Euroopa Komisjon

Transpordialase küberturvalisuse töövahend

Sissejuhatus

Euroopa Komisjoni liikuvuse ja transpordi peadirektoraat (DG MOVE) on sõlminud lepingu selle töövahendi väljatöötamiseks, et suurendada transpordivaldkonna sidusrühmade küberohtudealast teadlikkust ja valmisolekut. See aitab mõista küberohte ja leevendada nende mõju. Töövahend sisaldab kaht teadlikkuse tõstmise strateegiat, mis on ette nähtud eri profiilidele:

- kõik transporditöötajad (üldteabe ja suuniste andmine);
- Küberturvalisusealaste otsuste tegijad transpordi valdkonnas.

Hüperlingid ühendavad tööriista eri osi, et hõlbustada nende vahel liikumist.

Käesolevas töövahendis loetletud tavad on üksnes nõuandva iseloomuga. Ükski pakutud soovitus ei ole siduv ega kohustuslik. Lisaks ei kajasta käesolev töövahend Euroopa Komisjoni ametlikke seisukohti ning selle eesmärk ei ole tutvustada vahendeid praeguste või tulevaste ELi õigusaktide järgimiseks.

Küberturvalisusealase teadlikkuse profiilid

Profiil 1: kõik transporditöötajad. Esimene strateegia on suunatud kõigile transpordiorganisatsioonide töötajatele. See annab teavet, et paremini mõista kõige levinumaid küberohte transpordi valdkonnas. Lisaks annab see teavet, kuidas tulla toime võimalike küberohtudega, sealhulgas neid tuvastada, neist teatada ja küberturvalisusealaste heade tavade abil nende mõju leevendada.

Profiil 2: Küberturvalisusealaste otsuste tegijad transpordi valdkonnas. Teine strateegia on suunatud töötajatele, kes vastutavad transpordiorganisatsioonide küberturvalisusealaste otsuste tegemise eest. Selles strateegias tõstetakse esile eri transpordiliikidele kohandatud häid tavasid. Eelkõige tutvustatakse selles häid tavasid transpordiorganisatsioonide vastu suunatud uute küberohtude tuvastamiseks, nende eest kaitsmiseks, nende avastamiseks ja neile reageerimiseks.

Euroopa Komisjon

Transpordialase küberturvalisuse töövahend

Transpordivaldkonna ohtude maastik

Eri transpordiliike mõjutavad uued küberohud

Küberturvalisusealase teadlikkuse profiilid

Alternatiivsed küberturvalisusealase teadlikkuse suurendamise strateegiad, mis on ette nähtud transpordivaldkonna eri profiilidele

Euroopa Komisjon

Transpordi-valdkonna ohtude maastik

Küberohtude maastik on dünaamiline ja areneb pidevalt. Siiski on võimalik kindlaks teha küberohud, millega puutuvad kokku kõik transpordiliigid.

Euroopa Komisjon

Ohusubjektid

Isikud või organisatsioonid, kes võivad mõjutada transporditeenuste ja -süsteemide ohutust ning turvalisust

Uued küberohud

Valitud küberohud, mis võivad mõjutada transporditeenuste ja -süsteemide ohutust ning julgeolekut

Euroopa Komisjon

Ohusubjektid

Isikud või organisatsioonid võivad tahtlikult või tahtmatult paljastada ja ära kasutada nõrkusi, mis võivad põhjustada intsidente ja mõjutada transporditeenuseid, sealhulgas nende ohutust, turvalisust, äritegevust, rahastamist ja mainet.

Kõige olulisemad transpordiorganisatsioone tahtlikult ründavad pahatahtlikud ohusubjektid on **küberkurjategijad**, **insaiderid**, **rahvusriigid** ja **riiklikult toetatavad rühmitused**.
Sellised vastased nagu **küberkurjategijad** viivad läbi ulatuslikke ründekampaaniaid ja teevad seda sageli raha eest.

Insaiderid tunnevad nende organisatsioonide eripärasid, kelle heaks nad töötavad, ning on sageli teadlikud väikestest turvanõrkustest. Insaideriteks võivad olla rahulolematud töötajad, tarnijad ja konkreetsed töövõtjad.
Globaalsete geopoliitiliste pingete süvenedes on **rahvusriigid** ja **riiklikult toetatavad rühmitused** seadnud endale pikaajalised strateegilised eesmärgid. Nad püüavad ennast sageli varjata sügaval organisatsioonide süsteemides ja tundlikku teavet koguda. Kui riiklikult toetatavad ründajad on ennast süsteemidesse sisse seadnud, otsivad nad olukorda, mis suudaks tekitada suurima võimaliku kahju.

Mittepahatahtlikud osalejad on **insaiderid**, kes võivad tahtmatult või juhuslikult teha toiminguid, mille tulemuseks on küberturbesündmused ja halvimal juhul küberintsidendid.

Euroopa Komisjon

Uued küberohud

Transpordivaldkonda ähvardavad mitmesugused küberohud: **hajus teenusetõkestus**, **teenusetõkestus**, andmevargus, **pahavara** levitamine, **andmepüük**, tarkvara mõjutamine, **loata juurdepääs**, kahjustavad ründed, turvaettevõtja otsustusprotsessi võltsimine või sellest möödaminek, identiteedi varjamine, juurdepääsu eelisõiguste kuritarvitamine, **sotsiaalne manipulatsioon**, veebisaitide sodimine, pealtkuulamine, varade väärkasutus ja riistvara mõjutamine.
Üldsusele kättesaadavate dokumentide ja ekspertidega tehtud intervjuude põhjalikule uurimisele tuginedes on kõige pakilisemad transporti mõjutavad uued küberohud järgmised: pahavara, (hajutatud) teenusetõkestus, loata juurdepääs ja vargus ning tarkvara mõjutamine.

Euroopa Komisjon

Oht #1: pahavara

Pahatahtlik tarkvara, mis võib mõjutada üksikisikuid või organisatsioone eri transpordiliikide lõikes

Oht #2: (Hajus) teenuse-tõkestus

Küberründed, mis takistavad üksikisikute või organisatsioonide juurdepääsu asjaomastele transporditeenustele ja -ressurssidele

Oht #3: loata juurdepääs ja vargus

Loata juurdepääs kriitilise tähtsusega varale, selle omastamine ja kasutamine

Oht #4: tarkvara mõjutamine

Tarkvara vastu suunatud küberründed, mille eesmärk on selle käitumist muuta ja konkreetseid ründeid toime panna

Oht #1: pahavara

Pahavara koosneb pahatahtlikust tarkvarast, mis võib hõlmata eri liiki tarkvararakendusi, nagu viirused, Trooja hobused, ussviirused, lunavara, krüptorahakaevurid, või mis tahes tarkvarast, millel võib olla kahjulik mõju organisatsioonidele või üksikisikutele eri transpordiliikide lõikes.

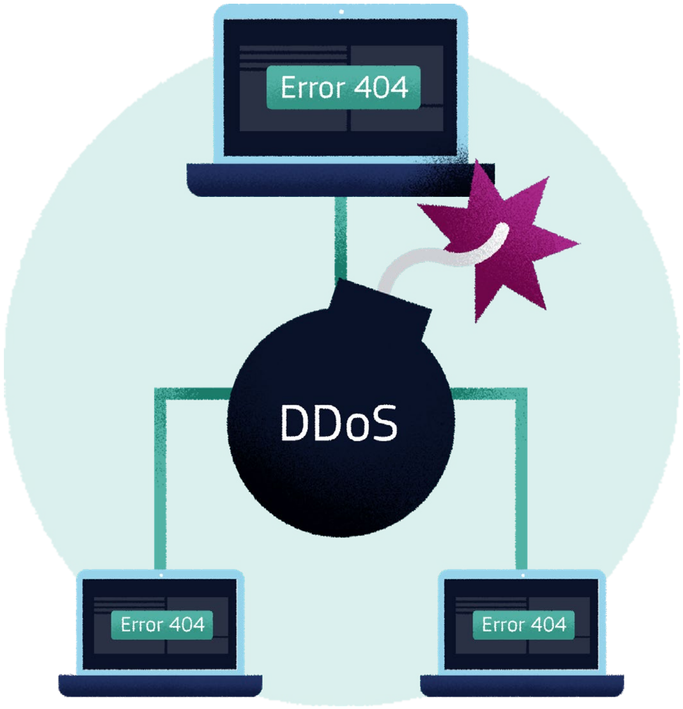
Arvutite, serverite, klientide, võrkude või kõigi nende tahtlikuks kahjustamiseks loodud pahavara leviku piiramine on kõigi transpordiliikide küberturvalisuse peamiste prioriteetide hulgas. Tüüpiline ründevektor võib hõlmata töötajatele suunatud andmepüügi e-kirju. Muud ründevektorid võivad hõlmata erinevaid ja keerukaid sotsiaalse manipulatsiooni strateegiaid, nagu USB-seadme ühendamine vabasse porti (nt mobiiltelefoni laadimine). Kahtlaste e-kirjade hüperlinkidel klõpsates või manustatud faile avades võib kasutaja enese teadmata installida pahavara.

Näiteks mõjutas WannaCry lunavara küberrünne rohkem kui 150 riiki ja nakatas üle 230 000 süsteemi. Ründeks kasutati lunavara, mis tavaliselt levib pahatahtlikke manuseid või hüperlinke sisaldavate andmepüügi e-kirjade kaudu. Seda tüüpi ründed kasutavad sotsiaalset manipulatsiooni, et pahatahtlikult panna süsteemi kasutajaid konkreetset pahavara installima (või aktiveerima).

Oht #2: (hajus) teenusetõkestus

Teenusetõkestusründed ja hajusad teenusetõkestusründed mõjutavad andmete, teenuste, süsteemide ja muude ressursside kättesaadavust ja juurdepääsetavust. Seda liiki ründed võivad olla eri kestusega ja olla suunatud korraga rohkem kui ühe teenuse või süsteemi vastu. Hajusate teenusetõkestusrünnete puhul kasutatakse mitut süsteemi (või ründekanalit), et sihtteenuseid või süsteeme päringutega üle koormata. Edukad ründed mõjutavad teenuste ja süsteemide suutlikkust tulla toime päringute ootamatult suurenenud mahuga. See tõkestab juurdepääsu teenustele ja ressurssidele.

Arvestada tuleb sellega, et transpordiorganisatsioonidele kuuluvaid kahjustatud teenuste ja süsteemide abil on võimalik korraldada teenusetõkestusründeid ja hajusaid teenusetõkestusründeid konkreetsete käitatavate süsteemide või teiste organisatsioonide vastu.
Nii võidakse sihtmärgiks võtta ettevõtte infosüsteemid (näiteks personaalarvutid ja -seadmed), et saada juurdepääs käidutehnoloogiale, mis võib olla ühendatud internetti või millel võib käitamisandmete edastamiseks olla juurdepääs võrkudele. Eri süsteemide ja võrkude vahelised ühendused (nt ettevõtete sisevõrgud, käidutehnoloogia ja kaughoolduse juurdepääsud) võivad kujutada endast nõrkusi, mida saab kasutada teenusetõkestusrünnete või hajusate teenusetõkestusrünnete tegemiseks kriitilise tähtsusega transporditeenustele ja -süsteemidele. Nii saab teenusetõkestusrünnete ja hajusate teenusetõkestus-rünnetega kasutada ära ühiseid võrgu- ning sideprotokolle, näiteks veebiteenuste dünaamilist tuvastust (WS-Discovery), mida esemevõrguseadmed võivad kasutada kohtvõrgu (LAN) kõigi sõlmede automaatseks avastamiseks. Kui esemevõrguseadmetel on nõrku kohti, võivad ründajad neid ära kasutada, et muid ühendatud seadmeid leida ja teenusetõkestusründeid või hajusaid teenusetõkestusründeid teha.



Oht #3: loata juurdepääs ja vargus

Ohusubjektid võivad soovida saada võrgule, süsteemile, rakendusele, andmetele või muule ressursile loogilist või füüsilist loata juurdepääsu, et viia läbi pahatahtlikku tegevust, sealhulgas tundlike andmete või ressursside (ka füüsiliste ressursside) vargust. Loata juurdepääs ja vargus võivad ohustada konfidentsiaalset ja ärisaladusena käsitatavat vara (sealhulgas isikusamasus, eeliskontode pääsumandaadid ja süsteemid ning muud liiki konfidentsiaalne ja ärisaladusena käsitatav teave). Nende ohtudega on võimalik kasutada ära süsteemide nõrkusi ning isikuid, kes avaldavad pahaaimamatult tundlikke andmeid, näiteks pääsumandaate (nt kasutajatunnus, salasõna jne) või isikuandmeid (nt e-post, isikukood jne).

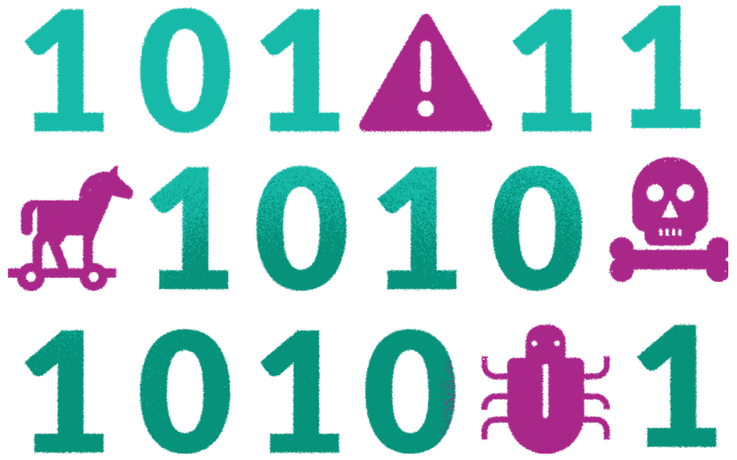
Loata juurdepääsu puhul on identiteedivargus isikuandmete või kordumatute tunnuste ebaseaduslik kasutamine isikute või teenuste ja süsteemide matkimiseks, et saada juurdepääs isiklikele või ärisaladusena käsitletavatele ressurssidele (nt rahalised ja füüsilised ressursid). Sellised küberohud võivad olla suunatud ka füüsilisele varale eri transpordiliikide lõikes.

Euroopa Komisjon

Oht #4: tarkvara mõjutamine

Tarkvara ja sellega seotud süsteemide või komponentide vääral konfigureerimisel ja nende mõjutamisel võib olla otsene mõju transporditeenuste ja -süsteemide turvalisusele. Tarkvara mõjutamist kasutavad küberründed muudavad tarkvaraseadeid või mõjutavad andmeterviklust, et muuta süsteemide ja teenuste käitumist. Ründajad võivad tahtlikult tarkvara (või selle osa) mõjutada, et tundlikest varadest kasu saada (nt loata juurdepääsu saamine, seaduslike isikute või süsteemide juurdepääsu tõkestamine vajalikele ressurssidele, tundliku teabe kogumine, funktsionaalse käitumise muutmine jne).

Näiteks võivad ründajad võtta sihikule tootjate sidekanalid, et käitatavatele teenustele ja süsteemidele (sealhulgas käidutehnoloogiale) pahatahtlikke uuendusi üles laadida. Ohusubjekt kasutab turvatud kaughooldusvõrgu liidesele juurdepääsuks rikutud pääsumandaati, et mõjutatud tarkvara installida ning muid juurdepääsetavaid teenuseid ja süsteeme ohtu seada. Ohusubjekt installib mõjutatud tarkvara, mis sihtteenuseid ja -süsteeme veelgi ohtu seab, või ründab muid ühendatud teenuseid või süsteeme.



Euroopa Komisjon

Küberturvalisusealase teadlikkuse profiilid

Euroopa Komisjon

1

Profiil 1: kõik transporditöötajad

Esimene strateegia on suunatud kõigile transpordiorganisatsioonide töötajatele alates käitamisega seotud personalist kuni haldustöötajateni. Selles strateegias antakse suuniseid kõige levinumate küberohtude paremaks mõistmiseks ja teadvustamiseks. Lisaks annab see teavet, kuidas tulla toime võimalike küberohtudega, sealhulgas neid tuvastada, neist teatada ja nende mõju leevendada. See strateegia on ühine kõikidele transpordiliikidele.

2

Profiil 2: Küberturvalisusealaste otsuste tegijad transpordi valdkonnas

Teine strateegia on suunatud töötajatele, kes vastutavad transpordiorganisatsioonide turvalisuse- või küberturvalisusealaste otsuste tegemise eest. Selles strateegias tutvustatakse häid tavasid, mis on kohandatud eri transpordiliikidele. Siin tutvustatakse häid tavasid transpordiorganisatsioonide vastu suunatud uute küberohtude tuvastamiseks, nende eest kaitsmiseks, nende avastamiseks ja neile reageerimiseks.

Euroopa Komisjon

Profiil 1: kõik transporditöötajad

See osa on mõeldud kõigile transpordiorganisatsioonide töötajatele alates käitamisega seotud personalist kuni haldustöötajateni. Selles antakse suuniseid kõige levinumate küberohtude paremaks mõistmiseks ja teadvustamiseks. Lisaks annab see teavet, kuidas tulla toime võimalike küberohtudega, sealhulgas neid tuvastada, neist teatada ja nende mõju leevendada. Selles osas tutvustatakse soovituslikke tavasid ja kasulikke nõuandeid, mis on asjakohased **kõigi transpordiliikide** puhul.

Euroopa Komisjon

Pahavaravastane hea tava

Saate aidata oma organisatsiooni kaitsta, järgides **pahavara tuvastamise ja levitamise ärahoidmise** häid tavasid, näiteks:

- ***järgige turvapõhimõtteid**, nagu salvestiste ja failide skannimine viiruste leidmiseks, teatavat liiki failide (nt selliste täitmisfailide nagu .exe, .bat, .com jne) avamise ja e-postiga saatmise vältimine, ainult volitatud tarkvara installimine, tarkvara (sealhulgas viirusetõrje) ajakohasuse ja nõuetekohase toimimise tagamine ning muud põhimõtted;*

- ***varundage oma andmeid** korrapäraselt turvalistes (ja volitatud) andmesalvestites või -teenustes, mis peaksid toetama krüpteerimismehhanisme, et andmeid jõudeolekus kaitsta ja tagada, et need oleksid taastamiseks kättesaadavad;*

- *kaitske **sobivate turvameetmetega** (nt salasõna, krüpteerimine jne) kõiki süsteeme, sealhulgas mobiilseid ja lõppseadmeid, ning lukustage turvaliselt kõik süsteemid (füüsiliselt ja digitaalselt), kui neid ei kasutata;*

- *vältige kummalise kehateksti või tundmatutelt saatjatelt ja tundmatutest internetidomeenidest pärinevates ootamatutes e-kirjades ja kahtlastes veebibrauseri hüpikakendes sisalduvate manuste avamist ja neis sisalduvatel hüperlinkidel klõpsamist;*

- *vältige oma arvutisse **ebausaldusväärsete või tundmatute irdseadmete**, näiteks mälupulkade, kõvaketaste ja muude salvestite sisestamist;*

- *vältige pahavaravastaste turvameetmete (nt viirusetõrjetarkvara, infosisu filtreerimise tarkvara, tulemüüri jne) desaktiveerimist;*

- ***ajakohastage installitud tarkvara** korrapäraselt uusimate kättesaadavate versioonideni (mida infoturbeametnikud või süsteemihaldurid võivad korrapäraste uuendustega väljastada);*

- *vältige eelisõigusega (nt halduri tasandi) kontode ja pääsumandaatide kasutamist tavapärasteks tegevusteks ja toiminguteks;*

- *teatage infoturbeametnikele või süsteemihalduritele igast kahtlasest e-kirjast või süsteemi ootamatust käitumisest.*

- *Keskenduge igapäevases rutiinses töös infoturbele, et IT-turvalisuse probleeme ära tunda ja neile vastavalt reageerida.*

(Hajusa) teenusetõkestuse vastased head tavad

Saate aidata kaitsta oma organisatsiooni, kui tuvastate **teenusetõkestusründed** ja **hajusad teenusetõkestusründed**. Peaksite viivitamata võtma ühendust oma turva- ja IT-üksustega, kui avastate või kogete oma teenuste või süsteemide puhul järgmisi võimaliku toimuva teenusetõkestusründe või hajusa teenusetõkestusründe tunnuseid:

- *päringute arvu suurenemine ammendab võrgu läbilaskevõime (seda tajutakse aeglase teenuse ja reageerimisena), mille tulemuseks on ülekoormusest tingitud teenuse- või süsteemirikked;*
- *selge põhjuseta kasvanud nõudlus mäluressursside kasutamise järele;*
- ***teenuste ja süsteemide ootamatu käitumine**, sagedased krahhid ja kummalised veateated, mis tulenevad arvutusressursside või võrguühenduste pahatahtlikust tarbimisest;*
- *seadmete **halvenenud toimivus**, lihtsate ülesannete pikad täitmisajad ja märgatav tegevus (nt ventilaator teeb häält, kui seade töötab aeglaselt);*
- ***katkendlik internetiühendus või ühenduse kadu** teenuste ja süsteemidega;*
- *vaevumärgatavad käitumuslikud muutused juhtseadises või käidutehnoloogiates, mis põhjustavad füüsilisi kahjustusi.*
- *Juurdepääsu keelamine eelis- või halduskontodele, millega takistatakse intsidentidele reageerimise protseduuride taastumist.*

Loata juurdepääsu ja varguse vastased head tavad

Et hoida ära loata juurdepääsu ja vargusega seotud ründeid, tuleb järgida selliseid põhimõtteid nagu „teadmisvajadus“ ning „vaikimisi turvalisus ja privaatsus“, millega rõhutatakse, et juurdepääs tundlikele ja konfidentsiaalsetele varadele (sealhulgas isikuandmed ja tundlikud andmed, transpordisüsteemid jne) peaks olema ainult neil, kellel on õigus nendega oma ülesannete täitmiseks tutvuda. Saate aidata oma organisatsiooni kaitsta, järgides loata juurdepääsu ja varguse tuvastamise ja ärahoidmise häid tavasid, näiteks:

- *järgige organisatsiooni turvapõhimõtteid;*

- *vältige veebipõhiste pääsumandaatide ja isikuandmete, sealhulgas sellist teavet sisaldada võivate piltide jagamist ja avaldamist;*

- *vältige pääsumandaatide ja isikuandmete (ja muude tundlike andmete) kasutamist või edastamist ebausaldusväärsetes ning ebaturvalistes võrkudes, seadmetes või veebiteenustes (nt veebisaidid, kus kasutatakse ebaturvalisi protokolle või http://-aadresse turvaliste https://-aadresside asemel);*

- ***ärge kunagi avaldage kellelegi oma pääsumandaate** (nt kasutajatunnus ja salasõna) isegi e-posti või telefoni teel;*

- *kaitske volitamata isikute eest klaviatuuriga sisestatud või ekraanil (sh mobiilseadmetel) kuvatavaid tundlikke andmeid, paigaldage ekraanifilter, vältige isiklike seadmetega töötamist avalikes kohtades ning mis tahes seadme lukustamata ja järelevalveta jätmist;*

- ***kasutage keerukaid salasõnu** (nt tähtnumbrilistest ja erimärkidest koosnev piisavalt pikk salasõna), mis vastavad asjaomastele organisatsiooni turvapõhimõtetele, et vältida loata juurdepääsu;*

- ***muutke** ühendatud süsteemide ja seadmete (nt printerid, ruuterid, kaamerad, nutilukud jne) **vaikeparoole**;*

- *vältige samade pääsumandaatide (nt kasutajatunnus ja salasõna) kasutamist mitme teenuse ja süsteemi puhul ning samade pääsumandaatide kasutamist teenuste ja süsteemide puhul, mis nõuavad eeliskontosid;*

- *saatke edastatud kaitstud failide (nt ZIP-arhiivide) jaoks paroolid ja võtmed ainult lisakanali kaudu (nt GSMi kaudu saadetav SMS või telefonikõne), mitte kunagi e-posti teel;*

- ***aktiveerige** võimaluse korral **kaksik- (2FA)** või mitmikautentimine (MFA).*

Euroopa Komisjon

Tarkvara mõjutamise vastased head tavad

Saate aidata oma organisatsiooni kaitsta, kui järgite tarkvara mõjutamise tuvastamise ja ärahoidmise häid tavasid, näiteks:

- *vältige ebausaldusväärse tarkvara installimist süsteemidesse ja seadmetesse (sealhulgas personaalarvutitesse, serveritesse, välisseadmetesse, võrguseadmetesse, nutitelefonidesse jne);*
- *installige ainult tarkvara ja uuendusi, mis on pärit ametlikest allikatest ja ametlikelt veebisaitidelt (nt tootjad, ettevõtte andmehoidlad jne);*
- *vältige tarkvara ja rakenduste (ning mis tahes failide) allalaadimist ebaseaduslikest allikatest;*
- *desinstallige ebavajalik või mõnda aega kasutamata tarkvara ning blokeerige ebavajalikud ühendused (nt võrguprotokollid ja -teenused), sealhulgas juurdepääs kaugteenustele (nt pilvsalvestusteenused);*
- *skannige tarkvara ja salvestusseadmeid usaldusväärse ja ajakohastatud viirusetõrjetarkvaraga;*
- *laadige alla ohutut äritarkvara (nt uuendused, paigad, uued tooted jne) usaldusväärsetelt tarnijatelt nn valge jaama põhimõtet kasutades;*
- *ajakohastage kogu installitud tarkvara kooskõlas organisatsiooni põhimõtete ja tavadega.*

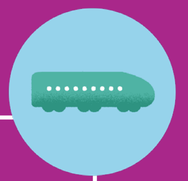
Euroopa Komisjon

Profiil 2: Küberturvalisusealaste otsuste tegijad transpordi valdkonnas

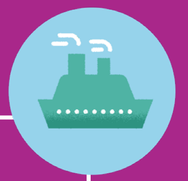
See osa on mõeldud töötajatele, kes vastutavad transpordiorganisatsioonides turvalisuse- või küberturvalisusealaste otsuste tegemise eest. Selles strateegias tõstetakse esile eri transpordiliikidele kohandatud häid tavasid. Eelkõige tutvustatakse siin häid tavasid uute küberohtude tuvastamiseks, nende eest kaitsmiseks, nende avastamiseks ja neile reageerimiseks.

Euroopa Komisjon

Lennutranspordile kohandatud küberturvalisuse head tavad



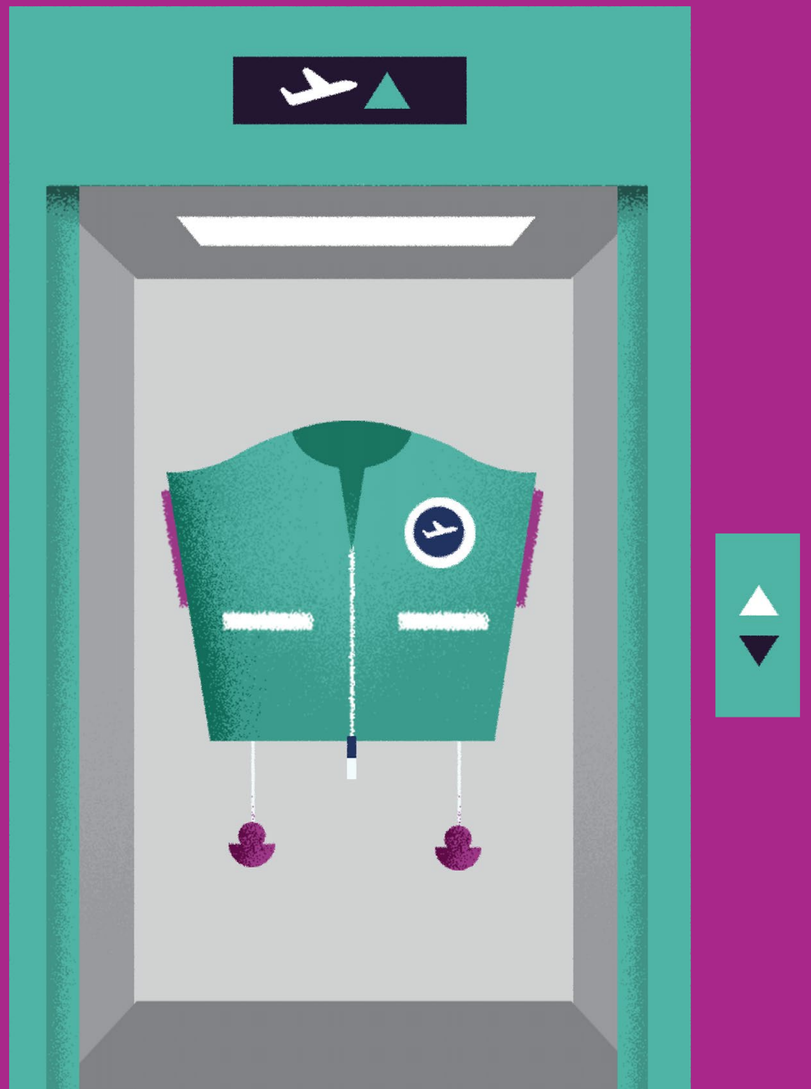
Maismaa-transpordile kohandatud küberturvalisuse head tavad



Meretranspordile kohandatud küberturvalisuse head tavad

Euroopa Komisjon

Lennutranspordile kohandatud head tavad ja turvameetmed



Euroopa Komisjon

Juhtimine

Lennundusorganisatsioonid vajavad selget arusaama uutest ohtudest, et määrata kindlaks oma lähenemisviisidega seotud juhtimispõhimõtted ja -protsessid ning suurendada teenuste ja kasutatavate süsteemide, sealhulgas info- ning käidutehnoloogia küberturvalisust.

Head tavad hõlmavad mis tahes suurusega organisatsiooni puhul järgmist:

- tagada, et kõrgema juhtkonna tasandid teavitavad küberturvalisusega seotud probleemidest juhte ja juhatust, kes saavad teha teadlikke otsuseid vahendite eraldamise kohta;

- määrata kõrgema juhtkonna liige, kes vastutab küberturvalisuse ja füüsilise julgeoleku eest ning üldiselt info- ja käidutehnoloogia turvalisuse haldamise eest, kuid kes huvide konflikti vältimiseks ise tegevuses ei osale;

- määrata kindlaks selged küberturvalisusega seotud rollid, vastutusalad, pädevused ja load ning sel teemal suhelda ja kokku leppida asjaomaste töötajate, eelkõige infoturbeintsidentidega tegelevate rühmade (CERTide) liikmetega;

- tagada küberturvalisuse juhtimine kogu turbealases tarne- ja teenusteahelas, sealhulgas nii füüsiliste kui ka digiliideste puhul, alates tehnoloogia tootjatest ning paigaldajatest kuni turvateenuste osutajateni;

- leppida küberturvalisuse riskide juhtimiseks kokku tegevuses ja kontrollides, sealhulgas jagatud vastutuses, ning tagada, et need kohustused säilivad kogu turbelahenduste ja -teenuste kasutusaja jooksul (nt teenuslepingute abil);

- määrata kindlaks juhtimismehhanismid (nt -põhimõtted), et täita kohustusi, mis tulenevad asjaomastest määrustest ja direktiividest, näiteks määrusest (EL) 2018/1139, mis käsitleb tsiviillennunduse valdkonna ühisnorme, ja komisjoni rakendusmäärusest (EL) 2017/373, millega sätestatakse lennuliikluse korraldamise teenuste ja aeronavigatsiooniteenuste osutajate ning muude lennuliikluse korraldamise võrgustiku funktsioonide suhtes ja kõigi nende järelevalve suhtes kohaldatavad ühisnõuded, ning küberturvalisuse direktiivist (ELi direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase).

Lennutranspordi teenuste ja süsteemide näited.
Infotehnoloogia näited on sellised, mis on kättesaadavad töötajatele (nt personaalarvutid, mobiiltelefonid, kontori välisseadmed jne) või reisijatele (nt avalikud WiFi-ruuterid ja -ühendused jne). Käidutehnoloogia näited on superviisorjuhtimis- ja andmehõivesüsteemid, kütte-, ventilatsiooni- ja kliimasüsteemid, käsipagasi kontrollpunktid julgestuspiirangualal, pagasikäitlemise süsteemid, juurdepääsukontroll, seire, järelevalve, häirele reageerimine, läbivaatustehnoloogia, lennuvälja valgustuse juhtimissüsteemid, radarisüsteemid ja andurid, globaalse asukoha määramise süsteemid, lennuliikluse korraldamise süsteemid, side-, navigatsiooni- ja seiresüsteemid, lennunduse infosüsteemid, meteoroloogilised süsteemid, turbekeskuse süsteemid, lennuettevõtja pardasüsteemid ja muud.

Küberohtude tuvastamine

Riskijuhtimine. Lennundusorganisatsioonid peavad võtma asjakohaseid meetmeid, et teha kindlaks, hinnata ja mõista küberturvalisuse riske võrgu- ja infosüsteemidele, mis toetavad põhifunktsioonide täitmist.

Selleks on vaja organisatsiooni üldist riskijuhtimise lähenemisviisi, mis hõlmab järgmist:

- *selge ülevaate tagamine eri teenuste osutamiseks kasutatavatest riist- ja tarkvarasüsteemidest. Lennunduses hõlmavad sellised süsteemid nii info- kui ka käidutehnoloogiat;*

- ***küberturvalisuse riskide hindamine**, milles võetakse arvesse uusi ohte, teadaolevaid nõrkusi ja käiduandmeid, mis on seotud kohaldamisalas olevate süsteemidega. Sellised organisatsioonid nagu Euroopa lennuliikluse korraldamise infoturbeintsidentidega tegelev rühm (EATM-CERT) ning lennundusteabe jagamise ja analüüsimise keskus (A-ISAC) võivad anda teavet lennutranspordi vastu suunatud ohtude kohta;*

- *tagamine, et riskihindamine hõlmaks ka riske, mis on seotud töötajate igapäevase tegevusega (nt sotsiaalmeedia kasutamine, isiklike seadmete kasutamine, andmetöötlus, teabe jagamine jne);*

- *riskijuhtimismeetmete ja küberturvalisuse riskide maandamise kavade koostamine ja rakendamine;*

- *ulatusliku **infoturbe haldussüsteemi** ja **eraelu puutumatust käsitleva teabe haldussüsteemi** rakendamine kooskõlas teiste haldussüsteemidega. Sellised haldussüsteemid (s.o infoturbe haldussüsteem ja eraelu puutumatust käsitleva teabe haldussüsteem) hõlmavad turvakontrollide (samuti andmekaitse ja eraelu puutumatuse kontrollide) rakendamist, et leevendada ja ennetada lennuteenuste ja -süsteemide (sh nende andmete) turvalisust mõjutavaid uusi ohte;*

- ***varahalduse ja ressursiplaneerimisega** seotud piirangute (st piirangud, mis võivad mõjutada lennutranspordi oluliste funktsioonide toimimiseks vajalike kriitilise tähtsusega süsteemide tarnimist, hooldamist ja toetamist) arvessevõtmine.*

Riskijuhtimisraamistike näited. Eri raamistikud (nt ISO/IEC 27000 standardisari, NISTi küberturvalisuse raamistik, MITRE ATT&CK raamistik, BSI IT-Grundschutz jne) võivad anda teavet ja toetada kohandatud riskijuhtimist lennutranspordi valdkonnas. Rahvusvahelised organisatsioonid, nagu Rahvusvaheline Lennutranspordi Assotsiatsioon (IATA) ja Rahvusvaheline Tsiviillennunduse Organisatsioon (ICAO), annavad suuniseid küberturvalisuse riskide hindamiseks. ENISA, EASA, EUROCONTROL ja Rahvusvaheline Lennujaamade Nõukogu (ACI) toovad muu hulgas esile lennujaamade turvamise, lennuliikluse korraldamise teenuseosutajate ja muude lennundusorganisatsioonide head tavad. Ühisettevõte SESAR koordineerib ja koondab kogu ELi lennuliikluse korraldamise alase teadus- ja arendustegevuse, mis hõlmab ka ohutuse ja turvalisuse aspekte.

Kaitse küberohtude eest

Lennutranspordiorganisatsioonid peaksid rakendama piisavaid ja proportsionaalseid turvameetmeid, et oma võrke ja infosüsteeme, sealhulgas info- ning käidutehnoloogiat, küberrünnete eest kaitsta. Need turvameetmed on muu hulgas alljärgnevad.

- ***Turvalisuse põhimõtted ja protsessid.*** *Määrata kindlaks, rakendada, edastada ja jõustada asjakohased põhimõtted ja protsessid, millega määratakse üldine lähenemisviis lennunduses oluliste ülesannete täitmist toetavate süsteemide ning andmete turvalisuse tagamiseks. Sellised turvapõhimõtted (nt salasõna- ja andmetalletuspõhimõtted) ja menetlused peaksid hõlmama ka riist- ning tarkvarasüsteemide (sealhulgas info- ja käidutehnoloogia) paikasid ja nõrkusehaldust, intsidendihaldust, süsteemi- ning võrgukaitset.*

- ***Identiteedi- ja pääsuhaldus.*** *Mõista, dokumenteerida ja hallata lennutranspordi põhifunktsioonide toimimist toetavate võrkude ja infosüsteemide (sealhulgas info- ja käidutehnoloogia) kättesaadavust. Kasutajad (või automatiseeritud funktsioonid), kellel (millel) on juurdepääs andmetele või süsteemidele, on nõuetekohaselt kontrollitud, autenditud ja volitatud. Seejuures tuleks arvesse võtta ka tava- ja eeliskontode eri rolle ning kohustusi.*

- ***Andmete ja süsteemi kaitse.*** *Kaitsta andmeid (elektrooniliselt salvestatud ja edastatud), kriitilise tähtsusega võrke ja infosüsteeme (sh info- ja käidutehnoloogia) küberrünnete eest. Riskipõhist lähenemisviisi arvesse võttes peaksid organisatsioonid rakendama turvameetmeid, et tõhusalt piirata ründaja võimalusi andmeid, võrke ja süsteeme ohtu seada. Need turvameetmed peaksid hõlmama ka krüpteerimise ja turvaliste sideprotokollide kasutuselevõtmist, et kaitsta jõudeolekus ja edastatavaid andmeid vahendusrünnet põhjustavate küberohtude eest. Selliseid meetmeid tuleb rakendada koos füüsiliste turvameetmetega, et kaitsta juurdepääsu süsteemidele (nt süsteemid peaksid asuma piiratud juurdepääsuga suletud ruumides).*

- ***Võrkude ja süsteemide vastupidavus.*** *Suurendada võrkude ja süsteemide (sealhulgas info- ja käidutehnoloogia) kavandamise ja rakendamise kaudu nende (ja nende käidukorra) vastupidavusvõimet, et seista vastu küberrünnete mõjule ja seda leevendada. Vastupidavusvõimet suurendavate disaini- ja rakenduslahenduste näited on järgmised: ametlikult kontrollitud kriitilise tähtsusega funktsioonid, süsteemide ja võrkude liiasus, võrkude lahusus (eelkõige info- ja käidutehnoloogia lahusus), mitmekihilised turvameetmed ning paljud muud. Arvestada tuleb sellega, et infoturbe seisukohast võivad sobivaid turvalahendusi pakkuda võrgu ja süsteemi lahusust rakendavad turvavaldkonnad. Süsteemide käiduvajadused (nt hooldus, andmeedastus jne) võivad siiski nõuda eri turvavaldkondadest möödahiilimist või nende ühendamist (nt lahutatud süsteemid ja võrgud), sealhulgas info- ja käidutehnoloogia ühendamist.*

Euroopa Komisjon

Küberohtude tuvastamine

Organisatsioonid peaksid tagama, et turvameetmed on jätkuvalt tõhusad, ning avastama mis tahes küberturvalisuse sündmused, mis mõjutavad või võivad mõjutada turvakontrolli meetmeid ning olulisi teenuseid ja süsteeme. Küberohtude avastamiseks on asjakohased alljärgnevad turvameetmed.

■ ***Turvaseire.*** *Lennutranspordi põhifunktsioonide täitmist toetavate võrkude ja infosüsteemide, sh info- ning käidutehnoloogia turvalisuse seire. Turvaseire toetamiseks võetakse arvesse näiteks järgmisi andmeid:*

- *turvalogid*
- *viirustuvastuslogid*
- *sissetungituvastuslogid*
- *identimis-, autentimis- ja autoriseerimislogid*
- *süsteemi- ja teenuslogid*
- *võrguliikluslogid*
- *andmetöötluslogid*

■ ***Turvasündmuse avastamine.*** *Selliste pahatahtlike tegevuste (st turvasündmuste) avastamine, mis mõjutavad või võivad mõjutada lennutranspordi põhifunktsioonide täitmist toetavate võrkude ja infosüsteemide (sealhulgas info- ja käidutehnoloogia) turvalisust.*

Need meetmed võivad nõuda eritehnoloogiate (nt turvateabe ja -sündmuste halduse, sissetungituvastussüsteemi, sissetungitõrjesüsteemi jne) kasutuselevõtmist ning infoturbekeskuse või samaväärse keskuse loomist. See tähendab vahendite väljatöötamist küberrünnete avastamiseks, analüüsimiseks, neile reageerimiseks ja nendest taastumiseks kohalikul tasandil.

Riiklikud küberturbe intsidentide lahendamise üksused (CSIRTid), valdkondlikud CERTid (nt EUROCONTROLi Euroopa lennuliikluse korraldamise infoturbeintsidentidega tegelev rühm EATM-CERT), lennuettevõtjate kommerts-CERTid ning lennundusteabe jagamise ja analüüsimise keskus (A-ISAC) võivad pakkuda küberohtudealast luureteavet, mis võimaldab turvaseiret ja avastamist.

Euroopa Komisjon

Reageerimis- ja taastemeetmete kavandamine

Organisatsioonid peaksid kindlaks määrama, rakendama ja testima intsidendihaldusmenetlusi, mille eesmärk on tagada teenuste ja süsteemide talitluspidevus küberintsidentide korral. Leevendusmeetmete eesmärk on kontrollida või piirata küberintsidentide mõju.

Reageerimis- ja taastamismeetmete kavandamisel tuleks arvesse võtta turvameetmeid, mis leevendavad konkreetsete küberrünnete mõju, näiteks:

- *koordineerida riiklikke CSIRTe, (avalik-õiguslikke ja kommerts-) CERTe ning teabe jagamise ja analüüsimise keskusi (ISACe) ning teha nendega koostööd küberintsidentide korral ja koordineerida intsidente ning kriise üleeuroopalisel tasandil;*

- *jagada teavet teiste organisatsioonidega, sealhulgas lennuteenuste tarneahelasse kuuluvate teenuseosutajatega;*

- *korraldada korrapäraseid **küberründeõppusi** (lauaõppus ja tehniline õppus), et hinnata turvameetmeid ja -menetlusi ning organisatsiooni vastupidavusvõimet küberintsidentidega toimetulekuks;*

- *tagada juurdepääs arhiveeritud või varundatud andmete asukohale juhuks, kui andmesalvestite terviklus ja kättesaadavus on ohus;*

- *koostada **turbejuhendid** koos üksikasjalike menetlustega küberintsidentide ohjamiseks ning teenuste ja süsteemide viimiseks tavapärastesse käidutingimustesse;*

- *suunata teenusetõkestusrünnete ajal võrguliiklus ümber liiastele teenustele;*

- *tagada käsijuhtimisega menetlused teenuste ja süsteemide käitamiseks halvenenud käidutingimustes;*

- *määrata kindlaks menetlused andmetega seotud rikkumiste käsitlemiseks, sealhulgas menetlused isikuandmetega seotud rikkumiste käsitlemiseks kooskõlas isikuandmete kaitse üldmääruse ja muude asjakohaste valdkondlike määruste või direktiividega;*

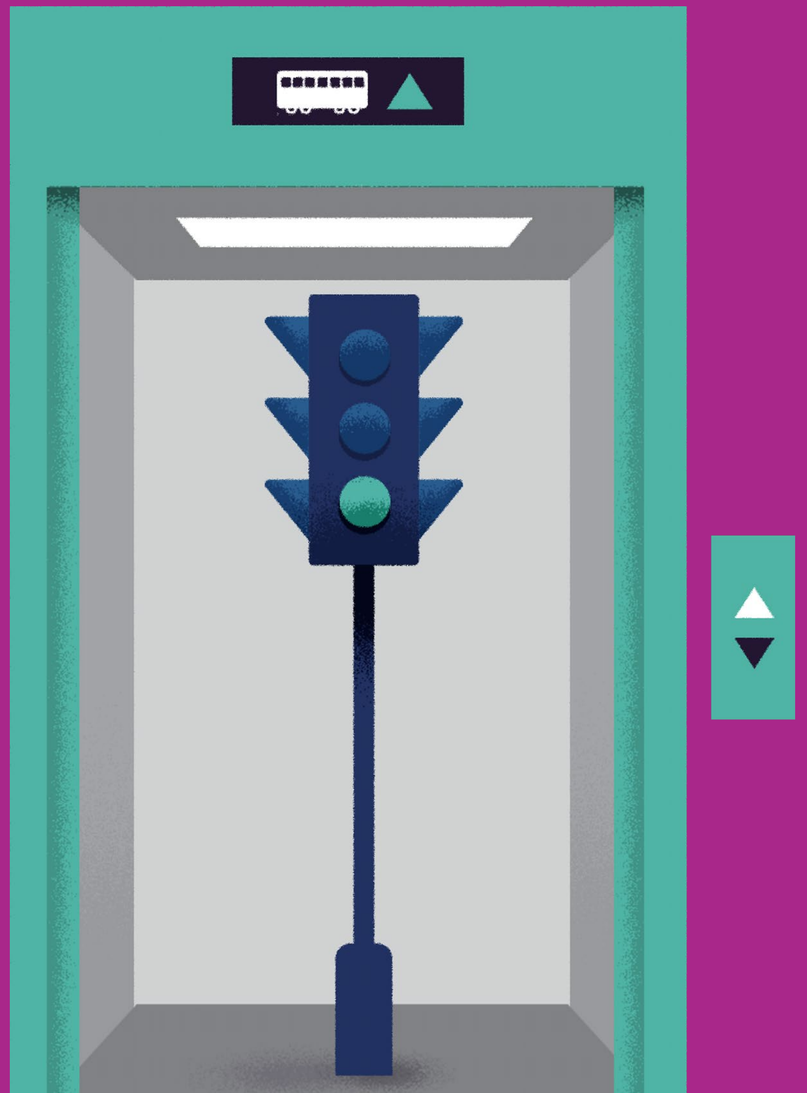
- *sõlmida **küberkindlustusleping**, et osaliselt tasakaalustada tõsiste küberintsidentidega seotud riski;*

- *sõlmida intsidentidele reageerimise leping ühe või mitme spetsialiseerunud ettevõtjaga, kellel on lisavõimekus ja -teadmised;*

- *määrata kindlaks menetlused **küberintsidentidest teatamiseks** asjaomastele sidusrühmadele, sealhulgas intsidentidest teatamise kord kooskõlas küberturvalisuse direktiiviga (direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus).*

Euroopa Komisjon

Maismaatranspordile kohandatud head tavad ja turvameetmed



Euroopa Komisjon

Juhtimine

Maismaatranspordi (raudtee- ja maanteetranspordi) organisatsioonid vajavad selget arusaama uutest ohtudest, et määrata kindlaks oma lähenemisviisidega seotud juhtimispõhimõtted ja -protsessid ning suurendada teenuste ja kasutatavate süsteemide, sealhulgas info- ning käidutehnoloogia küberturvalisust.

Head tavad hõlmavad mis tahes suurusega organisatsiooni puhul järgmist:

- *tagada, et kõrgema juhtkonna tasandid teavitavad küberturvalisusega seotud probleemidest juhte ja juhatust, kes saavad teha teadlikke otsuseid vahendite eraldamise kohta;*

- *määrata kõrgema juhtkonna liige, kes vastutab küberturvalisuse ja füüsilise julgeoleku eest ning üldiselt info- ja käidutehnoloogia turvalisuse haldamise eest, kuid kes huvide konflikti vältimiseks ise tegevuses ei osale;*

- *määrata kindlaks selged küberturvalisusega seotud rollid, vastutusalad, pädevused ja load ning sel teemal suhelda ja kokku leppida asjaomaste töötajatega. See on vajalik eelkõige infoturbeintsidentidega tegelevate rühmade (CERTide) liikmete jaoks;*

- *tagada küberturvalisuse juhtimine kogu turbealases tarne- ja teenusteahelas, sealhulgas nii füüsiliste kui ka digiliideste puhul, alates tehnoloogia tootjatest ning paigaldajatest kuni turvateenuste osutajateni;*

- *leppida küberturvalisuse riskide juhtimiseks kokku tegevuses ja kontrollides, sealhulgas jagatud vastutuses, ning tagada, et need kohustused säilivad kogu turbelahenduste ja -teenuste kasutusaja jooksul (nt teenuslepingute abil);*

- *määrata kindlaks juhtimismehhanismid (nt -põhimõtted), et täita asjaomastest määrustest ja direktiividest tulenevaid kohustusi. Selle alla kuulub suur hulk poliitikameetmeid, mis hõlmavad konkreetseid transpordiliike, eri liiki sidusrühmi (sealhulgas näiteks sõidukite ja raudteesüsteemide tootjad) ning küberturvalisuse direktiivi (direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase).*

Maismaatranspordi teenuste ja süsteemide näited. Infotehnoloogia näited on sellised, mis on kättesaadavad töötajatele (nt personaalarvutid, mobiiltelefonid, kontori välisseadmed jne) või reisijatele (nt avalikud WiFi-ruuterid ja -ühendused jne). Käidutehnoloogia näited on superviisorjuhtimis- ja andmehõivesüsteemid, kütte-, ventilatsiooni- ja kliimasüsteemid, globaalse asukoha määramise süsteemid, juurdepääsukontroll, seire, järelevalve, häirele reageerimine ja läbivaatustehnoloogia. Raudteetranspordi erisüsteemid on näiteks: käidu- (juhtkäskude süsteemid), sealhulgas signaalimissüsteemid, Euroopa raudteeliikluse juhtimissüsteem (ERTMS), rongisisesed süsteemid, hooldussüsteemid ja muu.

Euroopa Komisjon

Küberohtude tuvastamine

Riskijuhtimine. Maismaatranspordi organisatsioonid peavad võtma asjakohaseid meetmeid, et teha kindlaks, hinnata ja mõista küberturvalisuse riske võrgu- ning infosüsteemidele, mis toetavad põhifunktsioonide täitmist. Selleks on vaja organisatsiooni üldist riskijuhtimise lähenemisviisi, mis hõlmab järgmist:

- *selge ülevaate tagamine eri teenuste osutamiseks kasutatavatest riist- ja tarkvarasüsteemidest. Maismaatranspordi puhul hõlmavad sellised süsteemid nii info- kui ka käidutehnoloogiat;*

- ***küberturvalisuse riskide hindamine**, milles tuleks arvesse võtta uusi ohte, teadaolevaid nõrkusi ja käiduandmeid seoses kohaldamisalas olevate süsteemidega. Maismaatranspordi süsteemide näited on järgmised: maksesüsteemid, võrgu- ja sidesüsteemid (nt internet, raadioside, WiFi jne), sõiduki seadmestik, käitamise juhtimiskeskused, identiteedihaldussüsteemid, ohutussüsteemid ja muu. Raudteetaristu puhul on süsteemide näited järgmised: veerem, käitamise ja liikluskorralduse allsüsteemid, juhtkäskude ja signaalimise rongisisesed ning raudteeäärsed allsüsteemid ja muu;*

- *tagamine, et riskihindamine hõlmaks ka riske, mis on seotud töötajate igapäevase tegevusega (nt sotsiaalmeedia kasutamine, isiklike seadmete kasutamine, andmetöötlus, teabe jagamine jne);*

- *riskijuhtimismeetmete ja küberturvalisuse riskide maandamise kavade koostamine ja rakendamine. Näiteks ulatusliku **infoturbe haldussüsteemi** ja **eraelu puutumatust käsitleva teabe haldussüsteemi** rakendamine kooskõlas teiste haldussüsteemidega. Sellised haldussüsteemid (s.o infoturbe haldussüsteem ja eraelu puutumatust käsitleva teabe haldussüsteem) hõlmavad turvakontrollide- (samuti andmekaitse ja eraelu puutumatuse kontrollide) rakendamist, et leevendada ja ennetada maismaatranspordi teenuste ja -süsteemide (sh nende andmete) turvalisust mõjutavaid uusi ohte;*

- *mis tahes piirangute arvessevõtmine, mis on seotud **varahalduse ja ressursiplaneerimisega** (st piirangud, mis võivad mõjutada maismaatranspordi oluliste funktsioonide toimimiseks vajalike kriitilise tähtsusega süsteemide tarnimist, hooldamist ja toetamist).*

Riskijuhtimisraamistike näited. Eri raamistikud (nt ISO/IEC 27000 standardisari, NISTi küberturvalisuse raamistik, MITRE ATT&CK raamistik, BSI IT-Grundschutz jne) võivad anda teavet ja toetada kohandatud riskijuhtimist maismaa-ning raudteetranspordi valdkonnas. Sellised organisatsioonid nagu ENISA määratlevad nutiautode ja aruka ühistranspordi küberturvalisuse head tavad, millest saavad lähtuda valdkonna tootjad ja ühendused (nt Euroopa Autotootjate Ühendus). Raudteetranspordi valdkonnas määrab Euroopa Liidu Raudteeamet (ERA) kindlaks koostalitluse tehnilised kirjeldused, millele iga allsüsteem või allsüsteemi osa peab vastama, et täita olulisi nõudeid ja tagada Euroopa Liidu raudteesüsteemi koostalitlusvõime. Ühisettevõte Shift2Rail edendab ka innovatsioonialgatusi (sealhulgas küberturvalisuse alal) ja projekte raudteetranspordi valdkonnas.

Kaitse küberohtude eest

Maismaatranspordiorganisatsioonid peaksid rakendama piisavaid ja proportsionaalseid turvameetmeid, et oma võrke ja infosüsteeme, sealhulgas info- ning käidutehnoloogiat, küberrünnete eest kaitsta. Need turvameetmed on muu hulgas alljärgnevad.

- ***Turvalisuse põhimõtted ja protsessid.*** *Määrata kindlaks, rakendada, edastada ja jõustada asjakohased põhimõtted ja protsessid, millega määratakse üldine lähenemisviis maismaatranspordi oluliste ülesannete täitmist toetavate süsteemide ja andmete turvalisuse tagamiseks. Sellised turvapõhimõtted (nt salasõna- ja andmetalletuspõhimõtted) ja menetlused peaksid hõlmama ka riist- ning tarkvarasüsteemide (sealhulgas info- ja käidutehnoloogia) paikasid ja nõrkusehaldust, intsidendihaldust, süsteemi- ning võrgukaitset.*

- ***Identiteedi- ja pääsuhaldus.*** *Mõista, dokumenteerida ja hallata maismaatranspordi põhifunktsioonide toimimist toetavate võrkude ja infosüsteemide (sealhulgas info- ja käidutehnoloogia) kättesaadavust. Kasutajad (või automatiseeritud funktsioonid), kellel (millel) on juurdepääs andmetele või süsteemidele, on nõuetekohaselt kontrollitud, autenditud ja volitatud. Seejuures tuleks arvesse võtta ka tava- ja eeliskontode eri rolle ning kohustusi.*

- ***Andmete ja süsteemi kaitse.*** *Kaitsta andmeid (elektrooniliselt salvestatud ja edastatud), kriitilise tähtsusega võrke ning infosüsteeme (sh info- ja käidutehnoloogia) küberrünnete eest. Riskipõhist lähenemisviisi arvesse võttes peaksid organisatsioonid rakendama turvameetmeid, et tõhusalt piirata ründaja võimalusi andmeid, võrke ja süsteeme ohtu seada. Need turvameetmed peaksid hõlmama ka krüpteerimise ja turvaliste sideprotokollide kasutuselevõtmist, et kaitsta jõudeolekus ja edastatavaid andmeid vahendusrünnet põhjustavate küberohtude eest. Selliseid meetmeid tuleb rakendada koos füüsiliste turvameetmetega, et kaitsta süsteemidele juurdepääsu (nt süsteemid peaksid asuma piiratud juurdepääsuga suletud ruumides). See on väga oluline nende süsteemide puhul, mis võivad mõjutada inimelude ohutust.*

- ***Võrkude ja süsteemide vastupidavus.*** *Suurendada võrkude ja süsteemide (sealhulgas info- ja käidutehnoloogia) kavandamise ja rakendamise kaudu nende (ja nende käidukorra) vastupidavusvõimet, et seista vastu küberrünnete mõjule ja seda leevendada. Vastupidavusvõimet suurendavate disaini- ja rakenduslahenduste näited on järgmised: ametlikult kontrollitud kriitilise tähtsusega funktsioonid, süsteemide ja võrkude liiasus, võrkude lahusus (eelkõige info- ja käidutehnoloogia lahusus), mitmekihilised turvameetmed ning paljud muud. Arvestada tuleb sellega, et infoturbe seisukohast võivad sobivaid turvalahendusi pakkuda võrgu ja süsteemi lahusust rakendavad turvavaldkonnad. Süsteemide käiduvajadused (nt hooldus, andmeedastus jne) võivad siiski nõuda eri turvavaldkondadest möödahiilimist või nende ühendamist (nt lahutatud süsteemid ja võrgud), sealhulgas info- ja käidutehnoloogia ühendamist.*

Euroopa Komisjon

Küberohtude avastamine

Organisatsioonid peaksid tagama, et turvameetmed on jätkuvalt tõhusad, ning avastama mis tahes küberturvalisuse sündmused, mis mõjutavad või võivad mõjutada turvakontrolli meetmeid ning olulisi teenuseid ja süsteeme. Küberohtude avastamiseks on asjakohased alljärgnevad turvameetmed.

- ***Turvaseire.*** *Maismaatranspordi põhifunktsioonide täitmist toetavate võrkude ja infosüsteemide, sh info- ning käidutehnoloogia turvalisuse seire. See on vajalik võimalike turvaohtude avastamiseks ja turvameetmete jätkuva tõhususe jälgimiseks. Turvaseire toetamiseks võetakse arvesse näiteks järgmisi andmeid:*

  - *turvalogid*
  - *viirustuvastuslogid*
  - *sissetungituvastuslogid*
  - *identimis-, autentimis- ja autoriseerimislogid*
  - *süsteemi- ja teenuslogid*
  - *võrguliikluslogid*
  - *andmetöötluslogid*

- ***Turvasündmuse avastamine.*** *Selliste pahatahtlike tegevuste (st turvasündmuste) avastamine, mis mõjutavad või võivad mõjutada meretranspordi põhifunktsioonide täitmist toetavate võrkude ja infosüsteemide (sealhulgas info- ja käidutehnoloogia) turvalisust.*

Need meetmed võivad nõuda eritehnoloogiate (nt turvateabe ja -sündmuste halduse, sissetungituvastussüsteemi, sissetungitõrjesüsteemi jne) kasutuselevõtmist ning infoturbekeskuse või samaväärse keskuse loomist.
See tähendab vahendite väljatöötamist küberrünnete avastamiseks, analüüsimiseks, neile reageerimiseks ja nendest taastumiseks kohalikul tasandil.
Riiklikud küberturbe intsidentide lahendamise üksused (CSIRTid), valdkondlikud ja kommerts-CERTid või maanteeveo- ja raudteeveo-ettevõtjad ning Euroopa raudteeteabe jagamise ja analüüsimise keskus (ER-ISAC) võivad pakkuda küberohtudealast luureteavet, mis võimaldab turvaseiret ja avastamist.

Reageerimis- ja taastemeetmete kavandamine

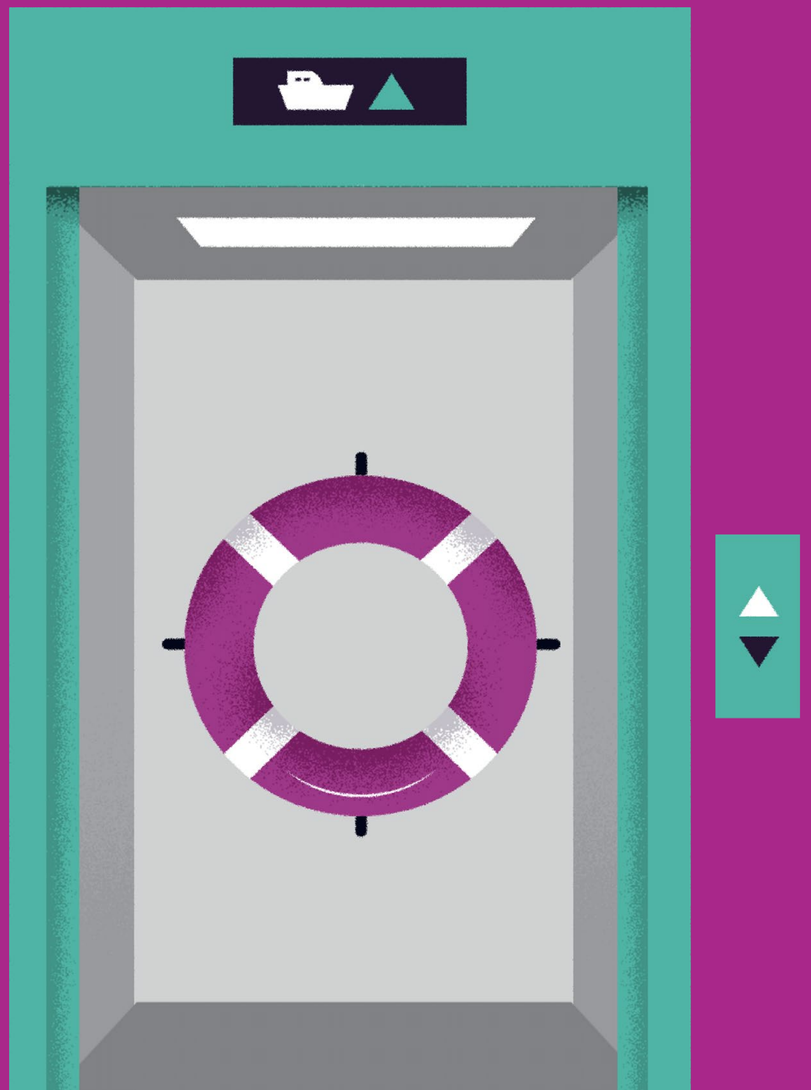
Organisatsioonid peaksid kindlaks määrama, rakendama ja testima intsidendihaldusmenetlusi, mille eesmärk on tagada teenuste ja süsteemide talitluspidevus küberintsidentide korral.

Reageerimis- ja taastamismeetmete kavandamisel tuleks arvesse võtta turvameetmeid, mis leevendavad konkreetsete küberrünnete mõju, näiteks:

- *koordineerida riiklikke CSIRTe, (avalik-õiguslikke ja kommerts-) CERTe ja ISACe, teha nendega koostööd küberintsidentide korral ning koordineerida intsidente ja kriise üleeuroopalisel tasandil;*
- *jagada teavet teiste organisatsioonidega, sealhulgas maismaatranspordi teenuste tarneahelasse kuuluvate teenuseosutajatega;*
- *korraldada korrapäraseid **küberründeõppusi** (lauaõppus ja tehniline õppus), et hinnata turvameetmeid ja -menetlusi ning organisatsiooni vastupidavusvõimet küberintsidentidega toimetulekuks;*
- *tagada juurdepääs arhiveeritud või varundatud andmete asukohale juhuks, kui andmesalvestite terviklus ja kättesaadavus on ohus;*
- *koostada **turbejuhendid** koos üksikasjalike menetlustega küberintsidentide ohjamiseks ning teenuste ja süsteemide viimiseks tavapärastesse käidutingimustesse;*
- *suunata teenusetõkestusrünnete ajal võrguliiklus ümber liiastele teenustele;*
- *tagada käsijuhtimisega menetlused teenuste ja süsteemide käitamiseks halvenenud käidutingimustes;*
- *määrata kindlaks menetlused andmetega seotud rikkumiste käsitlemiseks, sealhulgas menetlused isikuandmetega seotud rikkumiste käsitlemiseks kooskõlas isikuandmete kaitse üldmääruse ja muude asjakohaste valdkondlike määruste või direktiividega;*
- *sõlmida **küberkindlustusleping**, et osaliselt tasakaalustada tõsiste küberintsidentidega seotud riski;*
- *sõlmida intsidentidele reageerimise leping ühe või mitme spetsialiseerunud ettevõtjaga, kellel on lisavõimekus ja -teadmised;*
- *määrata kindlaks menetlused küberintsidentidest teatamiseks asjaomastele sidusrühmadele, sealhulgas intsidentidest teatamise kord kooskõlas küberturvalisuse direktiiviga (direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus).*

Euroopa Komisjon

Lennutranspordile kohandatud head tavad ja turvameetmed



Euroopa Komisjon

Juhtimine

Meretranspordiorganisatsioonid vajavad selget arusaama uutest ohtudest, et määrata kindlaks oma lähenemisviisidega seotud juhtimispõhimõtted ja -protsessid ning suurendada teenuste ja kasutatavate süsteemide, sealhulgas info- ja käidutehnoloogia küberturvalisust.

Head tavad hõlmavad mis tahes suurusega organisatsiooni puhul järgmist:

- *tagada, et kõrgema juhtkonna tasandid teavitavad küberturvalisusega seotud probleemidest juhte ja juhatust, kes saavad teha teadlikke otsuseid vahendite eraldamise kohta;*

- *määrata kõrgema juhtkonna liige, kes vastutab üldiselt info- ja käidutehnoloogia turvalisuse eest. See juhtkonna liige peaks vastutama nii küberturvalisuse kui ka füüsilise julgeoleku eest;*

- *määrata kindlaks selged küberturvalisusega seotud rollid, vastutusalad, pädevused ja load, kalda- ning pardapersonali vahelised võimutasandid ja sideliinid ning leppida sel teemal asjaomaste töötajatega kokku. See on vajalik eelkõige infoturbeintsidentidega tegelevate rühmade (CERTide) liikmete jaoks. Töötajad, kellel on ELi meresõidu turvalisust ja ohutust käsitlevate õigusaktidega seotud rollid, näiteks sadamarajatiste turvaülemad, sadamate ja ettevõtete turvaülemad, määratud isik kaldal ning kapten pardal, peaksid olema vähemalt kursis organisatsiooni võetud küberturvalisuse meetmetega;*

- *tagada küberturvalisuse juhtimine kogu turbealases tarne- ja teenusteahelas, sealhulgas nii füüsiliste kui ka digiliideste puhul, alates tehnoloogia tootjatest ning paigaldajatest kuni turvateenuste osutajateni;*

- *leppida küberturvalisuse riskide juhtimiseks kokku tegevustes ja kontrollides, sealhulgas jagatud vastutuses, ning tagada, et need kohustused säilivad kogu turbelahenduste ja -teenuste kasutusaja jooksul (nt teenuslepingute abil);*

- *määrata kindlaks juhtimismehhanismid (nt -põhimõtted), et täita kohustusi, mis tulenevad asjaomastest määrustest ja direktiividest, näiteks määrusest (EL) 2019/1239, millega luuakse Euroopa merenduse ühtsete kontaktpunktide keskkond, määrusest (EÜ) 725/2004 laevade ja sadamarajatiste turvalisuse tugevdamise kohta, direktiivist 2005/65/EÜ sadamate turvalisuse tugevdamise kohta, määrusest (EÜ) nr 336/2006, mis käsitleb meresõiduohutuse korraldamise rahvusvahelise koodeksi rakendamist, ning resolutsioonist A.741(18), millega võetakse vastu laevade ohutu ekspluateerimise ja reostuse vältimise korraldamise rahvusvaheline koodeks. Sellega seoses on asjakohane nimetada ka ühist teabejagamiskeskkonda (CISE), mis on ELi algatus, mille eesmärk on muuta Euroopa ja liikmesriikide seiresüsteemid koostalitlusvõimeliseks, et anda kõigile asjaomastele ametiasutustele juurdepääs salastatud ning salastamata teabele, mida nad vajavad merel korraldatavateks missioonideks.*

Meretranspordi teenuste ja süsteemide näited. Infotehnoloogia näited on sellised, mis on kättesaadavad töötajatele (nt personaalarvutid, mobiiltelefonid, kontori välisseadmed jne) või reisijatele (nt avalikud WiFi-ruuterid ja -ühendused jne). Käidutehnoloogia näited on superviisorjuhtimis- ja andmehõivesüsteemid, kütte-, ventilatsiooni- ja kliimasüsteemid, globaalse asukoha määramise süsteemid, juurdepääsukontroll, seire, järelevalve, häirele reageerimine, läbivaatustehnoloogia, pardanavigatsioonisüsteemid, SafeSeaNet, komandosilla juhtimissüsteemid, lasti käitlemise ja haldamise süsteemid, jõuseadmete ja mootori juhtimise süsteemid, juurdepääsu kontrollisüsteemid, reisijate teenindamise ja juhtimissüsteemid, reisijatele suunatud avalikud võrgud, haldustöötajate ja laevapere sotsiaalhoolekandesüsteemid, sidesüsteemid ja muu.

Euroopa Komisjon

Küberohtude tuvastamine

Riskijuhtimine. Merendusorganisatsioonid peavad võtma asjakohaseid meetmeid, et teha kindlaks küberturvalisuse riskid, neid analüüsida, hinnata ja neist teavitada ning neid aktsepteerida, neid vältida, üle kanda või vastuvõetava tasemeni leevendada. Selleks on vaja organisatsiooni üldist riskijuhtimise lähenemisviisi, mis hõlmab järgmist:

- *selge ülevaate tagamine eri teenuste osutamiseks kasutatavatest riist- ja tarkvarasüsteemidest. Meretranspordi kontekstis hõlmavad sellised süsteemid info- ja käidutehnoloogiat ning seda, kuidas need süsteemid ühenduvad ja integreeruvad kaldal asuvate süsteemidega, sealhulgas riigiasutuste, mereterminalide ja stividoridega;*

- *selliste peamiste laevapardal tehtavate toimingute kindlakstegemine ja hindamine, mis on küberrünnete suhtes haavatavad, ning küberturvalisuse riskide hindamine (sealhulgas tegevusele avalduva võimaliku mõju hindamine ja riskide esinemise tõenäosuse hindamine), võttes arvesse uusi ohte, teadaolevaid nõrkusi ja käiduandmeid seoses kohaldamisalas olevate süsteemidega. Vajaduse korral siduda need laevade, sadamarajatiste ja sadamate turvalisuse hindamistega, mis on tehtud vastavalt ELi meresõiduturvalisust käsitlevatele õigusaktidele. Nendega tehakse kindlaks võimalikud turvaohud sadamataristule ja turvanõrkused. Lisaks võivad mereorganisatsioonid, nagu Rahvusvaheline Mereorganisatsioon (IMO) ja merendusvaldkonna ISACid, anda teavet meretranspordile suunatud ohtude kohta;*

- *tagamine, et riskihindamine hõlmaks ka riske, mis on seotud töötajate igapäevase tegevusega (nt sotsiaalmeedia kasutamine, isiklike seadmete kasutamine, andmetöötlus, teabe jagamine jne);*

- *riskijuhtimismeetmete ja küberturvalisuse riskide maandamise kavade koostamine ja rakendamine. Näiteks ulatusliku infoturbe haldussüsteemi ja eraelu puutumatust käsitleva teabe haldussüsteemi rakendamine kooskõlas teiste haldussüsteemidega, nagu ohutusjuhtimissüsteemid, vastavalt laevade ohutu ekspluateerimise ja reostuse vältimise korraldamise rahvusvahelisele koodeksile. Sellised haldussüsteemid (s.o infoturbe haldussüsteem ja eraelu puutumatust käsitleva teabe haldussüsteem) hõlmavad turvakontrollide (samuti andmekaitse ja eraelu puutumatuse kontrollide) rakendamist, et leevendada ja ennetada merendusteenuste ja -süsteemide (sh nende andmete) turvalisust mõjutavaid uusi ohte;*

- *mis tahes piirangute arvessevõtmine, mis on seotud **varahalduse ja ressursiplaneerimisega** (st piirangud, mis võivad mõjutada meretranspordi oluliste funktsioonide toimimiseks vajalike kriitilise tähtsusega süsteemide tarnimist, hooldamist ja toetamist). Hindamise puhul viidatakse vajaduse korral nõuetele, mis on esitatud laevade ohutu ekspluateerimise ja reostuse vältimise korraldamise rahvusvahelises koodeksis, ohutusjuhtimissüsteemides ja julgeolekukavades, mis on ellu viidud kooskõlas ELi meresõiduohutust ja -turvalisust käsitlevate õigusaktidega.*

Riskijuhtimisraamistike näited. Eri raamistikud (nt ISM koodeks või ISO/IEC 27000 standardisari, NISTi küberturvalisuse raamistik, MITRE ATT&CK raamistik, BSI IT-Grundschutz jne) võivad anda teavet ja toetada kohandatud riskijuhtimist meretranspordi valdkonnas. NISTi küberturvalisuse raamistikku on kohandatud ka selleks, et käsitleda mereveos vedellasti ümberlaadimise, avamereoperatsioonide ja reisilaevade käitamise küberturvalisust. Sarnaselt on Balti ja Rahvusvaheline Merendusnõukogu (BIMCO) välja andnud suunised küberturvalisuse kohta laevadel („The Guidelines on Cyber Security Onboard Ships“) ning Rahvusvaheline Mereorganisatsioon (IMO) on välja andnud konkreetsed suunised merendusega seotud küberriskide juhtimise kohta („Guidelines on maritime cyber risk management“) (MSC-FAL.1/Circ.3). ENISA on teinud mitu uuringut, mis käsitlevad merenduse küberturvalisuse häid tavasid, eelkõige sadamate küberturvalisust. EMSA osutab merenduskogukonnale teenuseid, sealhulgas küberturvalisusealase teadlikkuse suurendamise koolitusi. Standarditega (nt IEC 61162-460:2018 merenavigatsiooni- ja raadiosideseadmete ja -süsteemide ohutuse ja turvalisuse kohta, ISO 16425:2013 laevade ja meretehnoloogia kohta, IEC 62443-4-1:2018 tööstuslike automaatika- ja juhtimissüsteemide turvalisuse kohta jne) määratakse kindlaks ka meretranspordi süsteemide ja võrkude konkreetsed turva- ja ohutusnõuded.

Euroopa Komisjon

Kaitse küberohtude eest

Meretranspordi organisatsioonid peaksid rakendama piisavaid ja proportsionaalseid turvameetmeid, et kaitsta oma võrke ning infosüsteeme, sealhulgas info- ja käidutehnoloogiat. Need turvameetmed on muu hulgas alljärgnevad.

- ***Turvalisuse põhimõtted ja protsessid.*** *Määrata kindlaks, rakendada, edastada ja jõustada asjakohased põhimõtted ja protsessid, millega määratakse kindlaks üldine lähenemisviis meretranspordi valdkonnas oluliste ülesannete täitmist toetavate süsteemide ja andmete turvalisuse tagamiseks. Turvameetmed (sealhulgas küberturvalisuse ja füüsilise julgeoleku meetmed) tuleks lisada asjaomastesse kavadesse, näiteks ohutusjuhtimissüsteemi ja laeva turvaplaani. Sellised turvapõhimõtted (nt salasõna- ja andmetalletuspõhimõtted) ja menetlused peaksid hõlmama ka riist- ning tarkvarasüsteemide (sealhulgas info- ja käidutehnoloogia) paikasid ja nõrkusehaldust, intsidendihaldust, süsteemi- ning võrgukaitset.*

- ***Identiteedi- ja pääsuhaldus.*** *Mõista, dokumenteerida ja hallata meretranspordi põhifunktsioonide toimimist toetavate võrkude ja infosüsteemide (sealhulgas info- ja käidutehnoloogia) kättesaadavust. Kasutajad (või automatiseeritud funktsioonid), kellel (millel) on juurdepääs andmetele või süsteemidele, on nõuetekohaselt kontrollitud, autenditud ja volitatud. Seejuures tuleks arvesse võtta ka tava- ja eeliskontode eri rolle ning kohustusi.*

- ***Andmete ja süsteemi kaitse.*** *Kaitsta andmeid (elektrooniliselt salvestatud ja edastatud), kriitilise tähtsusega võrke ja infosüsteeme (sh info- ja käidutehnoloogia) küberrünnete eest. Riskipõhist lähenemisviisi arvesse võttes peaksid organisatsioonid rakendama turvameetmeid, et tõhusalt piirata ründaja võimalusi andmeid, võrke ja süsteeme ohtu seada. Need turvameetmed peaksid hõlmama ka krüpteerimise ja turvaliste sideprotokollide kasutuselevõtmist, et kaitsta jõudeolekus ja edastatavaid andmeid vahendusrünnet põhjustavate küberohtude eest. Selliseid meetmeid tuleb rakendada koos füüsiliste turvameetmetega, et kaitsta süsteemidele juurdepääsu (nt süsteemid peaksid asuma piiratud juurdepääsuga suletud ruumides). See on väga oluline nende süsteemide puhul, mis võivad mõjutada inimelude ohutust (nt II ja III kategooria navigatsiooni- ja raadiosidesüsteemid).*

- ***Võrkude ja süsteemide vastupidavus.*** *Suurendada võrkude ja süsteemide (sealhulgas info- ja käidutehnoloogia) kavandamise ja rakendamise kaudu nende (ja nende käidukorra) vastupidavusvõimet, et seista vastu küberrünnete mõjule ja seda leevendada. Vastupidavusvõimet suurendavate disaini- ja rakenduslahenduste näited on järgmised: ametlikult kontrollitud kriitilise tähtsusega funktsioonid, süsteemide ja võrkude liiasus, võrkude lahusus (eelkõige info- ja käidutehnoloogia lahusus), mitmekihilised turvameetmed ning paljud muud. Arvestada tuleb sellega, et infoturbe seisukohast võivad sobivaid turvalahendusi pakkuda võrgu ja süsteemi lahusust rakendavad turvavaldkonnad. Süsteemide (nt autonoomsed mere pealveelaevad (Maritime Autonomous Surface Ships – MASS)) vajadused (nt hooldus, andmeedastus jne) võivad siiski nõuda eri turvavaldkondadest möödahiilimist või nende ühendamist (nt lahutatud süsteemid ja võrgud), sealhulgas info- ja käidutehnoloogia ühendamist.*

Küberohtude avastamine

Organisatsioonid peaksid tagama, et turvameetmed on jätkuvalt tõhusad, ning avastama mis tahes küberturvalisuse sündmused, mis mõjutavad või võivad mõjutada turvakontrolli meetmeid ning olulisi teenuseid ja süsteeme. Küberohtude avastamiseks on asjakohased alljärgnevad turvameetmed.

■ ***Turvaseire.*** *Meretranspordi põhifunktsioonide täitmist toetavate võrkude ja infosüsteemide, sh info- ning käidutehnoloogia turvalisuse seire. See on vajalik võimalike turvaohtude avastamiseks ja turvameetmete jätkuva tõhususe jälgimiseks. Turvaseire toetamiseks võetakse arvesse näiteks järgmisi andmeid:*

- *turvalogid*
- *viirustuvastuslogid*
- *sissetungituvastuslogid*
- *identimis-, autentimis- ja autoriseerimislogid*
- *süsteemi- ja teenuslogid*
- *võrguliikluslogid*
- *andmetöötluslogid*

■ ***Turvasündmuse avastamine.*** *Selliste pahatahtlike tegevuste (st turvasündmuste) avastamine, mis mõjutavad või võivad mõjutada meretranspordi põhifunktsioonide täitmist toetavate võrkude ja infosüsteemide (sealhulgas info- ja käidutehnoloogia) turvalisust.*

Need meetmed võivad nõuda eritehnoloogiate (nt turvateabe ja -sündmuste halduse, sissetungituvastussüsteemi, sissetungitõrjesüsteemi jne) kasutuselevõtmist ning infoturbekeskuse või samaväärse keskuse loomist.

See tähendab vahendite väljatöötamist küberrünnete avastamiseks, analüüsimiseks, neile reageerimiseks ja nendest taastumiseks kohalikul tasandil.

Riiklikud küberturbe intsidentide lahendamise üksused (CSIRTid), valdkondlikud CERTid ja merendusettevõtjate kommerts-CERTid ning merendusvaldkonna ISACid võivad pakkuda küberohtudealast luureteavet, mis võimaldab turvaseiret ja avastamist.

Euroopa Komisjon

Reageerimis- ja taastemeetmete kavandamine

Organisatsioonid peaksid kindlaks määrama, rakendama ja testima intsidendihaldusmenetlusi, mille eesmärk on tagada teenuste ja süsteemide talitluspidevus küberintsidentide korral.
Reageerimis- ja taastamismeetmete kavandamisel tuleks arvesse võtta turvameetmeid, mis leevendavad konkreetsete küberrünnete mõju, näiteks:

- *suunata teenusetõkestusrünnete ajal võrguliiklus ümber liiastele teenustele;*
- *tagada käsijuhtimisega menetlused teenuste ja süsteemide käitamiseks halvenenud käidutingimustes;*
- *luua õppuste ja harjutuse (nt lauaõppuste, tehniliste ja reageerimisharjutuste) kavad, et reageerida küberrünnetele ja hädaolukordadele ning hinnata turvameetmeid, menetlusi ja organisatsiooni vastupidavusvõimet küberintsidentidega toimetulekuks;*
- *tagada juurdepääs arhiveeritud või varundatud andmete asukohale juhuks, kui andmesalvestite terviklus ja kättesaadavus on ohus;*
- *koordineerida riiklikke CSIRTe, (avalik-õiguslikke ja kommerts-) CERTe ja ISACe, teha nendega koostööd küberintsidentide korral ning koordineerida intsidente ja kriise üleeuroopalisel tasandil;*
- *jagada teavet teiste organisatsioonidega, sealhulgas meretranspordi teenuste tarneahelasse kuuluvate teenuseosutajatega;*
- *koostada turbejuhendid koos üksikasjalike menetlustega küberintsidentide ohjamiseks ning teenuste ja süsteemide viimiseks tavapärastesse käidutingimustesse;*
- *määrata kindlaks menetlused andmetega seotud rikkumiste käsitlemiseks, sealhulgas menetlused isikuandmetega seotud rikkumiste käsitlemiseks kooskõlas isikuandmete kaitse üldmääruse ja muude asjakohaste valdkondlike määruste või direktiividega;*
- *sõlmida küberkindlustusleping, et osaliselt tasakaalustada tõsiste küberintsidentidega seotud riski;*
- *sõlmida intsidentidele reageerimise leping ühe või mitme spetsialiseerunud ettevõtjaga, kellel on lisavõimekus ja -teadmised;*
- *määrata kindlaks menetlused küberintsidentidest (sh lahknevustest, õnnetustest ja ohtlikest olukordadest) teatamiseks asjaomastele sidusrühmadele, sealhulgas intsidentidest teatamise kord kooskõlas küberturvalisuse direktiiviga (direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus);*

Luxembourg: Euroopa Liidu Väljaannete Talitus, 2021

Print ISBN 978-92-76-40488-0 doi:10.2832/875747 MI-05-21-230-ET-C
PDF ISBN 978-92-76-40487-3 doi:10.2832/064 MI-05-21-230-ET-N

Euroopa Liidu
Väljaannete Talitus