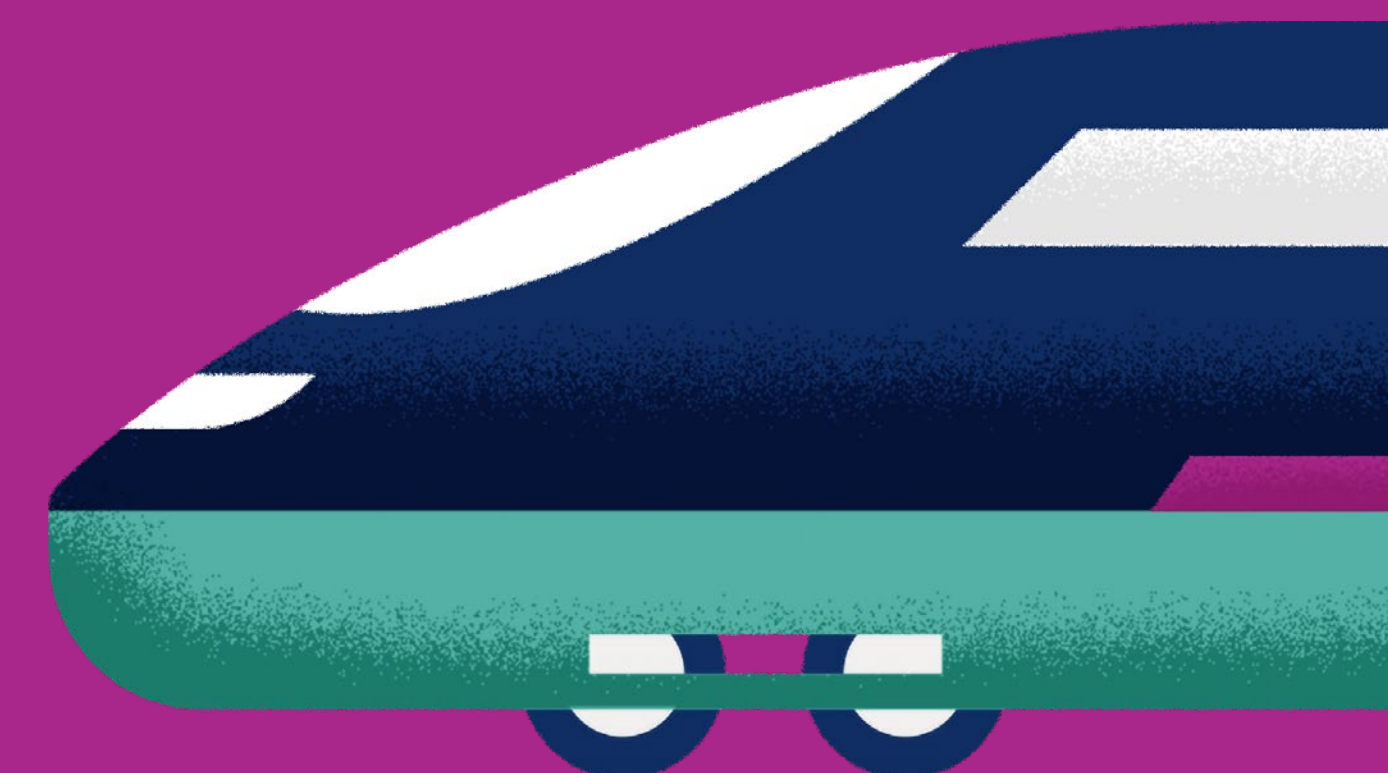
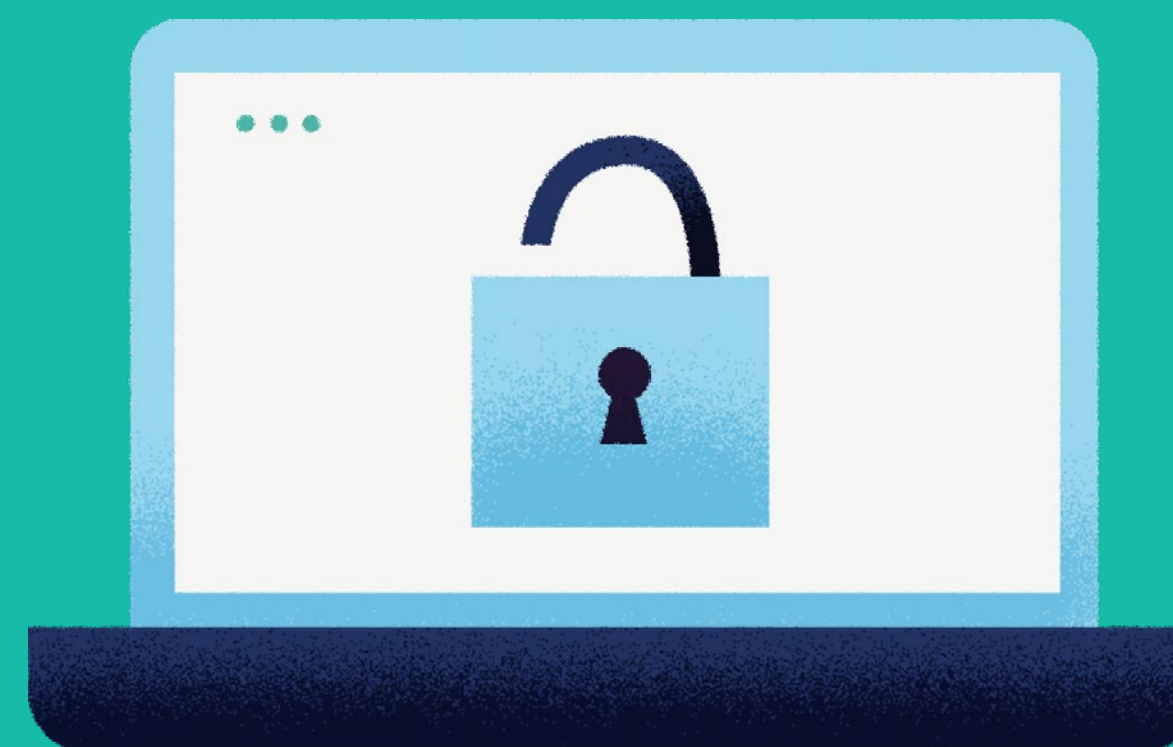
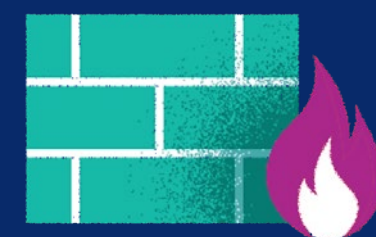
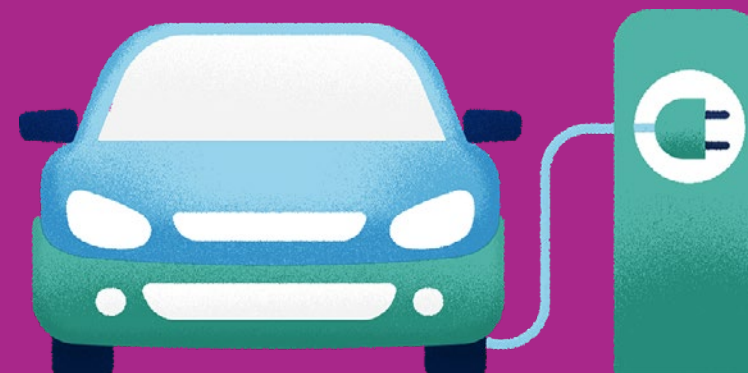
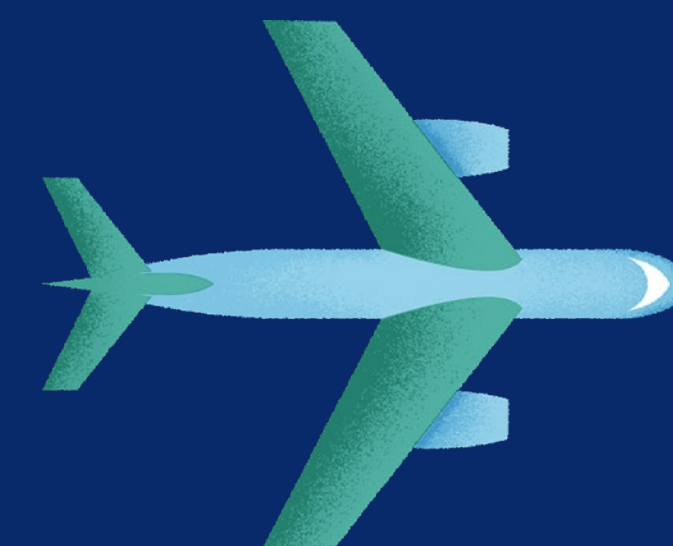


Transporta kiberdrošības rīkkopa



Ievads

Eiropas Komisijas Mobilitātes un transporta ģenerāldirektorāts (MOVE ĢD) ir noslēdzis līgumu par šīs rīkkopas izstrādi, lai vairotu transporta nozares ieinteresēto personu izpratni par kiberdraudiem un sagatavotību to īstenošanās gadījumiem. Šī rīkkopa sniedz ieskatu, kas palīdz izprast kiberdraudus un mazināt to ietekmi uz transporta pakalpojumiem, sistēmām un operācijām. Rīkkopa sniedz alternatīvus izpratnes uzlabošanas tematiskos virzienus dažādiem transporta profiliem:

- viss transporta nozares personāls (vispārīgas informācijas un norādījumu sniegšana);
- lēmumu pieņēmēji, kas darbojas dažādos transporta veidos un pieņem ar kiberdrošību saistītus lēmumus.

Dažādās rīkkopas sastāvdaļas ir savienotas ar hipersaitēm, lai uzlabotu specifiskiem transporta profiliem pielāgoto, izpratnes uzlabošanai paredzēto tematisko virzienu pārlūkošanu.

Šajā rīkkopā uzskaitītajiem prakses piemēriem ir tikai konsultatīvs raksturs. Neviens no formulētajiem ieteikumiem nav ne saistošs, ne obligāts. Turklāt šī rīkkopa neatspoguļo Eiropas Komisijas oficiālos uzskatus, un tā nav paredzēta kā rīkkopa, kurā ir norādīti līdzekļi, kas nodrošina atbilstību pastāvošiem vai nākotnē ieviešamiem ES tiesību aktiem.



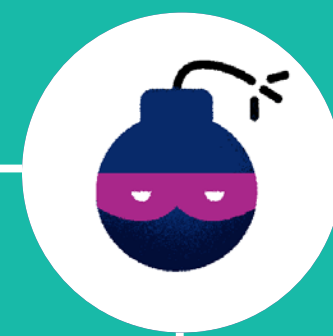
Kiberdrošības izpratnes profili

I profils – viss transporta nozares personāls. Pirmais tematiskais virziens ir vērsts uz visu transporta organizāciju personālu, sākot ar transporta pakalpojumu operācijās iesaistīto personālu un beidzot ar administratīvo personālu. Tajā ir sniegti norādījumi, kas skar visbiežāk sastopamo, uz transporta pakalpojumiem un sistēmām vērsto kiberdraudu apzināšanos un izpratni. Turklāt tas sniedz ieskatu, kā strādāt ar iespējamajiem kiberdraudiem, cita starpā aplūkojot to identificēšanu, ziņošanu par to pastāvēšanu, kā arī to mazināšanu, īstenojot labu kiberdrošības praksi.

II profils – transporta kiberdrošības lēmumu pieņēmēji. Otrais tematiskais virziens ir vērsts uz transporta organizāciju personālu, kas atbild par lēmumu pieņemšanu ar kiberdrošību saistītos jautājumos. Šajā tematiskajā virzienā ir akcentēta dažādiem transporta veidiem pielāgota labā prakse, kas ir paredzēta transporta organizāciju kiberdrošības stāvokļa uzlabošanai. Tajā galvenokārt parādīta labā prakse, kas ļauj identificēt un atklāt jaunus uz transporta organizācijām vērstus kiberdraudus, kā arī aizsargāt no tiem un reaģēt uz tiem.

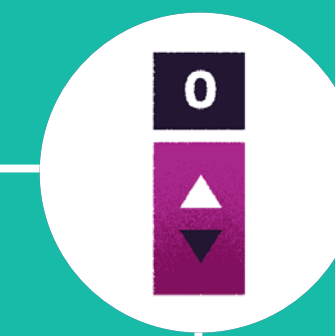


Transporta kiberdrošības rīkkopa



Transporta apdraudējuma aina

Jaunākie kiberdraudi, kas ietekmē dažādus transporta veidus



Kiberdrošības izpratnes profili

Alternatīvi kiberdrošības izpratnes tematiskie virzieni, kas ir vērsti uz dažādiem transporta profiliem

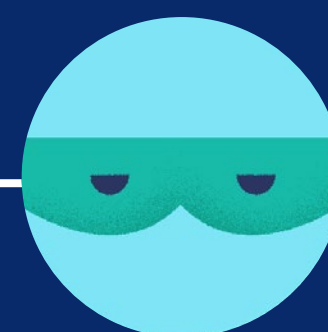
Transporta apdraudējuma aina

Kiberdraudu aina ir ļoti dinamiska, un tā nepārtraukti attīstās. Tomēr ir iespējams identificēt visus kiberdraudus, kuri ir vērsti uz visu transporta veidu pakalpojumu un sistēmu operācijām.



Apdraudētāji

Indivīdi vai organizācijas, kas potenciāli var ietekmēt transporta pakalpojumu un sistēmu drošumu un drošību



Jauni kiberdraudi

Izvēlēti kiberdraudi, kas potenciāli var pārstāvēt transporta pakalpojumu un sistēmu drošumu un drošību ietekmējošus uzbrukuma vektorus



Apdraudētāji

Indivīdi vai organizācijas var apzināti vai neapzināti atklāt un izmantot vājās vietas, kurām ir potenciāls izraisīt incidentus un ietekmēt transporta pakalpojumus, cita starpā to drošumu, drošību, saimniecisko darbību, finanses un reputāciju. Apdraudētāji cita starpā ir valsts sponsorētas grupas, kibernoiedznieki, kiberteroristi, haktīvistu, hakeri (arī hakeri iesācēji), un iekšnieki (arī privilēģēti iekšnieki).

Visnozīmīgākie ļaunprātīgie apdraudētāji, kas tieši vēršas pret transporta organizācijām, ir **kibernoiedznieki**, **iekšnieki**, **valstis** un **valsts sponsorētas grupas**.

Pretinieki, piemēram, **kibernoiedznieki**, īsteno masīvas uzbrukuma kampaņas un bieži cenšas gūt finansiālu labumu.

Iekšnieki pārzina unikālās īpatnības, kas piemīt organizācijām, kuru labā viņi strādā, un viņi bieži ir labi informēti par nelielām drošības vājajām vietām. Iekšnieku-

apdraudētāju vidū var būt neapmierināti darbinieki, piegādātāji un individuāli darbuzņēmēji.

Ģeopolitiskajai spriedzei kļūstot intensīvākai, **valstis** un **valsts sponsorētas grupas** vērš darbību uz stratēģiskiem ilgtermiņa mērķiem. Tās bieži cenšas slēpti iekļūt dziļi organizāciju sistēmās un ievākt sensitīvu informāciju. Tiklīdz tās iegūst atbalstpunktu sistēmās, valsts sponsorētie uzbrucēji cenšas iegūt pozīciju, kurai ir potenciāls radīt lielāko iespējamo kaitējumu. Piemēram, tās var vērst darbību uz citu organizāciju sistēmām, izmantojot organizācijas tīkla savienojumus.

Citu apdraudētāju vidū ir **iekšnieki**, kas neapzināti vai nejauši var veikt darbības, kuras rada kiberdrošību apdraudošus notikumus un — sliktākajā gadījumā — kiberincidentus, kas ietekmē transporta pakalpojumu drošumu un drošību.



Jauni kiberdraudi

Uz transportu ir vērsts ievērojams skaits dažādu veidu kiberdraudu: **izkliegtā pakalpojumatteice**, **pakalpojumatteice**, datu zādzība, **ļauņprogrammatūras** difūzija, **pikšķerēšana**, manipulēšana ar programmatūru, **neatļauta piekļuve**, destruktīvi uzbrukumi, drošības operatoru lēmumu procesa falsifikācija vai apiešana, identitātes maskarāde, piekļuves privilēģiju ļauņprātīga izmantošana, **sociālā inženierija**, sabojāšana, noklausīšanās, aktīvu ļauņprātīga izmantošana un manipulēšana ar aparāturu.

Balstoties uz visaptverošu publiski pieejamas dokumentācijas un ekspertu interviju literatūras izpēti, visaktuālākie jaunie kiberdraudi, kas ietekmē transportu, ir: ļauņprogrammatūra, (izkliegtā) pakalpojumatteice, neatļauta piekļuve un zādzība, manipulēšana ar programmatūru.



1. draudi – ļauņprogram- matūra

Ļauņprātīga programmatūra,
kas var ietekmēt indivīdus vai
organizācijas visos transporta
veidos



2. draudi – (izklīdētā) pakalpoju- matteice

Kiberuzbrukumi, kas atsaka
indivīdiem vai organizācijām
piekļuvi attiecīgajiem transporta
pakalpojumiem un resursiem



3. draudi – neatļauta piekļuve un zādzība

Neatļauta piekļuve kritiski
svarīgiem aktīviem, to
piesavināšana un lietošana



4. draudi – manipulēšana ar program- matūru

Kiberuzbrukumi, kas ir vērsti uz
programmatūru ar mērķi modificēt
tās darbību un veikt specifiskus
uzbrukumus



1. draudi – ļauņprogrammatūra

Ļauņprogrammatūru veido ļauņprātīga programmatūra, kas var ietvert dažādus programmatūras veidus, piemēram, vīrusus, Trojas zirgus, datortārpus, izspiedējprogrammatūru, kriptovalūtas ieguves programmatūru vai citu programmatūru, kura var ietekmēt indivīdus vai organizācijas visos transporta veidos.

Viena no galvenajām kiberdrošības prioritātēm visos transporta veidos ir tīšai datoru, serveru, klientu, tīklu vai visu nosaukto objektu bojāšanai izstrādātas ļauņprogrammatūras izplatīšanās mazināšana. Tipisks uzbrukuma vektors var ietvert uz darbiniekiem vērstus pikšķerēšanas e-pastus. Citi uzbrukuma vektori var ietvert dažādas un sarežģītas sociālās inženierijas stratēģijas, piemēram, *USB* atslēgas ievietošanu brīvā datora pieslēgvietā (piem., uzlādējot

mobilo tālruni). Noklikšķinot uz hipersaitēm aizdomīgos e-pastos vai atverot pielikuma failus, lietotājs var neapzināti veikt programmatūras instalāciju vai apzināti apdraudēt transporta pakalpojumus un resursus.

Piemēram, ar izspiedējprogrammatūru “WannaCry” īstenotais kiberuzbrukums skāra vairāk nekā 150 valstis un inficēja vairāk nekā 230 000 sistēmu. Tas ietvēra izspiedējprogrammatūru, kas parasti ātri izplatās ar ļauņprātīgus pielikumus vai hipersaites saturošu pikšķerēšanas e-pastu starpniecību. Šāda veida uzbrukums ļauņprātīgi izmanto sociālo inženieriju, lai maldinātu sistēmas lietotājus, liekot viņiem instalēt (vai aktivizēt) īpašu ļauņprogrammatūru.

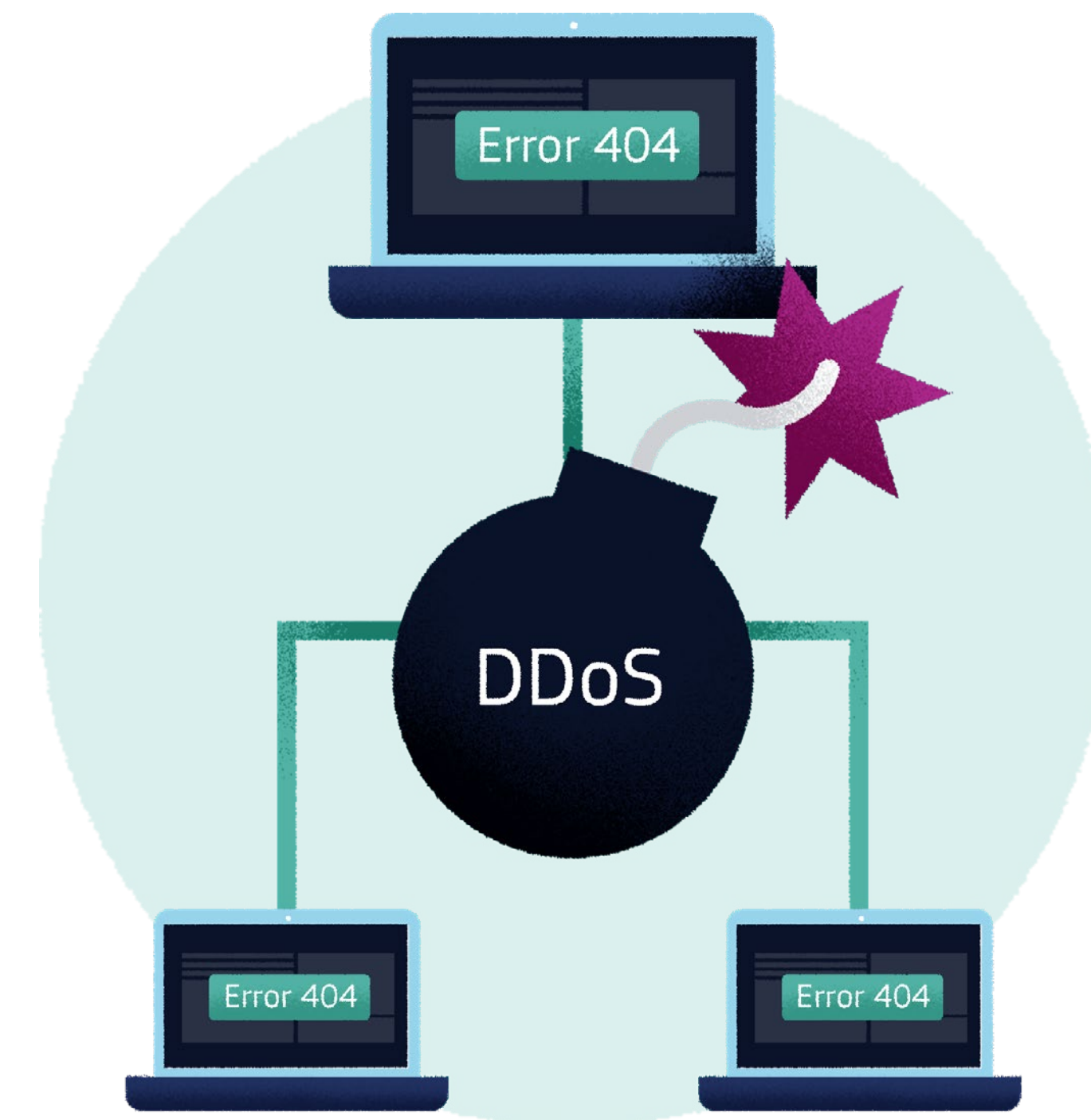


2. draudi – (izklienētā) pakalpojumatteice

Uzbrukumi, kuriem izmanto izklienēto pakalpojumatteici (*Distributed Denial of Service — DDoS*) un pakalpojumatteici (*Denial of Service — DoS*), ietekmē datu, pakalpojumu, sistēmu un citu resursu pieejamību un piekļūstamību tiem. Šāda veida uzbrukumiem var būt dažāds ilgums, un tie vienlaicīgi var būt vērsti uz vairāk nekā vienu pakalpojumu vai sistēmu. Mērķa pakalpojumu vai sistēmu pārslogošanai ar pieprasījumiem *DDoS* uzbrukumos izmanto vairākas sistēmas (vai uzbrukuma kanālus). Veiksmīgi uzbrukumi ietekmē pakalpojumu un sistēmu spēju apstrādāt negaidīti lielu pieprasījumu skaitu. Rezultātā piekļuve pakalpojumiem un resursiem tiek atteikta.

Ir jāņem vērā, ka transporta organizāciju pakalpojumus un sistēmas var izmantot arī *DDoS* un *DoS* uzbrukumiem specifiskām, operācijās izmantotām sistēmām vai citām organizācijām.

Piemēram, uz korporatīvām informācijas sistēmām (piemēram, personālajiem datoriem un ierīcēm) uzbrukumus var vērst ar mērķi piekļūt operacionālajām tehnoloģijām, kas var būt pieslēgtas internetam, vai piekļūt tīkliem ar mērķi pārsūtīt operacionālos datus. Dažādu sistēmu un tīklu (piemēram, korporatīvo tīklu, operacionālo tehnoloģiju un attālās uzturēšanas piekļuves) savienojumos var pastāvēt vājās vietas, kuras ir iespējams izmantot, lai vērstu *DDoS* vai *DoS* uzbrukumus pret kritiski svarīgiem transporta pakalpojumiem un sistēmām. Piemēram, *DDoS* un *DoS* uzbrukumos var izmantot vispārējos tīkla un sakaru protokolus, piemēram *Web Services Dynamic Discovery (WS-Discovery)*, kuru lietu interneta ierīces var izmantot katra lokālā tīkla (*Local Area Network — LAN*) mezgla automātiskai atrašanai. Ja lietu interneta ierīcēm ir vājās vietas, uzbrucēji tās var izmantot, lai atrastu citas savienotas ierīces un veiktu *DDoS* vai *DoS* uzbrukumus.



3. draudi – neatļauta piekļuve un zādzība

Apdraudētāji var vēlēties bez atļaujas iegūt loģisku vai fizisku kontroli pār tīklu, sistēmu, lietojumprogrammu, datiem vai citu resursu, lai varētu veikt ļaunprātīgas darbības, to vidū sensitīvu datu vai resursu (arī fizisku resursu) zādzību.

Neatļautas piekļuves un zādzības draudi ir vērsti uz konfidencialiem un ar īpašumtiesībām aizsargātiem aktīviem (arī personu identitātes datiem, privilēģētu kontu akreditācijas datiem, sistēmām un citiem konfidencialas un ar īpašumtiesībām aizsargātas informācijas veidiem). Šo draudu īstenošanā var izmantot sistēmu vājās vietas, kā arī nezinīgus indivīdus, kuri izpauž sensitīvus datus, piemēram, akreditācijas datus (piem., lietotājvārdu, paroli utt.) vai persondatus (piem., e-pasta adresi, personas identifikācijas numuru utt.).

Attiecībā uz neatļautu piekļuvi identitātes zādzība ir persondatu vai unikālu identifikatoru nelikumīga izmantošana ar mērķi uzdoties par citu personu vai izmantot pakalpojumus un sistēmas, lai piekļūtu privātiem vai ar īpašumtiesībām aizsargātiem resursiem (piemēram, finanšu un fiziskajiem resursiem). Šādi kiberdraudi var būt vērsti arī uz visu transporta veidu fiziskajiem aktīviem.

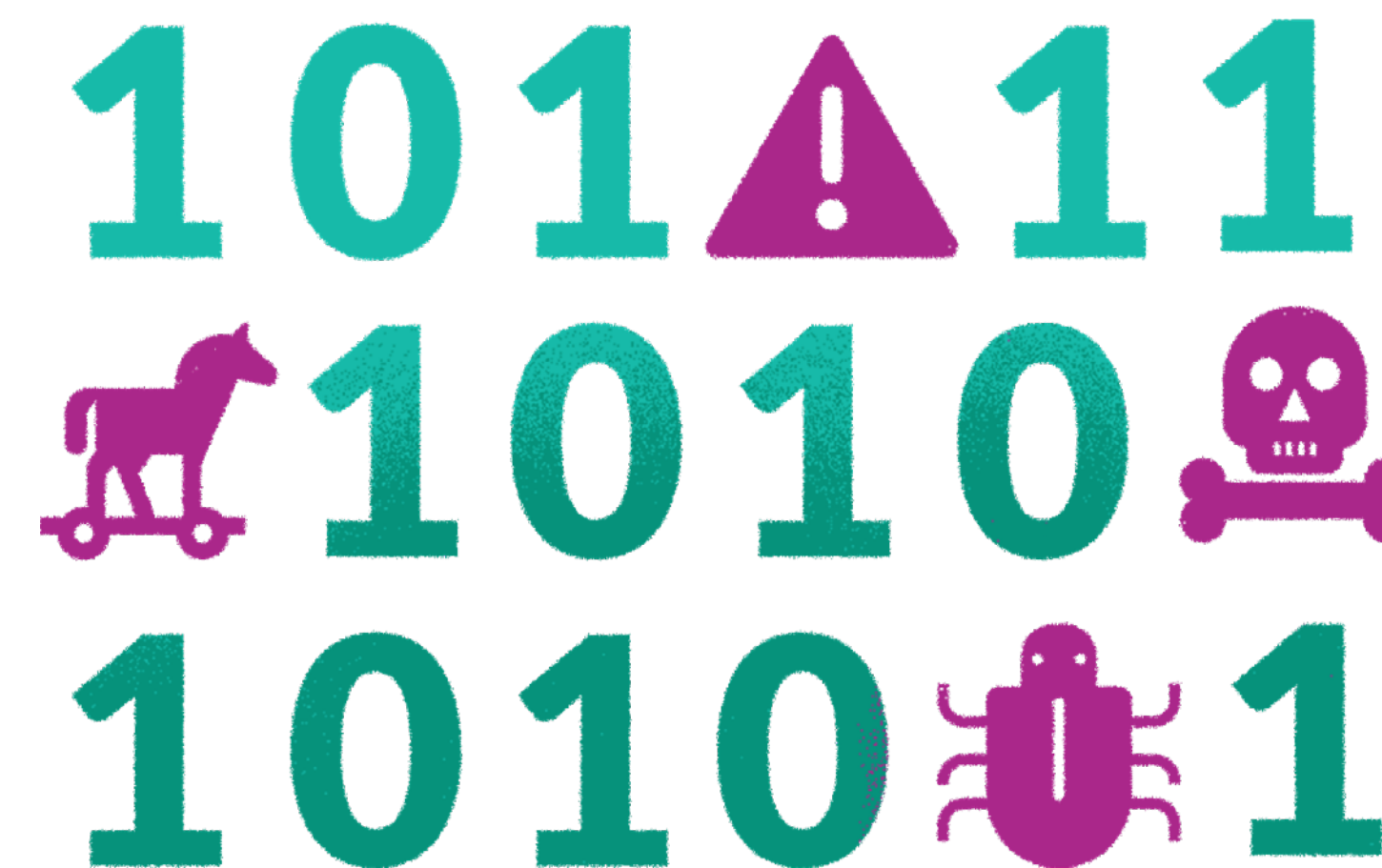


4. draudi – manipulēšana ar programmatūru

Nepareizas konfigurācijas un manipulēšana ar programmatūru, ar to saistītām sistēmām vai komponentiem var tieši ietekmēt transporta pakalpojumu un sistēmu drošības stāvokli.

Kiberuzbrukumi, kuros izmanto manipulēšanu ar programmatūru, modificē programmatūras iestatījumus vai ietekmē datu integritāti ar mērķi izmantīt sistēmu un pakalpojumu darbību. Uzbrucēji var apzināti manipulēt ar programmatūru (vai tās daļu), lai iegūtu priekšrocības (piem., neatļautu piekļuvi, iespēju atteikt legītīmiem indivīdiem vai sistēmām piekļuvi nepieciešamajiem resursiem, iespēju ievākt sensitīvu informāciju, mainīt funkcionālās darbības utt.) attiecībā uz sensitīviem aktīviem.

Piemēram, uzbrucēji var vērst uzbrukumu pret ražotāju sakaru kanāliem, lai augšupielādētu ļaunprogrammatūras atjauninājumus operācijās izmantotajos pakalpojumos un sistēmās (arī operacionālajās tehnoloģijās). Apdraudētājs izmanto kompromitētus autorizācijas akreditācijas datus, lai piekļūtu aizsargāta attālās uzturēšanas tīkla saskarnei ar mērķi instalēt manipulācijām pakļautu programmatūru un pēc tam kompromitētu citus pieejamos pakalpojumus un sistēmas. Apdraudētājs instalē manipulācijām pakļautu programmatūru, kas rada tālāku apdraudējumu mērķa pakalpojumiem un sistēmām, vai arī uzbrūk citiem savienotiem pakalpojumiem vai sistēmām.



Kiberdrošības izpratnes profili



1

I profils – viss transporta nozares personāls

Pirmais tematiskais virziens ir vērsts uz visu transporta organizāciju personālu, sākot ar operacionālo personālu un beidzot ar administratīvo personālu. Šajā tematiskajā virzienā ir sniegti norādījumi, kas skar visbiežāk sastopamo un uz transporta pakalpojumiem vērsto kiberdraudu padziļinātu apzināšanos un izpratni. Tajā ir sniegts arī ieskats darbā ar iespējamajiem kiberdraudiem, cita starpā aplūkojot to identificēšanu, ziņošanu par to pastāvēšanu, kā arī to mazināšanu ar kiberdrošības prakses palīdzību. Šis tematiskais virziens ir kopīgs visiem transporta veidiem.

2

II profils – transporta kiberdrošības lēmumu pieņēmēji

Otrais tematiskais virziens ir vērsts uz transporta organizāciju personālu, kas atbild par lēmumu pieņemšanu ar drošību vai kiberdrošību saistītos jautājumos. Šajā tematiskajā virzienā ir parādīta labā prakse, kas ir pielāgota dažādiem transporta veidiem. Tas rāda labu praksi, kas ļauj identificēt un atklāt jaunus uz transporta organizācijām vērstus kiberdraudus, kā arī aizsargāt no tiem un reaģēt uz tiem.

I profils – viss transporta nozares personāls

Šī daļa ir paredzēta visam transporta organizāciju personālam, sākot ar operacionālo personālu un beidzot ar administratīvo personālu. Tajā ir sniegti norādījumi, kas skar visbiežāk sastopamo un uz transporta pakalpojumiem vērsto kiberdraudu padziļinātu apzināšanos un izpratni. Tajā ir sniegts arī ieskats darbā ar iespējamajiem kiberdraudiem, cita starpā aplūkojot to identificēšanu, ziņošanu par to pastāvēšanu, kā arī to mazināšanu ar kiberdrošības prakses palīdzību.

Šajā daļā ir norādīta ieteicamā prakse un lietderīgi padomi, kas attiecas uz **visiem transporta veidiem**.



Labā prakse aizsardzībai pret ļaunprogrammatūru

Savu organizāciju var palīdzēt aizsargāt, ievērojot labo praksi **ļaunprogrammatūras identificēšanai un tās izplatīšanas novēršanai**, piemēram:

- **ievērojiet drošības politiku**, piemēram, skenējiet datu nesējus un failus ar mērķi atklāt datorvīrusus, neatveriet un e-pastā nenosūtiet noteiktu veidu failus (piem., tādus izpildāmos failus kā .exe, .bat, .com utt.), instalējiet tikai autorizētu programmatūru, nodrošiniet, ka programmatūra (arī antivīrusu programmatūra) ir atjaunināta un darbojas pareizi, kā arī ievērojiet citas politikas nostādnes;

- regulāri **veidojiet datu rezerves kopijas** drošās (un autorizētās) datu glabāšanas ierīcēs vai pakalpojumos, kuriem vajadzētu nodrošināt šifrēšanas mehānismus noglabāto datu aizsardzībai un būt pieejamiem datu atjaunošanas procedūrām;

- izmantojot piemērotus **drošības pasākumus** (piem., paroli, šifrēšanu utt.), aizsargājiet visas sistēmas, to vidū mobilās un galalietotāja ierīces, un atcerieties droši noslēgt (fiziski un digitāli) visas bez uzraudzības atstājamās sistēmas;

- neatveriet pielikumus un nenoklikšķiniet uz hipersaitēm, kas ir saņemtas negaidītos e-pastos un aizdomīgos tīmekļa pārlūkprogrammas uzniestošajos logos ar savādu tekstu vai kas ir saņemtas no nezināmiem sūtītājiem un interneta domēniem;

- nesavienojiet ar savu datoru **neuzticamas vai nezināmas portatīvās ierīces**, piemēram USB ierīces, cietos diskus un citas datu glabāšanas ierīces;

- neatspējojiet pret ļaunprogrammatūru aizsargājošos drošības elementus (piem., antivīrusu programmatūru, satura filtrēšanas programmatūru, ugunssmūri utt.);

- regulāri **atjauniniet instalēto programmatūru**, lai iegūtu jaunākās pieejamās versijas (kuras informācijas drošības speciālisti vai sistēmu administratori var izlaist ar regulāriem atjauninājumiem);

- neizmantojiet privilģētus (piem., administratora līmeņa) kontus un akreditācijas datus ikdienas darbībām un operācijām;

- par visiem aizdomīgiem e-pastiem vai negaidītu sistēmas uzvedību ziņojiet informācijas drošības speciālistiem vai sistēmu administratoriem.

- Ikdienas darba laikā koncentrējiet uzmanību uz informācijas drošību, lai atpazītu ar IT drošību saistītās bažas, un reaģējiet atbilstoši.

Labā prakse aizsardzībai pret (izkliedēto) pakalpojumatteici

Savu organizāciju var palīdzēt aizsargāt, identificējot uzbrukumus, kuriem izmanto **izkliedēto pakalpojumatteici (DDoS)** un **pakalpojumatteici (DoS)**. Atklājot vai konstatējot kādu no turpmāk uzskaitītajiem indikatoriem, kas vēsta par iespējamām DDoS un DoS uzbrukumiem pakalpojumiem vai sistēmām, būtu nekavējoties jāsaņem ar atbildīgajām drošības un IT vienībām:

- *palielināts pieprasījumu skaits, kas patērē tīkla kapacitāti (izpaužas kā lēni pakalpojumi un lēna reakcija), izraisot pakalpojuma vai sistēmas atteici pārslodzes dēļ;*
- *palielināts atmiņas resursu pieprasījums bez skaidri saskatāma cēloņa;*
- **negaidīta pakalpojumu un sistēmu uzvedība,** biežas avārijas un dīvaini kļūdu paziņojumi, kuru cēlonis ir

ļauprātīga datu apstrādes resursu vai tīkla savienojumu lietošana;

- **pasliktināta ierīču veikspēja,** pavisam vienkāršu uzdevumu ilga izpilde un pamanāmas darbības (piem., skaļš ventilators situācijā, kurā ierīces darbojas lēni);
- **negaidītu interneta savienojumu parādīšanās vai savienojumu zudums** pakalpojumiem un sistēmām;
- *operāciju vadības ierīcēs vai tehnoloģijās notiekošas nelielas izmaiņas, kas izraisa fiziskus bojājumus.*
- *Liegta piekļuve privilēģētiem vai administratīviem kontiem ar mērķi reaģēšanas procedūrām bloķēt iespēju atjaunot darbību.*



Labā prakse aizsardzībai pret neatļautu piekļuvi un zādzību

Lai novērstu uzbrukumus, kuri ietver neatļautu piekļuvi un zādzību, ir nepieciešams ievērot tādas principus kā “nepieciešamība zināt” un “drošība un privātums pēc noklusējuma”, kuros ir uzsvērts, ka sensitīviem un konfidenciāliem aktīviem (to vidū persondatiem un sensitīviem datiem, transporta sistēmām utt.) vajadzētu būt pieejamiem tikai tām personām, kurām šādas piekļuves tiesības ir piešķirtas darba pienākumu izpildes vajadzībām. Savu organizāciju var palīdzēt aizsargāt, ievērojot labo praksi neatļautas piekļuves un zādzības identificēšanai un novēršanai, piemēram:

- ievērojiet drošības organizatorisko politiku;
- nenododiet citiem un npublicējiet tiešsaistes akreditācijas datus un persondatus, to vidū fotogrāfijas, kas var saturēt šādu informāciju;
- neizmantojiet un nenosūtiet akreditācijas datus vai persondatus (un citus sensitīvus datus) uz neuzticamiem

un nedrošiem tīkliem, ierīcēm vai tīmekļa pakalpojumiem (piem., tīmekļa vietnēm, kurās ir izmantoti nedroši protokoli vai adreses, kas sākas ar “http://”, nevis drošas adreses, kas sākas ar “https://”);

- **nekad neatklājiet nevienam savus akreditācijas datus** (piem., lietotājmācību un paroli), arī ne ar e-pasta vai tālruna starpniecību;
- sensitīvus datus, kurus ievada ar klaviatūru vai attēlo ekrānos (arī mobilo ierīču ekrānos), aizsargājiet no neautorizētiem indivīdiem, uzstādiet privātuma aizsardzības ekrānus un nestrādājiet publiskās vietās ar privātām ierīcēm, kā arī nevienam ierīci neatstājiet nenoslēgtu un bez uzraudzības;
- **izmantojiet sarežģītas paroles** (piem., pietiekami garu paroli, kurā ir izmantoti burti, cipari un īpašās rakstzīmes), ievērojot attiecīgās organizācijas drošības politiku neatļautas piekļuves novēršanai;

■ **nomainiet** savienoto sistēmu un ierīču (piem., printeru, maršrutētāju, kameru, viedslēdzeņu utt.) **noklusējuma paroles**;

■ neizmantojiet vienu un tos pašus akreditācijas datus (piem., lietotājmācību un paroli) dažādiem pakalpojumiem un sistēmām, un neizmantojiet vienu un tos pašus akreditācijas datus pakalpojumiem un sistēmām, kurām ir nepieciešami privilēģēti konti;

■ nosūtītu aizsargātu failu (piem., ZIP arhīvu) paroles un atslēgas nosūtiet tikai un vienīgi pa ārpusjoslas kanālu (piem., SMS GSM tīklā vai ar tālruna zvana palīdzību), nekad pa e-pastu;

■ **aktivizējiet divfaktoru autentifikāciju (Two-Factor Authentication — 2FA)** vai daudzfaktoru autentifikāciju (Multi-Factor Authentication — MFA), ja iespējams.

Labā prakse aizsardzībai pret manipulēšanu ar programmatūru

Savu organizāciju var palīdzēt aizsargāt, ievērojot labo praksi, kuras mērķis ir identificēt un novērst manipulēšanu ar programmatūru, piemēram:

- *neinstalējiet neuzticamu programmatūru sistēmās un ierīcēs (to vidū personālajos datoros, serveros, perifērijas ierīcēs, tīkla ierīcēs, viedtālrunos utt.);*
- *programmatūru un atjauninājumus vienmēr instalējiet no oficiālajiem avotiem un tīmekļa vietnēm (piem., ražotāju, korporatīvo krātuvju utt.);*
- *nelejupielādējiet programmatūru un lietojumprogrammas (un nekādus failus) no nelikumīgiem avotiem;*
- *atinstalējiet nevajadzīgo vai pēdējā laikā neizmantoto programmatūru un atspējojiet nevajadzīgos savienojumus*

(piem., tīkla protokolus un pakalpojumus), to vidū piekļuvi attālinātiem pakalpojumiem (piem., mākoņglabāšanas pakalpojumiem);

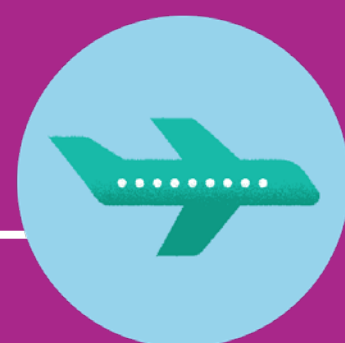
- *visas programmatūras un datu glabāšanas ierīces skenējiet ar uzticamu un atjauninātu antivīrusu programmatūru;*
- *drošu industriālo programmatūru (piemēram, atjauninājumus, ielāpus, jaunus produktus utt.) lejupielādējiet no uzticamiem piegādātājiem, izmantojot baltās stacijas (white station) principu;*
- *visu instalēto programmatūru atjauniniet atbilstoši organizācijas politikai un praksei.*



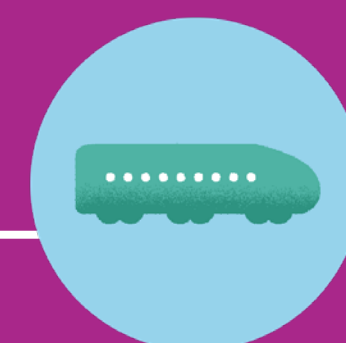
II profils – transporta kiberdrošības lēmumu pieņēmēji

Šī daļa ir vērsta uz transporta organizāciju personālu, kas atbild par lēmumu pieņemšanu ar drošību vai kiberdrošību saistītos jautājumos. Šajā tematiskajā virzienā ir akcentēta labā prakse, kas ir pielāgota dažādiem transporta veidiem. Jo īpaši tajā ir norādīta labā prakse, kas ļauj identificēt un atklāt jaunus kiberdraudus, kā arī aizsargāt no tiem un reaģēt uz tiem.

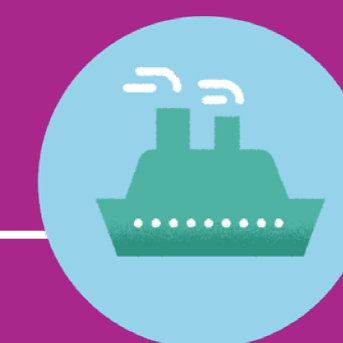




Kiberdrošības
labā prakse, kas
ir pielāgota gaisa
transportam

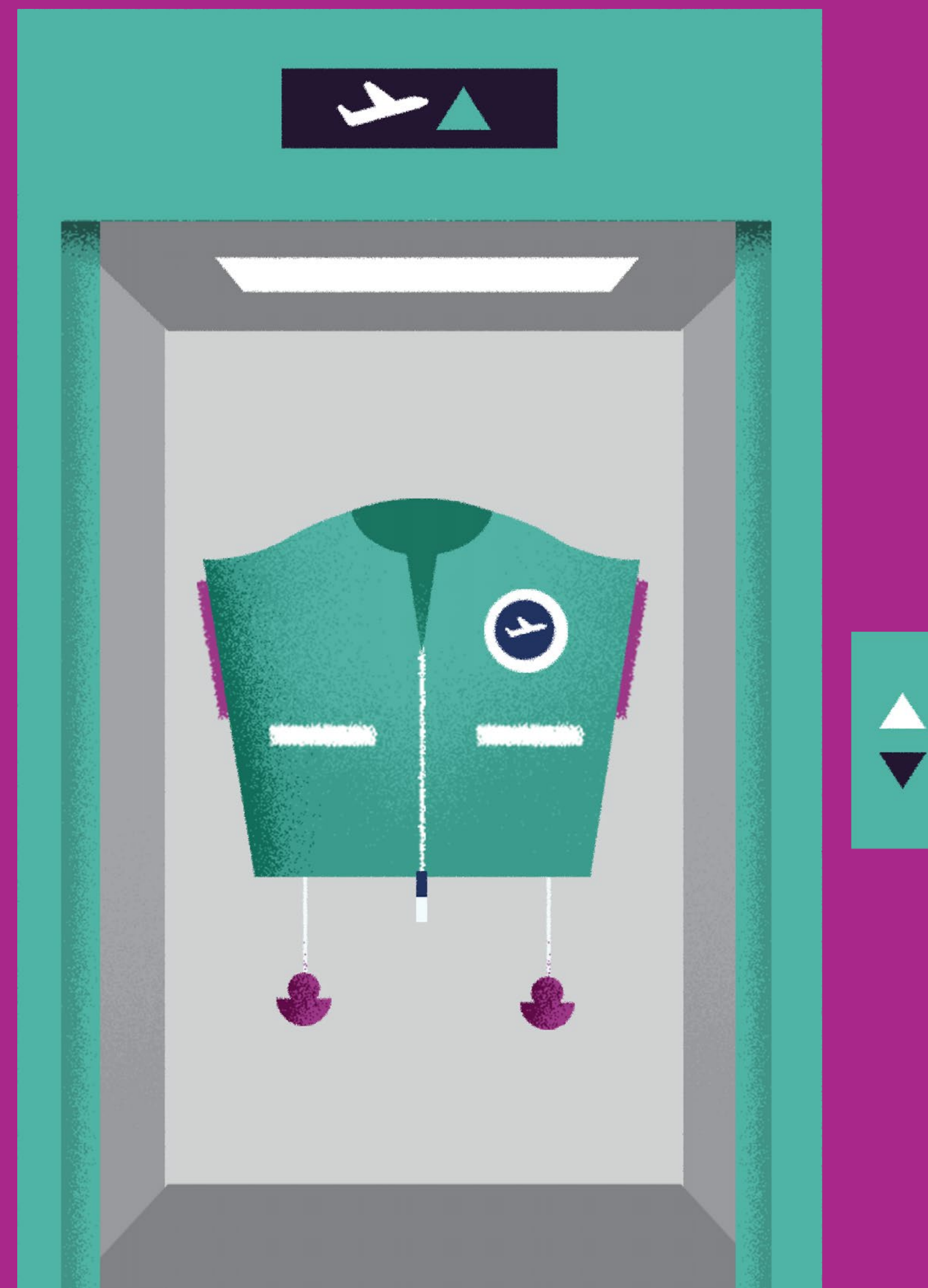


Kiberdrošības
labā prakse,
kas ir pielāgota
sauszemes
transportam



Kiberdrošības
labā prakse, kas
ir pielāgota jūras
transportam

Labā prakse un
drošības pasākumi,
kas ir pielāgoti gaisa
transportam



Pārvaldība

Aviācijas organizācijām ir nepieciešama skaidra izpratne par jaunajiem draudiem, lai definētu pārvaldības politiku un procesus savu pieeju pārvaldībai ar mērķi uzlabot kiberdrošību operācijās izmantotajiem pakalpojumiem un sistēmām, arī informācijas tehnoloģijām (IT) un operacionālajām tehnoloģijām (OT).

Labā prakse jebkura lieluma organizācijām ietver šādas darbības:

- nodrošināt, ka augstāko līmeņu vadība par bažām, kuras ir saistītas ar kiberdrošību, ziņo vadītājiem un valdēm, kas var pieņemt uz informāciju balstītus lēmumus par resursu piešķiršanu;

- iecelt galveno par kiberdrošību, kā arī fizisko drošību atbildīgo personu, kurai ir vispārēji vadības pienākumi attiecībā uz informācijas tehnoloģiju (IT) un operacionālo tehnoloģiju (OT) drošību, neiesaistot šo personu operācijās, lai izvairītos no interešu konfliktiem;

- skaidri noteikt lomas, atbildību, kompetences un pielāides attiecībā uz kiberdrošību, kā arī paziņot tās attiecīgajam personālam un vienoties par tām ar attiecīgo personālu, jo īpaši datorapdraudējumu reaģēšanas vienību (*Computer Emergency Response Team — CERT*) locekļiem;

- nodrošināt kiberdrošības pārvaldību visā drošības pakalpojumu ķēdē, ietverot gan fiziskas, gan digitālas saskarnes, sākot ar tehnoloģiju ražotājiem un instalētājiem un beidzot ar drošības pakalpojumu sniedzējiem;

- vienoties par pasākumiem un kontroli, arī dalīto atbildību, kiberdrošības risku pārvaldībai un nodrošināt, ka šī atbildība tiek uzturēta visa drošības risinājumu un pakalpojumu dzīves cikla laikā (piem., ar pakalpojumu līgumiem);

- definēt pārvaldības mehānismus (piem., politiku) ar mērķi nodrošināt atbilstību prasībām, kas noteiktas attiecīgajās regulās un direktīvās, piem., Regulā (ES) 2018/1139 par kopīgiem noteikumiem civilās aviācijas jomā un Komisijas Īstenošanas Regulā (ES) 2017/373, ar ko nosaka kopīgas prasības gaisa satiksmes pārvaldības/aeronavigācijas pakalpojumu sniedzējiem un citu gaisa satiksmes pārvaldības tīkla funkciju nodrošinātājiem un to uzraudzībai, kā arī *NIS* direktīvā (ES Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā).

Gaisa transporta pakalpojumu un sistēmu piemēri: IT

(informācijas tehnoloģiju) piemēri ir darbiniekiem pieejamie rīki (piem., personālie datori, mobilie tālruņi, biroja perifērijas ierīces utt.), kā arī pasažieriem pieejamie rīki (piem., publiskie *Wi-Fi* maršrutētāji un savienojumi utt.). OT (operacionālo tehnoloģiju) piemēri ir uzraudzības kontroles un datu iegūšanas (*Supervisory Controls and Data Acquisition — SCADA*) sistēmas, apkures, ventilācijas un gaisa kondicionēšanas (*heating, ventilation, and air conditioning — HVAC*) sistēmas, rokas bagāžas drošības kontroles punkti, bagāžas apstrādes sistēmas (*baggage handling systems — BHS*), piekļuves kontrole, monitorings, novērošana, signalizācija, skrīninga tehnoloģija, lidlauka apgaismojuma vadības sistēmas, radaru sistēmas un sensori, globālās pozicionēšanas sistēmas (GPS), gaisa satiksmes vadības (*Air Traffic Management — ATM*) sistēmas, sakaru, navigācijas un novērošanas sistēmas (*Communication, Navigation and Surveillance systems — CNS*), aeronavigācijas informācijas sistēmas, meteoroloģiskās sistēmas, drošības operāciju centru sistēmas, aviosabiedrību borta sistēmas un citas.



Kiberdraudu identificēšana

Riska pārvaldība – aviācijas organizācijām ir jāveic atbilstoši pasākumi, lai identificētu, novērtētu un izprastu kiberdrošības riskus, kas skar tīklu un informācijas sistēmas, kuras nodrošina pamatfunkciju darbību.

Tam ir nepieciešama visaptveroša organizatoriska pieeja riska pārvaldībai, un tas ietver šādus pasākumus:

- skaidra pārskata nodrošināšana par dažādajām aparatūras un programmatūras sistēmām, kuras izmanto dažādu pakalpojumu sniegšanai. Aviācijas kontekstā šādas sistēmas ir saistītas ar informācijas tehnoloģijām (IT) un operacionālajām tehnoloģijām (OT).
- **Kiberdrošības risku novērtējumu** veikšana, ņemot vērā jaunus draudus, zināmās vājās vietas un operacionālos

datumus saistībā ar attiecīgajām sistēmām. Ieskatoties par draudiem, kas ir vērsti uz gaisa transportu, var sniegt tādas organizācijas kā Eiropas Gaisa satiksmes pārvaldības datorapdraudējumu reaģēšanas vienība (European Air Traffic Management Computer Emergency Response Team — EATM-CERT) un Aviācijas informācijas apmaiņas un analīzes centrs (Aviation Information Sharing and Analysis Centre — A-ISAC).

- Ar personāla ikdienas darbībām (piem., sociālo mediju un personīgo ierīču lietošanu, datu apstrādi, informācijas apmaiņu utt.) saistīto risku ietveršana riska novērtējumā.
- Riska apstrādes pasākumu un kiberdrošības risku mazināšanas plānu identificēšana un ieviešana.

- Ar citām pārvaldības sistēmām saskaņotas visaptverošas **informācijas drošības pārvaldības sistēmas** (Information Security Management System — ISMS) un **privātuma informācijas pārvaldības sistēmas (Privacy Information Management System — PIMS)** ieviešana. Šādas pārvaldības sistēmas (t. i., ISMS un PIMS) ietver drošības (kā arī datu aizsardzības un privātuma) pasākumu ieviešanu ar mērķi mazināt un novērst jaunus draudus, kas ietekmē aviācijas pakalpojumu un sistēmu (arī tajās esošo datu) drošību.
- Rēķināšanās ar visiem ierobežojumiem, kas ir saistīti ar **aktīvu pārvaldību un resursu plānošanu** (proti, ierobežojumiem, kas var ietekmēt gaisa transporta pamatfunkciju darbībai kritiski svarīgo sistēmu piegādi, uzturēšanu un atbalstu).

Riska pārvaldības regulējumu piemēri: dažādi regulējumi (piem., *ISO/IEC 27000* saimes standarti, *NIST* kiberdrošības regulējums, *MITRE ATT&CK* regulējums, *BSI IT-Grundschutz* utt.) var sniegt informāciju un dot pamatu pielāgotas riska pārvaldības pieejai gaisa transportā. Starptautiskas organizācijas, piemēram *IATA* un *ICAO*, sniedz norādījumus par kiberdrošības risku novērtējumiem. *ENISA*, *EASA*, *EUROCONTROL*, un Starptautiskā lidostu padome (*Airports Council International — ACI*) ir dažas no organizācijām, kas akcentē labo praksi lidostu, gaisa satiksmes pārvaldības pakalpojumu sniedzēju un citu aviācijas organizāciju drošības nodrošināšanai. Kopuzņēmums *SESAR* koordinē un koncentrē visas ES pētniecības un izstrādes (*research and development — R&D*) darbības gaisa satiksmes pārvaldības jomā, ietverot arī drošuma un drošības aspektus.



Aizsardzība pret kiberdraudiem

Gaisa transporta organizācijām vajadzētu ieviest atbilstošus un proporcionālus drošības pasākumus, lai aizsargātu savus tīklus un informācijas sistēmas — to vidū informācijas tehnoloģijas (IT) un operacionālās tehnoloģijas (OT) — no kiberuzbrukumiem. Drošības pasākumi ir:

■ **drošības politika un procesi:** tādas atbilstošas politikas un procesu definēšana, izpildīšana, paziņošana un ieviešana, kas nosaka vispārēju pieeju aviācijas pamatfunkciju darbību atbalstošu sistēmu un datu nodrošināšanai. Šādai drošības politikai (piem., paroļu un datu glabāšanas politikai) un procedūrām vajadzētu aptvert arī aparatūras un programmatūras sistēmu (to vidū IT un OT), incidentu pārvaldības, sistēmas un tīkla aizsardzības drošības ielāpu un vājo vietu pārvaldību.

■ **Identitātes un piekļuves pārvaldība:** gaisa transporta pamatfunkciju darbību atbalstošu tīklu un informācijas sistēmu (arī IT un OT) izprašana, dokumentēšana un

piekļuves pārvaldība. Lietotāji (vai automatizētās funkcijas), kas var piekļūt datiem vai sistēmām, ir atbilstoši verificēti, autentificēti un autorizēti. Šajā pārvaldībā uzmanība būtu jāpievērš arī parasto un privilēģēto kontu dažādajām lomām un atbildībām.

■ **Datu un sistēmu drošība:** datu (saglabāto un elektroniski nosūtīto), kritiski svarīgo tīklu un informācijas sistēmu (to vidū IT un OT) aizsargāšana pret kiberuzbrukumiem. Ņemot vērā uz risku balstītu pieeju, organizācijām vajadzētu ieviest drošības pasākumus, lai efektīvi samazinātu uzbrucēju iespējas kompromitēt datus, tīklus un sistēmas. Šiem drošības pasākumiem vajadzētu ietvert arī šifrēšanas un drošu sakaru protokolu ieviešanu, kuras mērķis ir aizsargāt glabāšanā un tranzītā esošos datus pret kiberdraudiem, kuri rada pārtvērējuzbrukumus. Turklāt, lai aizsargātu piekļuvi sistēmām, šādi pasākumi jākombinē ar fiziskās drošības pasākumiem (piem., sistēmām vajadzētu būt uzstādītām norobežotās telpās ar ierobežotu piekļuvi).

■ **Tīklu un sistēmu noturība:** tīklu un sistēmu (to vidū IT un OT) noturības veidošana, izstrādājot un ieviešot tos (un to operacionālās procedūras) tādā veidā, lai pretotos kiberuzbrukumiem un mazinātu kiberuzbrukumu ietekmi. Noturību uzlabojoši izstrādes un ieviešanas risinājumu piemēri: oficiāli verificētas kritiski svarīgās funkcijas, sistēmu un tīklu dublēšana, tīklu nošķiršana (jo īpaši — IT un OT nošķiršana), daudzslāņu drošības pasākumi un daudzi citi pasākumi. Jāņem vērā, ka, no informācijas drošības skatpunkta raugoties, piemērotus drošības risinājumus var garantēt drošības domēni, kas īsteno tīkla un sistēmas nošķiršanu. Tomēr sistēmu operacionālajām vajadzībām (piem., apkalpošanas darbībām, datu pārsūtīšanai utt.) var būt nepieciešams apiet vai savienot dažādus drošības domēnus (piemēram, nošķirtas sistēmas un tīklus), arī savienot IT un OT.

Kiberdraudu atklāšana

Organizācijām vajadzētu nodrošināt, ka drošības pasākumu iedarbīgums saglabājas un ar tiem atklāj ar kiberdrošību saistītus notikumus, kuri ietekmē vai kuriem ir potenciāls ietekmēt drošības kontroli, kā arī svarīgus pakalpojumus un sistēmas. Kiberdraudu atklāšanai piemēroti drošības pasākumi:

■ **drošības monitorings:** gaisa transporta pakalpojumu pamatfunkciju darbību atbalstošo tīklu un informācijas sistēmu — arī informācijas tehnoloģiju (IT) un operacionālo tehnoloģiju (OT) — drošības statusa monitorings. Drošības monitoringa atbalstīšanas vajadzībām vērā ņemamie dati ir, piemēram:

- drošības žurnāli;
- datorvīrusu atklāšanas žurnāli;
- ielaušanās atklāšanas žurnāli;
- identifikācijas, autentifikācijas un autorizācijas žurnāli;

- sistēmas un pakalpojumu žurnāli;
- tīkla plūsmas žurnāli;
- datu apstrādes žurnāli.

■ **Ar drošību saistīto notikumu atklāšana:** tādu ļaunprātīgu darbību (t. i., ar drošību saistītu notikumu) atklāšana, kuras ietekmē vai kurām ir potenciāls ietekmēt gaisa transporta pakalpojumu pamatfunkciju darbību atbalstošo tīklu un informācijas sistēmu (arī IT un OT) drošību.

Šo pasākumu īstenošanai var būt nepieciešams ieviest specifiskas tehnoloģijas (piem., drošības informācijas un notikumu pārvaldību, ielaušanās atklāšanas sistēmu, ielaušanās novēršanas sistēmu utt.) un izveidot drošības operāciju centru (*Security Operations Centre — SOC*) vai ekvivalentus risinājumus. Citiem vārdiem sakot — jāizstrādā līdzekļi, ar kuru palīdzību ir iespējama kiberuzbrukumu lokāla

atklāšana, analīze, kā arī reaģēšana uz kiberuzbrukumiem un darbības atjaunošana pēc kiberuzbrukumiem.

Nacionālās datordrošības incidentu reaģēšanas vienības (*National Computer Security Incident Response Teams — CSIRT*), sektorālās datorapdraudējumu reaģēšanas vienības (*Computer Emergency Response Team — CERT*) (piem., *EUROCONTROL* Eiropas Gaisa satiksmes pārvaldības datorapdraudējumu reaģēšanas vienība (*EATM-CERT*)), aviokompāniju komerciālās datorapdraudējumu reaģēšanas vienības (*Computer Emergency Response Team — CERT*) un Aviācijas informācijas apmaiņas un analīzes centrs (*Aviation Information Sharing and Analysis Centre — A-ISAC*) var sniegt kiberdraudu izlūkdatus (*Cyber Threat Intelligence — CTI*), informējot drošības monitoringa un draudu atklāšanas īstenotājus.

Reaģēšana un darbības atjaunošanas plānošana

Organizācijām būtu jādefinē, jāievieš un jātestē incidentu pārvaldības procedūras, kuras ir paredzētas pakalpojumu un sistēmu darbības nepārtrauktības nodrošināšanai kibernetiskās drošības incidentu gadījumā. Ietekmes mazināšanas pasākumi ir paredzēti kibernetiskās drošības incidentu ietekmes kontrolēšanai vai ierobežošanai.

Reaģēšanas un darbības atjaunošanas plānošanā vajadzētu ņemt vērā drošības pasākumus, kas mazina specifisku kibernetiskās drošības ietekmi, piem.

- *koordinācija un sadarbība ar nacionālajām datordrošības incidentu reaģēšanas vienībām (CSIRT), (publiskajām un komerciālajām) datorapdraudējumu reaģēšanas vienībām (CERT) un informācijas apmaiņas un analīzes centriem (ISAC) kibernetiskās drošības incidentu, incidentu koordinācijas un visas Eiropas līmeņa krīžu laikā.*

- *Informācijas apmaiņa ar citām organizācijām, to vidū aviācijas pakalpojumu apgādes ķēdes pakalpojumu sniedzējiem.*

- *Periodisku **kibernetiskās drošības mēcību** īstenošana (teorētiskā, kā arī tehniskā koordinācija) ar mērķi novērtēt drošības pasākumus un procedūras, kā arī organizāciju noturību darbā ar kibernetiskās drošības incidentiem.*

- *Pieklūve arhīviem vai failu dublējumu glabāšanas vietām kompromitētas integritātes gadījumā un datu glabāšanas risinājumu pieejamība.*

- **Drošības shēmas** ar detalizētām procedūrām kibernetiskās drošības incidentu pārvaldībai un pakalpojumu un sistēmu atjaunošanai normālā operacionālā stāvoklī.

- *Tīkla plūsmas pārsūtīšana uz rezerves pakalpojumiem pakalpojumatteices uzbrukumu gadījumā.*

- *Manuālas procedūras darbā ar pakalpojumiem un sistēmām nepilnīgā operacionālajā režīmā.*

- *Tādu procedūru definēšana, kas paredzētas, lai risinātu datu aizsardzības pārkāpumus, to vidū procedūru definēšana*

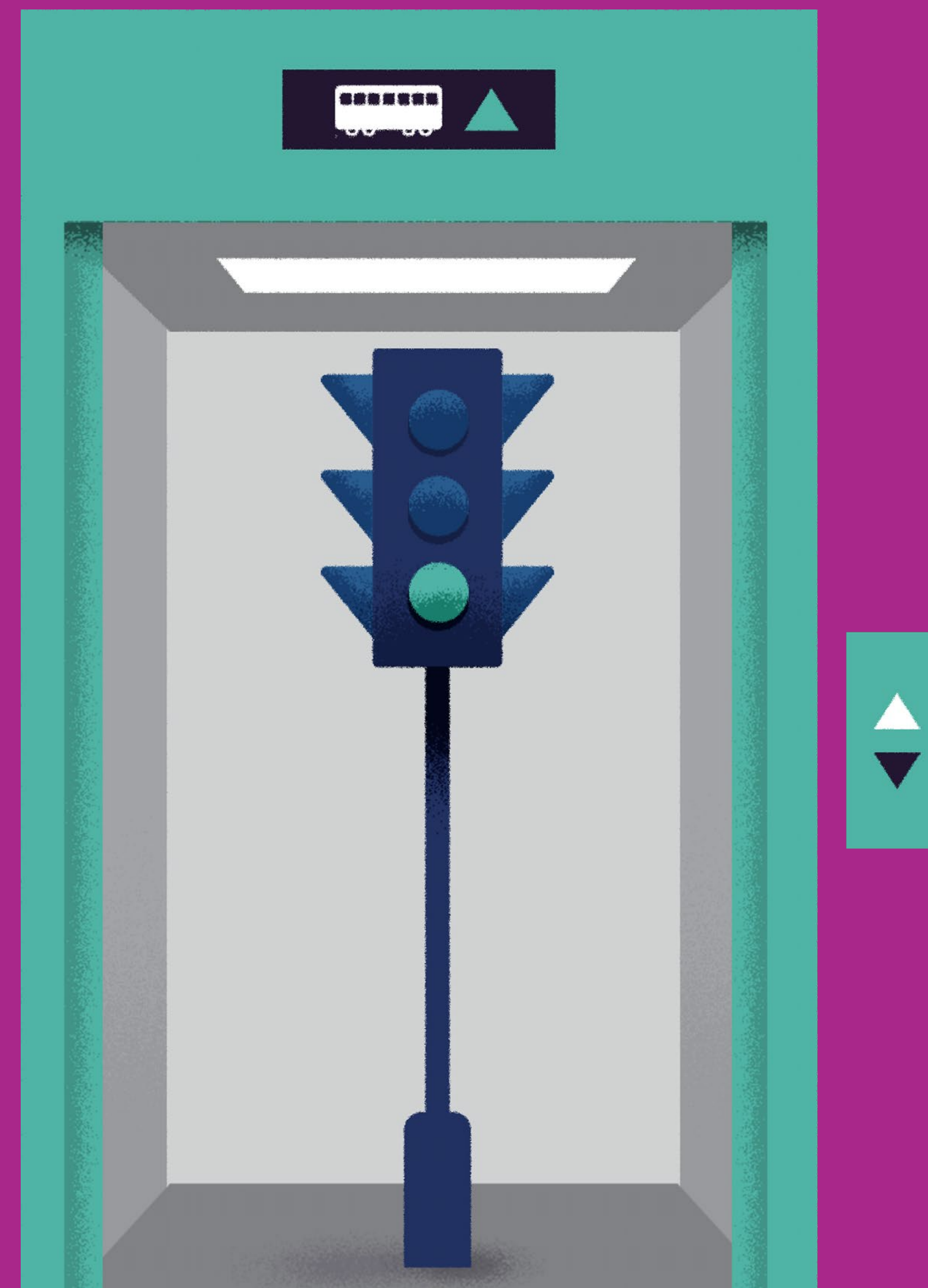
darbam ar datu aizsardzības pārkāpumiem, kas ir saistīti ar persondatiem, atbilstoši Vispārīgajai datu aizsardzības regulai (VDAR) vai citai nozares regulai vai direktīvai.

- **Kiberapdrošināšanas** iegāde ar mērķi daļēji mazināt ar smagiem kibernetiskās drošības incidentiem saistīto risku.

- *Līguma noslēgšana par reaģēšanu uz incidentiem ar vienu vai vairākiem specializētiem uzņēmumiem ar mērķi piesaistīt papildu spējas un speciālās zināšanas.*

- *Tādu procedūru definēšana, kurās ir noteikta **ar kibernetiskās drošības incidentiem saistītas informācijas apmaiņa** ar attiecīgajām ieinteresētajām personām, ietverot incidentu paziņošanas procedūras saskaņā ar NIS direktīvu (Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā).*

Labā prakse un
drošības pasākumi,
kas ir pielāgoti
sauszemes
transportam



Pārvaldība

Sauszemes transporta (ceļu un dzelzceļu) organizācijām ir nepieciešama skaidra izpratne par jaunajiem draudiem, lai definētu pārvaldības politiku un procesus savu pieeju pārvaldībai ar mērķi uzlabot kiberdrošību operācijās izmantotajiem pakalpojumiem un sistēmām, arī informācijas tehnoloģijām (IT) un operacionālajām tehnoloģijām (OT).

Labā prakse jebkura lieluma organizācijām ietver šādas darbības:

- *nodrošināt, ka augstāko līmeņu vadība par bažām, kuras ir saistītas ar kiberdrošību, ziņo vadītājiem un valdēm, kas var pieņemt uz informāciju balstītus lēmumus par resursu piešķiršanu;*

- *iecelt galveno par kiberdrošību, kā arī fizisko drošību atbildīgo personu, kurai ir vispārēji vadības pienākumi attiecībā uz informācijas tehnoloģiju (IT) un operacionālo tehnoloģiju (OT) drošību, neiesaistot šo personu operācijās, lai izvairītos no interešu konfliktiem;*

- *skaidri noteikt lomas, atbildību, kompetences un pielai des attiecībā uz kiberdrošību, kā arī paziņot tās attiecīgajam personālam un vienoties par tām ar attiecīgo personālu. Tas īpaši nepieciešams datorapdraudējumu reaģēšanas vienību (CERT) locekļiem;*

- *nodrošināt kiberdrošības pārvaldību visā drošības pakalpojumu ķēdē, ietverot gan fiziskas, gan digitālas saskarnes, sākot ar tehnoloģiju ražotājiem un instalētājiem un beidzot ar drošības pakalpojumu sniedzējiem;*

- *vienoties par pasākumiem un kontroli, arī dalīto atbildību, kiberdrošības risku pārvaldībai un nodrošināt, ka šī atbildība tiek uzturēta visa drošības risinājumu un pakalpojumu dzīves cikla laikā (piem., ar pakalpojumu līgumiem);*

- *definēt pārvaldības mehānismus (piem., politiku), lai izpildītu prasības, kas izriet no attiecīgajām regulām un direktīvām. Tas ietver plašu politikas nostādņu kopumu, kas aptver specifiskus transporta veidus, kā arī dažādu veidu ieinteresētās personas (piem., transportlīdzekļu un dzelzceļa sistēmu ražotājus), kā arī NIS direktīvu (Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā).*

Sauszemes transporta pakalpojumu un sistēmu

piemēri: IT (informācijas tehnoloģiju) piemēri ir darbiniekiem pieejamie rīki (piem., personālie datori, mobilie tālruņi, biroja perifērijas ierīces utt.), kā arī pasažieriem pieejamie rīki (piem., publiskie *Wi-Fi* maršrutētāji un savienojumi utt.). OT (operacionālo tehnoloģiju) piemēri ir uzraudzības kontroles un datu iegūšanas (*SCADA*) sistēmas, apkures, ventilācijas un gaisa kondicionēšanas (*HVAC*) sistēmas, globālās pozicionēšanas sistēmas (*GPS*), piekļuves kontroles, monitoringa, novērošanas, reaģēšanai uz trauksmi paredzētās sistēmas un skrīninga tehnoloģija. Specifiskas dzelzceļa transporta sistēmas ir, piemēram: operacionālās (vadības un komandu sistēmas), to vidū signalizēšanas sistēmas, Eiropas Dzelzceļa satiksmes vadības sistēma (*European Rail Traffic Management System — ERTMS*), vilcienu borta sistēmas, apkalpošanas sistēmas un citas sistēmas.



Kiberdraudu identificēšana

Riska pārvaldība – sauszemes transporta organizācijām ir jāveic atbilstoši pasākumi, lai identificētu, novērtētu un izprastu kiberdrošības riskus, kas skar tīklu un informācijas sistēmas, kuras nodrošina pamatfunkciju darbību. Tam ir nepieciešama visaptveroša organizatoriska pieeja riska pārvaldībai, un tas ietver šādus pasākumus:

- skaidra pārskata nodrošināšana par dažādajām aparatūras un programmatūras sistēmām, kuras izmanto dažādu pakalpojumu sniegšanai. Sauszemes transporta kontekstā šādas sistēmas ir saistītas ar informācijas tehnoloģijām (IT) un operacionālajām tehnoloģijām (OT).

- **Kiberdrošības risku novērtējumu** veikšana, kurā vajadzētu ņemt vērā jaunus draudus, zināmās vājās vietas un operacionālos datus saistībā ar attiecīgajām sistēmām.

Sauszemes transporta veidu sistēmu piemēri: maksājumu sistēmas, tīkla un sakaru sistēmas (piemēram, internets, radiosakari, Wi-Fi utt.), borta aprīkojums, operacionālās kontroles centri, identitātes pārvaldības sistēmas, drošības sistēmas u. c. Dzelzceļa infrastruktūras sistēmu piemēri: ritošā sastāva, darbības un satiksmes pārvaldības apakšsistēmas, kontroles vadība, signalizācijas borta un sliežu ceļa apakšsistēmas u. c.

- Ar personāla ikdienas darbībām (piem., sociālo mediju un personīgo ierīču lietošanu, datu apstrādi, informācijas apmaiņu utt.) saistīto risku ietveršana riska novērtējumā.

- Riska apstrādes pasākumu un kiberdrošības risku mazināšanas plānu identificēšana un ieviešana. Piemēram, ar citām pārvaldības sistēmām saskaņotas visaptverošas

informācijas drošības pārvaldības sistēmas (Information Security Management System —ISMS) un **privātuma informācijas pārvaldības sistēmas (Privacy Information Management System — PIMS)** ieviešana. Šādas pārvaldības sistēmas (t. i., ISMS un PIMS) ietver drošības (kā arī datu aizsardzības un privātuma) pasākumu ieviešanu ar mērķi mazināt un novērst jaunus draudus, kas ietekmē sauszemes transporta pakalpojumu un sistēmu (arī tajās esošo datu) drošību.

- Rēķināšanās ar visiem ierobežojumiem, kas ir saistīti ar **aktīvu pārvaldību un resursu plānošanu** (proti, ierobežojumiem, kas var ietekmēt sauszemes transporta pamatfunkciju darbībai kritiski svarīgo sistēmu piegādi, uzturēšanu un atbalstu).

Riska pārvaldības regulējumu piemēri: dažādi regulējumi (piem., *ISO/IEC 27000* saimes standarti, *NIST* kiberdrošības regulējums, *MITRE ATT&CK* regulējums, *BSI IT-Grundschutz* utt.) var sniegt informāciju un dot pamatu pielāgotas riska pārvaldības pieejai autotransportam un dzelzceļa transportam. Dažādas organizācijas, piemēram, *ENISA*, definē viedautomobiļu un intelektiskā publiskā transporta kiberdrošības labo praksi, kas sniedz informāciju nozares ražotājiem un asociācijām, piemēram, Eiropas Autoražotāju asociācijai (*European Automobile Manufacturers' Association — ACEA*). Attiecībā uz dzelzceļa transportu Eiropas Savienības Dzelzceļu aģentūra (*ERA*) definē savstarpējās izmantojamības tehniskās specifikācijas (*SITS*), kuras jāievēro visām apakšsistēmām vai apakšsistēmas daļām, lai tās atbilstu pamatprasībām un nodrošinātu Eiropas Savienības dzelzceļa sistēmas savstarpēju izmantojamību. Inovāciju (arī kiberdrošības) iniciatīvas un projektus dzelzceļa transporta jomā virza arī kopuzņēmums *Shift2Rail*.



Aizsardzība pret kiberdraudiem

Sauszemes transporta organizācijām vajadzētu ieviest atbilstošus un proporcionālus drošības pasākumus, lai aizsargātu savus tīklus un informācijas sistēmas — to vidū informācijas tehnoloģijas (IT) un operacionālās tehnoloģijas (OT) — no kiberuzbrukumiem. Drošības pasākumi ir:

■ **drošības politika un procesi:** tādas atbilstošas politikas un procesu definēšana, izpildīšana, paziņošana un ieviešana, kas nosaka vispārēju pieeju sauszemes transporta veidu pamatfunkciju darbību atbalstošu sistēmu un datu nodrošināšanai. Šādai drošības politikai (piem., paroļu un datu glabāšanas politikai) un procedūrām jāaptver arī aparatūras un programmatūras sistēmu (to vidū IT un OT), incidentu pārvaldības, sistēmas un tīkla aizsardzības drošības ielāpu un vājo vietu pārvaldība.

■ **Identitātes un piekļuves pārvaldība:** sauszemes transporta veidu pamatfunkciju darbību atbalstošu tīklu un informācijas sistēmu (arī IT un OT) izprašana, dokumentēšana un piekļuves pārvaldība. Lietotāji (vai automatizētās

funkcijas), kas var piekļūt datiem vai sistēmām, ir atbilstoši verificēti, autentificēti un autorizēti. Šajā pārvaldībā uzmanība būtu jāpievērš arī parasto un privilģēto kontu dažādajām lomām un atbildībām.

■ **Datu un sistēmu drošība:** datu (saglabāto un elektroniski nosūtīto), kritiski svarīgo tīklu un informācijas sistēmu (to vidū IT un OT) aizsargāšana pret kiberuzbrukumiem. Ņemot vērā uz risku balstītu pieeju, organizācijām vajadzētu ieviest drošības pasākumus, lai efektīvi samazinātu uzbrucēju iespējas kompromitēt datus, tīklus un sistēmas. Šiem drošības pasākumiem vajadzētu ietvert arī šifrēšanas un drošu sakaru protokolu ieviešanu, kuras mērķis ir aizsargāt glabāšanā un tranzītā esošos datus pret kiberdraudiem, kuri rada pārtvērējuzbrukumus. Turklāt, lai aizsargātu piekļuvi sistēmām, šādi pasākumi jākombinē ar fiziskās drošības pasākumiem (piem., sistēmām vajadzētu būt uzstādītām norobežotās telpās ar ierobežotu piekļuvi).

Tas ir ļoti svarīgi sistēmām, kas var ietekmēt dzīvības drošību.

■ **Tīklu un sistēmu noturība:** tīklu un sistēmu (to vidū IT un OT) noturības veidošana, izstrādājot un ieviešot tos (un to operacionālās procedūras) tādā veidā, lai pretotos kiberuzbrukumiem un mazinātu kiberuzbrukumu ietekmi. Noturību uzlabojoši izstrādes un ieviešanas risinājumu piemēri: oficiāli verificētas kritiski svarīgās funkcijas, sistēmu un tīklu dublēšana, tīklu nošķiršana (jo īpaši — IT un OT nošķiršana), daudzslāņu drošības pasākumi un daudzi citi pasākumi. Jāņem vērā, ka, no informācijas drošības skatpunkta raugoties, piemērotus drošības risinājumus var garantēt drošības domēni, kas īsteno tīkla un sistēmas nošķiršanu. Tomēr sistēmu operacionālajām vajadzībām (piem., apkalpošanas darbībām, datu pārsūtīšanai utt.) var būt nepieciešams apiet vai savienot dažādus drošības domēnus (piemēram, nošķirtas sistēmas un tīklus), arī savienot IT un OT.

Kiberdraudu atklāšana

Organizācijām vajadzētu nodrošināt, ka drošības pasākumu iedarbīgums saglabājas un ar tiem atklāj ar kiberdrošību saistītus notikumus, kuri ietekmē vai kuriem ir potenciāls ietekmēt drošības kontroli, kā arī svarīgus pakalpojumus un sistēmas. Kiberdraudu atklāšanai piemēroti drošības pasākumi:

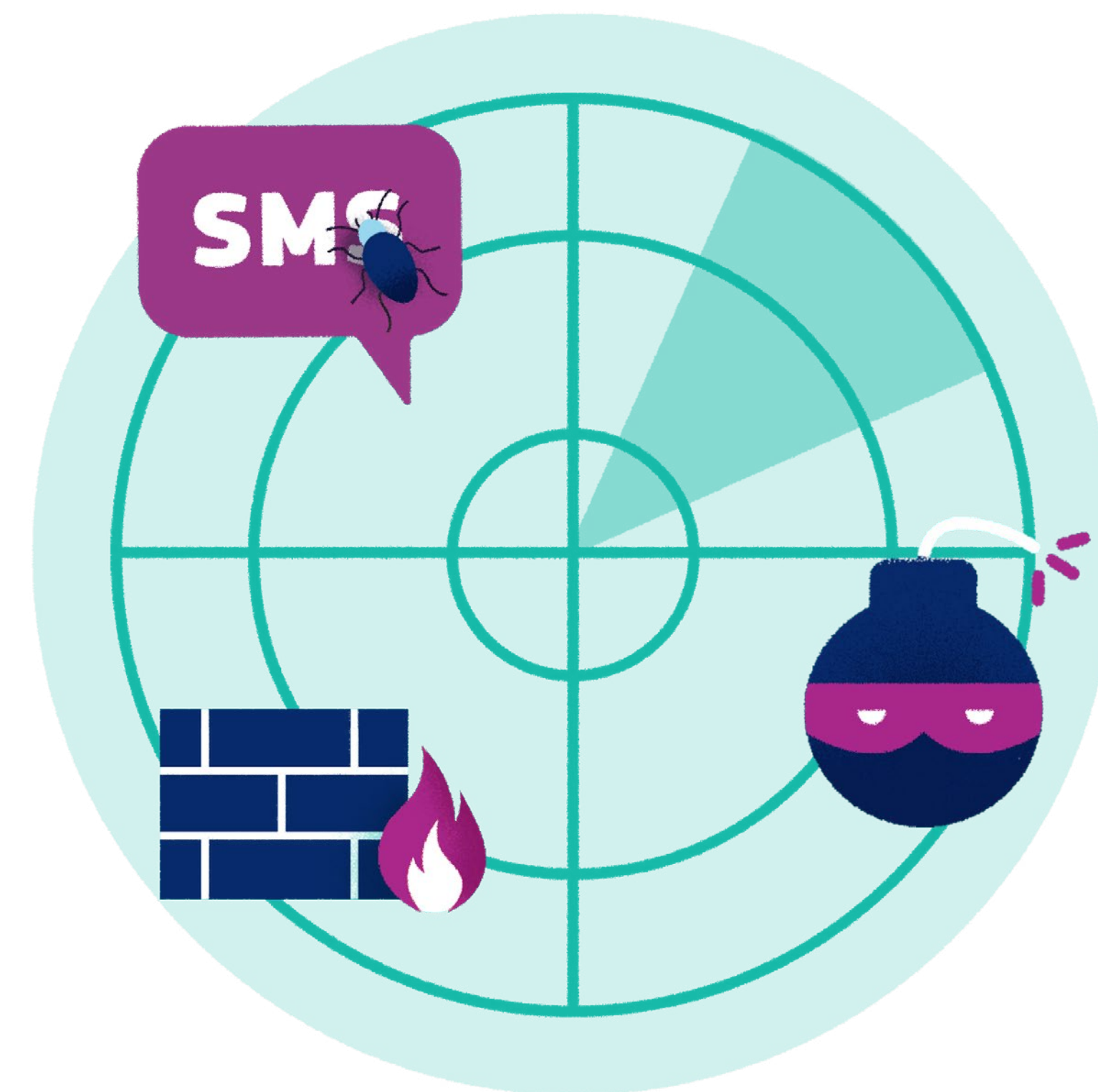
■ **drošības monitorings:** sauszemes transporta veidu pamatfunkciju darbību atbalstošo tīklu un informācijas sistēmu — arī informācijas tehnoloģiju (IT) un operacionālo tehnoloģiju (OT) — drošības statusa monitorings. Tas ir nepieciešams, lai atklātu potenciālus draudus drošībai un kontrolētu izmantoto aizsargājošo drošības pasākumu efektivitāti. Drošības monitoringa atbalstīšanas vajadzībām vērā ņemamie dati ir, piemēram:

- drošības žurnāli;
- datorvīrusu atklāšanas žurnāli;
- ielaušanās atklāšanas žurnāli;
- identifikācijas, autentifikācijas un autorizācijas žurnāli;
- sistēmas un pakalpojumu žurnāli;
- tīkla plūsmas žurnāli;
- datu apstrādes žurnāli.

■ **Ar drošību saistīto notikumu atklāšana:** tādu ļaunprātīgu darbību (t. i., ar drošību saistītu notikumu) atklāšana, kuras ietekmē vai kurām ir potenciāls ietekmēt pamatfunkciju darbību atbalstošo tīklu un informācijas sistēmu (arī IT un OT) drošību.

Šo pasākumu īstenošanai var būt nepieciešams ieviest specifiskas tehnoloģijas (piem., drošības informācijas un notikumu pārvaldību, ielaušanās atklāšanas sistēmu, ielaušanās novēršanas sistēmu utt.) un izveidot drošības operāciju centru (Security Operations Centre — SOC) vai ekvivalentus risinājumus. Citiem vārdiem sakot — jāizstrādā līdzekļi, ar kuru palīdzību ir iespējama kiberuzbrukumu lokāla atklāšana, analīze, kā arī reaģēšana uz kiberuzbrukumiem un darbības atjaunošana pēc kiberuzbrukumiem.

Nacionālās datordrošības incidentu reaģēšanas vienības (National Computer Security Incident Response Teams — CSIRT), sektorālās un komerciālas datorapdraudējumu reaģēšanas vienības (Computer Emergency Response Team — CERT) vai ceļu un dzelzceļa operatori un Eiropas Dzelzceļa informācijas apmaiņas un analīzes centrs (European Rail Information Sharing and Analysis Centre — ER-ISAC) var sniegt kiberdraudu izlūkdatumus (Cyber Threat Intelligence — CTI), informējot drošības monitoringa un draudu atklāšanas īstenotājus.



Reaģēšana un darbības atjaunošanas plānošana

Organizācijām būtu jādefinē, jāievieš un jātestē incidentu pārvaldības procedūras, kuras ir paredzētas pakalpojumu un sistēmu darbības nepārtrauktības nodrošināšanai kibernetiskās drošības incidentu gadījumā.

Reaģēšanas un darbības atjaunošanas plānošanā vajadzētu ņemt vērā drošības pasākumus, kas mazina specifisku kibernetiskās drošības ietekmi, piem.:

- *koordinācija un sadarbība ar nacionālajām datordrošības incidentu reaģēšanas vienībām (CSIRT), (publiskajām un komerciālajām) datorapdraudējumu reaģēšanas vienībām (CERT) un informācijas apmaiņas un analīzes centriem (ISAC) kibernetiskās drošības incidentu, incidentu koordinācijas un visas Eiropas līmeņa krīžu laikā.*

- *Informācijas apmaiņa ar citām organizācijām, to vidū sauszemes transporta pakalpojumu apgādes ķēdes pakalpojumu sniedzējiem*

- *Periodisku **kibernetiskās drošības mācību** īstenošana (teorētiskā, kā arī tehniskā koordinācija) ar mērķi novērtēt drošības pasākumus un procedūras, kā arī organizāciju noturību darbā ar kibernetiskās drošības incidentiem.*

- *Pieklūve arhīviem vai failu dublējumu glabāšanas vietām kompromitētas integritātes gadījumā un datu glabāšanas risinājumu pieejamība.*

- **Drošības shēmas** ar detalizētām procedūrām kibernetiskās drošības incidentu pārvaldībai un pakalpojumu un sistēmu atjaunošanai normālā operacionālā stāvoklī.

- *Tīkla plūsmas pārsūtīšana uz rezerves pakalpojumiem pakalpojumatteices uzbrukumu gadījumā.*

- *Manuālas procedūras darbam ar pakalpojumiem un sistēmām nepilnīgā operacionālajā režīmā.*

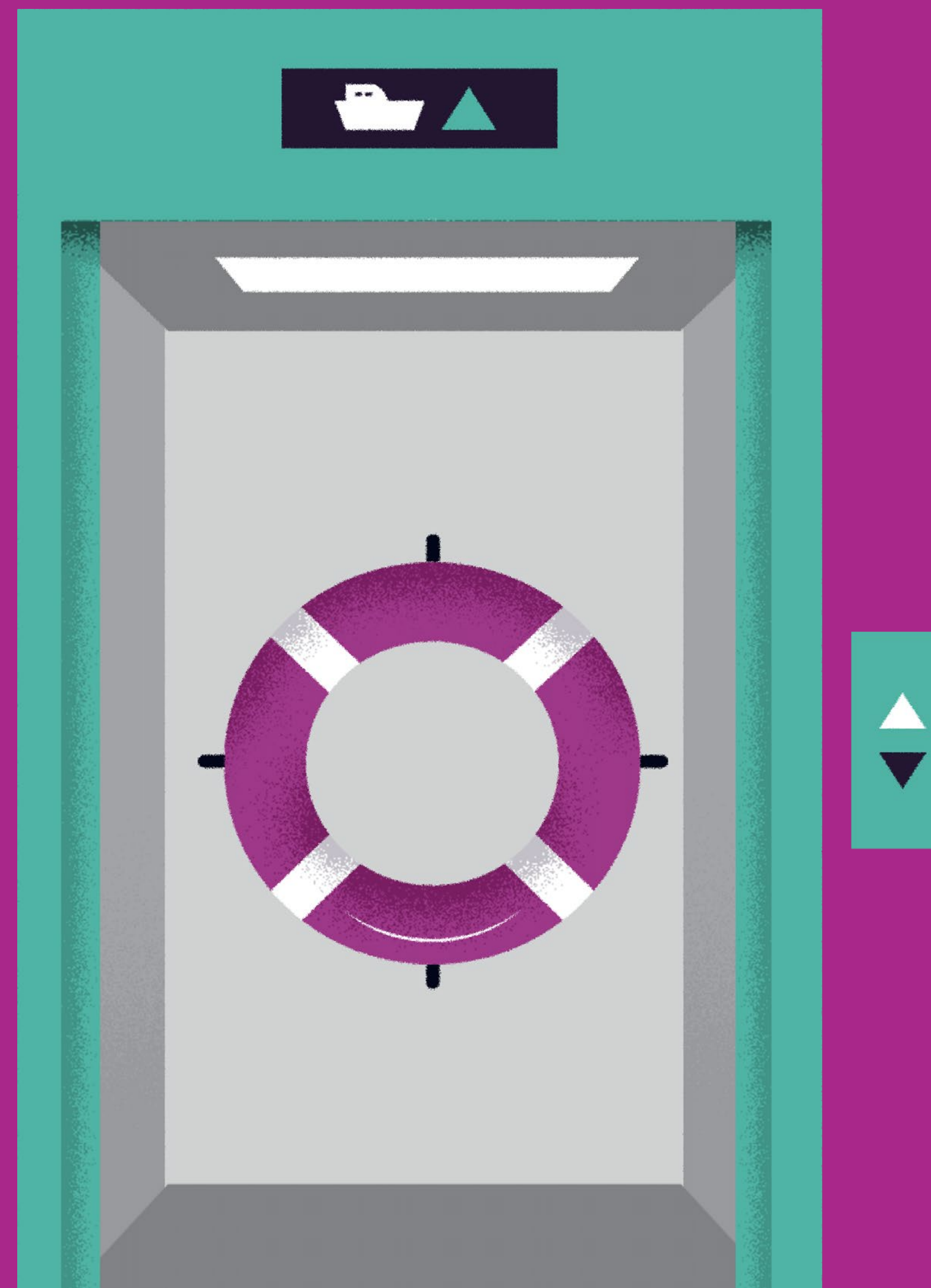
- *Tādu procedūru definēšana, kas paredzētas, lai risinātu datu aizsardzības pārkāpumus, to vidū procedūru definēšana darbam ar datu aizsardzības pārkāpumiem, kas ir saistīti ar persondatiem, atbilstoši Vispārīgajai datu aizsardzības regulai (VDAR) vai citai nozares regulai vai direktīvai.*

- **Kiberapdrošināšanas** iegāde ar mērķi daļēji mazināt ar smagiem kibernetiskās drošības incidentiem saistīto risku.

- *Līguma noslēgšana par reaģēšanu uz incidentiem ar vienu vai vairākiem specializētiem uzņēmumiem ar mērķi piesaistīt papildu spējas un speciālās zināšanas.*

- *Tādu procedūru definēšana, kurās ir noteikta ar kibernetiskās drošības incidentiem saistītas informācijas apmaiņa ar attiecīgajām ieinteresētajām personām, ietverot incidentu paziņošanas procedūras saskaņā ar NIS direktīvu (Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā).*

Labā prakse un
drošības pasākumi,
kas ir pielāgoti jūras
transportam



Pārvaldība

Jūras transporta organizācijām ir nepieciešama skaidra izpratne par jaunajiem draudiem, lai definētu pārvaldības politiku un procesus savu pieeju pārvaldībai ar mērķi uzlabot kiberdrošību operācijās izmantotajiem pakalpojumiem un sistēmām, arī informācijas tehnoloģijām (IT) un operacionālajām tehnoloģijām (OT).

Labā prakse jebkura lieluma organizācijām ietver šādas darbības:

- *nodrošināt, ka augstāko līmeņu vadība par bažām, kuras ir saistītas ar kiberdrošību, ziņo vadītājiem un valdēm, kas var pieņemt uz informāciju balstītus lēmumus par resursu piešķiršanu;*

- *iecelt atbildīgo personu, kurai ir vispārēji pārvaldības pienākumi attiecībā uz informācijas tehnoloģiju (IT) un operacionālo tehnoloģiju (OT) drošību. Šai personai jāatbild par kiberdrošību un fizisko drošību;*

- *skaidri noteikt lomas, atbildības, kompetences un pielāides attiecībā uz kiberdrošību, definēt pilnvaru līmeņus un sakaru kanālus starp krastā un uz kuģa strādājošo personālu, kā arī vienoties par viņiem ar attiecīgo personālu. Tas īpaši nepieciešams datorapdraudējumu reaģēšanas vienību (CERT) locekļiem. Personālam, kuru loma ir saistīta ar ES jūras drošības un drošuma tiesību aktiem, piemēram, par ostas iekārtu drošību atbildīgajām amatpersonām (Port Facility Security Officer), ostas drošības amatpersonām (Port Security Officers) vai uzņēmuma drošības amatpersonām (Company Security Officers), vai krastā izraudzītajai personai (Designated Person Ashore — DPA) un kuģa kapteinim (Master on board), būtu vismaz jāzina attiecīgās organizācijas kiberdrošības pasākumi;*

- *nodrošināt kiberdrošības pārvaldību visā drošības pakalpojumu ķēdē, ietverot gan fiziskas, gan digitālas saskarnes, sākot ar tehnoloģiju ražotājiem un instalētājiem un beidzot ar drošības pakalpojumu sniedzējiem;*

- *vienoties par pasākumiem un kontroli, arī dalīto atbildību, kiberdrošības risku pārvaldībai un nodrošināt, ka šī atbildība tiek uzturēta visa drošības risinājumu un pakalpojumu dzīves cikla laikā (piem., ar pakalpojumu līgumiem);*

- *definēt pārvaldības mehānismus (piem., politiku), lai izpildītu prasības, kas izriet no attiecīgajām regulām un direktīvām, piemēram, no Regulas (ES) 2019/1239 ar ko izveido Eiropas Jūras vienloga sistēmas vidi (EMSW), Regulas (EK) Nr. 725/2004 par kuģu un ostas iekārtu drošības pastiprināšanu, Direktīvas 2005/65/EK par ostu aizsardzības pastiprināšanu, Regulas (EK) Nr. 336/2006 par Starptautiskā drošības vadības (ISM) kodeksa īstenošanu un Rezolūcijas A.741 (18), ar ko pieņem ISM kodeksu drošai kuģu ekspluatācijai un piesārņojuma novēršanai. Šajā kontekstā ir svarīgi pieminēt arī vienoto informācijas apmaiņas vidi (CISE) — ES iniciatīvu, kuras mērķis ir padarīt Eiropas un dalībvalstu uzraudzības sistēmas sadarbspējīgas, lai nodrošinātu visām iesaistītajām iestādēm piekļuvi klasificētai un neklasificētai informācijai, kas tām ir nepieciešama misiju veikšanai jūrā.*

Jūras transporta pakalpojumu un sistēmu piemēri:

IT (informācijas tehnoloģiju) piemēri ir darbiniekiem pieejamie rīki (piem., personālie datori, mobilie tālruņi, biroja perifērijas ierīces utt.), kā arī pasažieriem pieejamie rīki (piem., publiskie *Wi-Fi* maršrutētāji un savienojumi utt.). OT piemēri ir uzraudzības kontroles un datu iegūšanas (*SCADA*) sistēmas, apkures, ventilācijas un gaisa kondicionēšanas (*HVAC*) sistēmas, globālās pozicionēšanas sistēmas (*GPS*), piekļuves kontrole, novērošana, pārraudzība, reaģēšana uz trauksmes signāliem, skrīninga tehnoloģija, borta navigācijas sistēmas, *SafeSeaNet*, tiltu sistēmas, kravu apstrādes un pārvaldības sistēmas, piedziņas, mašīnu pārvaldības un jaudas kontroles sistēmas, piekļuves kontroles sistēmas, pasažieru apkalpošanas un pārvaldības sistēmas, pasažieriem pieejamie publiskie tīkli, administratīvās un apkārtības labi iekārtotas sistēmas, sakaru sistēmas un citas sistēmas.



Kiberdraudu identificēšana

Riska pārvaldība: jūras organizācijām ir jāveic atbilstoši pasākumi, lai identificētu, analizētu, novērtētu un paziņotu kiberdraudu riskus un tos pieņemtu, novērstu, pārnestu vai mazinātu līdz pieņemamam līmenim. Tam ir nepieciešama visaptveroša organizatoriska pieeja riska pārvaldībai, un tas ietver šādus pasākumus:

- skaidra pārskata nodrošināšana par dažādajām aparatūras un programmatūras sistēmām, kuras izmanto dažādu pakalpojumu sniegšanai. Jūras transporta kontekstā šādas sistēmas ir saistītas ar informācijas tehnoloģijām (IT) un operacionālajām tehnoloģijām (OT), un to, kā šīs sistēmas ir savienojamas un integrējamās ar krastā esošajām sistēmām, to vidū tām, kuras izmanto publiskas iestādes, jūras termināļi un stividori.

- Galveno, pret kiberuzbrukumiem neaizsargāto kuģa borta operāciju identificēšana un novērtēšana un kiberdrošības risku novērtējumu veikšana (ieskaitot iespējamās ietekmes uz operacionālo darbību novērtēšanu un īstenošanās iespējamības novērtēšanu), kurā vajadzētu ņemt vērā

jaunos draudus, zināmās vājās vietas un operacionālos datus saistībā ar attiecīgajām sistēmām. Ja piemērojams, saiknes veidošana ar drošības novērtējumiem, kas ES jūras drošības tiesību aktu noteiktajā kārtībā ir veikti kuģiem (SSA), ostas iekārtām (PFSA) un ostām (PSA). Tajos ir identificēti iespējamie apdraudējumi ostas infrastruktūrai un vietas, kuru drošība ir pazemināta. Turklāt tādas jūrniecības organizācijas kā Starptautiskā jūrniecības organizācija (SJO) un jūras informācijas apmaiņas un analīzes centri (Information Sharing and Analysis Center — ISAC) var sniegt ieskatu par draudiem, kas ir vērsti uz jūras transportu.

- Ar personāla ikdienas darbībām (piem., sociālo mediju un personīgo ierīču lietošanu, datu apstrādi, informācijas apmaiņu utt.) saistīto risku ietveršana riska novērtējumā.

- Riska apstrādes pasākumu un kiberdrošības risku mazināšanas plānu identificēšana un ieviešana. Piemēram, ar citām pārvaldības sistēmām, piemēram, drošības pārvaldības sistēmām (Safety Management Systems — SMS), saskaņotas visaptverošas informācijas drošības pārvaldības

sistēmas (Information Security Management System — ISMS) un privātuma informācijas pārvaldības sistēmas (Privacy Information Management System — PIMS) ieviešana saskaņā ar Starptautisko drošības pārvaldības (International Safety Management — ISM) kodeksu. Šādas pārvaldības sistēmas (t. i., ISMS un PIMS) ietver drošības (kā arī datu aizsardzības un privātuma) pasākumu ieviešanu ar mērķi mazināt un novērst jaunos draudus, kas ietekmē jūras pakalpojumu un sistēmu (arī tajās esošo datu) drošību.

- Rēķināšanās ar visiem ierobežojumiem, kas ir saistīti ar **aktīvu pārvaldību un resursu plānošanu** (proti, ierobežojumiem, kas var ietekmēt jūras transporta pamatfunkciju darbībai kritiski svarīgo sistēmu piegādi, uzturēšanu un atbalstu). Novērtējam, ja iespējams, iekļaujiet mijnorādi uz ISM kodeksā, drošības pārvaldības sistēmās (SMS) un drošības plānos noteiktām prasībām un drošības plāniem, kas ir īstenoti saskaņā ar ES tiesību aktiem par drošumu un drošību jūrā.

Riska pārvaldības regulējumu piemēri: dažādi regulējumi (piem., *ISM* kodekss vai *ISO/IEC 27000* saimes standarti, *NIST* kiberdrošības regulējums, *MITRE ATT&CK* regulējums, *BSI IT-Grundschutz* utt.) var sniegt informāciju un dot pamatu pielāgotas riska pārvaldības pieejai jūras transportam. *NIST* kiberdrošības regulējums ir pielāgots arī jūras lielapjoma šķidrumu pārnesei (*Maritime Bulk Liquids Transfer — MBLT*), atkrastes operāciju un pasažieru kuģu operāciju kiberdrošības jautājumu risināšanai. Savukārt Baltijas un starptautiskā jūras padome (BSJP) ir izdevusi “Kuģu kiberdrošības pamatnostādnes” (“The Guidelines on Cyber Security Onboard Ships”) un Starptautiskā jūrniecības organizācija (SJO) ir izdevusi īpašu materiālu “Jūrniecības kiberrisku pārvaldības pamatnostādnes” (“Guidelines on maritime cyber risk management”) (MSC-FAL.1/Circ.3). *ENISA* ir veikusi vairākus pētījumus, kas ir bijuši saistīti ar jūrniecības, jo īpaši — ostu, kiberdrošības labo praksi. *EMSA* sniedz pakalpojumus jūrniecības kopienai, to vidū kiberdrošības izpratnes apmācību. Īpašas drošības un drošuma prasības jūras transporta sistēmām un tīkliem nosaka arī standarti (piem., *IEC 61162-460:2018* par jūras navigācijas un radiosakaru iekārtu un sistēmu drošumu un drošību, *ISO 16425:2013* par kuģiem un jūras tehnoloģijām, *IEC 62443-4-1:2018* par industriālās automatizācijas un vadības sistēmu drošību utt.).



Aizsardzība pret kiberdraudiem

Jūras transporta organizācijām vajadzētu ieviest atbilstošus un proporcionālus drošības pasākumus, lai aizsargātu savus tīklus un informācijas sistēmas — to vidū informācijas tehnoloģijas (IT) un operacionālās tehnoloģijas (OT). Drošības pasākumi ir:

■ **drošības politika un procesi:** tādas atbilstošas politikas un procesu definēšana, izpildīšana, paziņošana un ieviešana, kas nosaka vispārēju pieeju jūras transporta pamatfunkciju darbību atbalstošu sistēmu un datu nodrošināšanai. Drošības pasākumus (to vidū kiberdrošības un fiziskās drošības pasākumus) vajadzētu ietvert attiecīgajos plānos, piemēram drošības pārvaldības sistēmā (Safety Management System — SMS) un kuģa drošības plānā (Ship Security Plan — SSP). Šādai drošības politikai (piem., paroļu un datu glabāšanas politikai) un procedūrām jāaptver arī aparatūras un programmatūras sistēmu (to vidū IT un OT), incidentu pārvaldības, sistēmas un tīkla aizsardzības drošības ielāpu un vājo vietu pārvaldība.

■ **Identitātes un piekļuves pārvaldība:** jūras transporta pamatfunkciju darbību atbalstošu tīklu un informācijas

sistēmu (arī IT un OT) izprašana, dokumentēšana un piekļuves pārvaldīšana. Lietotāji (vai automatizētās funkcijas), kas var piekļūt datiem vai sistēmām, ir atbilstoši verificēti, autentificēti un autorizēti. Šajā pārvaldībā uzmanība būtu jāpievērš arī parasto un privilēģēto kontu dažādajām lomām un atbildībām.

■ **Datu un sistēmu drošība:** datu (saglabāto un elektroniski nosūtīto), kritiski svarīgo tīklu un informācijas sistēmu (to vidū IT un OT) aizsargāšana pret kiberuzbrukumiem. Ņemot vērā uz risku balstītu pieeju, organizācijām vajadzētu ieviest drošības pasākumus, lai efektīvi samazinātu uzbrucēju iespējas kompromitēt datus, tīklus un sistēmas. Šiem drošības pasākumiem vajadzētu ietvert arī šifrēšanas un drošu sakaru protokolu ieviešanu, kuras mērķis ir aizsargāt glabāšanā un tranzītā esošos datus pret kiberdraudiem, kuri rada pārtvērējuzbrukumus. Turklāt, lai aizsargātu piekļuvi sistēmām, šādi pasākumi jākombinē ar fiziskās drošības pasākumiem (piem., sistēmām vajadzētu būt uzstādītām norobežotās telpās ar ierobežotu piekļuvi). Tas ir ļoti svarīgi sistēmām, kas var ietekmēt dzīvības drošību

(piemēram, II un III kategorijas navigācijas un radiosakaru sistēmām).

■ **Tīklu un sistēmu noturība:** tīklu un sistēmu (to vidū IT un OT) noturības veidošana, izstrādājot un ieviešot tos (un to operacionālās procedūras) tādā veidā, lai pretotos kiberuzbrukumiem un mazinātu kiberuzbrukumu ietekmi. Noturību uzlabojoši izstrādes un ieviešanas risinājumu piemēri: oficiāli verificētas kritiski svarīgās funkcijas, sistēmu un tīklu dublēšana, tīklu nošķiršana (jo īpaši — IT un OT nošķiršana), daudzslāņu drošības pasākumi un daudzi citi pasākumi. Jāņem vērā, ka, no informācijas drošības skatpunkta raugoties, piemērotus drošības risinājumus var garantēt drošības domēni, kas īsteno tīkla un sistēmas nošķiršanu. Tomēr sistēmu (piem., Maritime Autonomous Surface Ships — MASS) vajadzībām (piem., apkalpošanas darbībām, datu pārsūtīšanai utt.) var būt nepieciešams apiet vai savienot dažādus drošības domēnus (piem., nošķirtas sistēmas un tīklus), arī savienot IT un OT.

Kiberdraudu atklāšana

Organizācijām vajadzētu nodrošināt, ka drošības pasākumu iedarbīgums saglabājas un ar tiem atklāj ar kiberdrošību saistītus notikumus, kuri ietekmē vai kuriem ir potenciāls ietekmēt drošības kontroli, kā arī svarīgus pakalpojumus un sistēmas. Kiberdraudu atklāšanai piemēroti drošības pasākumi:

■ **drošības monitorings:** jūras transporta pakalpojumu pamatfunkciju darbību atbalstošo tīklu un informācijas sistēmu — arī informācijas tehnoloģiju (IT) un operacionālo tehnoloģiju (OT) — drošības statusa monitorings. Tas ir nepieciešams, lai atklātu potenciālus draudus drošībai un kontrolētu izmantoto aizsargājošo drošības pasākumu efektivitāti. Drošības monitoringa atbalstīšanas vajadzībām vērā ņemamie dati ir, piemēram:

- drošības žurnāli;
- datorvīrusu atklāšanas žurnāli;

- ielaušanās atklāšanas žurnāli;
- identifikācijas, autentifikācijas un autorizācijas žurnāli;
- sistēmas un pakalpojumu žurnāli;
- tīkla plūsmas žurnāli;
- datu apstrādes žurnāli.

■ **Ar drošību saistīto notikumu atklāšana:** tādu ļaunprātīgu darbību (t. i., ar drošību saistītu notikumu) atklāšana, kuras ietekmē vai kurām ir potenciāls ietekmēt jūras transporta pakalpojumu pamatfunkciju darbību atbalstošo tīklu un informācijas sistēmu (arī IT un OT) drošību.

Šo pasākumu īstenošanai var būt nepieciešams ieviest specifiskas tehnoloģijas (piem., drošības informācijas un notikumu pārvaldību, ielaušanās atklāšanas sistēmu, ielaušanās novēršanas sistēmu utt.) un izveidot drošības operāciju centru (*Security Operations Centre — SOC*) vai

ekvivalentus risinājumus. Citiem vārdiem sakot — jāizstrādā līdzekļi, ar kuru palīdzību ir iespējama kiberuzbrukumu lokāla atklāšana, analīze, kā arī reaģēšana uz kiberuzbrukumiem un darbības atjaunošana pēc kiberuzbrukumiem.

Nacionālās datordrošības incidentu reaģēšanas vienības (*National Computer Security Incident Response Teams — CSIRT*), sektorālās datorapdraudējumu reaģēšanas vienības (*Computer Emergency Response Team — CERT*) un komerciālās jūras operatoru datorapdraudējumu reaģēšanas vienības (*Computer Emergency Response Team — CERT*), jūras informācijas apmaiņas un analīzes centri (*Information Sharing and Analysis Center — ISAC*) var sniegt kiberdraudu izlūkdatumus (*Cyber Threat Intelligence — CTI*), informējot drošības monitoringa un draudu atklāšanas īstenotājus.

Reaģēšana un darbības atjaunošanas plānošana

Organizācijām būtu jādefinē, jāievieš un jātestē incidentu pārvaldības procedūras, kuras ir paredzētas pakalpojumu un sistēmu darbības nepārtrauktības nodrošināšanai kibernetiskās drošības incidentu gadījumā.

Reaģēšanas un darbības atjaunošanas plānošanā vajadzētu ņemt vērā drošības pasākumus, kas mazina specifisku kibernetiskās drošības ietekmi, piem.:

- *tīkla plūsmas pārsūtīšana uz rezerves pakalpojumiem pakalpojumatteices uzbrukumu gadījumā.*
- *Manuālas procedūras darbam ar pakalpojumiem un sistēmām nepilnīgā operacionālajā režīmā.*
- *Praktisko vingrinājumu un apmācību programmu izveidošana (piemēram, teorētiskā koordinācija, tehniskie un reaģēšanas praktiskie vingrinājumi) ar mērķi reaģēt uz kibernetiskās drošības incidentiem un ārkārtas situācijām, kā arī novērtēt drošības pasākumus, procedūras un organizatorisko noturību darbā ar kibernetiskās drošības incidentiem.*

■ *Piekļuve arhīviem vai failu dublējumu glabāšanas vietām kompromitētas integritātes gadījumā un datu glabāšanas risinājumu pieejamība.*

■ *Koordinācija un sadarbība ar nacionālajām datordrošības incidentu reaģēšanas vienībām (CSIRT), (publiskajām un komerciālajām) datorapdraudējumu reaģēšanas vienībām (CERT) un informācijas apmaiņas un analīzes centriem (ISAC) kibernetiskās drošības incidentu, incidentu koordinācijas un visas Eiropas līmeņa krīžu laikā.*

■ *Informācijas apmaiņa ar citām organizācijām, to vidū jūras transporta apgādes ķēdes pakalpojumu sniedzējiem.*

■ *Drošības shēmas ar detalizētām procedūrām kibernetiskās drošības incidentu pārvaldībai un pakalpojumu un sistēmu atjaunošanai normālā operacionālā stāvoklī.*

■ *Tādu procedūru definēšana, kas paredzētas, lai risinātu datu aizsardzības pārkāpumus, to vidū procedūru definēšana*

darbam ar datu aizsardzības pārkāpumiem, kas ir saistīti ar persondatiem, atbilstoši Vispārīgajai datu aizsardzības regulai (VDAR) vai citai nozares regulai vai direktīvai.

■ *Kiberapdrošināšanas iegāde ar mērķi daļēji mazināt ar smagiem kibernetiskās drošības incidentiem saistīto risku.*

■ *Līguma noslēgšana par reaģēšanu uz incidentiem ar vienu vai vairākiem specializētiem uzņēmumiem ar mērķi piesaistīt papildu spējas un speciālās zināšanas.*

■ *Tādu procedūru definēšana, kurās ir noteikta ar kibernetiskās drošības incidentiem (to vidū neatbilstībām, negadījumiem un bīstamām situācijām) saistītas informācijas apmaiņa ar attiecīgajām ieinteresētajām personām, ietverot incidentu paziņošanas procedūras saskaņā ar NIS direktīvu (Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā).*

Par šajā ziņojumā izklāstīto informāciju un pausto viedokli atbild vienīgi autors(-i), un to nevar uzskatīt par Eiropas Komisijas oficiālo viedokli. Eiropas Komisija negarantē šajā ziņojumā iekļauto datu precizitāti. Ne Eiropas Komisija, ne personas, kuras rīkojas Komisijas vārdā, neatbild par to, kā tiek izmantota šajā ziņojumā iekļautā informācija.

Luksemburga: Eiropas Savienības Publikāciju birojs, 2021

© Eiropas Savienība, 2021

Atļauts izmantot citur, norādot avotu un nemainot dokumentu satura sākotnējo nozīmi. Eiropas Komisija nav atbildīga par jebkādām šīs publikācijas atkalizmantošanas sekām. Eiropas Komisijas dokumentu atkalizmantošanas politiku īsteno, pamatojoties uz Komisijas Lēmumu 2011/833/ES (2011. gada 12. decembris) par Komisijas dokumentu atkalizmantošanu (OV L 330, 14.12.2011., 39. lpp.).

Tādu elementu izmantošanai vai reproducēšanai, kuri nepieder Eiropas Savienībai, var būt jāsaņem atļauja tieši no attiecīgajiem tiesību turētājiem.

Print	ISBN 978-92-76-40474-3	doi:10.2832/45163	MI-05-21-230-LV-C
PDF	ISBN 978-92-76-40490-3	doi:10.2832/272058	MI-05-21-230-LV-N



Eiropas Savienības
Publikāciju birojs