikissa liikennemuodoissa.

Euroopan komissio

# Uhka #4: Ohjelmistojen manipulointi

Ohjelmistojen ja niihin liittyvien järjestelmien tai komponenttien virheellinen konfiguraatio ja niiden manipulointi voivat vaikuttaa suoraan liikennepalvelujen ja -järjestelmien turvallisuuteen.
Kyberturvallisuushyökkäyksissä, joihin liittyy ohjelmistojen manipulointia, muutetaan ohjelmistoasetuksia tai vaikutetaan tietojen eheyteen järjestelmien ja palvelujen toiminnan muuttamiseksi. Hyökkääjät voivat tarkoituksellisesti manipuloida ohjelmistoa (tai sen osaa) saadakseen arkaluonteisiin resursseihin liittyvää hyötyä (esim. luvattoman pääsyn hankkiminen, oikeutettujen henkilöiden tai järjestelmien pääsyn estäminen tarvittaviin resursseihin, arkaluonteisten tietojen kerääminen, toimintojen käyttäytymisen muuttaminen jne.).

Hyökkääjät voivat esimerkiksi kohdistaa hyökkäyksensä valmistajien viestintäkanaviin haitallisten ohjelmistopäivitysten lataamiseksi palveluihin ja järjestelmiin (mukaan lukien operatiivinen teknologia). Uhkatekijä käyttää vaarantuneita tunnuksia saadakseen pääsyn etäylläpidon suojattuun verkkorajapintaan ja asentaakseen manipuloituja ohjelmistoja ja tehdäkseen lisävahinkoa palveluihin ja järjestelmiin, joihin se on saanut pääsyn. Uhkatekijä asentaa manipuloituja ohjelmistoja, jotka aiheuttavat lisävahinkoa hyökkäyksen kohteena oleviin palveluihin ja järjestelmiin tai hyökkäävät muihin yhdistettyihin palveluihin tai järjestelmiin.



Euroopan komissio

# Kyberturvallisuutta koskevan tietoisuuden profiilit

Euroopan komissio

1

## Profiili I: kaikki liikennealan henkilöstö

Ensimmäinen polku on tarkoitettu kaikelle liikennealan organisaatioiden henkilöstölle operatiivisesta henkilöstöstä hallintohenkilöstöön. Tällä polulla annetaan ohjeita ymmärryksen ja tietoisuuden lisäämiseksi yleisimmistä kyberuhkista, joita liikennepalveluihin kohdistuu. Lisäksi siinä annetaan tietoa siitä, miten mahdollisia kyberuhkia voidaan käsitellä (niiden tunnistaminen, niistä raportointi ja niiden lieventäminen) kyberturvallisuutta koskevien käytäntöjen avulla. Tämä polku on yhteinen kaikille liikennemuodoille.

2

## Profiili II: liikenteen kyberturvallisuuden alan päätöksentekijät

Toinen polku on tarkoitettu henkilöstölle, joka vastaa liikennealan organisaatioiden turvallisuuteen tai kyberturvallisuuteen liittyvästä päätöksenteosta. Tällä polulla esitetään eri liikennemuotoihin räätälöityjä hyviä käytäntöjä. Siinä esitetään hyviä käytäntöjä, joiden avulla voidaan tunnistaa liikennealan organisaatioihin kohdistuvia uusia kyberuhkia sekä suojautua niiltä, havaita niitä ja vastata niihin.

Euroopan komissio

# Profiili I: kaikki liikennealan henkilöstö

Tämä osa on tarkoitettu kaikelle liikennealan organisaatioiden henkilöstölle operatiivisesta henkilöstöstä hallintohenkilöstöön. Siinä annetaan ohjeita ymmärryksen ja tietoisuuden lisäämiseksi yleisimmistä kyberuhkista, joita liikennepalveluihin kohdistuu. Lisäksi siinä annetaan tietoa siitä, miten mahdollisia kyberuhkia voidaan käsitellä (niiden tunnistaminen, niistä raportointi ja niiden lieventäminen) kyberturvallisuutta koskevien käytäntöjen avulla. Tässä osassa esitetään suositeltavia käytäntöjä ja hyödyllisiä vinkkejä, joista on hyötyä **kaikissa liikennemuodoissa**.

# Hyvät käytännöt haittaohjelmien torjumiseksi

Voit auttaa organisaatiosi suojaamisessa noudattamalla **haittaohjelmien tunnistamista ja niiden leviämisen ehkäisemistä** koskevia hyviä käytäntöjä, joita ovat muun muassa seuraavat:

- ***Noudata turvallisuuskäytäntöjä*** *eli esimerkiksi skannaa tallenteet ja tiedostot virusten varalta, vältä tietyntyyppisten tiedostojen (esim. .exe, .bat, .com jne.) avaamista ja lähettämistä, asenna vain hyväksyttyjä ohjelmistoja, varmista, että ohjelmistot (myös virustorjunta) ovat ajan tasalla ja toimivat asianmukaisesti ja noudata muita käytäntöjä.*

- ***Varmuuskopioi tietosi*** *säännöllisesti suojatulle (ja hyväksytylle) tallennusvälineelle tai tallennuspalveluun, jonka olisi tuettava salausmekanismeja, jotta voidaan suojata lepäävä data ja varmistaa, että se on käytettävissä tietojen palautusmenettelyjä varten.*

- *Suojaa kaikki järjestelmät, myös mobiililaitteet ja päätelaitteet, sopivilla* ***suojaustoimenpiteillä*** *(esim. salasanalla, salauksella jne.) ja muista lukita (fyysisesti ja digitaalisesti) turvallisesti kaikki järjestelmät, jos niitä ei valvota.*

- *Älä avaa liitteitä tai napsauta hyperlinkkejä, joita on odottamattomissa sähköpostiviesteissä ja epäilyttävissä verkkoselaimen ponnahdusikkunoissa, joissa on kummallinen teksti tai jotka ovat peräisin tuntemattomalta lähettäjältä tai internetsivulta.*

- *Älä liitä tietokoneeseesi* ***epäluotettavia tai tuntemattomia irrotettavia laitteita****, kuten USB-muistitikkuja, kovalevyjä ja muita tallennuslaitteita.*

- *Älä estä haittaohjelmien torjuntatoimia (esim. virustorjuntaohjelmistot, sisällönsuodatusohjelmistot, palomuurit jne.)*

- ***Päivitä asennetut ohjelmistot*** *säännöllisesti uusimpiin saatavilla oleviin versioihin (tietoturvavastaavat tai järjestelmänvalvojat voivat julkaista niihin säännöllisesti päivityksiä).*

- *Vältä etuoikeutettujen (esim. järjestelmänvalvojatason) tilien ja tunnusten käyttöä tavallisiin toimiin ja toimintoihin.*

- *Ilmoita tietoturvavastaavalle tai järjestelmänvalvojalle epäilyttävistä sähköpostiviesteistä tai järjestelmän odottamattomasta käytöksestä.*

- *Kiinnitä tietoturvallisuuteen huomiota osana päivittäisiä työrutiineja tietoturvallisuusuhkien tunnistamiseksi ja niihin reagoimiseksi sopivalla tavalla.*

Euroopan komissio

# Hyvät käytännöt (hajautetun) palveluneston torjumiseksi

Voit auttaa organisaatiosi suojaamisessa tunnistamalla **hajautettuun palvelunestoon (Distributed Denial of Service, DDoS)** ja **palvelunestoon (Denial of Service, DoS)** liittyvät hyökkäykset. Ota välittömästi yhteyttä turvallisuus- ja tietotekniikkatyöryhmään, jos havaitset seuraavia merkkejä mahdollisista käynnissä olevista DDoS- ja DoS-hyökkäyksistä käyttämiisi palveluihin tai järjestelmiin:

- *lisääntyneet pyynnöt, jotka kuluttavat verkkokapasiteettia (mikä näkyy hitaina palveluina ja vastauksina) ja näin ollen aiheuttavat ylikuormituksesta johtuvia palvelu- tai järjestelmähäiriöitä*
- *muistiresurssien kysynnän kasvu ilman selvää syytä*
- ***palveluiden ja järjestelmien odottamaton käyttäytyminen**, toistuvat kaatumiset ja oudot virheilmoitukset, jotka johtuvat laskentaresurssien tai verkkoyhteyksien ilkivaltaisesta käytöstä*
- ***laitteiden heikentynyt suorituskyky**, vähäisten tehtävien pitkä kesto ja havaittavat toiminnot (esim. kovaääninen tuuletin ja laitteiden hidas toiminta)*
- ***odottamattomat internetyhteydet tai yhteyksien menettäminen** palveluihin ja järjestelmiin*
- *operatiivisten laitteiden tai teknologioiden käytöksen hienoiset muutokset, jotka aiheuttavat fyysistä vahinkoa*
- *Pääsy etuoikeutettuihin tai hallinnollisiin tileihin estetään poikkeamiin reagointiin liittyvien menettelyjen estämiseksi.*

# Hyvät käytännöt luvattoman käytön ja varkauden torjumiseksi

Sellaisten hyökkäysten estämiseksi, joihin liittyy luvatonta käyttöä ja varkauksia, on noudatettava tiettyjä periaatteita, kuten ”*tiedonsaantitarve*” ja *”oletusarvoinen turvallisuus ja yksityisyys*”. Periaatteissa korostetaan, että arkaluonteisten ja luottamuksellisten resurssien (mukaan lukien henkilötiedot ja arkaluonteiset tiedot, kuljetusjärjestelmät jne.) olisi oltava ainoastaan sellaisten henkilöiden saatavilla, joilla on oikeus käyttää niitä tehtäviensä suorittamiseksi. Voit auttaa organisaatiosi suojaamisessa noudattamalla luvattoman käytön ja varkauksien tunnistamista ja ehkäisemistä koskevia hyviä käytäntöjä, joita ovat muun muassa seuraavat:

- *Noudata organisaation turvallisuuskäytäntöjä.*
- *Älä jaa tai julkaise verkossa tunnuksia tai henkilötietoja tai kuvia, jotka voivat sisältää tällaisia tietoja.*
- *Älä käytä tai välitä tunnuksia tai henkilötietoja (tai muita arkaluonteisia tietoja) epäluotettavissa ja turvattomissa verkoissa, laitteilla tai verkkopalveluissa (esim. verkkosivustot, jotka käyttävät turvattomia yhteyskäytäntöjä tai osoitteita (http://) turvallisten (https://) sijasta.*
- ***Älä koskaan paljasta kenellekään tunnuksiasi** (esim. sisäänkirjautumistunnus ja salasana) edes sähköpostitse tai puhelimitse.*
- *Suojaa näppäimistöllä kirjoitetut tai näytöllä näkyvät (myös mobiililaitteet) arkaluonteiset tiedot luvattomilta henkilöiltä, asenna näyttöösi tietoturvasuoja ja vältä työskentelyä julkisissa paikoissa yksityisenä pidettävällä laitteella. Älä jätä mitään laitetta lukitsematta ja valvomatta.*
- *Käytä organisaation turvallisuuskäytäntöjen mukaisia **monimutkaisia salasanoja** (esim. riittävän pitkä salasana, jossa on aakkosnumeerisia merkkejä ja erikoismerkkejä) luvattoman käytön estämiseksi.*
- ***Vaihda** liitettyjen järjestelmien ja laitteiden (esim. tulostimet, reitittimet, kamerat, älykäs lukitus jne.) **oletussalasanat**.*
- *Vältä samojen tunnusten (esim. sisäänkirjautumistunnus ja salasana) käyttöä useissa palveluissa ja järjestelmissä ja vältä samojen tunnusten käyttöä palveluissa ja järjestelmissä, jotka edellyttävät etuoikeutettuja käyttötilejä.*
- *Lähetä siirrettyjen suojattujen tiedostojen (esim. ZIP-tiedostot) salasanat ja avaimet vain kaistan ulkopuolisen kanavan kautta (esim. tekstiviesti GSM-järjestelmässä tai puhelu), ei koskaan sähköpostitse.*
- ***Aktivoi** mahdollisuuksien mukaan **kaksivaiheinen todennus** tai monivaiheinen todennus.*

# Hyvät käytännöt ohjelmistojen manipuloinnin torjumiseksi

Voit auttaa organisaatiosi suojaamisessa noudattamalla ohjelmistojen manipuloinnin tunnistamista ja ehkäisemistä koskevia hyviä käytäntöjä, joita ovat muun muassa seuraavat:

- *Älä asenna epäluotettavia ohjelmistoja järjestelmiin ja laitteisiin (mukaan lukien henkilökohtaiset tietokoneet, palvelimet, oheislaitteet, verkkolaitteet, älypuhelimet jne.).*
- *Asenna ohjelmistot ja päivitykset aina virallisista lähteistä ja verkkosivustoilta (esim. tuottajat, yritysten tietovarastot jne.).*
- *Älä lataa ohjelmistoja ja sovelluksia (tai mitään tiedostoja) laittomista lähteistä.*
- *Poista ohjelmistot, jotka ovat tarpeettomia tai joita et ole käyttänyt hiljattain, ja poista käytöstä tarpeettomat yhteydet (esim. verkkoprotokollat ja -palvelut), mukaan lukien yhteydet etäpalveluihin (esim. pilvitallennuspalvelut).*
- *Skannaa kaikki ohjelmistot ja tallennuslaitteet luotettavalla ja päivitetyllä virustorjuntaohjelmalla.*
- *Lataa turvalliset teollisuusohjelmistot (esim. päivitykset, korjaustiedostot, uudet tuotteet jne.) luotettavilta toimittajilta turvattuja asemia (”sandbox”) koskevan periaatteen mukaisesti.*
- *Päivitä kaikki asennetut ohjelmistot organisaation käytäntöjen mukaisesti.*

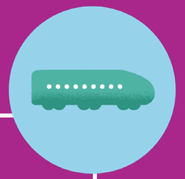
Euroopan komissio

# Profiili II: Liikenteen kyberturvallisuuden alan päätöksentekijät

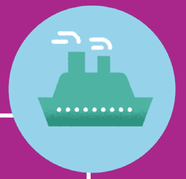
Tämä osa on tarkoitettu henkilöstölle, joka vastaa liikennealan organisaatioiden turvallisuuteen tai kyberturvallisuuteen liittyvästä päätöksenteosta. Tällä polulla korostetaan eri liikennemuotoihin räätälöityjä hyviä käytäntöjä. Siinä esitetään erityisesti hyviä käytäntöjä, joiden avulla voidaan tunnistaa uusia kyberuhkia sekä suojautua niiltä, havaita niitä ja vastata niihin.

Euroopan komissio

## Lentoliikenteeseen räätälöidyt kyberturvallisuutta koskevat hyvät käytännöt



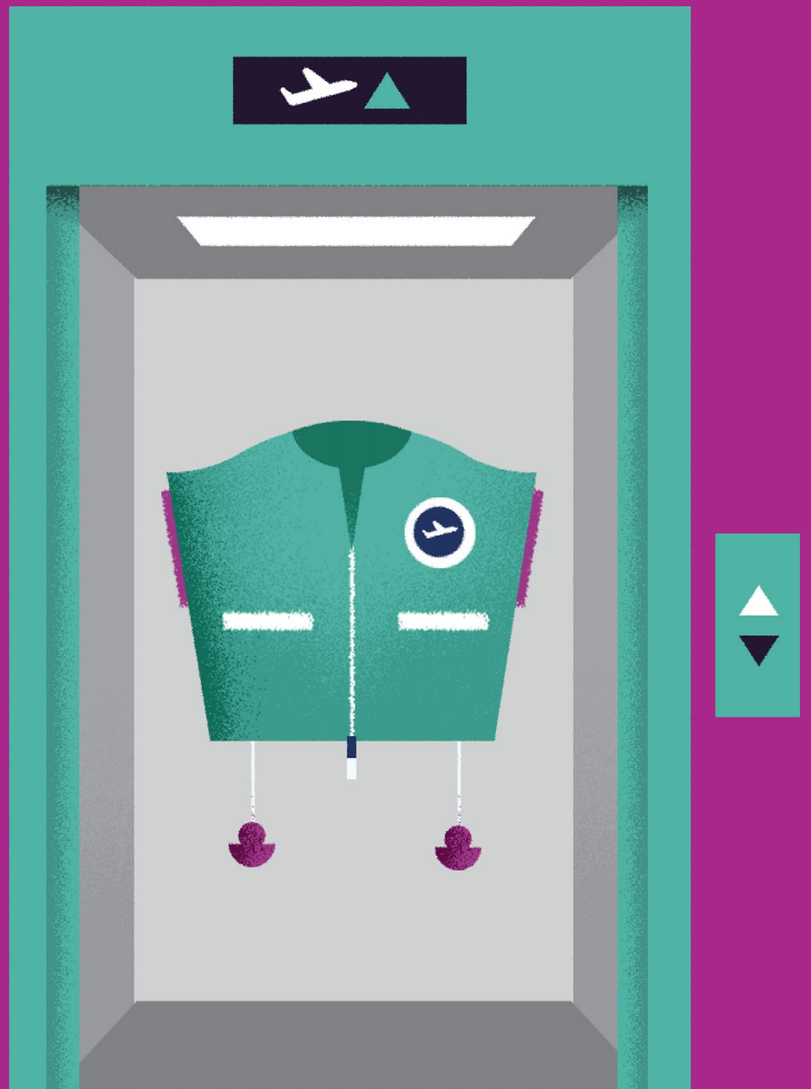
## Maaliikenteeseen räätälöidyt kyberturvallisuutta koskevat hyvät käytännöt



## Meriliikenteeseen räätälöidyt kyberturvallisuutta koskevat hyvät käytännöt

Euroopan komissio

# Lentoliikenteeseen räätälöidyt kyberturvallisuutta koskevat hyvät käytännöt ja turvallisuustoimenpiteet



# Hallinto

Ilmailualan organisaatioilla on oltava selkeä käsitys uusista uhkista, jotta voidaan määritellä johtamiskäytännöt ja -prosessit niiden toimintatapojen ohjaamiseksi. Tavoitteena on parantaa toiminnassa käytettävien palvelujen ja järjestelmien (myös tietotekniikka ja operatiivinen teknologia) kyberturvallisuutta.

Hyviä käytäntöjä kaikenkokoisille organisaatioille ovat muun muassa seuraavat:

- Varmistetaan, että ylin johto ilmoittaa kyberturvallisuuteen liittyvistä ongelmista johtajille ja johtokunnalle, jotka voivat tehdä tietoon perustuvia päätöksiä resurssien kohdentamisesta.

- Nimitetään kyberturvallisuudesta ja fyysisestä turvallisuudesta vastaava ylempi toimihenkilö, joka vastaa tietotekniikan ja operatiivisen teknologian turvallisuuden yleisestä hallinnoinnista mutta joka ei osallistu toimintaan eturistiriitojen välttämiseksi.

- Määritetään selkeästi kyberturvallisuuteen liittyvät tehtävät, vastuut, pätevyydet ja hyväksynnät ja tiedotetaan ja sovitaan niistä asiaankuuluvan henkilöstön, erityisesti tietotekniikan kriisiryhmien (Computer Emergency Response Team, CERT) jäsenten, kanssa.

- Taataan kyberturvallisuuden hallinta turvallisuuspalvelujen koko toimitusketjussa, mukaan lukien sekä fyysiset että digitaaliset rajapinnat, teknologian valmistajista ja asentajista turvallisuuspalvelujen tarjoajiin.

- Sovitaan kyberturvallisuusriskien hallintaan liittyvistä toimista ja valvonnasta, myös jaetusta vastuusta, ja varmistetaan, että nämä vastuut säilytetään turvallisuusratkaisujen ja -palvelujen koko elinkaaren ajan (esim. palvelusopimuksilla).

- Määritellään hallintomekanismit (esim. toimintapolitiikat), jotta voidaan noudattaa esimerkiksi seuraavista asiaa koskevista asetuksista ja direktiiveistä johtuvia velvoitteita: yhteisistä siviili-ilmailua koskevista säännöistä annettu asetus (EU) 2018/1139 ja ilmaliikenteen hallinta- ja lennonvarmistuspalvelujen sekä muiden ilmaliikenteen hallintaverkon toimintojen palveluntarjoajia koskevista yhteisistä vaatimuksista ja näiden palveluntarjoajien valvonnasta annettu komission täytäntöönpanoasetus (EU) 2017/373 sekä verkko- ja tietoturvadirektiivi (toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi annettu direktiivi (EU) 2016/1148).

**Esimerkkejä lentoliikenteen palveluista ja järjestelmistä:** Tietotekniikkaa on esimerkiksi sellainen tekniikka, jota on työntekijöiden (esim. henkilökohtaiset tietokoneet, matkapuhelimet, toimiston oheislaitteet jne.) sekä matkustajien (esim. julkiset langattomat reitittimet ja yhteydet) käytettävissä. Operatiiviseen teknologiaan kuuluvat esimerkiksi SCADA-järjestelmät (Supervisory Controls and Data Acquisition), lämmitys-, ilmanvaihto- ja ilmastointijärjestelmät, käsimatkatavaroiden turvatarkastuspisteet, matkatavaroiden käsittelyjärjestelmät, kulunvalvonta, seuranta, valvonta, hälytyskeskuspalvelut, turvatarkastusteknologia, lentokentän valaistuksenhallintajärjestelmät, tutkajärjestelmät ja anturit, maailmanlaajuiset paikannusjärjestelmät (GPS), ilmaliikenteen hallintajärjestelmät, viestintä-, suunnistus- ja valvontajärjestelmät, ilmailualan tietojärjestelmät, meteorologiset järjestelmät, turvallisuustoimien keskusjärjestelmät, lentoyhtiön lentokonejärjestelmät ynnä muut.

Euroopan komissio

# Kyberturvallisuusuhkien tunnistaminen

**Riskinhallinta:** Ilmailualan organisaatioiden on toteutettava asianmukaisia toimia keskeisiä toimintoja tukevien verkko- ja tietojärjestelmien kyberturvallisuusriskien tunnistamiseksi, arvioimiseksi ja ymmärtämiseksi.

Tämä edellyttää riskinhallinnan yleistä organisatorista lähestymistapaa, johon kuuluu seuraavat toimet:

- *Varmistetaan, että eri palvelujen tarjoamiseen käytettävistä eri laitteisto- ja ohjelmistojärjestelmistä on selkeä yleiskuva. Ilmailualalla tällaisia järjestelmiä ovat tietotekniikka ja operatiivinen teknologia.*

- *Toteutetaan **kyberturvallisuusriskien arviointeja**, joissa otetaan huomioon uudet uhkat, tunnetut haavoittuvuudet ja operatiiviset tiedot asiaankuuluvien järjestelmien osalta. Organisaatiot, kuten eurooppalainen ilmaliikenteen hallinnan tietotekniikan kriisiryhmä (European Air Traffic Management Computer Emergency Response Team, EATM-CERT) ja ilmailualan tiedonvaihto- ja analysointikeskus (Aviation Information Sharing and Analysis Centre, A-ISAC), voivat antaa tietoja lentoliikenteeseen kohdistuvista uhkista.*

- *Varmistetaan, että riskinarvioinneissa tarkastellaan myös henkilöstön päivittäiseen toimintaan liittyviä riskejä (esim. sosiaalisen median käyttö, henkilökohtaisten laitteiden käyttö, tietojen käsittely, tietojen jakaminen jne.).*

- *Tunnistetaan ja toteutetaan riskinhallintatoimenpiteitä ja -suunnitelmia kyberturvallisuusriskien lieventämiseksi.*

- *Toteutetaan kattava **tietoturvan hallintajärjestelmä** (Information Security Management System, ISMS) ja **tietosuojan hallintajärjestelmä** (Privacy Information Management System, PIMS), jotka ovat yhdenmukaisia muiden hallintajärjestelmien kanssa. Tällaisiin hallintajärjestelmiin (esim. ISMS ja PIMS) sisältyy turvallisuustarkastuksia (sekä tietoturvaan ja yksityisyyden suojaan liittyviä tarkastuksia) ilmailupalvelujen ja -järjestelmien (sekä niihin liittyvän datan) turvallisuuteen kohdistuvien uusien uhkien lieventämiseksi ja ehkäisemiseksi.*

- *Otetaan huomioon **mahdolliset omaisuuden hallinnointiin ja resurssien suunnitteluun** liittyvät rajoitteet (eli rajoitukset, jotka voivat vaikuttaa lentoliikenteen keskeisten toimintojen kriittisten järjestelmien toimittamiseen, ylläpitoon ja tukeen).*

**Esimerkkejä riskinhallintakehyksistä:** Erilaisista kehyksistä (esim. ISO/IEC 27000 -perheen standardit, Yhdysvaltain kansallisen standardi- ja teknologiainstituutin (National Institute of Standards and Technology, NIST) kyberturvallisuuskehys, MITRE ATT&CK -kehys, Saksan liittovaltion tietoturvaviraston (BSI) tietoturvamenettelyt (IT-Grundschutz) jne.) voidaan saada tietoa ja tukea lentoliikenteen räätälöityyn riskinhallintaan. Kansainväliset järjestöt, kuten Kansainvälinen ilmakuljetusliitto (IATA) ja Kansainvälinen siviili-ilmailujärjestö (ICAO), antavat ohjeita kyberturvallisuuden riskinarviointeja varten. Muun muassa Euroopan unionin kyberturvallisuusvirasto (ENISA), Euroopan unionin lentoturvallisuusvirasto (EASA), Euroopan lennonvarmistusjärjestö (EUROCONTROL) ja kansainvälinen lentoasemien järjestö (Airports Council International, ACI) korostavat hyviä käytäntöjä lentoasemien, ilmaliikenteen hallintapalvelujen tarjoajien ja muiden ilmailualan organisaatioiden turvaamiseksi. SESAR-yhteisyritys vastaa kaikkien ilmaliikenteen hallintaa sekä turvallisuusnäkökohtia koskevien EU:n tutkimus- ja kehitystoimien koordinoinnista ja keskittämisestä.

# Suojautuminen kyberturvallisuusuhkilta

Lentoliikenteen organisaatioiden olisi toteutettava riittävät ja oikeasuhteiset turvallisuustoimenpiteet verkkojensa ja tietojärjestelmiensä (myös tietotekniikka ja operatiivinen teknologia) suojaamiseksi kyberhyökkäyksiltä. Turvallisuustoimenpiteitä ovat muun muassa seuraavat:

- ***Turvallisuuskäytännöt ja -prosessit:*** *Määritellään ja toteutetaan asianmukaiset toimintaperiaatteet ja prosessit, joiden mukaan määritellään yleinen lähestymistapa ilmailun keskeisiä toimintoja tukevien järjestelmien ja tietojen turvaamista varten, sekä tiedotetaan niistä ja varmistetaan niiden toteutus. Tällaisten tietoturvakäytäntöjen (esim. salasana- ja tallennuskäytännöt) ja tietoturvamenettelyjen olisi katettava myös laitteisto- ja ohjelmistojärjestelmien (mukaan lukien tietotekniikka ja operatiivinen teknologia) korjaustiedostot ja haavoittuvuuksien hallinnan, häiriötilanteiden hallinnan sekä järjestelmän ja verkon suojauksen.*

- ***Identiteetin ja käyttöoikeuksien hallinta:*** *Lentoliikenteen keskeisiä toimintoja tukevien verkkojen ja tietojärjestelmien (mukaan lukien tietotekniikka ja operatiivinen teknologia) ymmärtäminen, dokumentointi ja hallinnointi. Käyttäjät (tai automaattiset toiminnot), jotka voivat käyttää tietoja tai järjestelmiä, on tarkistettu, todennettu ja hyväksytty asianmukaisesti. Tässä olisi otettava huomioon myös tavallisiin ja etuoikeutettuihin tileihin liittyvät erilaiset roolit ja vastuut.*

- ***Tietojen ja järjestelmän suojaus:*** *Tiedot (tallennetut ja sähköisesti välitetyt), kriittiset verkot ja tietojärjestelmät (mukaan lukien tietotekniikka ja operatiivinen teknologia) suojataan kyberhyökkäyksiltä. Riskilähtöisen lähestymistavan mukaan organisaatioiden olisi toteutettava turvallisuustoimenpiteitä, joilla rajoitetaan tehokkaasti hyökkääjien mahdollisuuksia vaarantaa tietoja, verkkoja ja järjestelmiä. Näihin turvatoimiin olisi kuuluttava myös salauksen ja suojattujen viestintäprotokollien käyttöönotto, jotta voidaan suojata lepääviä ja liikkuvia tietoja kyberturvallisuusuhkilta, jotka johtavat väliintulohyökkäyksiin. Lisäksi tällaiset toimenpiteet on tarpeen yhdistää fyysistä turvallisuutta koskeviin toimiin, jotta voidaan suojata pääsy järjestelmiin (esim. järjestelmät olisi sijoitettava suljettuihin tiloihin, joihin on rajoitettu pääsy).*

- ***Verkkojen ja järjestelmien häiriönsietokyky:*** *Verkkojen ja järjestelmien (mukaan lukien tietotekniikka ja operatiivinen teknologia) häiriönsietokyvyn kehittäminen suunnittelemalla ja toteuttamalla ne (ja niiden operatiiviset menettelyt) niin, että kyberhyökkäysten vaikutuksia voidaan torjua ja lieventää. Häiriönsietokykyä parantavia suunnittelu- ja toteutusratkaisuja ovat muun muassa seuraavat: virallisesti varmennetut kriittiset toiminnot, järjestelmien ja verkkojen redundanssi, verkkojen erottelu (erityisesti tietotekniikan ja operatiivisen teknologian erottelu), monitasoiset suojaustoimet ja monet muut toimet. On huomattava, että tietoturvan kannalta tietoturva-alueet, joilla verkkojen ja järjestelmien erottelu toteutetaan, voivat tarjota sopivia turvallisuusratkaisuja. Järjestelmien operatiiviset tarpeet (esim. ylläpito, tiedonsiirto jne.) saattavat kuitenkin edellyttää eri tietoturva-alueiden (esim. erilliset järjestelmät ja verkot) ohittamista tai liittämistä toisiinsa, kuten tietotekniikan ja operatiivisen teknologian yhdistämistä.*

# Kyberturvallisuusuhkien havaitseminen

Organisaatioiden olisi varmistettava, että turvallisuustoimenpiteet pysyvät tehokkaina, ja havaittava kaikki kyberturvallisuustapahtumat, jotka vaikuttavat tai voivat vaikuttaa turvatarkastuksiin sekä keskeisiin palveluihin ja järjestelmiin. Asiaankuuluvia turvallisuustoimenpiteitä kyberturvallisuusuhkien havaitsemiseksi ovat seuraavat:

- ***Turvallisuuden seuranta:*** *Seurataan lentoliikennepalvelujen keskeisiä toimintoja tukevien verkkojen ja tietojärjestelmien (mukaan lukien tietotekniikka ja operatiivinen teknologia) turvallisuustilannetta. Turvallisuuden seurannan tueksi huomioon otetaan muun muassa seuraavat tiedot:*

  - *tietoturvalokitiedot*
  - *virushavaintoja koskevat lokitiedot*
  - *tunkeutumishavaintoja koskevat lokitiedot*
  - *tunnistusta, todentamista ja valtuutusta koskevat lokitiedot*
  - *järjestelmiä ja palveluja koskevat lokitiedot*
  - *verkkoliikennettä koskevat lokitiedot*
  - *tietojen käsittelyä koskevat lokitiedot.*

- ***Tietoturvatapahtumien löytäminen:*** *Havaitaan haitalliset toimet (eli turvallisuustapahtumat), jotka vaikuttavat tai voivat vaikuttaa lentoliikennepalvelujen keskeisiä toimintoja tukevien verkkojen ja tietojärjestelmien (mukaan lukien tietotekniikka ja operatiivinen teknologia) turvallisuuteen.*

Nämä toimenpiteet voivat edellyttää erityisten teknologioiden (esim. turvallisuustietojen ja tietoturvatapahtumien hallinta, tunkeutumisenhavaitsemisjärjestelmä, tunkeutumisenestojärjestelmä jne.) käyttöönottoa ja turvallisuusoperaatiokeskuksen (Security Operations Centre, SOC) tai vastaavan keskuksen perustamista. Toisin sanoen on kehitettävä keinoja verkkohyökkäysten tunnistamiseksi, analysoimiseksi, niihin reagoimiseksi ja toipumiseksi paikallisella tasolla.

Kansalliset tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (Computer Security Incident Response Team, CSIRT), tietotekniikan kriisiryhmät (Computer Emergency Response Teams, CERT) (esim. EUROCONTROLin eurooppalainen ilmaliikenteen hallinnan tietotekniikan kriisiryhmä (EATM-CERT)), kaupallisten lentoyhtiöiden CERT-ryhmät ja ilmailualan tiedonvaihto- ja analysointikeskus (Aviation Information Sharing and Analysis Centre, A-ISAC) voivat tarjota kyberuhkatiedustelua turvallisuuden seurantaa ja turvallisuuspoikkeamien havaitsemista varten.

Euroopan komissio

# Reagoinnin ja elpymisen suunnittelu

Organisaatioiden olisi määriteltävä, toteutettava ja testattava tietoturvapoikkeamien hallintamenettelyt, joilla pyritään varmistamaan palvelujen ja järjestelmien toiminnan jatkuvuus kyberturvallisuuspoikkeamien sattuessa. Lieventävillä toimenpiteillä pyritään hillitsemään tai rajoittamaan kyberturvallisuuspoikkeamien vaikutusta.

Reagoinnin ja elpymisen suunnittelussa olisi otettava huomioon turvallisuustoimenpiteet, jotka lieventävät tiettyjen kyberturvallisuushyökkäysten vaikutuksia. Tällaisia toimenpiteitä ovat muun muassa seuraavat:

- *koordinointi ja yhteistyö kansallisten CSIRT-toimijoiden, (julkisten ja kaupallisten) CERT-ryhmien ja ISAC-keskusten kanssa kyberturvallisuuspoikkeamien aikana, poikkeamiin ja kriiseihin liittyvä koordinointi yleiseurooppalaisella tasolla*

- *tietojenvaihto muiden organisaatioiden kanssa, mukaan lukien ilmailupalvelujen toimitusketjuun kuuluvat palveluntarjoajat*

- *säännöllisten **kyberhyökkäysharjoitusten** järjestäminen (simuloitu koordinointiharjoitus ja tekninen harjoitus) turvallisuustoimenpiteiden ja -menettelyjen sekä organisaation häiriönsietokyvyn arvioimiseksi kyberturvallisuuspoikkeamien varalta*

- *pääsy arkistoihin tai varmuuskopioiden tallennuspaikkoihin, jos tietovarastojen eheys ja saatavuus ovat vaarantuneet*

- ***turvatoimia koskevat käsikirjat**, joissa esitetään yksityiskohtaiset menettelyt kyberturvallisuuspoikkeamien hallitsemiseksi ja palvelujen ja järjestelmien saattamiseksi takaisin normaaleihin toimintaolosuhteisiin*

- *verkkoliikenteen uudelleenohjaus rinnakkaisiin palveluihin palvelunestohyökkäysten aikana*

- *manuaaliset prosessit palvelujen ja järjestelmien käyttämiseksi heikentyneissä toimintatiloissa*

- *määritetään menettelyt tietoturvaloukkausten käsittelemiseksi, mukaan lukien menettelyt henkilötietoihin vaikuttavien tietoturvaloukkausten käsittelemiseksi yleisen tietosuoja-asetuksen ja muiden asiaankuuluvien alakohtaisten asetusten tai direktiivien mukaisesti*

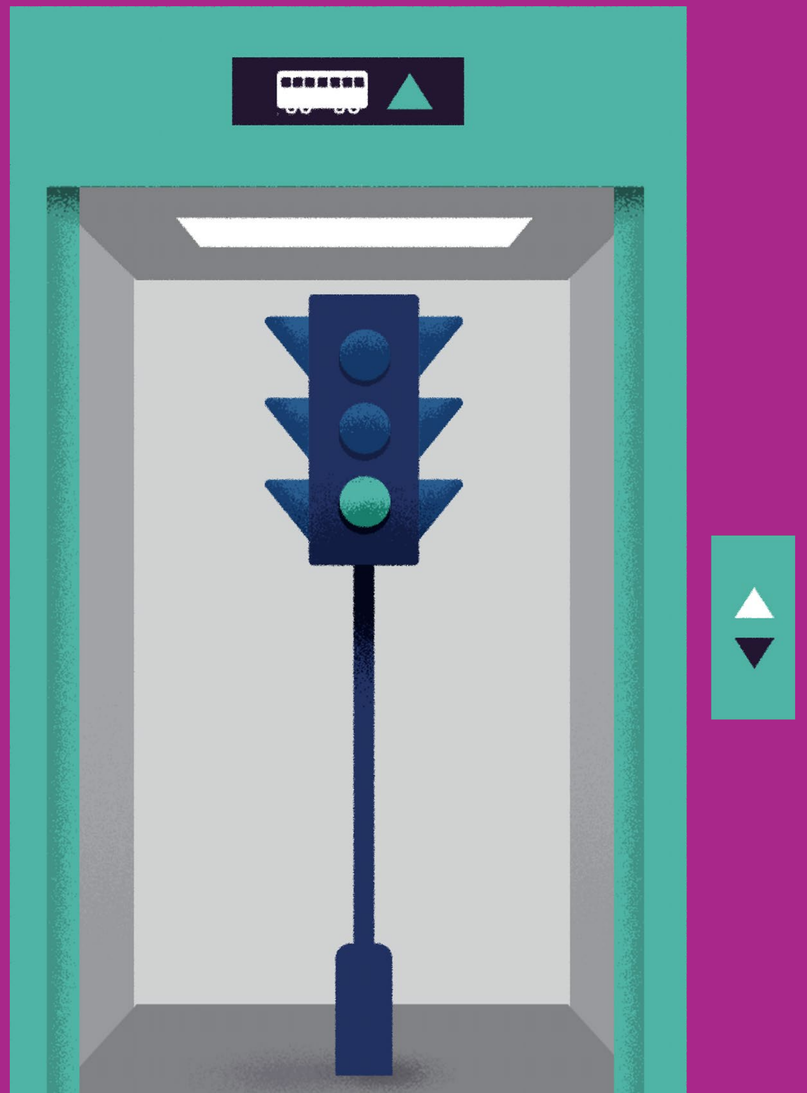
- ***kybervakuutuksen** hankkiminen, jotta voidaan kattaa osa vakaviin kyberturvallisuuspoikkeamiin liittyvästä riskistä*

- *tehdään poikkeamiin reagointiin liittyvä varaussopimus yhden tai useamman erikoistuneen yrityksen kanssa lisäkapasiteetin ja asiantuntemuksen hankkimiseksi*

- *määritetään menettelyt **kyberturvallisuuspoikkeamia koskevien tietojen jakamiseksi** asiaankuuluvien sidosryhmien kanssa, mukaan lukien menettelyt poikkeamien ilmoittamista varten verkko- ja tietoturvadirektiivin (toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annettu direktiivi (EU) 2016/1148) mukaisesti.*

Euroopan komissio

# Maaliikenteeseen räätälöidyt kyberturvallisuutta koskevat hyvät käytännöt ja turvallisuustoimenpiteet



Euroopan komissio

# Hallinto

Maaliikenteen (rautatie- ja maantieliikenne) organisaatioilla on oltava selkeä käsitys uusista uhkista, jotta voidaan määritellä johtamiskäytännöt ja -prosessit niiden toimintatapojen ohjaamiseksi. Tavoitteena on parantaa toiminnassa käytettävien palvelujen ja järjestelmien (myös tietotekniikka ja operatiivinen teknologia) kyberturvallisuutta.

Hyviä käytäntöjä kaikenkokoisille organisaatioille ovat muun muassa seuraavat:

- *Varmistetaan, että ylin johto ilmoittaa kyberturvallisuuteen liittyvistä ongelmista johtajille ja johtokunnalle, jotka voivat tehdä tietoon perustuvia päätöksiä resurssien kohdentamisesta.*

- *Nimitetään kyberturvallisuudesta ja fyysisestä turvallisuudesta vastaava ylempi toimihenkilö, joka vastaa tietotekniikan ja operatiivisen teknologian turvallisuuden yleisestä hallinnoinnista mutta joka ei osallistu toimintaan eturistiriitojen välttämiseksi.*

- *Määritellään selkeästi kyberturvallisuuteen liittyvät tehtävät, vastuualueet, toimivaltuudet ja hyväksynnät sekä viestitään ja sovitaan niistä asiaankuuluvan henkilöstön kanssa. Tämä on tarpeen erityisesti tietotekniikan kriisiryhmien (CERT) jäsenten osalta.*

- *Taataan kyberturvallisuuden hallinta turvallisuuspalvelujen koko toimitusketjussa, mukaan lukien sekä fyysiset että digitaaliset rajapinnat, teknologian valmistajista ja asentajista turvallisuuspalvelujen tarjoajiin.*

- *Sovitaan kyberturvallisuusriskien hallintaan liittyvistä toimista ja valvonnasta, myös jaetusta vastuusta, ja varmistetaan, että nämä vastuut säilytetään turvallisuusratkaisujen ja -palvelujen koko elinkaaren ajan (esim. palvelusopimuksilla).*

- *Määritetään hallintomekanismit (esim. käytännöt), jotta voidaan noudattaa asiaa koskevista asetuksista ja direktiiveistä johtuvia velvoitteita. Tähän sisältyy laaja joukko käytäntöjä, jotka koskevat tiettyjä liikennemuotoja sekä erityyppisiä sidosryhmiä (esim. ajoneuvojen ja rautatiejärjestelmien valmistajat) sekä verkko- ja tietoturvadirektiivi (toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annettu direktiivi (EU) 2016/1148).*

**Esimerkkejä maaliikenteen palveluista ja järjestelmistä:** Tietotekniikkaa on esimerkiksi sellainen tekniikka, jota on työntekijöiden (esim. henkilökohtaiset tietokoneet, matkapuhelimet, toimiston oheislaitteet jne.) sekä matkustajien (esim. julkiset langattomat reitittimet ja yhteydet) käytettävissä. Operatiiviseen teknologiaan kuuluvat esimerkiksi SCADA-järjestelmät (Supervisory Controls and Data Acquisition), lämmitys-, ilmanvaihto- ja ilmastointijärjestelmät, maailmanlaajuiset paikannusjärjestelmät (GPS), kulunvalvonta, seuranta, valvonta, hälytyskeskuspalvelut ja turvatarkastusteknologia. Erityisesti rautatieliikenteeseen liittyviä järjestelmiä ovat esimerkiksi operatiiviset järjestelmät (ohjaus- ja hallintajärjestelmät), mukaan lukien merkinantojärjestelmät, Euroopan rautatieliikenteen hallintajärjestelmä (ERTMS), junajärjestelmät, kunnossapitojärjestelmät ynnä muut järjestelmät.

Euroopan komissio

# Kyberturvallisuusuhkien tunnistaminen

**Riskinhallinta:** Maaliikenteen alan organisaatioiden on toteutettava asianmukaisia toimia keskeisiä toimintoja tukevien verkko- ja tietojärjestelmien kyberturvallisuusriskien tunnistamiseksi, arvioimiseksi ja ymmärtämiseksi. Tämä edellyttää riskinhallinnan yleistä organisatorista lähestymistapaa, johon kuuluu seuraavat toimet:

- *Varmistetaan, että eri palvelujen tarjoamiseen käytettävistä eri laitteisto- ja ohjelmistojärjestelmistä on selkeä yleiskuva. Maaliikenteen alalla tällaisiin järjestelmiin liittyy tietotekniikkaa ja operatiivista teknologiaa.*

- *Toteutetaan **kyberturvallisuusriskien arviointeja**, joissa olisi otettava huomioon uudet uhkat, tunnetut haavoittuvuudet ja operatiiviset tiedot asiaankuuluvien järjestelmien osalta. Maaliikennemuotojen järjestelmiä ovat esimerkiksi maksujärjestelmät, verkko- ja viestintäjärjestelmät (esim. internet, radioviestintä, WiFi), ajoneuvolaitteet, operatiiviset ohjauskeskukset, identiteetinhallintajärjestelmät, turvajärjestelmät ynnä muut. Rautatieinfrastruktuurien järjestelmiä ovat esimerkiksi liikkuvan kaluston, toiminnan ja liikenteen hallinnan osajärjestelmät sekä junien ja junaratojen ohjauksen, hallinnan ja merkinannon osajärjestelmät ynnä muut.*

- *Varmistetaan, että riskinarvioinneissa tarkastellaan myös henkilöstön päivittäiseen toimintaan liittyviä riskejä (esim. sosiaalisen median käyttö, henkilökohtaisten laitteiden käyttö, tietojen käsittely, tietojen jakaminen jne.).*

- *Tunnistetaan ja toteutetaan riskinhallintatoimenpiteitä ja -suunnitelmia kyberturvallisuusriskien lieventämiseksi. Toteutetaan kattava **tietoturvan hallintajärjestelmä** (Information Security Management System, ISMS) ja **tietosuojan hallintajärjestelmä** (Privacy Information Management System, PIMS), jotka ovat yhdenmukaisia muiden hallintajärjestelmien kanssa. Tällaisiin hallintajärjestelmiin (esim. ISMS ja PIMS) sisältyy turvallisuustarkastuksia (sekä tietoturvaan ja yksityisyyden suojaan liittyviä tarkastuksia) maaliikennepalvelujen ja -järjestelmien (sekä niihin liittyvän datan) turvallisuuteen kohdistuvien uusien uhkien lieventämiseksi ja ehkäisemiseksi.*

- *Otetaan huomioon mahdolliset **omaisuuden hallinnointiin ja resurssien suunnitteluun** liittyvät rajoitteet (eli rajoitukset, jotka voivat vaikuttaa maaliikenteen keskeisten toimintojen kriittisten järjestelmien toimittamiseen, ylläpitoon ja tukeen).*

**Esimerkkejä riskinhallintakehyksistä:** Erilaisista kehyksistä (esim. ISO/IEC 27000 -perheen standardit, Yhdysvaltain kansallisen standardi- ja teknologiainstituutin (National Institute of Standards and Technology, NIST) kyberturvallisuuskehys, MITRE ATT&CK -kehys, Saksan liittovaltion tietoturvaviraston (BSI) tietoturvamenettelyt (IT-Grundschutz) jne.) voidaan saada tietoa ja tukea maantie- ja rautatieliikenteen räätälöityyn riskinhallintaan. ENISAn kaltaiset organisaatiot määrittelevät älykkäiden autojen ja älykkään julkisen liikenteen kyberturvallisuuteen liittyviä hyviä käytäntöjä, joilla annetaan tietoa alan valmistajille ja yhdistyksille (esim. Euroopan autonvalmistajien yhdistys ACEA). Rautatieliikenteen alalla Euroopan unionin rautatievirasto (ERA) määrittelee yhteentoimivuuden tekniset eritelmät (YTE), jotka kunkin osajärjestelmän tai osajärjestelmän osan on täytettävä olennaisten vaatimusten täyttämiseksi ja Euroopan unionin rautatiejärjestelmän yhteentoimivuuden varmistamiseksi. Myös Shift2Rail-yhteisyritys edistää innovointia (myös kyberturvallisuutta) koskevia aloitteita ja hankkeita rautatieliikenteen alalla.

Euroopan komissio

# Suojautuminen kyberturvallisuusuhkilta

Maaliikenteen organisaatioiden olisi toteutettava riittävät ja oikeasuhteiset turvallisuustoimenpiteet verkkojensa ja tietojärjestelmiensä (myös tietotekniikka ja operatiivinen teknologia) suojaamiseksi kyberhyökkäyksiltä. Turvallisuustoimenpiteitä ovat muun muassa seuraavat:

- ***Turvallisuuskäytännöt ja -prosessit:*** *Määritellään ja toteutetaan asianmukaiset toimintaperiaatteet ja prosessit, joiden mukaan määritellään yleinen lähestymistapa maaliikennemuotojen keskeisiä toimintoja tukevien järjestelmien ja tietojen turvaamista varten, sekä tiedotetaan niistä ja varmistetaan niiden toteutus. Tällaisten tietoturvakäytäntöjen (esim. salasana- ja tallennuskäytännöt) ja tietoturvamenettelyjen olisi katettava myös laitteisto- ja ohjelmistojärjestelmien (mukaan lukien tietotekniikka ja operatiivinen teknologia) korjaustiedostot ja haavoittuvuuksien hallinnan, häiriötilanteiden hallinnan sekä järjestelmän ja verkon suojauksen.*

- ***Identiteetin ja käyttöoikeuksien hallinta:*** *Maaliikennemuotojen keskeisiä toimintoja tukevien verkkojen ja tietojärjestelmien (mukaan lukien tietotekniikka ja operatiivinen teknologia) ymmärtäminen, dokumentointi ja hallinnointi. Käyttäjät (tai automaattiset toiminnot), jotka voivat käyttää tietoja tai järjestelmiä, on tarkistettu, todennettu ja hyväksytty asianmukaisesti. Tässä olisi otettava huomioon myös tavallisiin ja etuoikeutettuihin tileihin liittyvät erilaiset roolit ja vastuut.*

- ***Tietojen ja järjestelmän suojaus:*** *Tiedot (tallennetut ja sähköisesti välitetyt), kriittiset verkot ja tietojärjestelmät (mukaan lukien tietotekniikka ja operatiivinen teknologia) suojataan kyberhyökkäyksiltä. Riskilähtöisen lähestymistavan mukaan organisaatioiden olisi toteutettava turvallisuustoimenpiteitä, joilla rajoitetaan tehokkaasti hyökkääjien mahdollisuuksia vaarantaa tietoja, verkkoja ja järjestelmiä. Näihin turvatoimiin olisi kuuluttava myös salauksen ja suojattujen viestintäprotokollien käyttöönotto, jotta voidaan suojata lepääviä ja liikkuvia tietoja kyberturvallisuusuhkilta, jotka johtavat väliintulohyökkäyksiin. Lisäksi tällaiset toimenpiteet on tarpeen yhdistää fyysistä turvallisuutta koskeviin toimiin, jotta voidaan suojata pääsy järjestelmiin (esim. järjestelmät olisi sijoitettava suljettuihin tiloihin, joihin on rajoitettu pääsy). Tämä on erittäin tärkeää niiden järjestelmien kannalta, joilla voi olla vaikutusta ihmishengen turvallisuuteen.*

- ***Verkkojen ja järjestelmien häiriönsietokyky:*** *Verkkojen ja järjestelmien (mukaan lukien tietotekniikka ja operatiivinen teknologia) häiriönsietokyvyn kehittäminen suunnittelemalla ja toteuttamalla ne (ja niiden operatiiviset menettelyt) niin, että kyberhyökkäysten vaikutuksia voidaan torjua ja lieventää. Häiriönsietokykyä parantavia suunnittelu- ja toteutusratkaisuja ovat muun muassa seuraavat: virallisesti varmennetut kriittiset toiminnot, järjestelmien ja verkkojen redundanssi, verkkojen erottelu (erityisesti tietotekniikan ja operatiivisen teknologian erottelu), monitasoiset suojaustoimet ja monet muut toimet. On huomattava, että tietoturvan kannalta tietoturva-alueet, joilla verkkojen ja järjestelmien erottelu toteutetaan, voivat tarjota sopivia turvallisuusratkaisuja. Järjestelmien operatiiviset tarpeet (esim. ylläpito, tiedonsiirto jne.) saattavat kuitenkin edellyttää eri tietoturva-alueiden (esim. erilliset järjestelmät ja verkot) ohittamista tai liittämistä toisiinsa, kuten tietotekniikan ja operatiivisen teknologian yhdistämistä.*

Euroopan komissio

# Kyberturvallisuusuhkien havaitseminen

Organisaatioiden olisi varmistettava, että turvallisuustoimenpiteet pysyvät tehokkaina, ja havaittava kaikki kyberturvallisuustapahtumat, jotka vaikuttavat tai voivat vaikuttaa turvatarkastuksiin sekä keskeisiin palveluihin ja järjestelmiin. Asiaankuuluvia turvallisuustoimenpiteitä kyberturvallisuusuhkien havaitsemiseksi ovat seuraavat:

- ***Turvallisuuden seuranta:*** *Seurataan maaliikennemuotojen toimintoja tukevien verkkojen ja tietojärjestelmien (mukaan lukien tietotekniikka ja operatiivinen teknologia) turvallisuustilannetta. Tämä on tarpeen, jotta voidaan havaita mahdolliset turvallisuusuhkat ja varmistaa seurannalla turvatoimien säilyminen tehokkaina. Turvallisuuden seurannan tueksi huomioon otetaan muun muassa seuraavat tiedot:*

  - *tietoturvalokitiedot*
  - *virushavaintoja koskevat lokitiedot*
  - *tunkeutumishavaintoja koskevat lokitiedot*
  - *tunnistusta, todentamista ja valtuutusta koskevat lokitiedot*
  - *järjestelmiä ja palveluja koskevat lokitiedot*
  - *verkkoliikennettä koskevat lokitiedot*
  - *tietojen käsittelyä koskevat lokitiedot.*

- ***Tietoturvatapahtumien löytäminen:*** *Havaitaan haitalliset toimet (eli turvallisuustapahtumat), jotka vaikuttavat tai voivat vaikuttaa keskeisiä toimintoja tukevien verkkojen ja tietojärjestelmien (mukaan lukien tietotekniikka ja operatiivinen teknologia) turvallisuuteen.*

*Nämä toimenpiteet voivat edellyttää erityisten teknologioiden (esim. turvallisuustietojen ja tietoturvatapahtumien hallinta, tunkeutumisenhavaitsemisjärjestelmä, tunkeutumisenestojärjestelmä jne.) käyttöönottoa ja turvallisuusoperaatiokeskuksen (Security Operations Centre, SOC) tai vastaavan keskuksen perustamista. Toisin sanoen on kehitettävä keinoja verkkohyökkäysten tunnistamiseksi, analysoimiseksi, niihin reagoimiseksi ja toipumiseksi paikallisella tasolla.*
*Kansalliset tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (Computer Security Incident Response Team, CSIRT), alakohtaiset ja kaupalliset CERT-ryhmät tai maantie- ja rautatieliikenteen toimijat sekä Euroopan rautatiealan tiedonvaihto- ja analysointikeskus (ER-ISAC) voivat tarjota kyberuhkatiedustelua turvallisuuden seurantaa ja turvallisuuspoikkeamien havaitsemista varten.*

Euroopan komissio

# Reagoinnin ja elpymisen suunnittelu

Organisaatioiden olisi määriteltävä, toteutettava ja testattava tietoturvapoikkeamien hallintamenettelyt, joilla pyritään varmistamaan palvelujen ja järjestelmien toiminnan jatkuvuus kyberturvallisuuspoikkeamien sattuessa.

Reagoinnin ja elpymisen suunnittelussa olisi otettava huomioon turvallisuustoimenpiteet, jotka lieventävät tiettyjen kyberturvallisuushyökkäysten vaikutuksia. Tällaisia toimenpiteitä ovat muun muassa seuraavat:

- *koordinointi ja yhteistyö kansallisten CSIRT-toimijoiden, (julkisten ja kaupallisten) CERT-ryhmien ja ISAC-keskusten kanssa kyberturvallisuuspoikkeamien aikana, poikkeamiin ja kriiseihin liittyvä koordinointi yleiseurooppalaisella tasolla*

- *tietojenvaihto muiden organisaatioiden kanssa, mukaan lukien maaliikennepalvelujen toimitusketjuun kuuluvat palveluntarjoajat*

- *säännöllisten **kyberhyökkäysharjoitusten** järjestäminen (simuloitu koordinointiharjoitus ja tekninen harjoitus) turvallisuustoimenpiteiden ja -menettelyjen sekä organisaation häiriönsietokyvyn arvioimiseksi kyberturvallisuuspoikkeamien varalta*

- *pääsy arkistoihin tai varmuuskopioiden tallennuspaikkoihin, jos tietovarastojen eheys ja saatavuus ovat vaarantuneet*

- ***turvatoimia koskevat käsikirjat**, joissa esitetään yksityiskohtaiset menettelyt kyberturvallisuuspoikkeamien hallitsemiseksi ja palvelujen ja järjestelmien saattamiseksi takaisin normaaleihin toimintaolosuhteisiin*

- *verkkoliikenteen uudelleenohjaus rinnakkaisiin palveluihin palvelunestohyökkäysten aikana*

- *manuaaliset prosessit palvelujen ja järjestelmien käyttämiseksi heikentyneissä toimintatiloissa*

- *määritetään menettelyt tietoturvaloukkausten käsittelemiseksi, mukaan lukien menettelyt henkilötietoihin vaikuttavien tietoturvaloukkausten käsittelemiseksi yleisen tietosuoja-asetuksen ja muiden asiaankuuluvien alakohtaisten asetusten tai direktiivien mukaisesti*

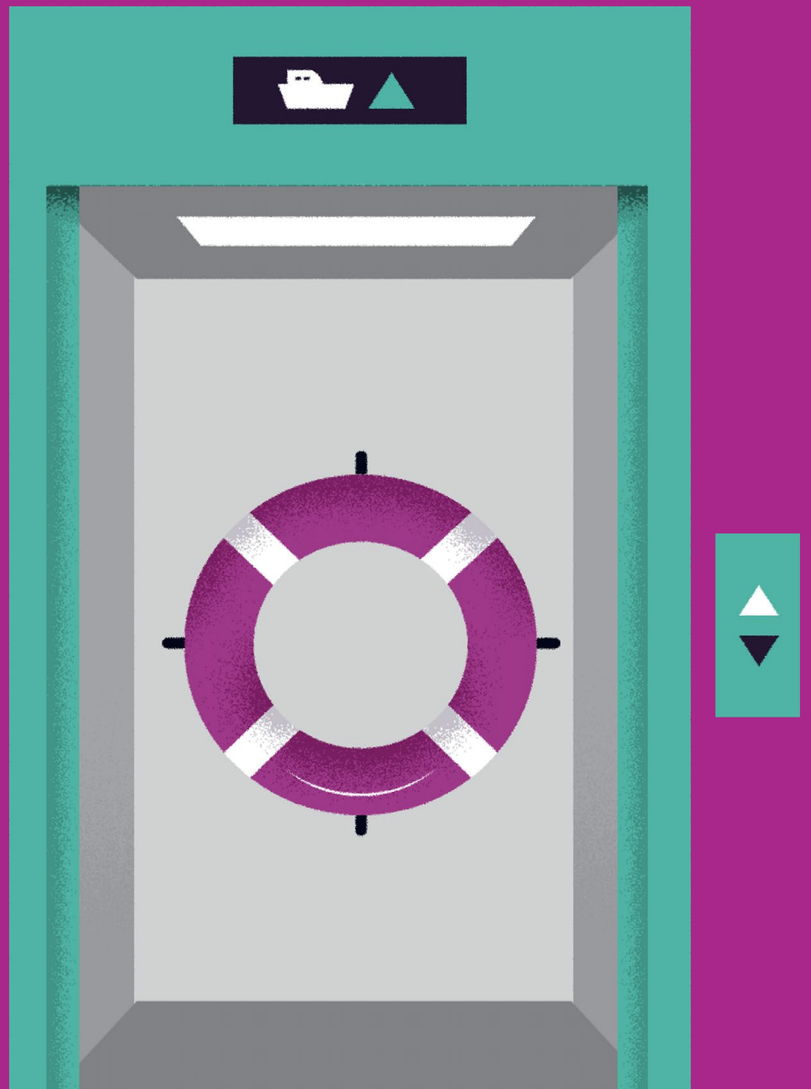
- ***kybervakuutuksen** hankkiminen, jotta voidaan kattaa osa vakaviin kyberturvallisuuspoikkeamiin liittyvästä riskistä*

- *tehdään poikkeamiin reagointiin liittyvä varaussopimus yhden tai useamman erikoistuneen yrityksen kanssa lisäkapasiteetin ja asiantuntemuksen hankkimiseksi*

- *määritetään menettelyt kyberturvallisuuspoikkeamia koskevien tietojen jakamiseksi asiaankuuluvien sidosryhmien kanssa, mukaan lukien menettelyt poikkeamien ilmoittamista varten verkko- ja tietoturvadirektiivin (toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annettu direktiivi (EU) 2016/1148) mukaisesti.*

Euroopan komissio

# Meriliikenteeseen räätälöidyt kyberturvallisuutta koskevat hyvät käytännöt ja turvallisuustoimenpiteet



Euroopan komissio

# Hallinto

Meriliikenteen organisaatioilla on oltava selkeä käsitys uusista uhkista, jotta voidaan määritellä johtamiskäytännöt ja -prosessit niiden toimintatapojen ohjaamiseksi. Tavoitteena on parantaa toiminnassa käytettävien palvelujen ja järjestelmien (myös tietotekniikka ja operatiivinen teknologia) kyberturvallisuutta.

Hyviä käytäntöjä kaikenkokoisille organisaatioille ovat muun muassa seuraavat:

- *Varmistetaan, että ylin johto ilmoittaa kyberturvallisuuteen liittyvistä ongelmista johtajille ja johtokunnalle, jotka voivat tehdä tietoon perustuvia päätöksiä resurssien kohdentamisesta.*

- *Nimitetään tietotekniikan ja operatiivisen teknologian turvallisuuden yleisestä hallinnoinnista vastaava ylempi toimihenkilö. Kyseisen toimihenkilön on vastattava kyberturvallisuudesta ja fyysisestä turvallisuudesta.*

- *Määritetään selkeästi kyberturvallisuuteen liittyvät tehtävät, vastuut, pätevyydet ja hyväksynnät, eri vastuutasot ja viestintälinjat aluksella ja maissa olevan henkilöstön kanssa ja henkilöstön keskuudessa, ja sovitaan niistä asiaankuuluvan henkilöstön kanssa. Tämä on tarpeen erityisesti tietotekniikan kriisiryhmien (CERT) jäsenten osalta. Henkilöstön, jolla on EU:n merenkulun turvallisuutta koskevaan lainsäädäntöön liittyviä tehtäviä, kuten satamarakenteiden turvapäälliköiden, satamien turvallisuuspäälliköiden tai yhtiöiden turvapäälliköiden tai maissa olevan nimetyn henkilön ja aluksen päällikön, olisi tunnettava vähintään organisaation toteuttamat kyberturvallisuustoimenpiteet.*

- *Taataan kyberturvallisuuden hallinta turvallisuuspalvelujen koko toimitusketjussa, mukaan lukien sekä fyysiset että digitaaliset rajapinnat, teknologian valmistajista ja asentajista turvallisuuspalvelujen tarjoajiin.*

- *Sovitaan kyberturvallisuusriskien hallintaan liittyvistä toimista ja valvonnasta, myös jaetusta vastuusta, ja varmistetaan, että nämä vastuut säilytetään turvallisuusratkaisujen ja -palvelujen koko elinkaaren ajan (esim. palvelusopimuksilla).*

- *Määritellään hallintomekanismit (esim. toimintapolitiikat), jotta voidaan noudattaa esimerkiksi seuraavista asiaa koskevista asetuksista ja direktiiveistä johtuvia velvoitteita: eurooppalaisen merenkulkualan yhdennetyn palveluympäristön perustamisesta annettu asetus (EU) 2019/1239, alusten ja satamarakenteiden turvallisuuden parantamisesta annettu asetus (EY) N:o 725/2004, satamien turvallisuuden parantamisesta annettu direktiivi 2005/65/EY ja kansainvälisen turvallisuusjohtamissäännöstön täytäntöönpanosta asetus (EY) N:o 336/2006 ja päätöslauselma A.741(18), jolla hyväksytään alusten turvallista toimintaa ja ympäristön pilaantumisen ehkäisemistä koskeva ISM-säännöstö. Tässä yhteydessä on myös tärkeää mainita yhteinen tietojenvaihtoympäristö (CISE) eli EU:n aloite, jonka tavoitteena on tehdä eurooppalaisista ja jäsenvaltioiden valvontajärjestelmistä yhteentoimivia, jotta kaikki asianomaiset viranomaiset saavat pääsyn turvaluokiteltuihin ja luokittelemattomiin tietoihin, joita ne tarvitsevat merioperaatioiden suorittamiseen.*

Euroopan komissio

**Esimerkkejä meriliikenteen palveluista ja järjestelmistä:** Tietotekniikkaa on esimerkiksi sellainen tekniikka, jota on työntekijöiden (esim. henkilökohtaiset tietokoneet, matkapuhelimet, toimiston oheislaitteet jne.) sekä matkustajien (esim. julkiset langattomat reitittimet ja yhteydet) käytettävissä. Operatiiviseen teknologiaan kuuluvat esimerkiksi SCADA-järjestelmät (Supervisory Controls and Data Acquisition), lämmitys-, ilmanvaihto- ja ilmastointijärjestelmät, maailmanlaajuiset paikannusjärjestelmät (GPS), kulunvalvonta, seuranta, valvonta, hälytyskeskuspalvelut, turvatarkastusteknologia, alusten navigointijärjestelmät, SafeSeaNet-järjestelmä, siltajärjestelmät, lastinkäsittely- ja hallintajärjestelmät, käyttövoimajärjestelmät ja koneiden hallintajärjestelmät sekä tehonsäätöjärjestelmät, kulunvalvontajärjestelmät, matkustajapalvelu- ja -hallintajärjestelmät, matkustajille tarkoitetut julkiset verkot, hallinnolliset järjestelmät ja miehistön hyvinvointijärjestelmät, viestintäjärjestelmät ynnä muut.

Euroopan komissio

# Kyberturvallisuusuhkien tunnistaminen

**Riskinhallinta:** Merenkulkualan organisaatioiden on toteutettava asianmukaiset toimet kyberturvallisuusriskien tunnistamiseksi, analysoimiseksi, arvioimiseksi ja niistä tiedottamiseksi sekä niiden hyväksymiseksi, välttämiseksi, siirtämiseksi tai lieventämiseksi hyväksyttävälle tasolle. Tämä edellyttää riskinhallinnan yleistä organisatorista lähestymistapaa, johon kuuluu seuraavat toimet:

- *Varmistetaan, että eri palvelujen tarjoamiseen käytettävistä eri laitteisto- ja ohjelmistojärjestelmistä on selkeä yleiskuva. Meriliikenteen alalla tällaisiin järjestelmiin kuuluu tietotekniikka ja operatiivinen teknologia sekä se, miten nämä järjestelmät on liitetty ja integroitu maan puolen rakenteisiin (mukaan lukien viranomaiset, meriterminaalit ja ahtaajat).*

- *Määritetään ja arvioidaan keskeisiä alusten toimintoja, jotka ovat alttiita kyberhyökkäyksille, ja tehdään kyberturvallisuutta koskevia riskinarviointeja (mukaan lukien mahdollisten operatiivisten vaikutusten ja esiintymistodennäköisyyden arviointi), joissa olisi otettava huomioon uudet uhkat, tunnetut haavoittuvuudet ja operatiiviset tiedot soveltamisalaan kuuluvista järjestelmistä. Tarvittaessa luodaan yhteys alusten, satamarakenteiden ja satamien turva-arviointeihin EU:n meriturvallisuuslainsäädännön mukaisesti. Turva-arvioinneissa tunnistetaan satamainfrastruktuuriin mahdollisesti kohdistuvat uhkat ja satamainfrastruktuurin turvallisuuteen liittyvät heikkoudet. Lisäksi merenkulkualan järjestöt, kuten Kansainvälinen merenkulkujärjestö (IMO) ja merenkulun ISAC-keskukset, voivat antaa tietoja meriliikenteeseen kohdistuvista uhkista.*

- *Varmistetaan, että riskinarvioinneissa tarkastellaan myös henkilöstön päivittäiseen toimintaan liittyviä riskejä (esim. sosiaalisen median käyttö, henkilökohtaisten laitteiden käyttö, tietojen käsittely, tietojen jakaminen jne.).*

- *Tunnistetaan ja toteutetaan riskinhallintatoimenpiteitä ja -suunnitelmia kyberturvallisuusriskien lieventämiseksi. Toteutetaan kattava tietoturvan hallintajärjestelmä (Information Security Management System, ISMS) ja tietosuojan hallintajärjestelmä (Privacy Information Management System, PIMS), jotka ovat yhdenmukaisia muiden hallintajärjestelmien kanssa (esim. turvallisuusjohtamisjärjestelmät), kansainvälisen turvallisuusjohtamissäännöstön (ISM-säännöstön) mukaisesti. Tällaisiin hallintajärjestelmiin (esim. ISMS ja PIMS) sisältyy turvallisuustarkastuksia (sekä tietoturvaan ja yksityisyyden suojaan liittyviä tarkastuksia) meriliikennepalvelujen ja -järjestelmien (sekä niihin liittyvän datan) turvallisuuteen kohdistuvien uusien uhkien lieventämiseksi ja ehkäisemiseksi.*

- *Otetaan huomioon **mahdolliset omaisuuden hallinnointiin ja resurssien suunnitteluun** liittyvät rajoitteet (eli rajoitukset, jotka voivat vaikuttaa meriliikenteen keskeisten toimintojen kriittisten järjestelmien toimittamiseen, ylläpitoon ja tukeen). Arvioinneissa viitataan tarvittaessa ISM-säännöstön, turvallisuusjohtamisjärjestelmien ja EU:n meriturvallisuuslainsäädännön mukaisesti laadittujen turvasuunnitelmien vaatimuksiin.*

**Esimerkkejä riskinhallintakehyksistä:** Erilaisista kehyksistä (esim. ISM-säännöstö tai ISO/IEC 27000 -perheen standardit, Yhdysvaltain kansallisen standardi- ja teknologiainstituutin (National Institute of Standards and Technology, NIST) kyberturvallisuuskehys, MITRE ATT&CK -kehys, Saksan liittovaltion tietoturvaviraston (BSI) tietoturvamenettelyt (IT-Grundschutz) jne.) voidaan saada tietoa ja tukea meriliikenteen räätälöityyn riskinhallintaan. Yhdysvaltain kansallisen standardi- ja teknologiainstituutin kyberturvallisuuskehys on myös räätälöity niin, että siinä käsitellään meriliikenteessä toteutettavan nesteiden säiliökuljetuksen (Maritime Bulk Liquids Transfer, MBLT), merellä toteutettavien toimien sekä matkustaja-alusten toiminnan kyberturvallisuutta. Samoin merenkulkujärjestö Baltic and International Maritime Council (BIMCO) on julkaissut alusten kyberturvallisuutta koskevat ohjeet *"The Guidelines on Cyber Security Onboard Ships"*, ja Kansainvälinen merenkulkujärjestö (IMO) on antanut erityiset merenkulun kyberriskien hallintaa koskevat ohjeet *"Guidelines on maritime cyber risk management"* (MSC-FAL.1/Circ.3). ENISA on tehnyt useita tutkimuksia, jotka koskevat merialan kyberturvallisuuteen ja erityisesti satamien kyberturvallisuuteen liittyviä hyviä käytäntöjä. EMSA tarjoaa merenkulkuyhteisölle palveluja, kuten koulutuksia kyberturvallisuutta koskevan tietoisuuden lisäämiseksi. Standardeissa (esim. navigointi- ja radioviestintälaitteiden ja -järjestelmien turvallisuutta koskeva IEC 61162-460:2018, aluksia ja meriteknologiaa koskeva ISO 16425:2013, teollisuuden automaatio- ja valvontajärjestelmien turvatoimia koskeva IEC 62443-4-1:2018) määritellään myös meriliikenteen järjestelmiä ja verkkoja koskevia erityisiä turvavaatimuksia.

# Suojautuminen kyberturvallisuusuhkilta

Meriliikenteen organisaatioiden olisi toteutettava riittävät ja oikeasuhteiset turvallisuustoimenpiteet verkkojensa ja tietojärjestelmiensä (myös tietotekniikka ja operatiivinen teknologia) suojaamiseksi. Turvallisuustoimenpiteitä ovat muun muassa seuraavat:

- ***Turvallisuuskäytännöt ja -prosessit:*** *Määritellään ja toteutetaan asianmukaiset toimintaperiaatteet ja prosessit, joiden mukaan määritellään yleinen lähestymistapa meriliikenteen keskeisiä toimintoja tukevien järjestelmien ja tietojen turvaamista varten, sekä tiedotetaan niistä ja varmistetaan niiden toteutus. Turvallisuustoimenpiteet (mukaan lukien kyberturvallisuustoimenpiteet ja fyysiset turvatoimet) olisi sisällytettävä asiaankuuluviin suunnitelmiin, kuten turvallisuusjohtamisjärjestelmään ja alusten turvasuunnitelmiin. Tällaisten tietoturvakäytäntöjen (esim. salasana- ja tallennuskäytännöt) ja tietoturvamenettelyjen olisi katettava myös laitteisto- ja ohjelmistojärjestelmien (mukaan lukien tietotekniikka ja operatiivinen teknologia) korjaustiedostot ja haavoittuvuuksien hallinnan, häiriötilanteiden hallinnan sekä järjestelmän ja verkon suojauksen.*

- ***Identiteetin ja käyttöoikeuksien hallinta:*** *Meriliikenteen keskeisiä toimintoja tukevien verkkojen ja tietojärjestelmien (mukaan lukien tietotekniikka ja operatiivinen teknologia) ymmärtäminen, dokumentointi ja hallinnointi. Käyttäjät (tai automaattiset toiminnot), jotka voivat käyttää tietoja tai järjestelmiä, on tarkistettu, todennettu ja hyväksytty asianmukaisesti. Tässä olisi otettava huomioon myös tavallisiin ja etuoikeutettuihin tileihin liittyvät erilaiset roolit ja vastuut.*

- ***Tietojen ja järjestelmän suojaus:*** *Tiedot (tallennetut ja sähköisesti välitetyt), kriittiset verkot ja tietojärjestelmät (mukaan lukien tietotekniikka ja operatiivinen teknologia) suojataan kyberhyökkäyksiltä. Riskilähtöisen lähestymistavan mukaan organisaatioiden olisi toteutettava turvallisuustoimenpiteitä, joilla rajoitetaan tehokkaasti hyökkääjien mahdollisuuksia vaarantaa tietoja, verkkoja ja järjestelmiä. Näihin turvatoimiin olisi kuuluttava myös salauksen ja suojattujen viestintäprotokollien käyttöönotto, jotta voidaan suojata lepääviä ja liikkuvia tietoja kyberturvallisuusuhkilta, jotka johtavat väliintulohyökkäyksiin. Lisäksi tällaiset toimenpiteet on tarpeen yhdistää fyysistä turvallisuutta koskeviin toimiin, jotta voidaan suojata pääsy järjestelmiin (esim. järjestelmät olisi sijoitettava suljettuihin tiloihin, joihin on rajoitettu pääsy). Tämä on erittäin tärkeää niiden järjestelmien kannalta, joilla voi olla vaikutusta ihmishengen turvallisuuteen (esim. luokan I ja II navigointi- ja radioviestintäjärjestelmät).*

- ***Verkkojen ja järjestelmien häiriönsietokyky:*** *Verkkojen ja järjestelmien (mukaan lukien tietotekniikka ja operatiivinen teknologia) häiriönsietokyvyn kehittäminen suunnittelemalla ja toteuttamalla ne (ja niiden operatiiviset menettelyt) niin, että kyberhyökkäysten vaikutuksia voidaan torjua ja lieventää. Häiriönsietokykyä parantavia suunnittelu- ja toteutusratkaisuja ovat muun muassa seuraavat: virallisesti varmennetut kriittiset toiminnot, järjestelmien ja verkkojen redundanssi, verkkojen erottelu (erityisesti tietotekniikan ja operatiivisen teknologian erottelu), monitasoiset suojaustoimet ja monet muut toimet. On huomattava, että tietoturvan kannalta tietoturva-alueet, joilla verkkojen ja järjestelmien erottelu toteutetaan, voivat tarjota sopivia turvallisuusratkaisuja. Järjestelmien (esim. merenkulun autonomiset pinta-alukset eli Maritime Autonomous Surface Ships, MASS) tarpeet (esim. ylläpito, tiedonsiirto jne.) saattavat kuitenkin edellyttää eri tietoturva-alueiden (esim. erilliset järjestelmät ja verkot) ohittamista tai liittämistä toisiinsa, kuten tietotekniikan ja operatiivisen teknologian yhdistämistä.*

Euroopan komissio

# Kyberturvallisuusuhkien havaitseminen

Organisaatioiden olisi varmistettava, että turvallisuustoimenpiteet pysyvät tehokkaina, ja havaittava kaikki kyberturvallisuustapahtumat, jotka vaikuttavat tai voivat vaikuttaa turvatarkastuksiin sekä keskeisiin palveluihin ja järjestelmiin. Asiaankuuluvia turvallisuustoimenpiteitä kyberturvallisuusuhkien havaitsemiseksi ovat seuraavat:

■ ***Turvallisuuden seuranta:*** *Seurataan meriliikennepalvelujen keskeisiä toimintoja tukevien verkkojen ja tietojärjestelmien (mukaan lukien tietotekniikka ja operatiivinen teknologia) turvallisuustilannetta. Tämä on tarpeen, jotta voidaan havaita mahdolliset turvallisuusuhkat ja varmistaa seurannalla turvatoimien säilyminen tehokkaina. Turvallisuuden seurannan tueksi huomioon otetaan muun muassa seuraavat tiedot:*

- *tietoturvalokitiedot*
- *virushavaintoja koskevat lokitiedot*
- *tunkeutumishavaintoja koskevat lokitiedot*
- *tunnistusta, todentamista ja valtuutusta koskevat lokitiedot*
- *järjestelmiä ja palveluja koskevat lokitiedot*
- *verkkoliikennettä koskevat lokitiedot*
- *tietojen käsittelyä koskevat lokitiedot.*

■ ***Tietoturvatapahtumien löytäminen:*** *Havaitaan haitalliset toimet (eli turvallisuustapahtumat), jotka vaikuttavat tai voivat vaikuttaa meriliikennepalvelujen keskeisiä toimintoja tukevien verkkojen ja tietojärjestelmien (mukaan lukien tietotekniikka ja operatiivinen teknologia) turvallisuuteen.*

Nämä toimenpiteet voivat edellyttää erityisten teknologioiden (esim. turvallisuustietojen ja tietoturvatapahtumien hallinta, tunkeutumisenhavaitsemisjärjestelmä, tunkeutumisenestojärjestelmä jne.) käyttöönottoa ja turvallisuusoperaatiokeskuksen (Security Operations Centre, SOC) tai vastaavan keskuksen perustamista. Toisin sanoen on kehitettävä keinoja verkkohyökkäysten tunnistamiseksi, analysoimiseksi, niihin reagoimiseksi ja toipumiseksi paikallisella tasolla.

Kansalliset tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (Computer Security Incident Response Team, CSIRT), alakohtaiset CERT-ryhmät ja meriliikenteen toimijoiden kaupalliset CERT-ryhmät voivat tarjota kyberuhkatiedustelua turvallisuuden seurantaa ja turvallisuuspoikkeamien havaitsemista varten.

Euroopan komissio

# Reagoinnin ja elpymisen suunnittelu

Organisaatioiden olisi määriteltävä, toteutettava ja testattava tietoturvapoikkeamien hallintamenettelyt, joilla pyritään varmistamaan palvelujen ja järjestelmien toiminnan jatkuvuus kyberturvallisuuspoikkeamien sattuessa. Reagoinnin ja elpymisen suunnittelussa olisi otettava huomioon turvallisuustoimenpiteet, jotka lieventävät tiettyjen kyberturvallisuushyökkäysten vaikutuksia. Tällaisia toimenpiteitä ovat muun muassa seuraavat:

- *verkkoliikenteen uudelleenohjaus rinnakkaisiin palveluihin palvelunestohyökkäysten aikana*
- *manuaaliset prosessit palvelujen ja järjestelmien käyttämiseksi heikentyneissä toimintatiloissa*
- *harjoituksia koskevien ohjelmien laatiminen (esim. simuloitu koordinointiharjoitukset, tekniset harjoitukset ja reagointiharjoitukset), jotta voidaan reagoida kyberhyökkäyksiin ja hätätilanteisiin sekä arvioida turvallisuustoimenpiteitä, menettelyjä ja organisatorista häiriönsietokykyä kyberturvallisuuspoikkeamien varalta*
- *pääsy arkistoihin tai varmuuskopioiden tallennuspaikkoihin, jos tietovarastojen eheys ja saatavuus ovat vaarantuneet*
- *koordinointi ja yhteistyö kansallisten CSIRT-toimijoiden, (julkisten ja kaupallisten) CERT-ryhmien ja ISAC-keskusten kanssa kyberturvallisuuspoikkeamien aikana, poikkeamiin ja kriiseihin liittyvä koordinointi yleiseurooppalaisella tasolla*
- *tietojenvaihto muiden organisaatioiden kanssa, mukaan lukien meriliikennepalvelujen toimitusketjuun kuuluvat palveluntarjoajat*
- *turvatoimia koskevat käsikirjat, joissa esitetään yksityiskohtaiset menettelyt kyberturvallisuuspoikkeamien hallitsemiseksi ja palvelujen ja järjestelmien saattamiseksi takaisin normaaleihin toimintaolosuhteisiin*
- *määritetään menettelyt tietoturvaloukkausten käsittelemiseksi, mukaan lukien menettelyt henkilötietoihin vaikuttavien tietoturvaloukkausten käsittelemiseksi yleisen tietosuoja-asetuksen ja muiden asiaankuuluvien alakohtaisten asetusten tai direktiivien mukaisesti*
- *kybervakuutuksen hankkiminen, jotta voidaan kattaa osa vakaviin kyberturvallisuuspoikkeamiin liittyvästä riskistä*
- *tehdään poikkeamiin reagointiin liittyvä varaussopimus yhden tai useamman erikoistuneen yrityksen kanssa lisäkapasiteetin ja asiantuntemuksen hankkimiseksi*
- *määritetään menettelyt kyberturvallisuuspoikkeamia (mukaan luettuina vaatimustenvastaisuudet, onnettomuudet ja vaaratilanteet) koskevien tietojen jakamiseksi asiaankuuluvien sidosryhmien kanssa, mukaan lukien menettelyt poikkeamien ilmoittamista varten verkko- ja tietoturvadirektiivin (toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annettu direktiivi (EU) 2016/1148) mukaisesti.*

Luxemburg: Euroopan unionin julkaisutoimisto, 2021



Print ISBN 978-92-76-40497-2 doi:10.2832/384199 MI-05-21-230-FI-C
PDF ISBN 978-92-76-40498-9 doi:10.2832/87574 MI-05-21-230-FI-N

Euroopan unionin julkaisutoimisto