Europos Komisija

Transporto kibernetinio saugumo priemonių rinkinys

Įvadas

Europos Komisijos mobilumo ir transporto generalinis direktoratas (DG MOVE) sudarė sutartį dėl šio priemonių rinkinio sukūrimo siekdamas padidinti transporto sektoriaus suinteresuotųjų šalių informuotumą apie kibernetines grėsmes ir pasirengimą joms. Priemonių rinkinyje pateikiamos įžvalgos, padedančios suprasti kibernetines grėsmes ir sušvelninti jų poveikį transporto paslaugoms, sistemoms ir operacijoms. Jame pateikiami alternatyvūs informuotumo didinimo būdai skirtingoms transporto sektoriaus grupėms:

- visiems transporto darbuotojams (teikiama bendroji informacija ir rekomendacijos);
- įvairių transporto rūšių kibernetinio saugumo sprendimus priimantys asmenys.

Kad būtų patogiau rasti konkrečioms transporto sektoriaus grupėms skirtus informuotumo didinimo būdus, įvairias priemonių rinkinį sudarančias dalis jungia saitai.

Šiame priemonių rinkinyje nurodytos priemonės yra tik patariamojo pobūdžio. Jokia suformuluota rekomendacija nėra nei įpareigojanti, nei privaloma. Be to, šis priemonių rinkinys neatspindi oficialios Europos Komisijos nuomonės ir juo nesiekiama suteikti galiojančių ar būsimų ES teisės aktų laikymosi priemonių.

Informuotumo apie kibernetinį saugumą didinimo grupės

1 grupė. Visi transporto darbuotojai. Pirmasis būdas skirtas visiems transporto organizacijų darbuotojams, nuo transporto paslaugų operacijų darbuotojų iki administracijos personalo. Jame pateikiamos rekomendacijos, kaip geriau suprasti ir įsisąmoninti dažniausias kibernetines grėsmes, nukreiptas prieš transporto paslaugas ir sistemas. Be to, jame pateikiama įžvalgų, kaip apsisaugoti nuo potencialių kibernetinių grėsmių, įskaitant jų nustatymą, pranešimą apie jas ir jų poveikio mažinimą taikant gerąją kibernetinio saugumo praktiką.

II grupė. Transporto kibernetinio saugumo sprendimus priimantys asmenys. Antrasis būdas skirtas darbuotojams, kurie transporto organizacijose yra atsakingi už sprendimų dėl kibernetinio saugumo priėmimą. Šis būdas susijęs su transporto organizacijų kibernetinio saugumo stiprinimo gerąja praktika, pritaikyta skirtingoms transporto rūšims. Visų pirma pateikiami gerosios praktikos pavyzdžiai, kaip nustatyti kylančias prieš transporto organizacijas nukreiptas kibernetines grėsmes, nuo jų apsisaugoti, jas aptikti ir į jas reaguoti.

Europos Komisija

Transporto kibernetinio saugumo priemonių rinkinys

Grėsmių transportui padėtis

Kylančios kibernetinio saugumo grėsmės, darančios poveikį įvairioms transporto rūšims

Informuotumo apie kibernetinį saugumą didinimo grupės

Alternatyvūs informuotumo apie kibernetinį saugumą didinimo būdai skirtingoms transporto sektoriaus grupėms

Europos Komisija

Grėsmių transportui padėtis

Kibernetinių grėsmių padėtis yra dinamiška ir nuolat kinta. Nepaisant to, galima nustatyti kibernetines grėsmes, su kuriomis susiduriama visose transporto rūšyse vykdant paslaugų ir sistemų operacijas.

Europos Komisija

Priešiški subjektai

Asmenys arba organizacijos, galintys turėti įtakos transporto paslaugų ir sistemų saugai ir saugumui

Kylančios kibernetinės grėsmės

Atrinktos kibernetinės grėsmės, kurių pagrindu gali būti surengtos atakos, darančios poveikį transporto paslaugų ir sistemų saugai ir saugumui

Europos Komisija

Priešiški subjektai

Asmenys arba organizacijos gali tyčia arba netyčia atskleisti ir išnaudoti pažeidžiamumą, kuris gali sukelti incidentus ir paveikti transporto paslaugas, įskaitant jų saugą, saugumą, verslą, finansus ir reputaciją. Priešiškais subjektais laikomos, pavyzdžiui, valstybės remiamos grupuotės, kibernetiniai nusikaltėliai, kibernetiniai teroristai, įsilaužėliai aktyvistai, programišiai (įskaitant pradedančiuosius įsilaužėlius) ir vidaus subjektai (įskaitant privilegijuotus vidaus subjektus).

Svarbiausi piktavaliai veikėjai, kurie tyčia taikosi į transporto organizacijas, yra **kibernetiniai nusikaltėliai**, **vidaus subjektai, valstybės** ir **valstybių remiamos grupuotės**. Tokie piktavaliai asmenys kaip **kibernetiniai nusikaltėliai** vykdo masines atakos kampanijas ir dažnai siekia piniginio atlygio.

Vidaus subjektai žino organizacijų, kuriose jie dirba, ypatumus ir dažnai gerai suvokia subtilias silpnąsias saugumo vietas. Šie priešiški vidaus subjektai gali būti nepatenkinti darbuotojai, tiekėjai ir pavieniai rangovai. Pasaulyje didėjant geopolitinei įtampai, **valstybės** ir **valstybių remiamos grupuotės** siekia strateginių ilgalaikių tikslų. Jos dažnai bando nepastebėtos įsiskverbti į organizacijų sistemas ir rinkti neskelbtiną informaciją. Įsitvirtinę tokiose sistemose valstybių remiami užpuolikai bando užimti tokią padėtį, kurioje būtų galima padaryti kuo didesnę žalą. Pavyzdžiui, jie gali pulti kitų organizacijų sistemas pasinaudodami organizacijų tinklo ryšiais.

Kiti priešiški subjektai yra **vidaus subjektai**, dėl kurių tyčinių arba netyčinių veiksmų kyla kibernetinio saugumo incidentai, kurie, blogiausiu atveju, neigiamai paveikia transporto paslaugų saugą ir saugumą.

Europos Komisija

Kylančios kibernetinės grėsmės

Prieš transporto sektorių nukreipiama gana daug kibernetinių grėsmių: **paskirstytasis paslaugos trikdymas (DDoS)**, **paslaugos trikdymas (DoS)**, duomenų vagystės, **kenkimo programų** platinimas, **duomenų viliojimas**, manipuliavimas programine įranga, **neteisėta prieiga**, destruktyvios atakos, saugumo operatoriaus sprendimų priėmimo proceso klastojimas ar apėjimas, netikra tapatybė, piktnaudžiavimas prieigos teisėmis, **socialinė inžinerija**, svetainės turinio iškraipymas, pasiklausymas, netinkamas turto naudojimas ir manipuliavimas aparatine įranga.

Remiantis išsamiais viešos literatūros tyrimais ir pokalbiais su ekspertais, aktualiausios kylančios kibernetinės grėsmės, kurios daro didelę įtaką transportui, yra: kenkimo programos, (paskirstytasis) paslaugos trikdymas (DDoS), neteisėta prieiga ir vagystė bei manipuliavimas programine įranga.

Europos Komisija

1 grėsmė. Kenkimo programos

Kenkimo programinė įranga, kuri gali turėti įtakos skirtingų transporto rūšių organizacijoms ar jų asmenims

2 grėsmė. (Paskirstytasis) paslaugos trikdymas (DDoS)

Kibernetinės atakos, trukdančios asmenims ar organizacijai naudotis atitinkamomis transporto paslaugomis ir ištekliais

3 grėsmė. Neteisėta prieiga ir vagystės

Neteisėta prieiga prie ypatingos svarbos turto, jo pasisavinimas ir naudojimas

4 grėsmė. Manipuliavimas programine įranga

Kibernetinės atakos, nukreiptos prieš programinę įrangą siekiant pakeisti jos veikimą ir vykdyti konkrečias atakas

1 grėsmė. Kenkimo programos

Kenkimo programos – tai kenkimo programinė įranga, kuri gali apimti įvairias taikomąsias programas, tokias kaip virusai, Trojos arkliai, kirminai, išpirkos reikalaujančios programos, kriptovaliutų gavybos priemonės ar kita programinė įranga, kuri gali turėti neigiamą poveikį įvairių transporto rūšių organizacijoms ar asmenims.

Kenkimo programų, skirtų sąmoningai kenkti kompiuteriams, serveriams, klientams, tinklams ar visiems jiems kartu, sklaidos mažinimas yra vienas iš pagrindinių visų transporto rūšių kibernetinio saugumo prioritetų. Tipinė ataka gali atrodyti kaip darbuotojui siunčiami duomenų viliojimo el. laiškai. Kitos atakos gali būti susijusios su skirtingomis ir sudėtingomis socialinės inžinerijos strategijomis, pavyzdžiui, USB rakto prijungimu prie laisvo prievado (pvz., įkraunant mobilųjį telefoną). Spustelėjęs saitus įtartinuose el. laiškuose ar atidaręs prisegtus failus, naudotojas gali pats to nežinodamas įdiegti programinę įrangą arba sąmoningai pakenkti transporto paslaugoms ir ištekliams.

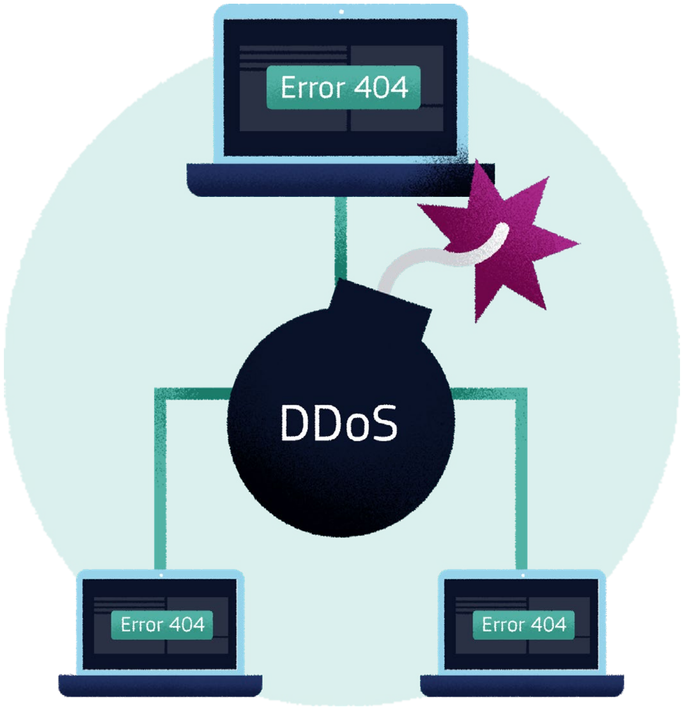
Pavyzdžiui, išpirkos reikalaujanti kibernetinė ataka „WannaCry“ paveikė daugiau kaip 150 šalių ir užkrėtė daugiau kaip 230 000 sistemų. Tai buvo išpirkos reikalaujanti programa, kuri paprastai platinama duomenų viliojimo el. laiškais, kuriuose yra kenkimo priedų ar saitų. Tokio pobūdžio atakose piktybiškai pasitelkiama socialinė inžinerija siekiant apgaulės būdu paskatinti sistemos naudotojus įdiegti (arba aktyvinti) konkrečias kenkimo programas.

2 grėsmė. (Paskirstytasis) paslaugos trikdymas

Paskirstytojo paslaugos trikdymo (DDoS) ir paslaugos trikdymo (DoS) atakos neigiamai paveikia duomenų, paslaugų, sistemų ir kitų išteklių prieinamumą ir pasiekiamumą. Tokio pobūdžio atakų trukmė gali būti įvairi, jos vienu metu gali būti nukreiptos prieš kelias paslaugas ar sistemas. DDoS atakoms naudojamos kelios sistemos (arba atakos kanalai) siekiant perkrauti užklausomis tikslines paslaugas arba sistemas. Sėkmingos atakos paveikia paslaugų ir sistemų galimybes reaguoti į netikėtos apimties užklausas. Dėl to paslaugos ir ištekliai tampa neprieinami.

Atkreipkite dėmesį – transporto organizacijoms priklausančios paveiktos paslaugos ir sistemos gali būti panaudotos DDoS ir DoS atakoms vykdyti prieš konkrečias operacijų arba kitų organizacijų sistemas.

Pavyzdžiui, gali būti taikomasi į įmonių informacines sistemas (pvz., asmeninius kompiuterius ir įrenginius) norint gauti prieigą prie operacijų technologijų, kurios gali būti prijungtos prie interneto arba tinklų veiklos duomenims perduoti. Jungtys tarp skirtingų sistemų ir tinklų (pvz., įmonių tinklų, operacijų technologijų ir nuotolinės priežiūros prieigos) gali būti pažeidžiamos ir tai būtų įmanoma išnaudoti DDoS arba DoS atakoms vykdyti prieš ypatingos svarbos transporto paslaugas ir sistemas. Pavyzdžiui, vykdant DDoS ir DoS atakas gali būti pasinaudota tokiais bendrais tinklo ir ryšių protokolais kaip saityno paslaugų dinaminis aptikimas („WS-Discovery“), kai daiktų interneto įrenginiai gali automatiškai aptikti kiekvieną vietinio tinklo (LAN) mazgą. Jei daiktų interneto įrenginiai yra pažeidžiami, atakuotojai gali jais pasinaudoti, kad aptiktų kitus prijungtus įrenginius ir vykdytų DDoS ar DoS atakas.



Europos Komisija

3 grėsmė. Neteisėta prieiga ir vagystė

Priešiški subjektai gali norėti gauti loginę arba fizinę prieigą neturėdami leidimo prisijungti prie tinklo, sistemos, programos, duomenų ar kitų išteklių, kad įvykdytų kenkimo veiklą, be kita ko ir slaptų duomenų arba išteklių (įskaitant fizinius išteklius) vagystę. Neteisėtos prieigos ir vagystės atveju grėsmė kyla konfidencialiam ir nuosavybiniam turtui (įskaitant asmens tapatybę, privilegijuotų sąskaitų kredencialus, sistemas ir kitokio pobūdžio konfidencialią bei nuosavybinę informaciją). Šios grėsmės gali būti susijusios su sistemų pažeidžiamumu, taip pat su asmenimis, kurie to nenorėdami atskleidžia tokius slaptus duomenis kaip prisijungimo kredencialai (pvz., prisijungimo vardas, slaptažodis) arba asmens duomenis (pvz., el. paštas, asmens kodas ir kt.).

Su neteisėta prieiga susijusi tapatybės vagystė yra neteisėtas asmens duomenų arba unikalių identifikatorių naudojimas siekiant apsimesti kitais asmenimis ar tarnybomis ir sistemomis norint gauti prieigą prie privačių arba nuosavybinių išteklių (pvz., finansinių ir fizinių išteklių). Tokios kibernetinio saugumo grėsmės gali būti nukreiptos ir į įvairių transporto rūšių fizinį turtą.

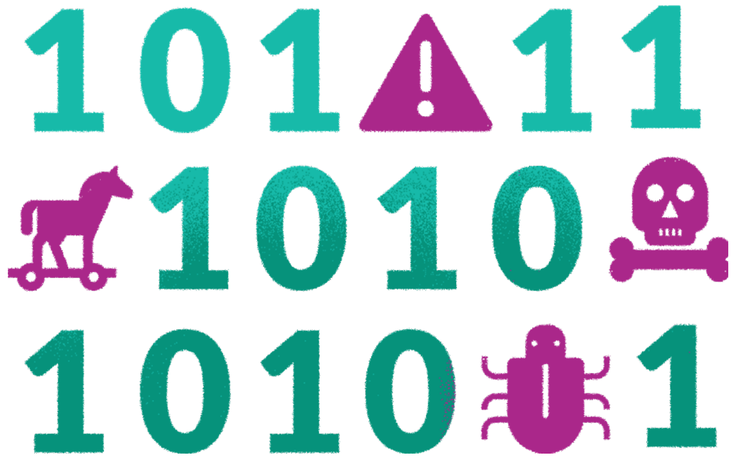
Europos Komisija

4 grėsmė. Manipuliavimas programine įranga

Netinkamas programinės įrangos ir susijusių sistemų arba komponentų konfigūravimas ir manipuliavimas jais gali tiesiogiai paveikti transporto paslaugų ir sistemų saugumo būklę.

Kibernetinio saugumo atakos, vykdomos manipuliuojant programine įranga, pakeičia programinės įrangos nuostatas arba daro neigiamą poveikį duomenų vientisumui siekiant pakeisti sistemų ir paslaugų veikimą. Atakuotojai gali sąmoningai manipuliuoti programine įranga (arba jos dalimi), kad įgytų pranašumų (pvz., gautų neteisėtą prieigą, neleistų teisėtiems asmenims ar sistemoms pasiekti būtinų išteklių, rinktų neskelbtiną informaciją, pakeistų funkcijų veikimą ir pan.), kurie leistų išnaudoti jautrius išteklius.

Pavyzdžiui, atakuotojai gali taikytis į gamintojų ryšių kanalus, kad su paslaugų ir sistemų (įskaitant operacijų technologijas) naujinimais įkeltų kenkimo programinę įrangą. Grėsmės sukėlėjas naudoja gautus leidimus, kad prisijungtų prie saugios nuotolinės priežiūros tinklo sąsajos ir įdiegtų manipuliuojamą programinę įrangą, taip sukeldamas pavojų kitoms pasiekiamoms paslaugoms ir sistemoms. Grėsmės sukėlėjas įdiegia manipuliuojamą programinę įrangą, kuri toliau kelia pavojų tikslinėms paslaugoms ir sistemoms arba atakuoja kitas susijusias paslaugas arba sistemas.



Europos Komisija

Informuotumo apie kibernetinį saugumą didinimo grupės

Europos Komisija

1

I grupė. Visi transporto darbuotojai

Pirmasis būdas skirtas visiems transporto organizacijų darbuotojams, nuo operacijų darbuotojų iki administracijos personalo. Jame pateikiamos rekomendacijos, kaip geriau suprasti ir įsisąmoninti dažniausias kibernetinio saugumo grėsmes, nukreiptas prieš transporto paslaugas. Be to, jame pateikiama įžvalgų, kaip kovoti su potencialiomis kibernetinio saugumo grėsmėmis, įskaitant jų nustatymą, pranešimą apie jas ir jų poveikio mažinimą taikant gerąją kibernetinio saugumo praktiką. Šis būdas yra bendras visoms transporto rūšims.

2

II grupė. Transporto kibernetinio saugumo sprendimus priimantys asmenys

Antrasis būdas skirtas darbuotojams, kurie transporto organizacijose yra atsakingi už sprendimų dėl saugumo arba kibernetinio saugumo priėmimą. Šis būdas užtikrina gerąją praktiką, pritaikytą skirtingoms transporto rūšims. Pateikiami gerosios praktikos pavyzdžiai, kaip nustatyti, apsaugoti, aptikti ir reaguoti į kylančias kibernetinio saugumo grėsmes, nukreiptas prieš transporto organizacijas.

Europos Komisija

1 grupė. Visi transporto darbuotojai

Šis būdas skirtas visiems transporto organizacijų darbuotojams, nuo operacijų darbuotojų iki administracijos personalo. Jame pateikiamos rekomendacijos, kaip geriau suprasti ir įsisąmoninti dažniausias kibernetinio saugumo grėsmes, nukreiptas prieš transporto paslaugas. Be to, jame pateikiama įžvalgų, kaip kovoti su potencialiomis kibernetinio saugumo grėsmėmis, įskaitant jų nustatymą, pranešimą apie jas ir jų poveikio mažinimą taikant gerąją kibernetinio saugumo praktiką.
Šioje dalyje pateikiama rekomenduojama praktika ir naudingi patarimai, kurie aktualūs **visoms transporto rūšims**.

Europos Komisija

Geroji kovos su kenkimo programomis praktika

Galite padėti apsaugoti savo organizaciją laikydamiesi gerosios **kenkimo programų atpažinimo ir sklaidos prevencijos** praktikos:

- ***Laikykitės saugumo politikos**, pvz., tikrinkite saugojimo laikmenas ir failus antivirusine programa, venkite atidaryti ir siųsti el. paštu tam tikrų tipų failus (pvz., tokius vykdomuosius failus kaip .exe, .bat, .com), diekite tik leidžiamą programinę įrangą, užtikrinkite, kad programinė įranga (įskaitant antivirusines programas) būtų atnaujinta ir tinkamai veiktų, taip pat kitos politikos.*

- *Reguliariai **kurkite atsargines duomenų kopijas** saugiuose (ir leidžiamuose) duomenų saugojimo įrenginiuose arba naudodamiesi paslaugomis, kurios turėtų palaikyti šifravimo mechanizmus, kad duomenys būtų apsaugoti ir tada, kai jie laikomi, ir duomenų atkūrimo procedūras.*

- *Visas sistemas, taip pat ir mobiliuosius bei galinius įrenginius, apsaugokite tinkamomis **saugumo priemonėmis** (pvz., slaptažodžiu, šifravimu ir pan.) ir nepamirškite saugiai užrakinti (fiziškai ir skaitmeniniu būdu) visų sistemų, kai jos neprižiūrimos.*

- *Neatidarykite priedų ir nespauskite saitų, esančių nelauktuose el. laiškuose ir įtartinuose žiniatinklio naršyklės iššokančiuose languose su keistu tekstiniu turiniu arba gautų iš nežinomų siuntėjų ir interneto domenų.*

- *Nestatykite į savo kompiuterį **nepatikimų arba nežinomų išimamų įrenginių**, pvz., USB atmintukų, standžiųjų diskų ir kitų duomenų saugojimo įrenginių.*

- *Neišjunkite apsaugos nuo kenkimo programų priemonių (pvz., antivirusinių programų, turinio filtravimo programų, užkardos ir pan.).*

- *Reguliariai **naujinkite įdiegtą programinę įrangą** į naujausias prieinamas versijas (kurias informacijos saugumo pareigūnai arba sistemos administratoriai gali išleisti su reguliariais atnaujinimais).*

- *Nenaudokite privilegijuotų (pvz., administratoriaus lygio) paskyrų ir kredencialų įprastai veiklai ir operacijoms.*

- *Praneškite informacijos saugumo pareigūnams arba sistemos administratoriams apie bet kokį įtartiną el. laišką arba neįprastą sistemos veikimą.*

- *Sutelkite dėmesį į informacijos saugumą kasdieniame darbe, kad atpažintumėte IT saugumo problemas ir atitinkamai reaguotumėte.*

Geroji kovos su (paskirstytuoju) paslaugos trikdymu praktika

Galite padėti apsaugoti savo organizaciją atpažindami **paskirstytojo paslaugos trikdymo (DDoS)** ir **paslaugos trikdymo (DoS)** atakas. Nedelsdami kreipkitės į savo saugumo ir IT komandas, jei aptikote arba patyrėte bet kurį iš šių prieš jūsų paslaugas ar sistemas potencialiai vykdomos DDoS ir DoS atakos požymių:

- *Padaugėjo tinklo pajėgumus naudojančių užklausų (kai pastebimai sulėtėja paslaugos ir reakcijos laikas), dėl kurių paslaugos ar sistema per daug apkraunamos ir sutrinka.*

- *Padidėjo atminties išteklių naudojimo paklausa be akivaizdžios priežasties.*

- ***Netikėtas paslaugų ir sistemų veikimas**, dažnas strigimas ir keisti klaidos pranešimai dėl kenkimo programų naudojamų kompiuterinių išteklių ar tinklo ryšių.*

- ***Prasčiau veikia** įrenginiai, ilgai vykdomos smulkios užduotys ir kiti pastebimi požymiai (pvz., triukšmingai veikia ventiliatorius, nors įrenginiai veikia lėtai).*

- ***Vyksta netikėti prisijungimai prie interneto arba prarandamas ryšys** su paslaugomis ir sistemomis.*

- *Subtilūs operacijų valdiklių ar technologijų veikimo pokyčiai, dėl kurių patiriama fizinė žala.*

- *Prieigos prie privilegijuotų ar administracinių paskyrų nesuteikimas siekiant neleisti atkurti reagavimo į incidentus procedūrų.*

Geroji kovos su neteisėta prieiga ir vagyste praktika

Siekiant užkirsti kelią su neteisėta prieiga ir vagyste susijusioms atakoms, būtina laikytis tokių principų kaip *„būtinybė žinoti“* ir *„pirmiausia – saugumas ir privatumas“*, kuriais pabrėžiama, kad neskelbtini ir konfidencialūs ištekliai (įskaitant asmens ir neskelbtinus duomenis, transporto sistemas ir pan.) turėtų būti prieinami tik tiems asmenims, kurie turi teisę su jais susipažinti, kad galėtų vykdyti savo pareigas. Galite padėti apsaugoti savo organizaciją laikydamiesi neteisėtos prieigos ir vagystės atpažinimo ir prevencijos gerosios praktikos:

- *Laikykitės organizacijos saugumo politikos.*

- *Nebendrinkite ir neskelbkite internete kredencialų ir asmens duomenų, įskaitant paveikslėlius, kuriuose gali būti tokios informacijos.*

- *Nenaudokite ir neperduokite kredencialų ir asmens duomenų (ir kitų neskelbtinų duomenų) į nepatikimus ir nesaugius tinklus, įrenginius ar internetines paslaugas (pvz., svetaines, kuriose naudojami nesaugūs protokolai arba adresai http://, o ne saugūs https://).*

- ***Niekada niekam neatskleiskite savo kredencialų** (pvz., prisijungimo vardo ir slaptažodžio) net el. paštu ar telefonu.*

- *Neleiskite, kad leidimo neturintys asmenys pamatytų neskelbtinus duomenis, įvedamus klaviatūra arba rodomus ekranuose (įskaitant mobiliųjų įrenginių ekranus), įdiekite privatumo ekranus ir nedirbkite viešose vietose naudodami privačius įrenginius, taip pat nepalikite įrenginio atrakinto ir neprižiūrimo.*

- ***Naudokite sudėtingus slaptažodžius** (pvz., pakankamai ilgus slaptažodžius, kuriuose būtų raidžių ir specialiųjų simbolių), atitinkančius aktualią organizacijos saugumo politiką, kad užkirstumėte kelią neteisėtai prieigai.*

- ***Pakeiskite numatytuosius** prijungtų sistemų ir įrenginių (pvz., spausdintuvų, maršruto parinktuvų, kamerų, išmaniojo užrakto ir pan.) **slaptažodžius**.*

- *Nenaudokite tų pačių kredencialų (pvz., prisijungimo vardo ir slaptažodžio) kelioms paslaugoms ir sistemoms, taip pat nenaudokite tų pačių kredencialų paslaugoms ir sistemoms, kurioms reikia privilegijuotų paskyrų.*

- *Perduodamų apsaugotų failų (pvz., ZIP archyvų) slaptažodžius ir raktus siųskite tik ne pagrindiniu kanalu (pvz., SMS žinute per GSM ir telefonu) ir niekada nesiųskite jų el. paštu.*

- *Jei įmanoma, **įjunkite dvielementį tapatumo nustatymą (2FA)** arba kelių elementų tapatumo nustatymą (MFA).*

Geroji kovos su manipuliavimu programine įranga praktika

Galite padėti apsaugoti savo organizaciją laikydamiesi gerosios manipuliavimo programine įranga atpažinimo ir prevencijos praktikos:

- *Nediekite sistemose ir įrenginiuose (įskaitant asmeninius kompiuterius, serverius, išorinius įrenginius, tinklo įrenginius, išmaniuosius telefonus ir pan.) nepatikimos programinės įrangos.*
- *Visada diekite programinę įrangą ir naujinimus iš oficialių šaltinių ir svetainių (pvz., gamintojų, įmonių saugyklų ir pan.).*
- *Nesiųskite programinės įrangos ir programų (ir jokių failų) iš neteisėtų šaltinių.*
- *Išdiekite nereikalingą arba seniai nenaudotą programinę įrangą ir atjunkite nereikalingus ryšius (pvz., tinklo protokolus ir paslaugas), įskaitant prieigą prie nuotolinių paslaugų (pvz., duomenų saugojimo debesyje paslaugų).*
- *Skenuokite kiekvieną programinę įrangą ar saugojimo įrenginius patikima ir atnaujinta antivirusine programa.*
- *Siųskitės saugią pramoninę programinę įrangą (pvz., naujinimus, pataisas, naujus produktus ir pan.) iš patikimų tiekėjų laikydamiesi „baltosios stoties“ (angl. „White station“) principo.*
- *Atnaujinkite visą įdiegtą programinę įrangą laikydamiesi organizacijos politikos ir praktikos.*

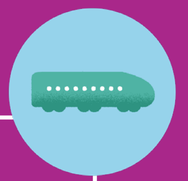
Europos Komisija

II grupė. Transporto kibernetinio saugumo sprendimus priimantys asmenys

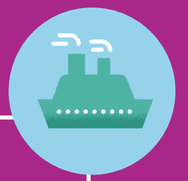
Ši dalis skirta darbuotojams, kurie transporto organizacijose yra atsakingi už sprendimų dėl saugumo arba kibernetinio saugumo priėmimą. Pabrėžiama geroji praktika, pritaikyta skirtingoms transporto rūšims. Visų pirma pateikiami gerosios praktikos pavyzdžiai, kaip nustatyti kylančias kibernetines grėsmes, nuo jų apsisaugoti, jas aptikti ir į jas reaguoti.

Europos Komisija

Geroji kibernetinio saugumo praktika, pritaikyta oro transportui



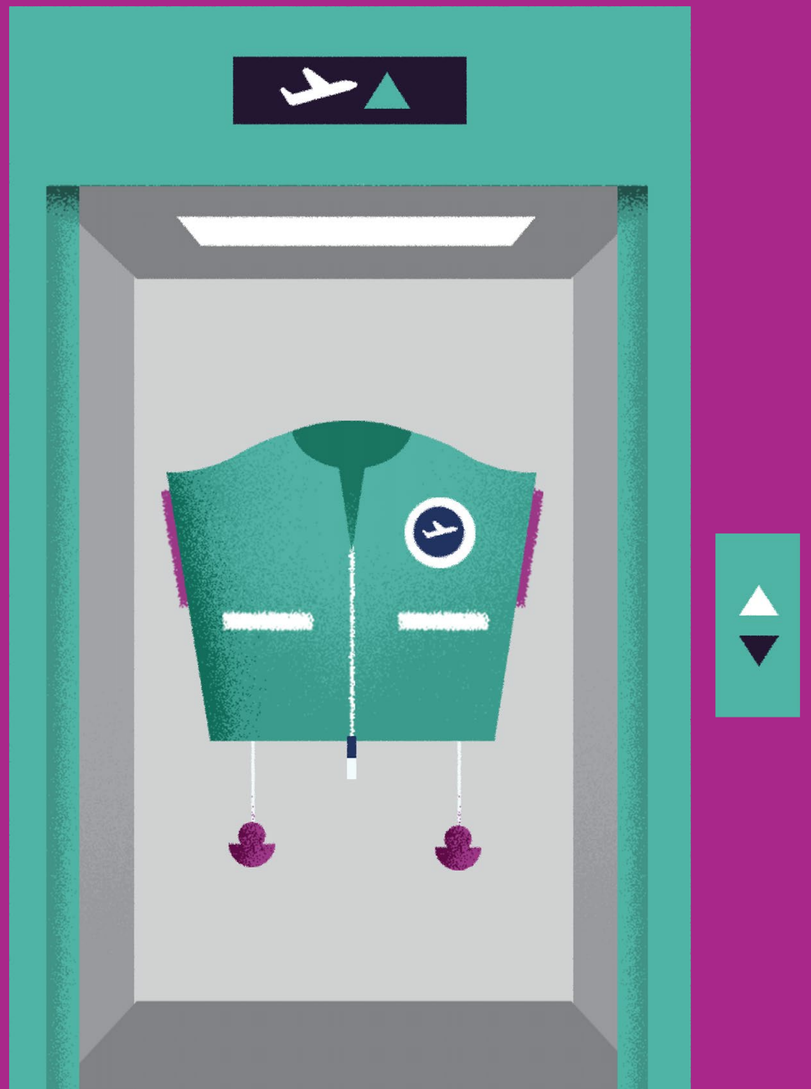
Geroji kibernetinio saugumo praktika, pritaikyta sausumos transportui



Geroji kibernetinio saugumo praktika, pritaikyta jūrų transportui

Europos Komisija

Geroji praktika ir saugumo priemonės, pritaikytos oro transportui



Valdymas

Aviacijos organizacijoms reikia aiškiai suprasti kylančias grėsmes, kad galėtų nustatyti valdymo politiką ir procesus, kurie padėtų didinti veiklos paslaugų ir sistemų, tarp jų ir informacinių technologijų (IT) bei operacijų technologijų (OT), kibernetinį saugumą.

Geroji praktika bet kokio dydžio organizacijoms:

- užtikrinti, kad vyresnioji vadovybė apie kibernetinio saugumo problemas praneštų direktoriams ir valdyboms, kurie galėtų priimti informacija pagrįstus sprendimus dėl išteklių paskirstymo;

- paskirti vyresnįjį pareigūną, atsakingą už kibernetinį ir fizinį saugumą bei bendrą informacinių technologijų (IT) ir operacijų technologijų (OT) saugumo valdymą, tačiau nedalyvaujantį operacijose, kad būtų išvengta interesų konfliktų;

- aiškiai apibrėžti su kibernetiniu saugumu susijusias pareigas, atsakomybę, kompetencijas ir leidimus, apie juos pranešti ir sutarti su atitinkamais darbuotojais, visų pirma kompiuterinių incidentų tyrimo tarnybų (CERT) nariais;

- užtikrinti kibernetinio saugumo valdymą visoje saugumo paslaugų grandinėje, įskaitant fizines ir skaitmenines sąsajas, nuo technologijų gamintojų ir montuotojų iki saugumo paslaugų teikėjų;

- sutarti dėl kibernetinio saugumo rizikos valdymo veiklos ir kontrolės, taip pat ir bendros atsakomybės, bei užtikrinti, kad ši atsakomybė išliktų visą saugumo sprendimų ir paslaugų gyvavimo laiką (pvz., sudarant paslaugų teikimo sutartis);

- nustatyti valdymo mechanizmus (pvz., politiką), kad būtų laikomasi atitinkamuose reglamentuose ir direktyvose nustatytų įpareigojimų, pvz., Reglamente (ES) 2018/1139 dėl bendrųjų civilinės aviacijos taisyklių, Komisijos įgyvendinimo reglamente (ES) 2017/373, kuriuo nustatomi oro eismo valdymo ir oro navigacijos paslaugų teikėjų, kitų oro eismo valdymo tinklo funkcijų vykdytojų ir tų subjektų priežiūros bendrieji reikalavimai, taip pat TIS direktyvoje (ES direktyvoje 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui užtikrinti).

Oro transporto paslaugų ir sistemų pavyzdžiai. IT pavyzdžiai yra sistemos, prieinamos darbuotojams (pvz., asmeniniai kompiuteriai, mobilieji telefonai, biuro išoriniai įrenginiai ir pan.) bei keleiviams (pvz., viešojo „Wi-Fi“ maršruto parinktuvai, jungtys ir pan.). OT pavyzdžiai yra prižiūrimosios kontrolės ir duomenų įgijimo (SCADA) sistemos, šildymo, vėdinimo ir oro kondicionavimo (HVAC) sistemos, salono bagažo saugumo kontrolės punktai, bagažo tvarkymo sistemos (BHS), prieigos kontrolės, stebėsenos, sekimo, reagavimo į pavojaus signalus, filtravimo technologijos, oro uosto apšvietimo kontrolės sistemos, radarų sistemos ir jutikliai, globalinės padėties nustatymo sistemos (GPS), oro eismo valdymo (OEV) sistemos, ryšių, navigacijos ir stebėjimo (RNS) sistemos, aeronautikos informacinės sistemos, meteorologijos sistemos, saugumo operacijų centro sistemos, vidinės lėktuvų sistemos ir kitos.

Europos Komisija

Kibernetinio saugumo grėsmių nustatymas

Rizikos valdymas. Aviacijos organizacijos turi imtis atitinkamų veiksmų, kad nustatytų, įvertintų ir suprastų tinklui ir informacinėms sistemoms, palaikančioms būtinųjų funkcijų vykdymą, kylančią kibernetinio saugumo riziką.

Tam reikia bendro organizacinio rizikos valdymo, kuris turėtų:

- *užtikrinti aiškią įvairių aparatinės ir programinės įrangos sistemų, naudojamų skirtingoms paslaugoms, apžvalgą. Aviacijos srityje tokios sistemos apima informacines technologijas (IT) ir operacijų technologijas (OT);*

- *vykdyti **kibernetinio saugumo rizikos vertinimus**, kuriuose būtų atsižvelgiama į kylančias grėsmes, žinomą pažeidžiamumą ir veiklos duomenis, susijusius su taikomomis sistemomis. Įžvalgų apie grėsmes, nukreiptas prieš oro transportą, gali pateikti tokios organizacijos kaip Europos oro eismo valdymo kompiuterinių incidentų tyrimo tarnyba (EATM-CERT) ir Aviacijos keitimosi informacija ir jos analizės centras (A-ISAC);*

- *užtikrinti, kad rizikos vertinimai taip pat apimtų riziką, susijusią su kasdiene darbuotojų veikla (pvz., socialinių tinklų naudojimu, asmeninių įrenginių naudojimu, duomenų tvarkymu, keitimusi informacija ir pan.);*

- *nustatyti ir įgyvendinti rizikos valdymo priemones bei kibernetinio saugumo rizikos mažinimo planus;*

- *įgyvendinti visapusišką **informacijos saugumo valdymo sistemą** (ISMS) ir **privatumo informacijos valdymo sistemą** (PIMS), suderintą su kitomis valdymo sistemomis. Tokios valdymo sistemos (t. y. ISMS ir PIMS) apima saugumo (taip pat duomenų apsaugos ir privatumo) kontrolės įgyvendinimą siekiant sumažinti kylančias grėsmes, kurios turi poveikį aviacijos paslaugų ir sistemų (įskaitant jų duomenis) saugumui, ir užkirsti joms kelią;*

- *atsižvelgti į visus apribojimus, susijusius su **turto valdymu ir išteklių planavimu** (t. y. apribojimus, kurie gali turėti įtakos ypatingos svarbos sistemų veikimui, priežiūrai ir palaikymui vykdant esmines oro transporto funkcijas).*

Europos Komisija

Rizikos valdymo sistemų pavyzdžiai. Oro transportui pritaikytas rizikos valdymas gali būti pagrįstas įvairiomis sistemomis (pvz., ISO/IEC 27000 serijos standartais, NIST kibernetinio saugumo sistema, MITRE ATT&CK sistema, BSI IT-Grundschutz ir pan.). Rekomendacijas dėl kibernetinio saugumo rizikos vertinimo teikia tokios tarptautinės organizacijos kaip IATA ir ICAO. Gerąją oro uostų, oro eismo valdymo paslaugų teikėjų ir kitų aviacijos organizacijų saugumo užtikrinimo praktiką teikia ENISA, EASA, Eurokontrolė, Tarptautinė oro uostų taryba (ACI) ir kitos organizacijos. Bendroji įmonė SESAR koordinuoja ir telkia visą ES mokslinių tyrimų ir plėtros (MTP) veiklą oro eismo valdymo srityje, apimančią ir saugos bei saugumo aspektus.

Europos Komisija

Apsauga nuo kibernetinio saugumo grėsmių

Oro transporto organizacijos turėtų įgyvendinti tinkamas ir proporcingas saugumo priemones, kad apsaugotų savo tinklus ir informacines sistemas, tarp jų ir informacines technologijas (IT) bei operacijų technologijas (OT), nuo kibernetinių atakų. Šios saugumo priemonės yra:

- ***Saugumo politika ir procesai:*** *atitinkamos politikos ir procesų, kuriais apibrėžiama bendra esmines aviacijos funkcijas vykdyti padedančių sistemų ir duomenų apsauga, nustatymas, įgyvendinimas, pranešimas ir vykdymo užtikrinimas. Tokia saugumo politika (pvz., slaptažodžių ir duomenų saugojimo politika) bei procedūros taip pat turėtų apimti aparatinės ir programinės įrangos sistemų (įskaitant IT ir OT) pataisas ir pažeidžiamumo valdymą, incidentų valdymą, sistemos ir tinklo apsaugą.*

- ***Tapatybės ir prieigos valdymas:*** *prieigos prie tinklų ir informacinių sistemų (įskaitant IT ir OT), padedančių vykdyti esmines oro transporto funkcijas, supratimas, dokumentavimas ir valdymas. Naudotojai (arba automatinės funkcijos), turintys prieigą prie duomenų ar sistemų, tinkamai patikrinami, patvirtinama jų tapatybė ir jiems išduodami leidimai. Taip pat reikėtų atsižvelgti į skirtingus įprastų ir privilegijuotų paskyrų vaidmenis ir atsakomybę.*

- ***Duomenų ir sistemų saugumas:*** *duomenų (saugomų ir perduodamų elektroniniu būdu), ypač svarbių tinklų ir informacinių sistemų (įskaitant IT ir OT) apsauga nuo kibernetinių atakų. Atsižvelgdamos į riziką organizacijos turėtų įgyvendinti saugumo priemones, veiksmingai apribojančias atakuotojų galimybes pakenkti duomenims, tinklams ir sistemoms. Šios saugumo priemonės taip pat turėtų apimti šifravimo ir saugaus ryšio protokolų taikymą, kad duomenys, kai jie laikomi ar perduodami, būtų apsaugoti nuo kibernetinio saugumo grėsmių dėl tarpininko atakų. Be to, siekiant apsaugoti prieigą prie sistemų, tokias priemones būtina derinti su fizinio saugumo priemonėmis (pvz., sistemos turėtų būti įrengtos uždarose patalpose, į kurias patekimas ribojamas).*

- ***Tinklų ir sistemų atsparumas:*** *tinklų ir sistemų (įskaitant IT ir OT) atsparumo didinimas jas (ir jų veiklos procedūras) projektuojant ir įgyvendinant taip, kad jos būtų apsaugotos nuo kibernetinių atakų poveikio ir jis būtų sušvelnintas. Atsparumą didinančių projektavimo ir įgyvendinimo sprendimų pavyzdžiai: formaliai tikrinamos ypatingos svarbos funkcijos, sistemų ir tinklų atsarginiai pajėgumai, tinklų atskyrimas (visų pirma IT ir OT atskyrimas), daugialymenės saugumo priemonės ir daugelis kitų. Atminkite, kad informacijos saugumo požiūriu tinkami saugumo sprendimai gali būti tinklo ir sistemos atskyrimą įgyvendinantys saugumo domenai. Tačiau dėl sistemų veikimo poreikių (pvz., priežiūros veiklos, duomenų perdavimo ir pan.) gali reikėti apeiti tokius domenus arba sujungti skirtingus saugumo domenus (pvz., atskirtas sistemas ir tinklus), įskaitant IT ir OT sujungimą.*

Kibernetinio saugumo grėsmių aptikimas

Organizacijos turėtų užtikrinti nuolatinį saugumo priemonių veiksmingumą ir aptikti kibernetinio saugumo įvykius, turinčius arba galinčius turėti įtakos saugumo kontrolei bei būtinosioms paslaugoms ir sistemoms. Aptikti kibernetinio saugumo grėsmes padedančios saugumo priemonės:

- ***Saugumo stebėsena:*** *tinklų ir informacinių sistemų, įskaitant informacines technologijas (IT) ir operacijų technologijas (OT), padedančių vykdyti esmines oro transporto paslaugų funkcijas, saugumo būklės stebėsena. Duomenys, į kuriuos atsižvelgiama vykdant saugumo stebėseną, yra, pvz.:*

  - *saugos žurnalai;*
  - *virusų aptikimo žurnalai;*
  - *įsibrovimo aptikimo žurnalai;*
  - *tapatybės nustatymo, atpažinimo ir įgaliojimų žurnalai;*
  - *sistemų ir paslaugų žurnalai;*
  - *tinklo srautų žurnalai;*
  - *duomenų tvarkymo žurnalai.*

- ***Saugumo įvykių aptikimas:*** *kenkimo veiklos (t. y. saugumo įvykių), turinčios arba galinčios turėti įtakos tinklų ir informacinių sistemų (įskaitant IT ir OT), padedančių vykdyti esmines oro transporto paslaugų funkcijas, saugumui, aptikimas.*

Dėl šių priemonių gali reikėti taikyti konkrečias technologijas (pvz., saugumo informacijos ir įvykių valdymą, įsibrovimų aptikimo sistemą, įsibrovimų prevencijos sistemą ir pan.) ir įsteigti SOC (saugumo operacijų centrą) arba lygiavertę struktūrą. Kitaip tariant, reikia sukurti priemones, skirtas aptikti kibernetines atakas, jas analizuoti, į jas reaguoti ir po jų atkurti įprastą veikimą.

Nacionalinės reagavimo į kompiuterių saugumo incidentus tarnybos (CSIRT), Eurokontrolės sektorinės CERT (pvz., Europos oro eismo valdymo kompiuterinių incidentų tyrimo tarnyba EATM-CERT), komercinės oro linijų CERT ir Aviacijos keitimosi informacija ir jos analizės centras (A-ISAC) gali teikti žvalgybos informaciją apie kibernetines grėsmes (CTI) saugumo stebėsenos ir aptikimo tikslais.

Europos Komisija

Reagavimo ir atkūrimo planavimas

Organizacijos turėtų nustatyti, įgyvendinti ir išbandyti incidentų valdymo procedūras, kuriomis siekiama užtikrinti paslaugų ir sistemų veiklos tęstinumą kibernetinio saugumo incidentų atveju. Poveikio mažinimo priemonėmis siekiama suvaldyti arba apriboti kibernetinio saugumo incidentų poveikį.

Rengiant reagavimo ir atkūrimo planus, turėtų būti numatytos saugumo priemonės, kurios mažina konkrečių kibernetinių atakų poveikį, pavyzdžiui:

- *veiksmų koordinavimas ir bendradarbiavimas su nacionalinėmis CSIRT, viešosiomis ir komercinėmis CERT bei ISAC kibernetinio saugumo incidentų, incidentų koordinavimo ir krizių metu visos Europos lygmeniu;*

- *keitimasis informacija su kitomis organizacijomis, įskaitant aviacijos paslaugų teikėjus tiekimo grandinėje;*

- *periodinių **kibernetinės atakos pratybų** vykdymas (teorinio modeliavimo ir techninis koordinavimas) vertinant saugumo priemones ir procedūras, taip pat organizacijos atsparumą kibernetiniams incidentams;*

- *prieiga prie archyvų arba atsarginių saugyklų, jei kiltų pavojus duomenų saugyklų vientisumui ir prieinamumui;*

- ***saugumo vadovai** su išsamiomis kibernetinio saugumo incidentų valdymo ir paslaugų bei sistemų grąžinimo į įprastas veiklos sąlygas procedūromis;*

- *tinklo srauto peradresavimas į atsargines paslaugas, kol vyksta paslaugos trikdymo atakos;*

- *neautomatinės darbo su paslaugomis ir sistemomis prastesniuose veikimo režimuose procedūros;*

- *tvarkymosi su duomenų pažeidimais procedūrų nustatymas, įskaitant procedūras dėl duomenų pažeidimų, darančių poveikį asmens duomenims pagal Bendrąjį duomenų apsaugos reglamentą (BDAR) ir bet kurį kitą aktualų sektorinį reglamentą ar direktyvą;*

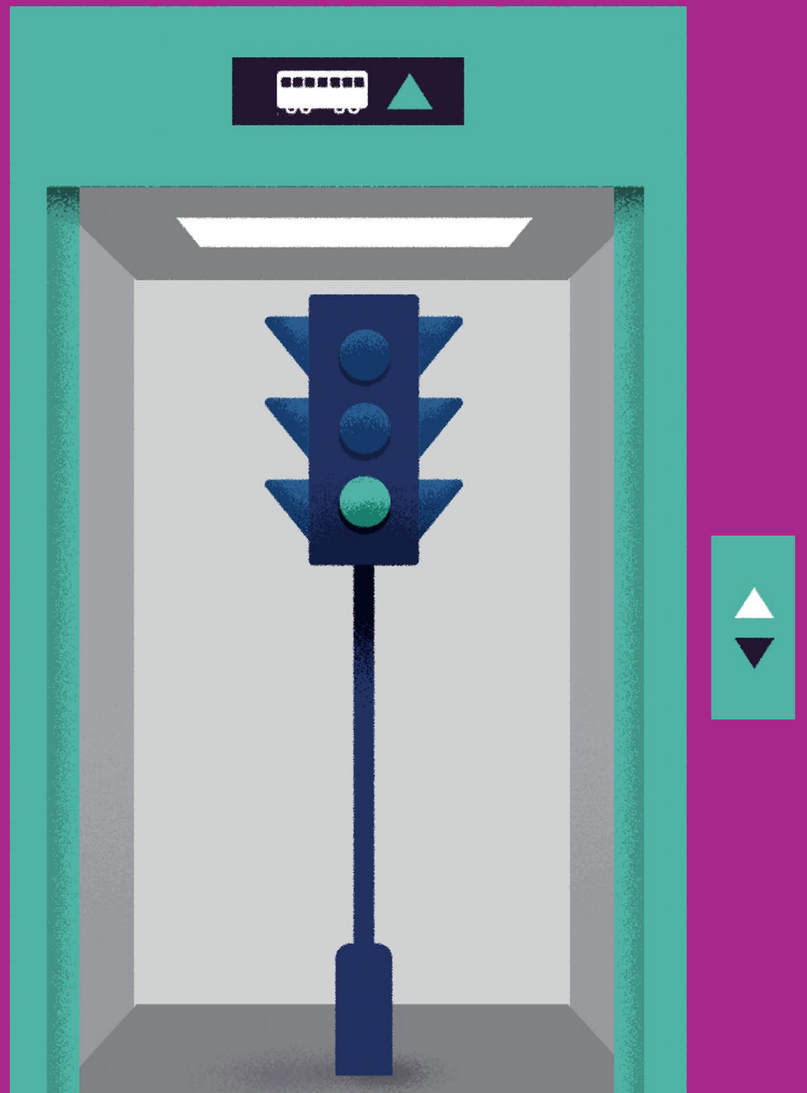
- ***kibernetinio draudimo** įsigijimas taip iš dalies kompensuojant riziką, susijusią su rimtais kibernetiniais incidentais;*

- *sutarties su viena ar keliomis specializuotomis įmonėmis sudarymas dėl papildomų pajėgumų ir kompetencijų;*

- ***keitimosi informacija apie kibernetinio saugumo incidentus** procedūrų, įskaitant pranešimo apie incidentus procedūras, nustatymas su atitinkamomis suinteresuotosiomis šalimis pagal TIS direktyvą (ES direktyva 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti).*

Europos Komisija

Geroji praktika ir saugumo priemonės, pritaikytos sausumos transportui



Valdymas

Sausumos (geležinkelių ir kelių) transporto organizacijoms reikia aiškiai suprasti kylančias grėsmes, kad galėtų nustatyti valdymo politiką ir procesus, kurie padėtų didinti veiklos paslaugų ir sistemų, tarp jų ir informacinių technologijų (IT) bei operacijų technologijų (OT), kibernetinį saugumą.

Geroji praktika bet kokio dydžio organizacijoms:

- *užtikrinti, kad vyresnioji vadovybė apie kibernetinio saugumo problemas praneštų direktoriams ir valdyboms, kurios galėtų priimti informacija pagrįstus sprendimus dėl išteklių paskirstymo;*

- *paskirti vyresnįjį pareigūną, atsakingą už kibernetinį ir fizinį saugumą bei bendrą informacinių technologijų (IT) ir operacijų technologijų (OT) saugumo valdymą, tačiau nedalyvaujantį operacijose, kad būtų išvengta interesų konfliktų;*

- *aiškiai apibrėžti su kibernetiniu saugumu susijusias pareigas, atsakomybę, kompetencijas ir leidimus, apie juos pranešti ir sutarti su atitinkamais darbuotojais. Tai ypač svarbu kompiuterinių incidentų tyrimo tarnybų (CERT) nariams;*

- *užtikrinti kibernetinio saugumo valdymą visoje saugumo paslaugų grandinėje, įskaitant fizines ir skaitmenines sąsajas, nuo technologijų gamintojų ir montuotojų iki saugumo paslaugų teikėjų;*

- *sutarti dėl kibernetinio saugumo rizikos valdymo veiklos ir kontrolės, taip pat ir bendros atsakomybės, bei užtikrinti, kad ši atsakomybė išliktų visą saugumo sprendimų ir paslaugų gyvavimo laiką (pvz., sudarant paslaugų teikimo sutartis);*

- *nustatyti valdymo mechanizmus (pvz., politiką), kad būtų laikomasi atitinkamuose reglamentuose ir direktyvose nustatytų įpareigojimų. Tai platus politikos priemonių rinkinys, apimantis konkrečias transporto rūšis, įvairaus pobūdžio suinteresuotąsias šalis (pvz., transporto priemonių ir geležinkelių sistemų gamintojus) bei TIS direktyvą (ES direktyva 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui užtikrinti).*

Europos Komisija

Sausumos transporto paslaugų ir sistemų pavyzdžiai. IT pavyzdžiai yra sistemos, prieinamos darbuotojams (pvz., asmeniniai kompiuteriai, mobilieji telefonai, biuro išoriniai įrenginiai ir pan.) bei keleiviams (pvz., viešojo „Wi-Fi“ maršruto parinktuvai, jungtys ir pan.). OT pavyzdžiai yra prižiūrimosios kontrolės ir duomenų įgijimo (SCADA) sistemos, šildymo, vėdinimo ir oro kondicionavimo (HVAC) sistemos, pasaulinės padėties nustatymo sistemos (GPS), prieigos kontrolės, stebėsenos, sekimo, reagavimo į pavojaus signalus ir filtravimo technologijos. Specialiai geležinkelių transportui skirtų sistemų pavyzdžiai: operacijų (kontrolės ir valdymo) sistemos, įskaitant signalizavimo sistemas, Europos geležinkelių eismo valdymo sistemą (ERTMS), traukinio sistemas, priežiūros sistemas ir kitas.

Kibernetinio saugumo grėsmių nustatymas

Rizikos valdymas. Sausumos transporto organizacijos turi imtis atitinkamų veiksmų, kad nustatytų, įvertintų ir suprastų tinklui ir informacinėms sistemoms, palaikančioms būtinųjų funkcijų vykdymą, kylančią kibernetinio saugumo riziką. Tam reikia bendro organizacinio rizikos valdymo, kuris turėtų:

- *užtikrinti aiškią įvairių aparatinės ir programinės įrangos sistemų, naudojamų skirtingoms paslaugoms, apžvalgą. Sausumo transporto srityje tokios sistemos apima informacines technologijas (IT) ir operacijų technologijas (OT);*

- *vykdyti **kibernetinio saugumo rizikos vertinimus**, kuriuose atsižvelgiama į kylančias grėsmes, žinomą pažeidžiamumą ir veiklos duomenis, susijusius su sistemomis, patenkančiomis į vertinimo taikymo sritį. Sausumos transporto sistemų pavyzdžiai: mokėjimo sistemos, tinklo ir ryšių sistemos (pvz., internetas, radijo ryšys, „WiFi“ ir pan.), vidinė įranga, operacijų kontrolės centrai, tapatybės valdymo sistemos, saugos sistemos ir kitos. Geležinkelių infrastruktūros sistemų pavyzdžiai: riedmenų, traukinių eismo organizavimo ir valdymo posistemiai, kontrolės, valdymo ir signalizavimo posistemiai traukinyje ir geležinkelio kelyje ir kiti;*

- *užtikrinti, kad rizikos vertinimai taip pat apimtų riziką, susijusią su kasdiene darbuotojų veikla (pvz., socialinių tinklų naudojimu, asmeninių įrenginių naudojimu, duomenų tvarkymu, keitimusi informacija ir pan.);*

- *nustatyti ir įgyvendinti rizikos valdymo priemones bei kibernetinio saugumo rizikos mažinimo planus. Pavyzdžiui, įgyvendinti visapusišką **informacijos saugumo valdymo sistemą** (ISMS) ir **privatumo informacijos valdymo sistemą** (PIMS), suderintą su kitomis valdymo sistemomis. Tokios valdymo sistemos (t. y. ISMS ir PIMS) apima saugumo (taip pat duomenų apsaugos ir privatumo) kontrolės įgyvendinimą siekiant sumažinti kylančias grėsmes, kurios turi poveikį sausumos transporto paslaugų ir sistemų (įskaitant jų duomenis) saugumui ir užkirsti joms kelią;*

- *atsižvelgti į visus apribojimus, susijusius su **turto valdymu ir išteklių planavimu** (t. y. apribojimus, kurie gali turėti įtakos ypatingos svarbos sistemų veikimui, priežiūrai ir palaikymui vykdant esmines sausumos transporto funkcijas).*

Rizikos valdymo sistemų pavyzdžiai. Kelių ir geležinkelių transportui pritaikytas rizikos valdymas gali būti pagrįstas įvairiomis sistemomis (pvz., ISO/IEC 27000 serijos standartais NIST kibernetinio saugumo sistema, MITRE ATT&CK sistema, BSI IT-Grundschutz ir pan.). Tokios organizacijos kaip ENISA nustato gerąją išmaniųjų automobilių ir išmaniojo viešojo transporto kibernetinio saugumo praktiką, kuria gali vadovautis šių sričių gamintojai ir asociacijos (pvz., Europos automobilių gamintojų asociacija – ACEA). Geležinkelių transporto srityje Europos Sąjungos geležinkelių agentūra (ESGA) nustato techninės sąveikos specifikacijas (TSS), kurias turi atitikti kiekvienas posistemis arba posistemio dalis, kad būtų įvykdyti esminiai reikalavimai ir užtikrintas Europos Sąjungos geležinkelių sistemos sąveikumas. Geležinkelių transporto inovacijų (taip pat ir kibernetinio saugumo srityje) iniciatyvas bei projektus rengia ir bendroji įmonė „Shift2Rail“.

Apsauga nuo kibernetinio saugumo grėsmių

Sausumos transporto organizacijos turėtų įgyvendinti tinkamas ir proporcingas saugumo priemones, kad apsaugotų savo tinklus ir informacines sistemas, tarp jų ir informacines technologijas (IT) bei operacijų technologijas (OT), nuo kibernetinių atakų. Šios saugumo priemonės yra:

- ***Saugos politika ir procesai:*** *atitinkamos politikos ir procesų, kuriais apibrėžiama bendra esmines sausumos transporto funkcijas vykdyti padedančių sistemų ir duomenų apsauga, nustatymas, įgyvendinimas, pranešimas ir vykdymo užtikrinimas. Tokia saugumo politika (pvz., slaptažodžių ir duomenų saugojimo politika) bei procedūros taip pat turėtų apimti aparatinės ir programinės įrangos sistemų (įskaitant IT ir OT) pataisas ir pažeidžiamumo valdymą, incidentų valdymą, sistemos ir tinklo apsaugą.*

- ***Tapatybės ir prieigos valdymas:*** *prieigos prie tinklų ir informacinių sistemų (įskaitant IT ir OT), padedančių vykdyti esmines sausumos transporto funkcijas, supratimas, dokumentavimas ir valdymas. Naudotojai (arba automatinės funkcijos), turintys prieigą prie duomenų ar sistemų, tinkamai patikrinami, patvirtinama jų tapatybė ir jiems išduodami leidimai. Taip pat reikėtų atsižvelgti į skirtingus įprastų ir privilegijuotų paskyrų vaidmenis ir atsakomybę.*

- ***Duomenų ir sistemų saugumas:*** *duomenų (saugomų ir perduodamų elektroniniu būdu), ypatingos svarbos tinklų ir informacinių sistemų (įskaitant IT ir OT) apsauga nuo kibernetinių atakų. Atsižvelgdamos į riziką organizacijos turėtų įgyvendinti saugumo priemones, veiksmingai apribojančias atakuotojų galimybes pakenkti duomenims, tinklams ir sistemoms. Šios saugumo priemonės taip pat turėtų apimti šifravimo ir saugaus ryšio protokolų taikymą, kad duomenys, kai jie laikomi ar perduodami, būtų apsaugoti nuo kibernetinio saugumo grėsmių dėl tarpininko atakų. Be to, siekiant apsaugoti prieigą prie sistemų, tokias priemones būtina derinti su fizinio saugumo priemonėmis (pvz., sistemos turėtų būti įrengtos uždarose patalpose, į kurias patekimas ribojamas). Tai labai svarbu sistemoms, kurios gali turėti įtakos žmonių gyvybės saugumui.*

- ***Tinklų ir sistemų atsparumas:*** *tinklų ir sistemų (įskaitant IT ir OT) atsparumo didinimas jas (ir jų veiklos procedūras) projektuojant ir įgyvendinant taip, kad jos būtų apsaugotos nuo kibernetinių atakų poveikio ir jis būtų sušvelnintas. Atsparumą didinančių projektavimo ir įgyvendinimo sprendimų pavyzdžiai: formaliai tikrinamos ypatingos svarbos funkcijos, sistemų ir tinklų atsarginiai pajėgumai, tinklų atskyrimas (visų pirma IT ir OT atskyrimas), daugialygmenės saugumo priemonės ir daugelis kitų. Atminkite, kad informacijos saugumo požiūriu tinkami saugumo sprendimai gali būti tinklo ir sistemos atskyrimą įgyvendinantys saugumo domenai. Tačiau dėl sistemų veikimo poreikių (pvz., priežiūros veiklos, duomenų perdavimo ir pan.) gali reikėti apeiti tokius domenus arba sujungti skirtingus saugumo domenus (pvz., atskirtas sistemas ir tinklus), įskaitant IT ir OT sujungimą.*

Europos Komisija

Kibernetinio saugumo grėsmių aptikimas

Organizacijos turėtų užtikrinti nuolatinį saugumo priemonių veiksmingumą ir aptikti kibernetinio saugumo įvykius, turinčius arba galinčius turėti įtakos saugumo kontrolei bei būtinosioms paslaugoms ir sistemoms. Aptikti kibernetinio saugumo grėsmes padedančios saugumo priemonės:

- ***Saugumo stebėsena:*** *tinklų ir informacinių sistemų, įskaitant informacines technologijas (IT) ir operacijų technologijas (OT), padedančių vykdyti esmines sausumos transporto paslaugų funkcijas, saugumo būklės stebėsena. Ji būtina norint aptikti galimas grėsmes saugumui ir stebėti nuolatinį saugumo priemonių veiksmingumą. Duomenys, į kuriuos atsižvelgiama vykdant saugumo stebėseną, yra, pvz.:*

  - *saugos žurnalai;*
  - *virusų aptikimo žurnalai;*
  - *įsibrovimo aptikimo žurnalai;*
  - *tapatybės nustatymo atpažinimo ir įgaliojimų žurnalai;*
  - *sistemų ir paslaugų žurnalai;*
  - *tinklo srautų žurnalai;*
  - *duomenų tvarkymo žurnalai.*

- ***Saugumo įvykių aptikimas:*** *kenkimo veiklos (t. y. saugumo įvykių), turinčios arba galinčios turėti įtakos tinklų ir informacinių sistemų (įskaitant IT ir OT), padedančių vykdyti esmines funkcijas, saugumui aptikimas.*

Dėl šių priemonių gali reikėti taikyti konkrečias technologijas (pvz., saugumo informacijos ir įvykių valdymą, įsibrovimų aptikimo sistemą, įsibrovimų prevencijos sistemą ir pan.) ir įsteigti SOC (saugumo operacijų centrą) arba lygiavertę struktūrą. Kitaip tariant, reikia sukurti priemones, skirtas aptikti kibernetines atakas, jas analizuoti, į jas reaguoti ir po jų atkurti įprastą veikimą.
Nacionalinės reagavimo į kompiuterių saugumo incidentus tarnybos (CSIRT), sektorinės ir komercinės CERT arba kelių ir geležinkelių operatoriai ir Europos keitimosi informacija ir jos analizės centras (ER-ISAC) gali teikti žvalgybos informaciją apie kibernetines grėsmes (CTI) saugumo stebėsenos ir aptikimo tikslais.

Reagavimo ir atkūrimo planavimas

Organizacijos turėtų nustatyti, įgyvendinti ir išbandyti incidentų valdymo procedūras, kuriomis siekiama užtikrinti paslaugų ir sistemų veiklos tęstinumą kibernetinio saugumo incidentų atveju.

Rengiant reagavimo ir atkūrimo planus, turėtų būti numatytos saugumo priemonės, kurios mažina konkrečių kibernetinių atakų poveikį, pavyzdžiui:

- *veiksmų koordinavimas ir bendradarbiavimas su nacionalinėmis CSIRT, viešosiomis ir komercinėmis CERT bei ISAC kibernetinio saugumo incidentų, incidentų koordinavimo ir krizių metu visos Europos lygmeniu;*

- *keitimasis informacija su kitomis organizacijomis, įskaitant sausumos transporto paslaugų teikėjus tiekimo grandinėje;*

- *periodinių **kibernetinės atakos pratybų** vykdymas (teorinio modeliavimo ir techninis koordinavimas) vertinant saugumo priemones ir procedūras, taip pat organizacijų atsparumą kibernetiniams incidentams;*

- *prieiga prie archyvų arba atsarginių saugyklų, jei kiltų pavojus duomenų saugyklų vientisumui ir prieinamumui;*

- ***saugumo vadovai** su išsamiomis kibernetinio saugumo incidentų valdymo ir paslaugų bei sistemų grąžinimo į įprastas veiklos sąlygas procedūromis;*

- *tinklo srauto peradresavimas į atsargines paslaugas, kol vyksta paslaugos trikdymo atakos;*

- *neautomatinės darbo su paslaugomis ir sistemomis prastesnio veikimo režimuose procedūros;*

- *tvarkymosi su duomenų pažeidimais procedūrų nustatymas, įskaitant procedūras dėl duomenų pažeidimų, darančių poveikį asmens duomenims pagal Bendrąjį duomenų apsaugos reglamentą (BDAR) ir bet kurį kitą aktualų sektorinį reglamentą ar direktyvą;*

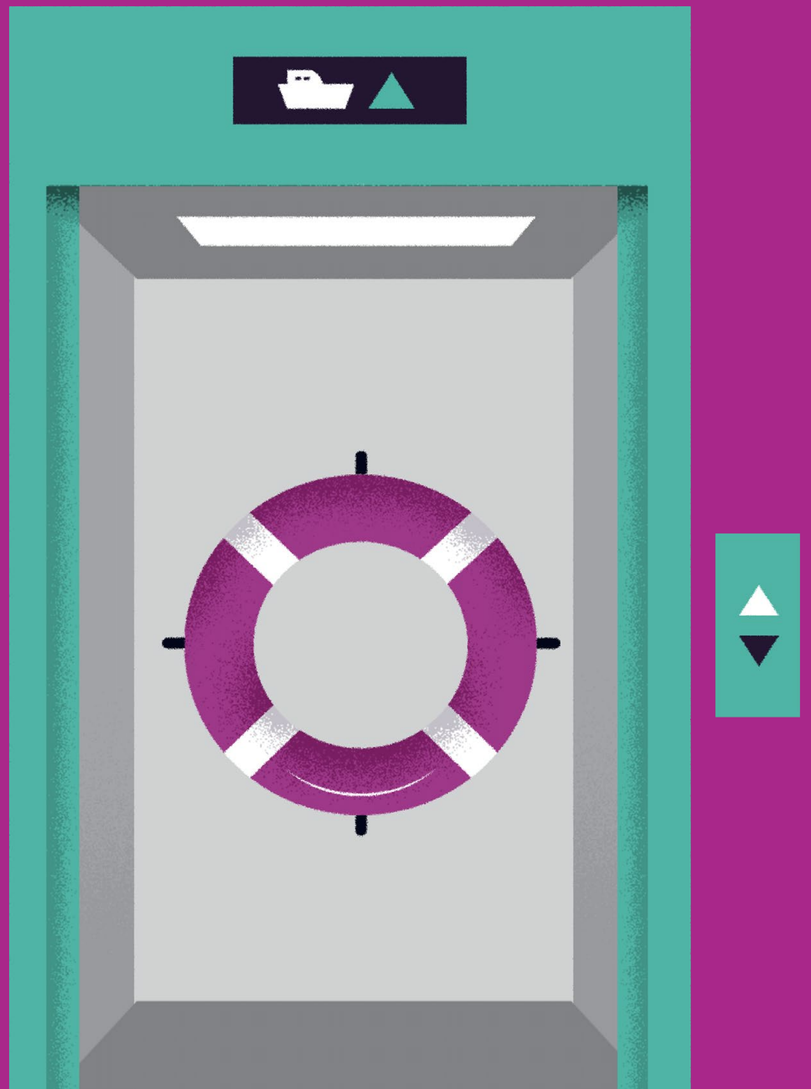
- ***kibernetinio draudimo** įsigijimas taip iš dalies kompensuojant riziką, susijusią su rimtais kibernetiniais incidentais;*

- *sutarties su viena ar keliomis specializuotomis įmonėmis sudarymas dėl papildomų pajėgumų ir kompetencijų;*

- *keitimosi informacija apie kibernetinio saugumo incidentus procedūrų, įskaitant pranešimo apie incidentus procedūras, nustatymas su atitinkamomis suinteresuotosiomis šalimis pagal TIS direktyvą (ES direktyva 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti).*

Europos Komisija

Geroji praktika ir saugumo priemonės, pritaikytos jūrų transportui



Europos Komisija

Valdymas

Jūrų transporto organizacijoms reikia aiškiai suprasti kylančias grėsmes, kad galėtų nustatyti valdymo politiką ir procesus, kurie padėtų didinti veiklos paslaugų ir sistemų, tarp jų ir informacinių technologijų (IT) bei operacijų technologijų (OT), kibernetinį saugumą.

Geroji praktika bet kokio dydžio organizacijoms:

- *užtikrinti, kad vyresnioji vadovybė apie kibernetinio saugumo problemas praneštų direktoriams ir valdyboms, kurios galėtų priimti informacija pagrįstus sprendimus dėl išteklių paskirstymo;*

- *paskirti vyresnįjį pareigūną, atsakingą už bendrą informacinių technologijų (IT) ir operacijų technologijų (OT) saugumo valdymą. Šis pareigūnas turėtų būti atsakingas tiek už kibernetinį, tiek už fizinį saugumą;*

- *aiškiai apibrėžti su kibernetiniu saugumu susijusias pareigas, atsakomybę, kompetencijas ir leidimus, apibrėžti pakrantės ir laivų darbuotojų įgaliojimų lygius ir tarpusavio ryšio linijas bei dėl to sutarti su atitinkamais darbuotojais. Tai ypač svarbu kompiuterinių incidentų tyrimo tarnybų (CERT) nariams. Darbuotojai, kurių pareigos susijusios su tokiais ES jūrų saugumo ir saugios laivybos aktais, pavyzdžiui, uosto objektų saugumo pareigūnai, uosto saugumo pareigūnai, įmonių saugumo pareigūnai arba paskirtasis asmuo krante (DPA) ir laivo kapitonas, turėtų bent jau būti susipažinę su organizacijos taikomomis kibernetinio saugumo priemonėmis;*

- *užtikrinti kibernetinio saugumo valdymą visoje saugumo paslaugų grandinėje, įskaitant fizines ir skaitmenines sąsajas, nuo technologijų gamintojų ir montuotojų iki saugumo paslaugų teikėjų;*

- *sutarti dėl kibernetinio saugumo rizikos valdymo veiklos ir kontrolės, taip pat ir bendros atsakomybės, bei užtikrinti, kad ši atsakomybė išliktų visą saugumo sprendimų ir paslaugų gyvavimo laiką (pvz., sudarant paslaugų teikimo sutartis);*

- *nustatyti valdymo mechanizmus (pvz., politiką), kad būtų laikomasi atitinkamuose reglamentuose ir direktyvose nustatytų įpareigojimų, pavyzdžiui, Reglamente (ES) 2019/1239, kuriuo nustatoma Europos jūrų sektoriaus vieno langelio aplinka, Reglamente (EB) Nr. 725/2004 dėl laivų ir uostų įrenginių apsaugos stiprinimo, Direktyvoje 2005/65/EB dėl uostų apsaugos stiprinimo, Reglamente (EB) Nr. 336/2006 dėl Tarptautinio saugaus valdymo kodekso įgyvendinimo ir Rezoliucijoje A.741 (18), kuria patvirtinamas Tarptautinis saugaus laivų eksploatavimo ir taršos prevencijos valdymo kodeksas. Šiuo atveju taip pat svarbu paminėti bendrą keitimosi informacija aplinką (BKIA) – ES iniciatyvą, kuria siekiama užtikrinti, kad Europos ir valstybių narių stebėjimo sistemos turėtų gerą tarpusavio sąveiką, kad visos susijusios institucijos galėtų susipažinti su įslaptinta ir neįslaptinta informacija, kurios joms reikia, kad galėtų vykdyti misijas jūroje.*

Jūrų transporto paslaugų ir sistemų pavyzdžiai. IT pavyzdžiai yra sistemos, prieinamos darbuotojams (pvz., asmeniniai kompiuteriai, mobilieji telefonai, biuro išoriniai įrenginiai ir pan.) bei keleiviams (pvz., viešojo „Wi-Fi“ maršruto parinktuvai, jungtys ir pan.). OT pavyzdžiai yra prižiūrimosios kontrolės ir duomenų įgijimo (SCADA) sistemos, šildymo, vėdinimo ir oro kondicionavimo (HVAC) sistemos, pasaulinės padėties nustatymo sistemos (GPS), prieigos kontrolės, stebėsenos, sekimo, reagavimo į pavojaus signalus, filtravimo technologijos, laivo navigacijos sistemos, „SafeSeaNet“, tiltų sistemos, krovinių tvarkymo ir valdymo sistemos, variklių ir mašinų valdymo ir elektros kontrolės sistemos, prieigos kontrolės sistemos, keleivių aptarnavimo ir valdymo sistemos, į keleivius orientuoti viešieji tinklai, administracinės ir įgulos gerovės sistemos, ryšių sistemos ir kitos.

Europos Komisija

Kibernetinio saugumo grėsmių nustatymas

Rizikos valdymas. Jūrų organizacijos turi imtis atitinkamų veiksmų, kad gebėtų nustatyti, analizuoti, įvertinti ir pranešti apie kibernetinio saugumo riziką, taip pat gebėtų šią riziką priimti, jos išvengti, ją perkelti arba sumažinti iki priimtino lygio. Tam reikia bendro organizacinio rizikos valdymo, kuris turėtų:

- *užtikrinti aiškią įvairių aparatinės ir programinės įrangos sistemų, naudojamų skirtingoms paslaugoms, apžvalgą. Jūrų transporto srityje tokios sistemos apima informacines technologijas (IT) ir operacijų technologijas (OT) ir jų ryšio bei integracijos su pakrante, įskaitant valdžios institucijas, jūrų terminalus ir uosto krovėjus, pobūdį;*

- *nustatyti ir įvertinti pagrindines laivų operacijas, kurias gali pažeisti kibernetinės atakos, ir vykdyti kibernetinio saugumo rizikos vertinimus (taip pat ir vertinant galimą poveikį veiklai bei jo tikimybę), kuriuose turėtų būti atsižvelgiama į kylančias grėsmes, žinomą pažeidžiamumą ir veiklos duomenis, susijusius su taikomomis sistemomis. Jei reikia, pateikiamos nuorodos į laivų (SSA), uosto objektų (PFSA) ir uostų (PSA) saugumo vertinimus, nustatytus ES jūrų saugumo teisės aktuose. Juose įvardijamos galimos saugumo grėsmės uosto infrastruktūrai ir saugumo trūkumai. Be to, įžvalgų apie prieš jūrų transportą nukreiptas grėsmes gali pateikti tokios jūrų organizacijos kaip Tarptautinė jūrų organizacija (IMO) ir jūrų ISAC;*

- *užtikrinti, kad rizikos vertinimai taip pat apimtų riziką, susijusią su kasdiene darbuotojų veikla (pvz., socialinių tinklų naudojimu, asmeninių įrenginių naudojimu, duomenų tvarkymu, keitimusi informacija ir pan.);*

- *nustatyti ir įgyvendinti rizikos valdymo priemones bei kibernetinio saugumo rizikos mažinimo planus. Pavyzdžiui, įgyvendinti visapusišką informacijos saugumo valdymo sistemą (ISMS) ir privatumo informacijos valdymo sistemą (PIMS), suderintą su kitomis valdymo sistemomis, pavyzdžiui, saugos valdymo sistemomis pagal tarptautinį saugaus valdymo (ISM) kodeksą. Tokios valdymo sistemos (t. y. ISMS ir PIMS) apima saugumo (taip pat duomenų apsaugos ir privatumo) kontrolės įgyvendinimą siekiant sumažinti kylančias grėsmes, kurios turi poveikį jūrų paslaugų ir sistemų (įskaitant jų duomenis) saugumui, ir užkirsti joms kelią;*

- *atsižvelgti į visus apribojimus, susijusius su **turto valdymu ir išteklių planavimu** (t. y. apribojimus, kurie gali turėti įtakos ypatingos svarbos sistemų veikimui, priežiūrai ir palaikymui vykdant esmines jūrų transporto funkcijas). Atlikdami vertinimus, prireikus pateikite kryžmines nuorodas į ISM kodekso, saugos valdymo sistemų ir saugumo planų, įgyvendinamų pagal ES jūrų saugos ir saugumo teisės aktus, reikalavimus.*

Rizikos valdymo sistemų pavyzdžiai. Jūrų transportui pritaikytas rizikos valdymas gali būti pagrįstas įvairiomis sistemomis (pvz., ISM kodeksu arba ISO/IEC 27000 serijos standartais, NIST kibernetinio saugumo sistema, MITRE ATT&CK sistema, BSI IT-Grundschutz ir pan.). NIST kibernetinio saugumo sistema taip pat pritaikyta jūrinių skystų piltinių krovinių perdavimo (MBLT), operacijų jūroje ir keleivinių laivų operacijų kibernetiniam saugumui užtikrinti. Panašiai, Baltijos ir tarptautinė jūrininkystės taryba (BIMCO) išleido dokumentą *„The Guidelines on Cyber Security Onboard Ships“*, o Tarptautinė jūrų organizacija (IMO) paskelbė konkrečias gaires *„Guidelines on maritime cyber risk management“* (MSC-FAL.1/Circ.3). ENISA atliko keletą tyrimų, susijusių su gerąja jūrų (visų pirma uostų) kibernetinio saugumo praktika. EMSA teikia paslaugas jūrų bendruomenei, tarp jų ir informuotumo apie kibernetinį saugumą mokymus. Konkretūs saugumo ir saugos reikalavimai jūrų transporto sistemoms ir tinklams taip pat nustatyti atitinkami standartuose (pvz. IEC 61162-460:2018 dėl jūrų navigacijos ir radijo ryšio įrangos bei sistemų saugos ir saugumo, ISO 16425:2013 dėl laivų ir jūrų technologijų, IEC 62443-4-1:2018 dėl pramonės automatizavimo ir valdymo sistemų saugumo).

Apsauga nuo kibernetinio saugumo grėsmių

Jūrų transporto organizacijos turėtų įgyvendinti tinkamas ir proporcingas saugumo priemones, kad apsaugotų savo tinklus ir informacines sistemas, tarp jų ir informacines technologijas (IT) bei operacijų technologijas (OT). Šios saugumo priemonės yra:

- ***Saugos politika ir procesai:*** *atitinkamos politikos ir procesų, kuriais apibrėžiama bendra esmines jūrų transporto funkcijas vykdyti padedančių sistemų ir duomenų apsauga, nustatymas, įgyvendinimas, pranešimas ir vykdymo užtikrinimas. Saugumo priemonės (įskaitant kibernetinio ir fizinio saugumo priemones) turėtų būti įtrauktos į atitinkamus planus, pavyzdžiui, saugos valdymo sistemą ir laivo saugumo planą. Tokia saugumo politika (pvz., slaptažodžių ir duomenų saugojimo politika) bei procedūros taip pat turėtų apimti aparatinės ir programinės įrangos sistemų (įskaitant IT ir OT) pataisas ir pažeidžiamumo valdymą, incidentų valdymą, sistemos ir tinklo apsaugą.*

- ***Tapatybės ir prieigos valdymas:*** *prieigos prie tinklų ir informacinių sistemų (įskaitant IT ir OT), padedančių vykdyti esmines jūrų transporto funkcijas, supratimas, dokumentavimas ir valdymas. Naudotojai (arba automatinės funkcijos), turintys prieigą prie duomenų ar sistemų, tinkamai patikrinami, patvirtinama jų tapatybė ir jiems išduodami leidimai. Taip pat reikėtų atsižvelgti į skirtingus įprastų ir privilegijuotų paskyrų vaidmenis ir atsakomybę.*

- ***Duomenų ir sistemų saugumas:*** *duomenų (saugomų ir perduodamų elektroniniu būdu), ypatingos svarbos tinklų ir informacinių sistemų (įskaitant IT ir OT) apsauga nuo kibernetinių atakų. Atsižvelgdamos į riziką organizacijos turėtų įgyvendinti saugumo priemones, veiksmingai apribojančias atakuotojų galimybes pakenkti duomenims ir sistemoms. Šios saugumo priemonės taip pat turėtų apimti šifravimo ir saugaus ryšio protokolų taikymą, kad duomenys, kai jie laikomi ar perduodami, būtų apsaugoti nuo kibernetinio saugumo grėsmių dėl tarpininko atakų. Be to, siekiant apsaugoti prieigą prie sistemų, tokias priemones būtina derinti su fizinio saugumo priemonėmis (pvz., sistemos turėtų būti įrengtos uždarose patalpose, į kurias patekimas ribojamas). Tai labai svarbu sistemoms, kurios gali turėti įtakos žmonių gyvybės saugumui (pvz., II ir III kategorijų navigacijos ir radijo ryšio sistemoms).*

- ***Tinklų ir sistemų atsparumas:*** *tinklų ir sistemų (įskaitant IT ir OT) atsparumo didinimas jas (ir jų veiklos procedūras) projektuojant ir įgyvendinant taip, kad jos būtų apsaugotos nuo kibernetinių atakų poveikio ir jis būtų sušvelnintas. Atsparumą didinančių projektavimo ir įgyvendinimo sprendimų pavyzdžiai: formaliai tikrinamos ypatingos svarbos funkcijos, sistemų ir tinklų atsarginiai pajėgumai, tinklų atskyrimas (visų pirma IT ir OT atskyrimas), daugialygmenės saugumo priemonės ir daugelis kitų. Atminkite, kad informacijos saugumo požiūriu tinkami saugumo sprendimai gali būti tinklo ir sistemos atskyrimą įgyvendinantys saugumo domenai. Tačiau dėl sistemų (pvz., autonominių antvandeninių jūrų laivų, MASS) poreikių (pvz., priežiūros veiklos, duomenų perdavimo ir pan.) gali reikėti apeiti tokius domenus arba sujungti skirtingus saugumo domenus (pvz., atskirtas sistemas ir tinklus), įskaitant IT ir OT sujungimą.*

Kibernetinio saugumo grėsmių aptikimas

Organizacijos turėtų užtikrinti nuolatinį saugumo priemonių veiksmingumą ir aptikti kibernetinio saugumo įvykius, turinčius arba galinčius turėti įtakos saugumo kontrolei bei būtinosioms paslaugoms ir sistemoms. Aptikti kibernetinio saugumo grėsmes padedančios saugumo priemonės:

- ***Saugumo stebėsena:*** *tinklų ir informacinių sistemų, įskaitant informacines technologijas (IT) ir operacijų technologijas (OT), padedančių vykdyti esmines jūrų transporto paslaugų funkcijas, saugumo būklės stebėsena. Ji būtina norint aptikti galimas grėsmes saugumui ir stebėti nuolatinį saugumo priemonių veiksmingumą. Duomenys, į kuriuos atsižvelgiama vykdant saugumo stebėseną, yra, pvz.:*

  - *saugos žurnalai;*
  - *virusų aptikimo žurnalai;*
  - *įsibrovimo aptikimo žurnalai;*
  - *tapatybės nustatymo atpažinimo ir įgaliojimų žurnalai;*
  - *sistemų ir paslaugų žurnalai;*
  - *tinklo srautų žurnalai;*
  - *duomenų tvarkymo žurnalai.*

- ***Saugumo įvykių aptikimas:*** *kenkimo veiklos (t. y. saugumo įvykių), turinčios arba galinčios turėti įtakos tinklų ir informacinių sistemų (įskaitant IT ir OT), padedančių vykdyti esmines jūrų transporto paslaugų funkcijas, saugumui aptikimas.*

Dėl šių priemonių gali reikėti taikyti konkrečias technologijas (pvz., saugumo informacijos ir įvykių valdymą, įsibrovimų aptikimo sistemą, įsibrovimų prevencijos sistemą ir pan.) ir įsteigti SOC (saugumo operacijų centrą) arba lygiavertę struktūrą. Kitaip tariant, reikia sukurti priemones, skirtas aptikti kibernetines atakas, jas analizuoti, į jas reaguoti ir po jų atkurti įprastą veikimą.

Nacionalinės reagavimo į kompiuterių saugumo incidentus tarnybos (CSIRT), sektorinės CERT ir komercinės jūrų operatorių CERT, jūrų ISAC gali teikti žvalgybos informaciją apie kibernetines grėsmes (CTI) saugumo stebėsenos ir aptikimo tikslais.

Reagavimo ir atkūrimo planavimas

Organizacijos turėtų nustatyti, įgyvendinti ir išbandyti incidentų valdymo procedūras, kuriomis siekiama užtikrinti paslaugų ir sistemų veiklos tęstinumą kibernetinio saugumo incidentų atveju.
Rengiant reagavimo ir atkūrimo planus, turėtų būti numatytos saugumo priemonės, kurios mažina konkrečių kibernetinių atakų poveikį, pavyzdžiui:

- *tinklo srauto peradresavimas į atsargines paslaugas, kol vyksta paslaugos trikdymo atakos;*
- *neautomatinės darbo su paslaugomis ir sistemomis prastesnio veikimo režimuose procedūros;*
- *treniruočių ir pratybų programų sukūrimas (pvz., teorinio modeliavimo, techninės ir reagavimo pratybos) siekiant reaguoti į kibernetines atakas ir ekstremalias situacijas bei vertinti saugumo priemones, procedūras ir organizacijos atsparumą kibernetiniams incidentams;*
- *prieiga prie archyvų arba atsarginių saugyklų, jei kiltų pavojus duomenų saugyklų vientisumui ir prieinamumui;*
- *veiksmų koordinavimas ir bendradarbiavimas su nacionalinėmis CSIRT, viešosiomis ir komercinėmis CERT bei ISAC kibernetinio saugumo incidentų, incidentų koordinavimo ir krizių metu visos Europos lygmeniu;*
- *keitimasis informacija su kitomis organizacijomis, įskaitant jūrų transporto paslaugų teikėjus tiekimo grandinėje;*
- *saugumo vadovai su išsamiomis kibernetinio saugumo incidentų valdymo ir paslaugų bei sistemų grąžinimo į įprastas veiklos sąlygas procedūromis;*
- *tvarkymosi su duomenų pažeidimais procedūrų nustatymas, įskaitant procedūras dėl duomenų pažeidimų, darančių poveikį asmens duomenims pagal Bendrąjį duomenų apsaugos reglamentą (BDAR) ir bet kurį kitą aktualų sektorinį reglamentą ar direktyvą;*
- *kibernetinio draudimo įsigijimas taip iš dalies kompensuojant riziką, susijusią su rimtais kibernetiniais incidentais;*
- *sutarties su viena ar keliomis specializuotomis įmonėmis sudarymas dėl papildomų pajėgumų ir kompetencijų;*
- *keitimosi informacija apie kibernetinio saugumo incidentus (taip pat neatitikties atvejus, avarijas ir pavojingas situacijas) procedūrų, įskaitant pranešimo apie incidentus procedūras, nustatymas su atitinkamomis suinteresuotosiomis šalimis pagal TIS direktyvą (ES direktyva 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti).*

Liuksemburgas: Europos Sąjungos leidinių biuras, 2021

Print ISBN 978-92-76-40506-1 doi:10.2832/105389 MI-05-21-230-LT-C
PDF ISBN 978-92-76-40478-1 doi:10.2832/776967 MI-05-21-230-LT-N

Europos Sąjungos leidinių biuras