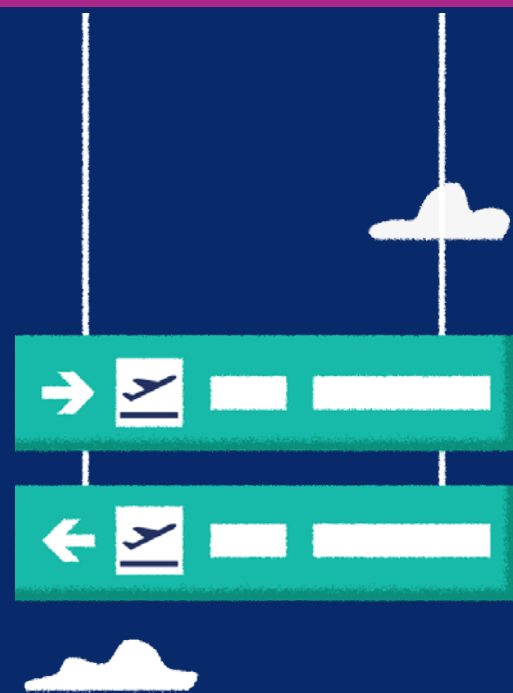
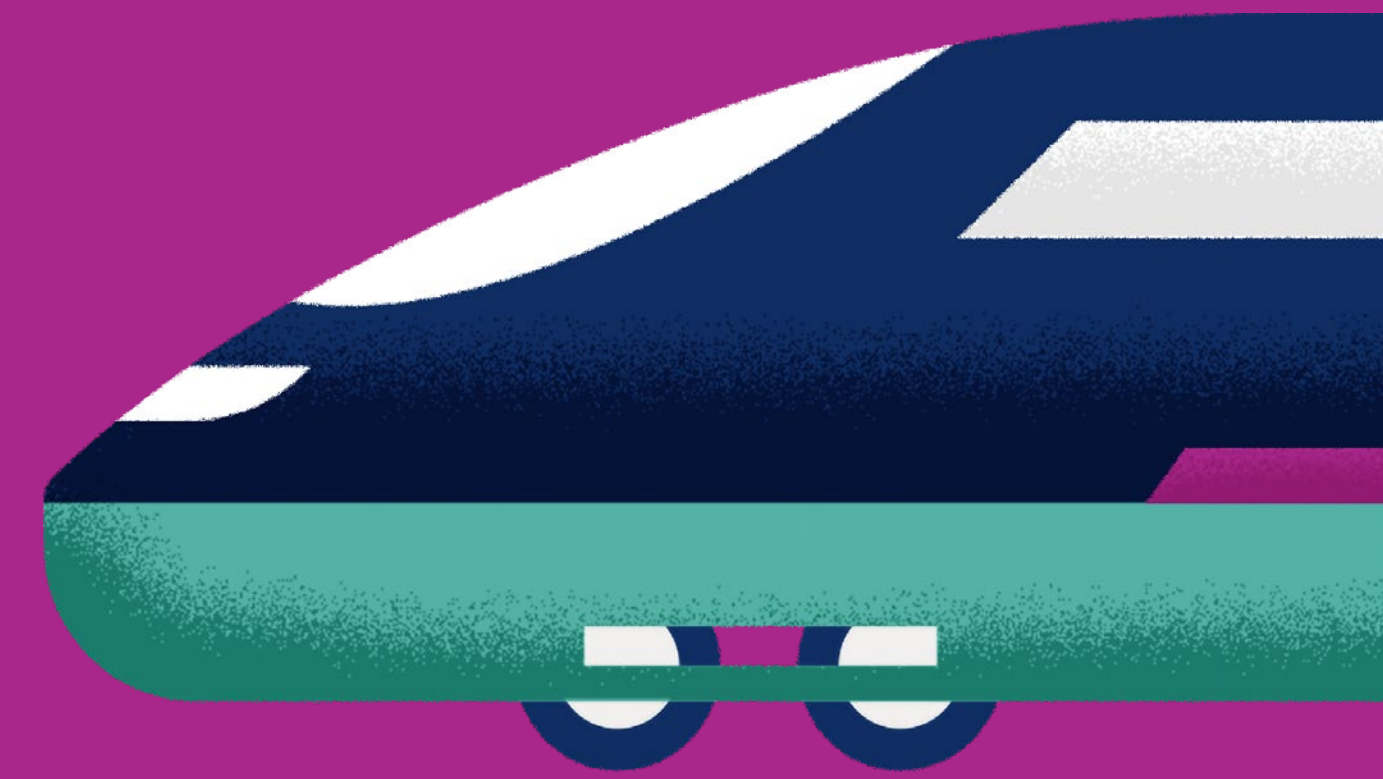
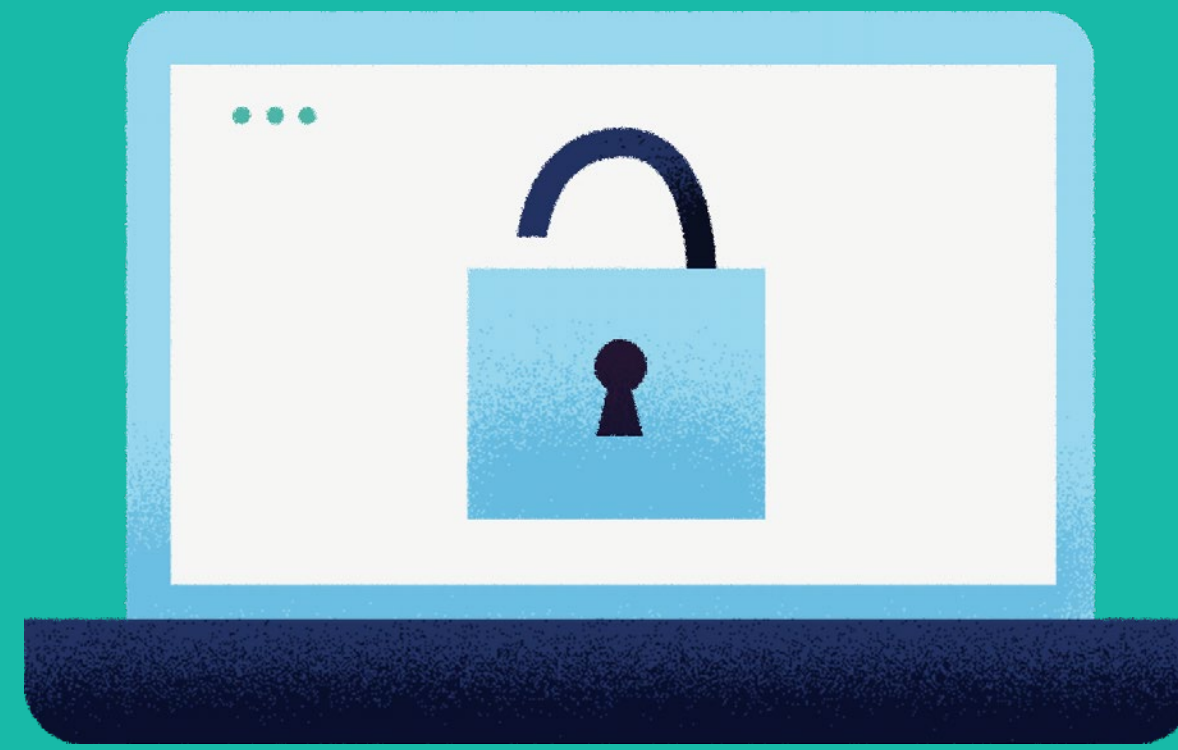
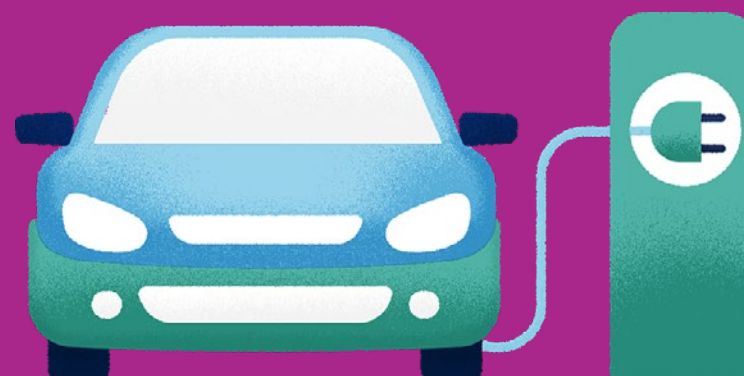
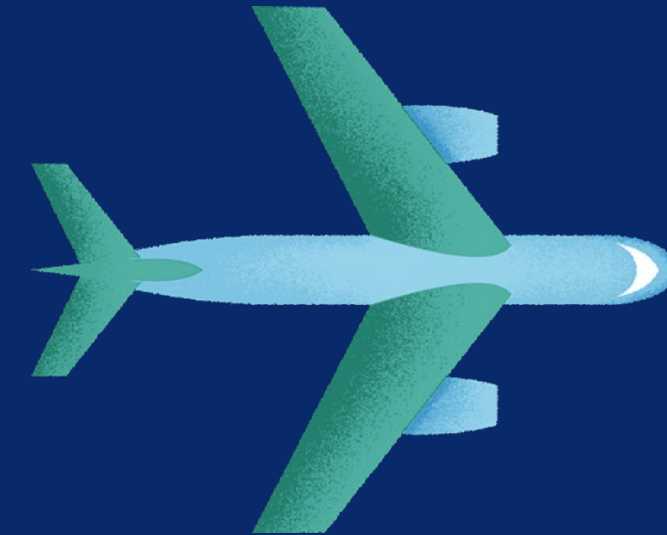
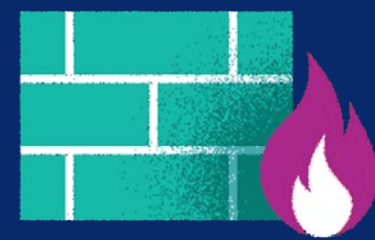


Setul de instrumente privind securitatea cibernetică în domeniul transporturilor



Introducere

Direcția Generală Mobilitate și Transporturi a Comisiei Europene (DG MOVE) a contractat elaborarea acestui set de instrumente pentru a spori gradul de conștientizare și de pregătire a părților interesate din domeniul transporturilor la amenințările cibernetice. Acesta oferă informații pentru înțelegerea amenințărilor cibernetice și pentru atenuarea impactului acestora asupra serviciilor, sistemelor și operațiunilor de transport. Prezentul set de instrumente oferă căi alternative de conștientizare care se adresează diferitelor profiluri de transport:

- întregul personal din sectorul transporturilor (furnizarea de informații și orientări generale)
- factorii de decizie în materie de securitate cibernetică în domeniul transporturilor pentru diferitele moduri de transport.

Hyperlinkurile conectează diferitele părți care alcătuiesc setul de instrumente în scopul sprijinirii navigabilității printre căile de conștientizare adaptate la profilurile de transport specifice.

Practicile enumerate în prezentul set de instrumente au un caracter pur consultativ. Orice recomandare formulată nu creează obligații și nu este obligatorie. În plus, prezentul set de instrumente nu reprezintă opiniile oficiale ale Comisiei Europene și nu este menit să ofere mijloace de conformare cu legislația existentă sau viitoare a UE.



Profiluri de conștientizare a securității cibernetice

Profilul I: întregul personal din sectorul transporturilor. Prima cale se adresează întregului personal din cadrul organizațiilor de transport, de la personalul implicat în operațiunile serviciilor de transport până la personalul administrativ. Aceasta oferă orientări pentru sporirea gradului de înțelegere și de conștientizare a celor mai frecvente amenințări cibernetice care vizează serviciile și sistemele de transport. În plus, aceasta oferă informații cu privire la modul de abordare a potențialelor amenințări cibernetice, inclusiv identificarea, raportarea și combaterea acestora cu ajutorul celor mai bune practici în materie de securitate cibernetică.

Profilul II: factorii de decizie în materie de securitate cibernetică în domeniul transporturilor. A doua cale se adresează personalului cu responsabilități decizionale în materie de securitate cibernetică din cadrul organizațiilor de transport. Această cale evidențiază bunele practici adaptate la diferitele moduri de transport pentru consolidarea poziției organizațiilor de transport în materie de securitate cibernetică. În special, aceasta oferă bune practici pentru a identifica, proteja, detecta și răspunde la amenințările cibernetice emergente care vizează organizațiile de transport.

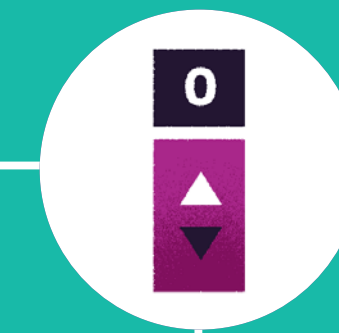


Setul de instrumente privind securitatea cibernetică în domeniul transporturilor



Peisajul amenințărilor în sectorul transporturilor

Amenințări emergente la adresa securității cibernetice
care afectează diferite moduri de transport



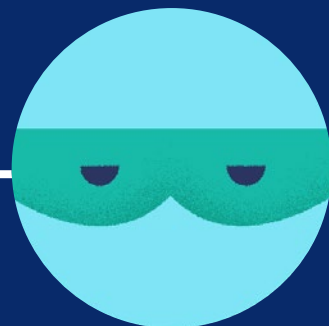
Profiluri de conștientizare a securității cibernetice

Căi alternative de conștientizare care vizează diferite
profiluri de transport

Peisajul amenințărilor în sectorul transporturilor

Peisajul amenințărilor cibernetice este dinamic și evoluează în permanență. Cu toate acestea, este posibilă identificarea amenințărilor cibernetice cu care se confruntă toate modurile de transport în cadrul operațiunilor serviciilor și sistemelor.





Actorii care generează amenințări

Persoane fizice sau organizații care ar putea avea un impact asupra siguranței și securității serviciilor și sistemelor de transport



Amenințări cibernetice emergente

Amenințări cibernetice selectate care ar putea reprezenta vectori de atac care au un impact asupra siguranței și securității serviciilor și sistemelor de transport

Actorii care generează amenințări

Persoane fizice sau organizații pot expune și exploata în mod intenționat sau neintenționat vulnerabilitățile care au potențialul de a provoca incidente și de a afecta serviciile de transport, inclusiv siguranța, securitatea, afacerile, finanțele și reputația acestora. Actorii care generează amenințări includ, printre alții, grupuri sponsorizate de stat, infractori cibernetici, teroriști cibernetici, hacktiviști, hackeri (inclusiv script kiddies) și persoane interne (inclusiv persoane care au acces la informații privilegiate).

Cei mai importanți actori răuvoitori care vizează în mod intenționat organizațiile de transport sunt **infractori cibernetici, persoane interne, state naționale și grupuri sponsorizate de stat**.

Adversari precum **infractorii cibernetici** desfășoară campanii ample de atac și se află adesea în joc pentru recompense financiare.

Persoanele interne cunosc particularitățile organizațiilor pentru care lucrează și sunt adesea foarte familiarizate

cu anumite vulnerabilități subtile în materie de securitate. Actorii care generează amenințări din interior pot include angajați, furnizori și contractanți individuali nemulțumiți. Pe măsură ce tensiunile geopolitice globale se intensifică, **statele naționale și grupurile sponsorizate de stat** vizează obiective strategice pe termen lung. Adesea, acestea încearcă să infiltreze în profunzimea sistemelor organizațiilor și să colecteze informații sensibile. Odată ce își stabilesc baza în sisteme, atacatorii sponsorizați de stat încearcă să obțină o poziție cu potențial de a provoca cele mai grave prejudicii posibile. De exemplu, aceștia pot viza sistemele altor organizații prin exploatarea conexiunilor acestora la rețea.

Alți actori care generează amenințări includ **persoane interne**, care pot efectua, în mod neintenționat sau accidental, acțiuni care conduc la evenimente de securitate cibernetică și, în cele mai grave cazuri, la incidente cibernetice care afectează siguranța și securitatea serviciilor de transport.



Amenințări cibernetice emergente

Există un număr considerabil de amenințări cibernetice care vizează transporturile: **blocarea distribuită a serviciului**, **blocarea serviciului**, furtul de date, difuzarea de **programe malware**, **phishingul**, manipularea software-ului, **accesul neautorizat**, atacurile distructive, falsificarea sau ocolirea procesului decizional al operatorului de securitate, mascarea identității, abuzul de privilegii de acces, **ingineria socială**, vandalizarea, atacurile de interceptare, utilizarea abuzivă a activelor și manipularea hardware-ului. Pe baza cercetărilor cuprinzătoare din literatura de specialitate a documentelor disponibile publicului și a interviurilor cu experți, cele mai presante amenințări cibernetice emergente care afectează transporturile sunt: programe malware, blocarea (distribuită) a serviciului, accesul neautorizat și furtul, precum și manipularea software-ului.



Amenințarea #1: Program malware

Software răuvoitor care ar putea afecta persoane sau organizații din toate modurile de transport



Amenințarea #2: Blocarea (distribuită) a serviciului

Atacuri de securitate cibernetică care împiedică accesul persoanelor fizice sau al organizațiilor la serviciile și resursele de transport relevante



Amenințarea #3: Accesul neautorizat și furtul

Accesul, însușirea și exploatarea neautorizate ale unor active strategice



Amenințarea #4: Manipularea software-ului

Atacuri de securitate cibernetică care vizează modificarea comportamentului software-ului pentru a desfășura atacuri specifice



Amenințarea #1: Programe malware

Programul malware este un software răuvoitor, care poate include diferite tipuri de aplicații software, cum ar fi viruși, troieni, viermi, programe de tip ransomware, mineri de criptomonede sau orice software care ar putea avea efecte negative asupra unor organizații sau persoane fizice din toate modurile de transport.

Atenuarea răspândirii programelor malware concepute pentru a aduce prejudicii în mod intenționat unor computere, servere, clienți, rețele sau tuturor acestora la un loc se numără printre prioritățile în materie de securitate cibernetică în toate modurile de transport. Un vector de atac tipic poate implica phishingul de e-mailuri care îi vizează pe angajați. Alți vectori de atac pot implica strategii diferite și sofisticate de inginerie socială, cum ar fi conectarea

unei unități flash pentru USB la un port liber (de exemplu, încărcarea telefonului mobil). Făcând clic pe hyperlinkuri în e-mailuri suspecte sau prin deschiderea unor fișiere atașate, utilizatorul poate instala în necunoștință de cauză un software sau poate pune în pericol cu bună știință servicii și resurse de transport.

De exemplu, atacul cibernetic de tip ransomware WannaCry a afectat peste 150 de țări și a infectat peste 230 000 de sisteme. Aceasta a implicat un program de tip ransomware care se răspândește de obicei prin phishingul unor e-mailuri care conțin fișiere atașate sau hyperlinkuri răuvoitoare. Acest tip de atac exploatează ingineria socială în mod răuvoitor pentru a-i determina în mod eronat pe utilizatorii sistemului să instaleze (sau să activeze) programe malware specifice.

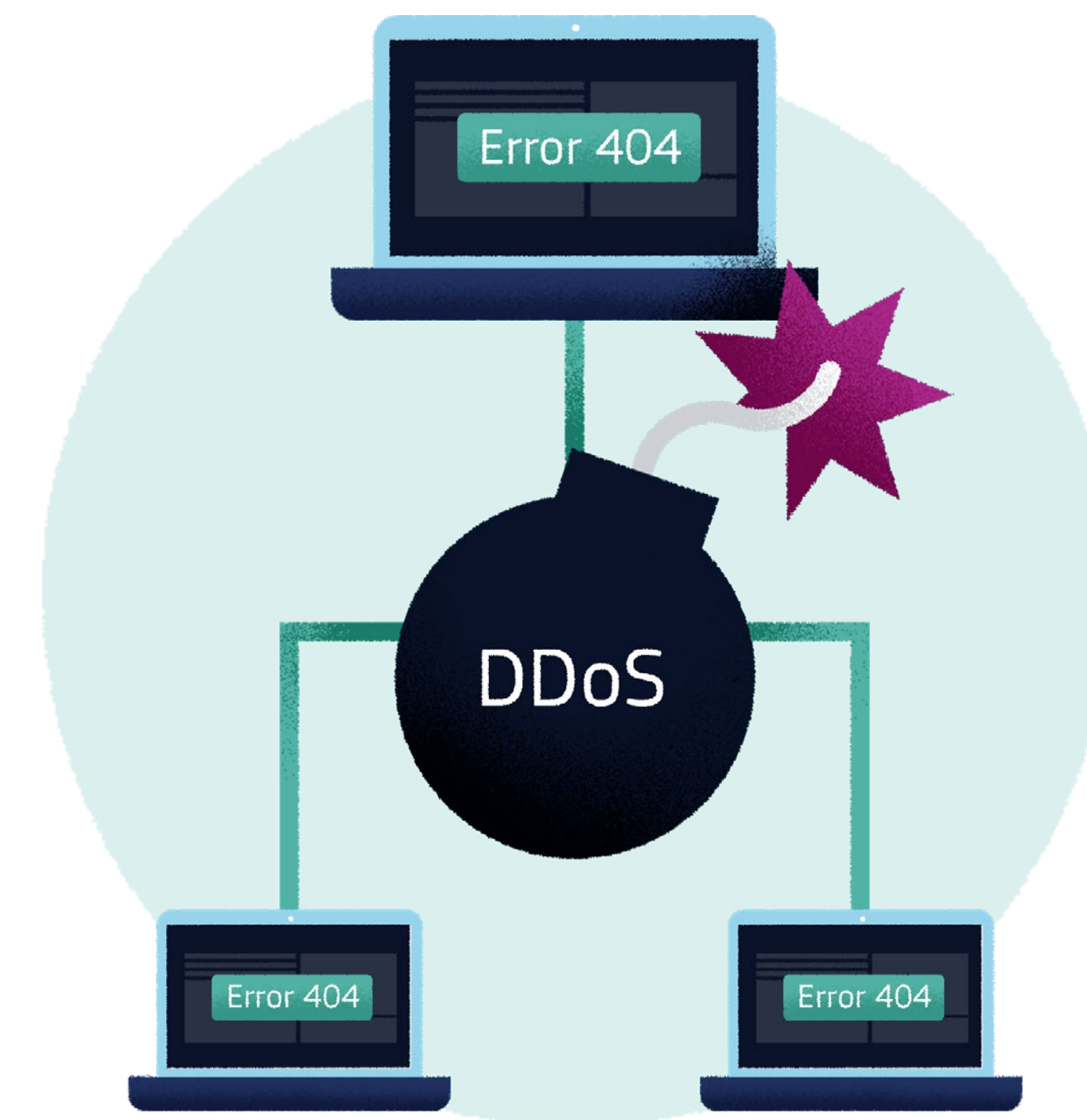


Amenințarea #2: Blocarea (distribuită) a serviciului

Atacurile de tip blocarea distribuită a serviciului (Distributed Denial of Service - DDoS) și blocarea serviciului (Denial of Service - DoS) afectează disponibilitatea și accesibilitatea datelor, serviciilor, sistemelor și a altor resurse. Aceste tipuri de atacuri pot avea o durată mai mare și pot viza simultan mai multe servicii sau sisteme. Atacurile de tip DDoS utilizează mai multe sisteme (sau canale de atac) pentru a supraîncărca cu cereri serviciile sau sistemele vizate. Atacurile reușite afectează capacitățile serviciului și ale sistemului de prelucra un număr neașteptat de mare de cereri. Acest lucru duce la blocarea accesului la servicii și la resurse.

Trebuie remarcat faptul că serviciile și sistemele afectate ale unor organizații de transport pot fi exploatate pentru a desfășura atacuri de tip DDoS sau DoS pentru a viza sisteme specifice în cadrul operațiunilor sau al altor organizații.

De exemplu, pot fi vizate sisteme corporative de informații (cum ar fi computere și dispozitive portabile) pentru a accesa tehnologii de operare, care pot fi conectate la internet sau pot accesa rețele pentru a transfera date operaționale. Conexiunile dintre diferite sisteme și rețele (cum ar fi accesul la rețele corporative, tehnologii de operare și la operațiuni de întreținere de la distanță) pot reprezenta vulnerabilități care pot fi exploatate pentru desfășurarea de atacuri de tip DDoS sau DoS asupra unor servicii și sisteme strategice de transport. De exemplu, atacurile de tip DDoS și DoS pot exploata rețele și protocoale de comunicare comune, cum ar fi descoperirea dinamică a serviciilor web (Web Services Dynamic Discovery - WS-Discovery), pe care dispozitivele IoT le pot utiliza pentru a descoperi automat fiecare nod de pe rețelele locale (LAN-uri). Dacă dispozitivele IoT prezintă vulnerabilități, atacatorii le pot exploata pentru a descoperi alte dispozitive conectate și pentru a desfășura atacuri de tip DDoS sau DoS.



Amenințarea #3: Accesul neautorizat și furtul

Actorii care generează amenințări ar putea dori să obțină acces logic sau fizic fără permisiune la o rețea, la un sistem, la o aplicație, la date sau la o altă resursă pentru a desfășura activități răuvoitoare, inclusiv furtul de date sau resurse sensibile (inclusiv resurse fizice).

Amenințările generate de accesul neautorizat și de furt vizează activele confidențiale și proprietare (inclusiv identitățile personale, acreditările pentru conturi privilegiate, sisteme și alte tipuri de informații confidențiale și proprietare). Aceste amenințări pot exploata vulnerabilitățile sistemelor, precum și persoanele care divulgă în necunoștință de cauză date sensibile, cum ar fi acreditările (de exemplu, nume de utilizator, parolă etc.) sau date cu caracter personal (de exemplu, e-mail, cod numeric personal etc.).

În ceea ce privește accesul neautorizat, furtul de identitate reprezintă utilizarea ilicită a datelor cu caracter personal sau a identificatorilor unici în scopul asumării identității unor persoane sau servicii și sisteme pentru a obține acces la resurse private sau proprietare (de exemplu, inclusiv resurse financiare și fizice). Astfel de amenințări la adresa securității cibernetice pot viza, de asemenea, activele fizice din toate modurile de transport.

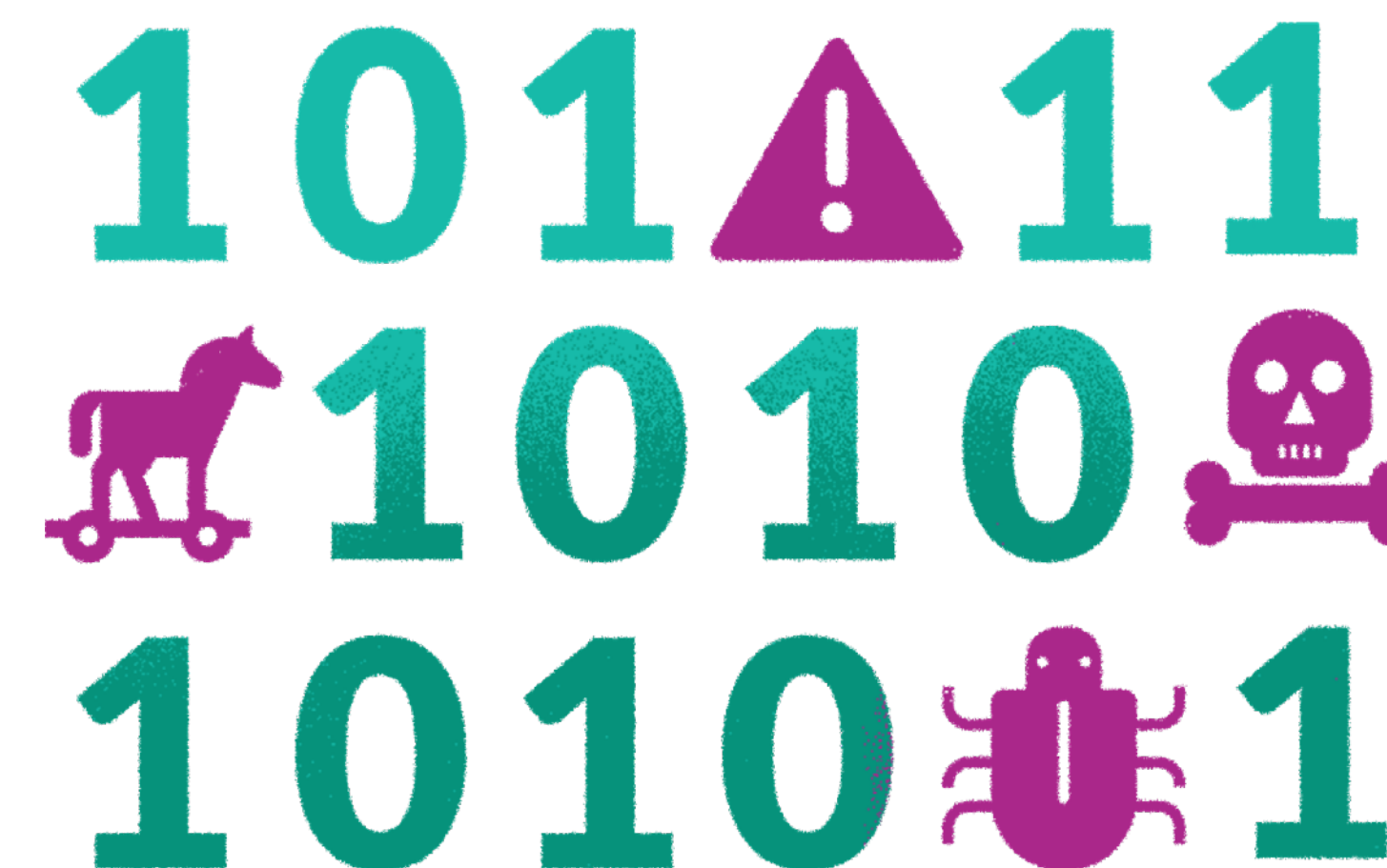


Amenințarea #4: Manipularea software-ului

Configurările eronate și manipulările software-ului și ale sistemelor sau componentelor conexe pot avea un impact direct asupra poziției de securitate a serviciilor și sistemelor de transport.

Atacurile cibernetice care exploatează manipulările software-ului modifică setările software-ului sau afectează integritatea datelor în scopul modificării comportamentelor sistemelor și ale serviciilor. Atacatorii pot manipula intenționat software-ul (sau o parte a acestuia) pentru a obține avantaje (de exemplu, obținerea accesului neautorizat, împiedicarea accesului legitim al unor persoane sau sisteme la resursele necesare, colectarea de informații sensibile, modificarea comportamentelor funcționale etc.) în detrimentul activelor sensibile.

De exemplu, atacatorii pot viza canalele de comunicare ale producătorilor pentru a încărca actualizări răuvoitoare ale software-ului pe servicii și sisteme (inclusiv tehnologii de operare) în cadrul unor operațiuni. Un agent care generează amenințări utilizează acreditări de autorizare compromise pentru a accesa interfața unei rețele securizate de întreținere de la distanță în scopul instalării unui software manipulat și al compromiterii ulterioare a altor servicii și sisteme accesibile. Agentul care generează amenințări instalează un software manipulat care compromite ulterior serviciile și sistemele vizate sau atacă alte servicii sau sisteme conectate.



Profiluri de conștientizare a securității cibernetice



1

Profilul I: întregul personal din sectorul transporturilor

Prima cale se adresează întregului personal din cadrul organizațiilor de transport, de la personalul operațional la cel administrativ. Această cale oferă orientări pentru sporirea gradului de înțelegere și de conștientizare cu privire la cele mai frecvente amenințări la adresa securității cibernetice care vizează serviciile de transport. Aceasta oferă, de asemenea, informații cu privire la modul de abordare a potențialelor amenințări la adresa securității cibernetice, inclusiv identificarea, raportarea și combaterea acestora cu ajutorul unor practici în materie de securitate cibernetică. Această cale este comună tuturor modurilor de transport.

2

Profilul II: factorii de decizie în materie de securitate cibernetică în domeniul transporturilor

A doua cale se adresează personalului cu responsabilități decizionale în materie de securitate sau de securitate cibernetică din cadrul organizațiilor de transport. Această cale oferă bune practici adaptate diferitelor moduri de transport. Aceasta oferă bune practici pentru a identifica, proteja, detecta și răspunde la amenințările emergente la adresa securității cibernetice care vizează organizațiile de transport.

Profilul I: întregul personal din sectorul transporturilor

Această parte se adresează întregului personal din cadrul organizațiilor de transport, de la personalul operațional la cel administrativ. Aceasta oferă orientări pentru sporirea gradului de înțelegere și de conștientizare cu privire la cele mai frecvente amenințări la adresa securității cibernetice care vizează serviciile de transport. Aceasta oferă, de asemenea, informații cu privire la modul de abordare a potențialelor amenințări la adresa securității cibernetice, inclusiv identificarea, raportarea și combaterea acestora cu ajutorul unor practici în materie de securitate cibernetică.

Această parte oferă practici recomandate și sfaturi utile, relevante **pentru toate modurile de transport.**



Bune practici pentru protecția împotriva programelor malware

Puteți contribui la protejarea organizației dumneavoastră prin respectarea unor bune practici de **identificare și prevenire a răspândirii programelor malware**, după cum urmează:

- **Respectați politicile de securitate**, și anume, scanați pentru viruși suporturile de stocare și fișierele, evitați deschiderea și transmiterea prin e-mail a anumitor tipuri de fișiere (de exemplu, fișiere executabile precum .exe, .bat, .com etc.), instalați exclusiv software-uri autorizate, asigurați-vă că software-urile (inclusiv software-ul antivirus) sunt actualizate și funcționează în mod corespunzător, precum și alte politici

- **Creați periodic de copii de rezervă a propriilor date** pe dispozitive sau servicii securizate (și autorizate) de stocare a datelor, care ar trebui să sprijine mecanismele de criptare pentru a proteja datele inactive și pentru a fi disponibile pentru procedurile de recuperare a datelor

- Protejați, prin **măsuri de securitate** adecvate (de exemplu, parolă, criptare etc.), toate sistemele, inclusiv

dispozitivele mobile și terminale, și nu uitați să blocați (fizic și digital) în mod corespunzător toate sistemele în cazul în care acestea nu sunt supravegheate

- Evitați deschiderea unor fișiere atașate și accesarea unor hyperlinkuri conținute în e-mailuri neașteptate și a unor ferestre pop-up suspecte din browserul web care includ un corp de text neobișnuit sau care provin de la expeditori și domenii de internet necunoscute

- Evitați introducerea în propriul computer a unor **dispozitive amovibile necunoscute sau nesigure**, cum ar fi unități flash pentru USB, hard diskuri și alte tipuri de dispozitive de stocare

- Evitați dezactivarea măsurilor de securitate împotriva programelor malware (de exemplu, software antivirus, software de filtrare a conținutului, firewall etc.)

- **Actualizați periodic software-ul** instalat cu cele mai recente versiuni disponibile (pe care agenții de securitate a informațiilor sau administratorii de sistem le pot lansa cu actualizări periodice)

- Evitați utilizarea de conturi și de acreditări privilegiate (de exemplu, la nivel de administrator) pentru activități și operațiuni obișnuite

- Raportați ofițerilor de securitate informatică sau administratorilor de sistem orice e-mail suspect sau orice comportament neașteptat al sistemului

- Concentrați-vă atenția asupra securității informațiilor în timpul desfășurării activității zilnice de rutină pentru a identifica problemele legate de securitatea informatică și pentru a reacționa în consecință.

Bune practici pentru protecția împotriva blocării (distribuite) a serviciului

Puteți contribui la protejarea organizației dumneavoastră prin identificarea atacurilor de tip **blocarea (distribuită) a serviciului (DDoS)** și **blocarea serviciului (DoS)**.

Trebuie să contactați imediat echipele dumneavoastră de securitate și de tehnologia informației în cazul în care descoperiți sau vă confrunțați cu oricare dintre următorii indicatori ai unor posibile atacuri de tip DDoS și DoS asupra serviciilor sau sistemelor dumneavoastră:

- Creșterea numărului de cereri care consumă capacitatea rețelei (percepută ca servicii și răspunsuri lente), ceea ce duce la defecțiuni ale serviciului sau ale sistemului din cauza supraîncărcării

- Creșterea cererii de utilizare a resurselor de memorie fără un motiv evident

- **Comportamente neașteptate ale serviciilor și sistemelor**, întreruperi frecvente și mesaje de eroare neobișnuite din cauza unor consumuri rău intenționate ale resurselor computaționale sau ale conexiunilor la rețea

- **Performanțe degradate** ale dispozitivelor, execuții de lungă durată pentru sarcini nesemnificative și activități observabile (de exemplu, un ventilator zgomotos în timp ce dispozitivele funcționează în mod lent)

- **Conexiuni neașteptate la internet sau pierderi neașteptate ale conexiunilor** la servicii și sisteme

- Modificări de comportament subtile ale comenzilor de operare sau ale tehnologiilor, care provoacă daune fizice

- Refuzuri ale accesului la conturi privilegiate sau administrative pentru a bloca recuperarea procedurilor de răspuns la incidente.



Bune practici pentru protecția împotriva accesului neautorizat și al furtului

Pentru a preveni atacurile care implică accesul neautorizat și furtul, este necesară respectarea unor principii precum „necesitatea de a cunoaște” și „securitatea și confidențialitatea implicite”, care evidențiază faptul că activele sensibile și confidențiale (inclusiv datele cu caracter personal și datele sensibile, sistemele de transport etc.) ar trebui să fie accesibile numai persoanelor care au dreptul de a le accesa pentru a-și îndeplini sarcinile. Puteți contribui la protejarea organizației dumneavoastră prin respectarea bunelor practici pentru identificarea și prevenirea accesului neautorizat și a furtului, după urmează:

- *Respectați politicile de securitate ale organizației*
- *Evitați partajarea și publicarea online de acreditări și de date cu caracter personal, inclusiv de imagini care pot conține astfel de informații*

■ *Evitați utilizarea sau transmiterea de acreditări și de date cu caracter personal (și de alte date sensibile) către rețele, dispozitive sau servicii web care nu sunt de încredere și securizate (de exemplu, site-uri internet care utilizează protocoale sau adrese nesigure de tipul http:// și nu securizate de tip https://)*

■ **Nu dezvăluți niciunei persoane datele dumneavoastră de identificare** (de exemplu, numele de utilizator și parola), nici măcar prin e-mail sau telefon

■ *Protejați datele sensibile tastate pe tastatură sau afișate pe ecran (inclusiv pe dispozitive mobile) împotriva persoanelor neautorizate, instalați ecrane de confidențialitate și evitați lucrul în locuri publice cu dispozitive private și evitați să lăsați orice dispozitiv neblocat și nesupravegheat*

■ **Utilizați parole complexe** (de exemplu, parole suficient de lungi care combină caractere alfanumerice și caractere

speciale) care respectă politicile de securitate relevante ale organizației pentru a preveni accesul neautorizat

■ **Schimbați parolele implicite** pentru sistemele și dispozitivele conectate (de exemplu, imprimante, routere, camere video, încuietori inteligente etc.)

■ *Evitați utilizarea acelorași acreditări (de exemplu, nume de utilizator și parolă) pentru mai multe servicii și sisteme, precum și pentru servicii și sisteme care implică conturi privilegiate*

■ *Trimiteți parole și chei pentru fișierele protejate transferate (de exemplu, arhive ZIP) numai prin intermediul unui canal în afara benzii (de exemplu, SMS prin GSM și apel telefonic) și niciodată prin e-mail*

■ **Activați autentificarea pe două niveluri (2FA)** sau, dacă este posibil, autentificarea pe mai multe niveluri (MFA).

Bune practici pentru protecția împotriva manipulării software-ului

Puteți contribui la protejarea organizației dumneavoastră prin respectarea bunelor practici de identificare și de prevenire a operațiunilor de manipulare a software-ului, după cum urmează:

- *Evitați instalarea de software-uri nesigure pe sisteme și dispozitive (inclusiv pe computere portabile, servere, periferice, dispozitive de rețea, telefoane inteligente etc.)*
- *Instalați întotdeauna software-uri și actualizări din surse și site-uri web oficiale (de exemplu, producători, depozite corporative etc.)*
- *Evitați descărcarea unor software-uri și aplicații (și a oricărui fișier) din surse ilegale*
- *Dezinstalați software-urile inutile sau neutilizate recent și dezactivați conexiunile inutile (de exemplu, protocoale și servicii de rețea), inclusiv accesul la servicii la distanță (de exemplu, servicii de stocare în cloud)*
- *Scanați orice software sau dispozitiv de stocare cu un software antivirus sigur și actualizat*
- *Descărcați software-uri industriale sigure (de exemplu, actualizări, corecții, produse noi etc.) de la furnizori de încredere, utilizând principiul stației albe*
- *Actualizați toate software-urile instalate în conformitate cu politicile și practicile organizației.*



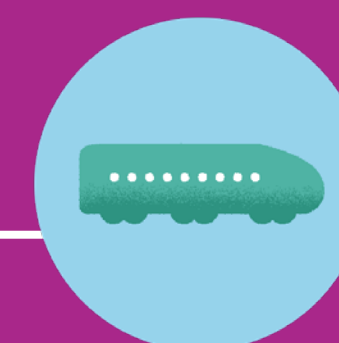
Profilul II: factorii de decizie în materie de securitate cibernetică în domeniul transporturilor

Această parte se adresează personalului cu responsabilități decizionale în materie de securitate sau de securitate cibernetică din cadrul organizațiilor de transport. Această cale evidențiază bunele practici adaptate diferitelor moduri de transport. În special, aceasta oferă bune practici pentru a identifica, proteja, detecta și răspunde la amenințările cibernetice emergente.

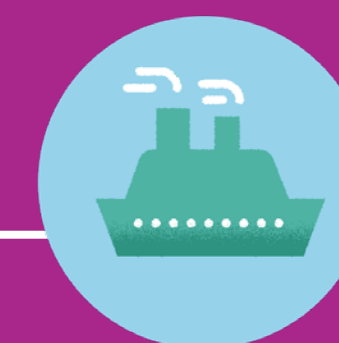




Bune practici
în materie
de securitate
cibernetică
adaptate la
transportul aerian

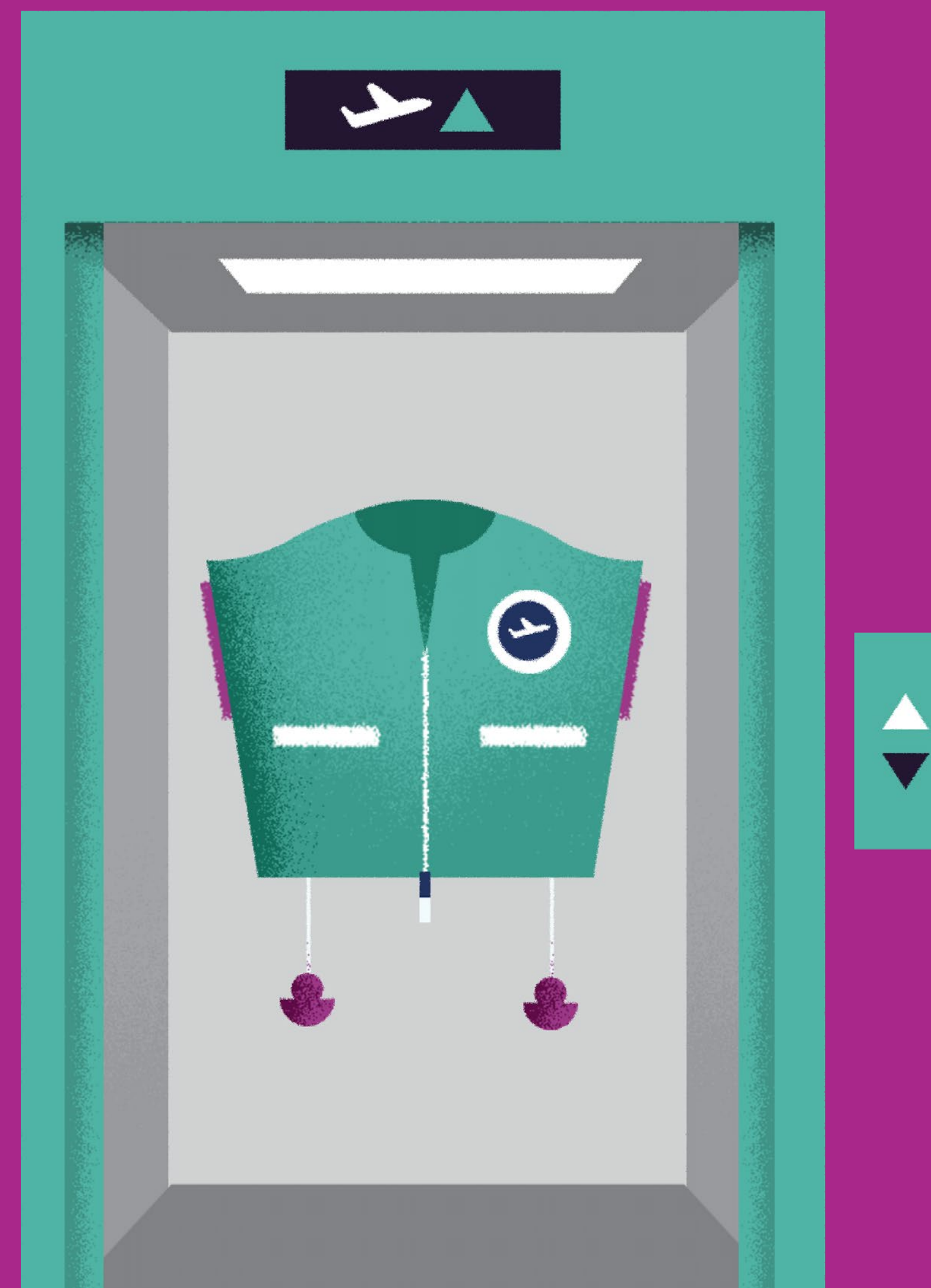


Bune practici
în materie
de securitate
cibernetică
adaptate la
transportul terestru



Bune practici
în materie
de securitate
cibernetică
adaptate la
transportul maritim

Bune practici și măsuri de securitate adaptate la transportul aerian



Guvernanță

Organizațiile din sectorul aviației au nevoie de o înțelegere clară a amenințărilor emergente pentru a elabora politici și procese de management care să le reglementeze abordările în vederea consolidării securității cibernetice a serviciilor și sistemelor în cadrul operațiunilor, inclusiv a tehnologiei informației (IT) și a tehnologiei operaționale (OT).

Bunele practici pentru organizațiile de orice dimensiune includ:

- Asigurarea faptului că nivelurile de conducere de nivel superior raportează preocupările legate de securitatea cibernetică cadrelor de conducere și consiliilor de administrație, care pot lua decizii în cunoștință de cauză cu privire la alocarea resurselor
- Numirea unei persoane cu funcție de conducere de nivel superior, responsabilă cu securitatea cibernetică, precum și cu securitatea fizică, cu responsabilități generale de conducere

pentru securitatea în domeniul tehnologiei informației (TI) și al tehnologiei operaționale (OT), dar neimplicată în operațiuni pentru a se evita conflictele de interese

- Definirea clară a funcțiilor, a responsabilităților, a competențelor și a autorizărilor legate de securitatea cibernetică și comunicarea și convenirea acestora cu personalul competent, în special în cazul membrilor echipelor de răspuns la incidente de securitate cibernetică (CERT)
- Asigurarea guvernanței în materie de securitate cibernetică de-a lungul întregului lanț de servicii de securitate, inclusiv interfețe fizice și digitale, de la producătorii și instalatorii de tehnologii la furnizorii de servicii de securitate
- Convenirea asupra activităților și controalelor, inclusiv asupra responsabilităților partajate, pentru gestionarea riscurilor în materie de securitate cibernetică și asigurarea

menținerii acestor responsabilități pe toată durata ciclului de viață (de exemplu, prin acorduri de servicii) a soluțiilor și serviciilor de securitate

- Definirea mecanismelor de guvernanță (de exemplu, politici) în vederea îndeplinirii obligațiilor care decurg din regulamentele și directivele relevante, cum ar fi, de exemplu, Regulamentul (UE) 2018/1139 privind normele comune în domeniul aviației civile și Regulamentul de punere în aplicare (UE) 2017/373 al Comisiei de stabilire a unor cerințe comune pentru furnizorii de management al traficului aerian/servicii de navigație aeriană și de alte funcții ale rețelei de management al traficului aerian și pentru supravegherea acestora, precum și Directiva NIS [Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice].

Exemple de servicii și de sisteme din sectorul

transportului aerian: exemple în domeniul IT: serviciile și sistemele accesibile angajaților (de exemplu, computere portabile, telefoane mobile, periferice de birou etc.), precum și pasagerilor (de exemplu, routere și conexiuni Wi-Fi publice etc.). Exemple în domeniul OT: sistemele de monitorizare, control și achiziții de date (SCADA), sistemele de încălzire, de ventilare și de climatizare (HVAC), punctele de control de securitate pentru bagajele de mână, sistemele de manipulare a bagajelor (BHS), sistemele de control al accesului, sistemele de monitorizare, sistemele de supraveghere, sistemele de reacție în caz de alarmă, tehnologia de verificare, sistemele de control al iluminatului pistelor de aterizare, sistemele radar și senzori, sistemele de poziționare globală (GPS), sistemele de management al traficului aerian (ATM), sistemele de comunicații, de navigație și de supraveghere (CNS), sistemele de informații aeronautice, sistemele meteorologice, sistemele centrelor de operațiuni, sistemele de la bord ale companiilor aeriene și altele.



Identificarea amenințărilor la adresa securității cibernetice

Gestionarea riscurilor: Organizațiile din sectorul aviației trebuie să ia măsuri adecvate pentru a identifica, evalua și înțelege riscurile în materie de securitate cibernetică pentru rețeaua de transport și sistemele informatice care sprijină operațiunile desfășurate de persoanele cu funcții esențiale.

Acest lucru necesită o abordare organizațională globală a gestionării riscurilor, care implică:

- Asigurarea unei imagini de ansamblu clare asupra diferitelor sisteme hardware și software utilizate pentru furnizarea diferitelor servicii. În cadrul sectorului aviației, astfel de sisteme implică tehnologia informației (IT), precum și tehnologiile operaționale (OT)
- Efectuarea de **evaluări ale riscurilor în materie de securitate cibernetică**, care iau în considerare amenințările emergente, vulnerabilitățile cunoscute și datele operaționale

în legătură cu sistemele vizate. Organizații precum Centrul de răspuns la incidente de securitate cibernetică pentru sistemul european de management al traficului aerian (EATM-CERT) și Centrul de schimb și analiză de informații în sectorul aviației (A-ISAC) pot oferi informații cu privire la amenințările care vizează transportul aerian

- Asigurarea faptului că evaluările riscurilor acoperă, de asemenea, riscurile legate de activitățile zilnice ale personalului (de exemplu, utilizarea platformelor de comunicare socială, utilizarea de dispozitive portabile, prelucrarea datelor, schimbul de informații etc.)
- Identificarea și punerea în aplicare de măsuri de gestionare a riscurilor și de planuri de atenuare a riscurilor în materie de securitate cibernetică

- Instituirea unui **sistem cuprinzător de management al securității informațiilor** (ISMS) și a unui **sistem de management al informațiilor cu caracter personal**, corelate cu alte sisteme de management. Astfel de sisteme de gestionare (și anume, ISMS și PIMS) implică efectuarea unor controale de securitate (precum și în ceea ce privește protecția și confidențialitatea datelor) pentru a atenua și a preveni amenințările emergente care afectează securitatea serviciilor și a sistemelor din sectorul aviației (inclusiv a datelor acestora)
- Luarea în considerare a oricăror constrângeri legate de **gestionarea activelor și planificarea resurselor** (și anume, constrângerile care pot afecta furnizarea, întreținerea și sprijinirea sistemelor strategice pentru operațiunile desfășurate de persoanele cu funcții esențiale din sectorul transportului aerian).

Exemple de cadre de gestionare a riscurilor: diferite cadre (de exemplu, standardele din categoria ISO/IEC 27000, cadrul de securitate cibernetică NIST, cadrul MITRE ATT&CK, BSI IT-Grundschutz etc.) pot furniza informații și pot sprijini o abordare adaptată de gestionare a riscurilor pentru transportul aerian. Organizații internaționale precum Asociația Internațională de Transport Aerian (IATA) și Organizația Aviației Civile Internaționale (OACI) oferă orientări cu privire la evaluările riscurilor în materie de securitate cibernetică. ENISA, AESA, EUROCONTROL și Consiliul Internațional al Aeroporturilor (ACI) evidențiază, printre altele, bunele practici pentru asigurarea securității pentru aeroporturi, pentru furnizorii de servicii de management al traficului aerian și alte organizații din sectorul aviației. Întreprinderea comună SESAR coordonează și concentrează toate activitățile de cercetare și dezvoltare (C&D) ale UE în domeniul managementului traficului aerian, acoperind, de asemenea, aspecte legate de siguranță și de securitate.



Protecția împotriva amenințărilor la adresa securității cibernetice

Organizațiile din sectorul transportului aerian ar trebui să pună în aplicare măsuri de securitate adecvate și proporționale pentru a-și proteja rețelele și sistemele informatice – inclusiv tehnologia informației (IT) și tehnologia operațională (OT) împotriva atacurilor cibernetice. Măsurile de securitate includ:

■ **Politici și procese de securitate:** definirea, punerea în aplicare, comunicarea și asigurarea respectării unor politici și procese adecvate, care definesc o abordare globală pentru securizarea sistemelor și a datelor care sprijină operațiunile desfășurate de persoanele cu funcții esențiale din sectorul aviației. Astfel de politici și de proceduri de securitate (de exemplu, politici privind parolele și stocarea) ar trebui să acopere, de asemenea, corecții și gestionarea vulnerabilităților sistemelor hardware și software (inclusiv IT și OT), gestionarea incidentelor, protecția sistemelor și a rețelelor.

■ **Gestionarea identității și a accesului:** înțelegerea, documentarea și gestionarea accesului la rețele și sisteme

informatice (inclusiv IT și OT) care sprijină operațiunile desfășurate de persoanele cu funcții esențiale din sectorul transportului aerian. Utilizatorii (sau funcțiile automate) care pot accesa date sau sisteme sunt verificați, autentificați și autorizați în mod corespunzător. Acest lucru ar trebui să țină seama, de asemenea, de diferitele roluri și responsabilități ale conturilor obișnuite și ale celor privilegiate.

■ **Securitatea datelor și a sistemelor:** protecția datelor (stocate și transmise în format electronic), a rețelelor și a sistemelor informatice critice (inclusiv IT și OT) împotriva atacurilor cibernetice. Ținând seama de o abordare bazată pe riscuri, organizațiile ar trebui să pună în aplicare măsuri de securitate pentru a limita în mod eficient posibilitățile atacatorilor de a compromite date, rețele și sisteme. Aceste măsuri de securitate ar trebui să includă, de asemenea, adoptarea de protocoale de criptare și de comunicații securizate pentru a proteja datele inactive și datele în tranzit împotriva amenințărilor la adresa securității cibernetice generate de atacuri de tip „man-in-the-middle”. În plus, este necesar ca

aceste măsuri să fie combinate cu măsuri de securitate fizică pentru a proteja accesul la sisteme (de exemplu, sistemele ar trebui amplasate în încăperi închise cu acces restricționat).

■ **Reziliența rețelelor și sistemelor:** consolidarea rezilienței rețelelor și a sistemelor (inclusiv IT și OT) prin conceperea și implementarea acestora (și a procedurilor operaționale ale acestora) pentru a rezista la atacuri cibernetice și pentru a atenua impactul respectivelor atacuri. Exemple de soluții de proiectare și implementare care cresc gradul de reziliență: funcțiile critice verificate în mod oficial, redundanța sistemelor și a rețelelor, segregarea rețelelor (în special, segregarea IT și OT), măsuri de securitate pe mai multe niveluri etc. Trebuie remarcat faptul că, din punctul de vedere al securității informațiilor, domeniile de securitate care implementează segregări de rețea și de sistem pot oferi soluții de securitate adecvate. Cu toate acestea, nevoile operaționale (de exemplu, activități de întreținere, transferuri de date etc.) ale sistemelor pot implica ocolirea sau conectarea unor domenii de securitate diferite (de exemplu, sisteme și rețele separate), inclusiv conectarea IT și OT.

Detectarea amenințărilor la adresa securității cibernetice

Organizațiile ar trebui să se asigure că măsurile de securitate sunt în continuare eficace și să detecteze orice eveniment de securitate cibernetică care afectează sau poate afecta controalele de securitate, precum și serviciile și sistemele esențiale. În scopul detectării amenințărilor la adresa securității cibernetice, măsurile de securitate relevante sunt următoarele:

■ **Monitorizarea securității:** monitorizarea stării securității rețelelor și sistemelor informatice – inclusiv tehnologia informației (IT) și tehnologia operațională (OT) – care sprijină operațiunile desfășurate de persoanele cu funcții esențiale din sectorul serviciilor de transport aerian. Pentru a sprijini activitatea de monitorizare a securității, datele luate în considerare sunt, de exemplu:

- *jurnale de securitate*
- *jurnale privind activitățile de detectare a virușilor*

- *jurnale privind activitățile de detectare a intruziunilor*
- *jurnale privind activitățile de identificare, de autentificare și de autorizare*
- *jurnale privind sistemele și serviciile*
- *jurnale privind traficul în rețea*
- *jurnale privind activitățile de prelucrare a datelor*

■ **Descoperirea unui eveniment de securitate:** detectarea activităților răuvoitoare (și anume, evenimente de securitate) care afectează sau au potențialul de a afecta securitatea rețelelor și a sistemelor informatice (inclusiv IT și OT) care sprijină operațiunile desfășurate de persoanele cu funcții esențiale din sectorul serviciilor de transport aerian.

Aceste măsuri pot implica adoptarea unor tehnologii specifice (de exemplu, gestionarea informațiilor și a evenimentelor de securitate, sistemul de detectare a intruziunilor, sistemul de prevenire a intruziunilor etc.) și

înființarea unui centru de operațiuni de securitate (SOC) sau a unui centru echivalent, și anume, dezvoltarea de mijloace de detectare, analiză, răspuns și redresare în urma atacurilor cibernetice la nivel local.

Echipele naționale de intervenție în caz de incidente de securitate informatică (CSIRT), echipele CERT sectoriale [de exemplu, Centrul de răspuns la incidente de securitate cibernetică pentru sistemul european de management al traficului aerian (EATM-CERT) din cadrul EUROCONTROL], echipele CERT comerciale ale companiilor aeriene și Centrul de schimb și analiză de informații în sectorul aviației (A-ISAC) pot furniza informații în materie de amenințări cibernetice care includ informații cu privire la activitățile de monitorizare și de identificare a evenimentelor de securitate.

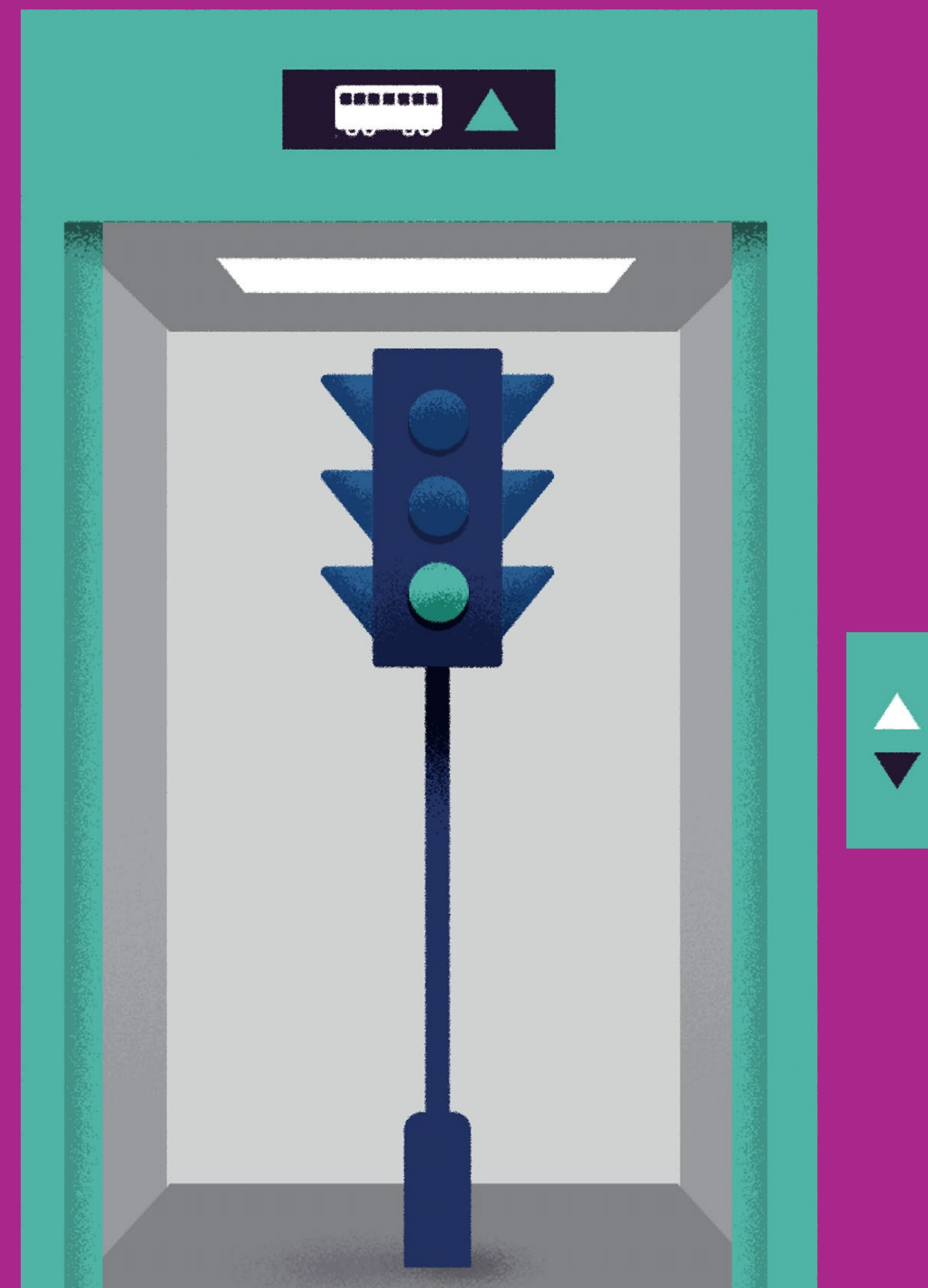
Planificarea acțiunilor de răspuns și de redresare

Organizațiile ar trebui să definească, să instituie și să testeze proceduri de gestionare a incidentelor, în scopul asigurării continuității activităților serviciilor și sistemelor în cazul unor incidente de securitate cibernetică. Măsurile de atenuare intenționează să diminueze sau să limiteze impactul incidentelor de securitate cibernetică.

Planificarea acțiunilor de răspuns și de redresare ar trebui să țină seama de măsurile de securitate care atenuează impactul atacurilor specifice de securitate cibernetică, cum ar fi:

- *Coordonarea și colaborarea cu echipele CSIRT naționale, echipele CERT (publice și comerciale) și centrele ISAC în timpul incidentelor de securitate cibernetică, al activităților de coordonare a incidentelor și al crizelor de securitate cibernetică la nivel paneuropean*
- *Schimbul de informații cu alte organizații, inclusiv cu furnizori din cadrul lanțului de aprovizionare al serviciilor din sectorul aviației*
- *Efectuarea de **exerciții periodice de simulare de atacuri cibernetice** (exerciții de coordonare teoretice, dar și tehnice) pentru evaluarea măsurilor și a procedurilor de securitate, precum și a rezilienței organizațiilor în ceea ce privește gestionarea incidentelor cibernetice*
- *Accesul la locațiile de stocare a datelor arhivate sau de rezervă în caz de compromitere a integrității și disponibilității datelor stocate*
- ***Manuale de proceduri de securitate** care includ proceduri detaliate privind gestionarea incidentelor de securitate cibernetică și restabilirea condițiilor normale de funcționare a serviciilor și a sistemelor*
- *Redirecționarea traficului de rețea către servicii redundante în timpul atacurilor de tip „blocare a serviciului”*
- *Proceduri manuale de operare cu servicii și sisteme în moduri de funcționare în condiții de avarie*
- *Definirea procedurilor pentru tratarea cazurilor de încălcare a securității datelor, inclusiv a procedurilor de abordare a situațiilor de încălcare a securității datelor care afectează date cu caracter personal, în conformitate cu Regulamentul general privind protecția datelor (RGPD) și cu orice alt regulament/altă directivă sectorial(ă) relevant(ă)*
- *Achiziționarea de **polițe de asigurare împotriva atacurilor cibernetice** pentru a acoperi parțial riscul asociat incidentelor cibernetice grave*
- *Încheierea unui contract tip abonament de servicii de răspuns la incidente cu una sau mai multe firme specializate pentru capacități și expertiză suplimentare*
- *Definirea procedurilor pentru **schimbul de informații privind incidentele de securitate cibernetică** cu părțile interesate relevante, inclusiv a procedurilor de notificare a incidentelor în conformitate cu Directiva NIS [Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune].*

Bune practici și măsuri de securitate adaptate la transportul terestru



Guvernanță

Organizațiile din sectorul transporturilor terestre (feroviare și rutiere) au nevoie de o înțelegere clară a amenințărilor emergente pentru a elabora politici și procese de management care să le reglementeze abordările în vederea consolidării securității cibernetice a serviciilor și sistemelor în cadrul operațiunilor, inclusiv a tehnologiei informației (IT) și a tehnologiei operaționale (OT).

Bunele practici pentru organizațiile de orice dimensiune includ:

- Asigurarea faptului că nivelurile de conducere de nivel superior raportează preocupările legate de securitatea cibernetică cadrelor de conducere și consiliilor de administrație, care pot lua decizii în cunoștință de cauză cu privire la alocarea resurselor
- Numirea unei persoane cu funcție de conducere de nivel superior, responsabilă cu securitatea cibernetică, precum și cu

securitatea fizică, cu responsabilități generale de conducere pentru securitatea în domeniul tehnologiei informației (TI) și al tehnologiei operaționale (OT), dar neimplicată în operațiuni pentru a se evita conflictele de interese

- *Definirea clară a funcțiilor, a responsabilităților, a competențelor și a autorizărilor legate de securitatea cibernetică și comunicarea și convenirea acestora cu personalul competent. Acest lucru este necesar, în special, pentru membrii echipelor de răspuns la incidente de securitate cibernetică (CERT)*
- *Asigurarea guvernanței în materie de securitate cibernetică de-a lungul întregului lanț de servicii de securitate, inclusiv interfețe fizice și digitale, de la producătorii și instalatorii de tehnologii la furnizorii de servicii de securitate*

■ *Convenirea asupra activităților și controalelor, inclusiv asupra responsabilităților partajate, pentru gestionarea riscurilor în materie de securitate cibernetică și asigurarea menținerii acestor responsabilități pe toată durata ciclului de viață (de exemplu, prin acorduri de servicii) a soluțiilor și serviciilor de securitate*

■ *Definirea mecanismelor de guvernanță (de exemplu, a politicilor) în scopul respectării obligațiilor care decurg din regulamentele și directivele relevante. Acestea includ un set larg de politici care acoperă modurile de transport specifice, diferite tipuri de părți interesate (de exemplu, inclusiv producătorii de vehicule și de sisteme feroviare), precum și Directiva NIS [Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice].*

Exemple de servicii și de sisteme din sectorul

transporturilor terestre: exemple în domeniul IT:

serviciile și sistemele accesibile angajaților (de exemplu, computere portabile, telefoane mobile, periferice de birou etc.), precum și pasagerilor (de exemplu, routere și conexiuni Wi-Fi publice etc.). Exemple în domeniul OT: sistemele de monitorizare, control și achiziții de date (SCADA), sistemele de încălzire, de ventilare și de climatizare (HVAC), sistemele de poziționare globală (GPS), sistemele de control al accesului, sistemele de monitorizare, sistemele de supraveghere, sistemele de reacție în caz de alarmă și tehnologia de verificare. Sistemele specifice pentru transportul feroviar sunt, de exemplu: sisteme operaționale (sisteme de control-comandă), inclusiv sistemele de semnalizare, Sistemul european de management al traficului feroviar (ERTMS), sistemele de la bordul trenurilor, sistemele de întreținere etc.



Identificarea amenințărilor la adresa securității cibernetice

Gestionarea riscurilor: Organizațiile din sectorul transporturilor terestre trebuie să ia măsuri adecvate pentru a identifica, evalua și înțelege riscurile în materie de securitate cibernetică pentru rețeaua de transport și sistemele informatice care sprijină operațiunile desfășurate de persoanele cu funcții esențiale. Acest lucru necesită o abordare organizațională globală a gestionării riscurilor, care implică:

- Asigurarea unei imagini de ansamblu clare asupra diferitelor sisteme hardware și software utilizate pentru furnizarea diferitelor servicii. În cadrul sectorului transporturilor terestre, astfel de sisteme implică tehnologia informației (IT), precum și tehnologiile operaționale (OT)

- Efectuarea de **evaluări ale riscurilor în materie de securitate cibernetică**, care ar trebui să ia în considerare amenințările emergente, vulnerabilitățile cunoscute și datele operaționale în legătură cu sistemele vizate. Exemple de

sisteme pentru modurile de transport terestru: sisteme de plată, rețele și sisteme de comunicații (de exemplu, internet, comunicații radio, WiFi etc.), echipamente de bord, centre de control operațional, sisteme de gestionare a identității, sisteme de siguranță etc. Exemple de sisteme pentru infrastructurile feroviare: material rulant, subsisteme de exploatare și gestionare a traficului, subsisteme de control-comandă și subsisteme de semnalizare la bord și de cale etc.

- Asigurarea faptului că evaluările riscurilor acoperă, de asemenea, riscurile legate de activitățile zilnice ale personalului (de exemplu, utilizarea platformelor de comunicare socială, utilizarea de dispozitive portabile, prelucrarea datelor, schimbul de informații etc.)

- Identificarea și punerea în aplicare de măsuri de gestionare a riscurilor și de planuri de atenuare a riscurilor în materie de securitate cibernetică, cum ar fi instituirea unui **sistem cuprinzător de management al securității**

informațiilor (ISMS) și a unui **sistem de management al informațiilor cu caracter personal** (PIMS), corelate cu alte sisteme de management. Astfel de sisteme de gestionare (și anume, ISMS și PIMS) implică efectuarea unor controale de securitate (precum și în ceea ce privește protecția și confidențialitatea datelor) pentru a atenua și a preveni amenințările emergente care afectează securitatea serviciilor și a sistemelor din sectorul transporturilor terestre (inclusiv a datelor acestora)

- Luarea în considerare a oricăror constrângeri legate de **gestionarea activelor și planificarea resurselor** (și anume, constrângerile care pot afecta furnizarea, întreținerea și sprijinirea sistemelor strategice pentru operațiunile desfășurate de persoanele cu funcții esențiale din sectorul transporturilor terestre).

Exemple de cadre de gestionare a riscurilor: Diferite cadre (de exemplu, standardele din categoria ISO/IEC 27000, cadrul de securitate cibernetică NIST, cadrul MITRE ATT&CK, BSI IT-Grundschutz etc.) pot furniza informații și pot sprijini o abordare adaptată de gestionare a riscurilor pentru transportul rutier și cel feroviar. Organizații precum ENISA elaborează bune practici cu privire la securitatea cibernetică a autoturismelor inteligente și a mijloacelor de transport public inteligente, care oferă informații producătorilor și asociațiilor din sector (de exemplu, Asociația Constructorilor Europeni de Automobile – ACEA). În sectorul transportului feroviar, Agenția Uniunii Europene pentru Căile Ferate (ERA) definește specificațiile tehnice de interoperabilitate (STI) care trebuie respectate de fiecare subsistem sau parte a unui subsistem pentru a îndeplini cerințele esențiale și pentru a asigura interoperabilitatea sistemului feroviar al Uniunii Europene. Întreprinderea comună Shift2Rail coordonează, de asemenea, inițiative și proiectele de inovare (inclusiv în materie de securitate cibernetică) pentru sectorul transportului feroviar.



Protecția împotriva amenințărilor la adresa securității cibernetice

Organizațiile din sectorul transporturilor terestre ar trebui să pună în aplicare măsuri de securitate adecvate și proporționale pentru a-și proteja rețelele și sistemele informatice – inclusiv tehnologia informației (IT) și tehnologia operațională (OT) împotriva atacurilor cibernetice. Măsurile de securitate includ:

- **Politici și procese de securitate:** definirea, punerea în aplicare, comunicarea și asigurarea respectării unor politici și procese adecvate, care definesc o abordare globală pentru securizarea sistemelor și a datelor care sprijină operațiunile desfășurate de persoanele cu funcții esențiale din sectorul transporturilor terestre. Astfel de politici și de proceduri de securitate (de exemplu, politici privind parolele și stocarea) ar trebui să acopere, de asemenea, corecții și gestionarea vulnerabilităților sistemelor hardware și software (inclusiv IT și OT), gestionarea incidentelor, protecția sistemelor și a rețelelor.
- **Gestionarea identității și a accesului:** înțelegerea, documentarea și gestionarea accesului la rețele și sisteme informatice (inclusiv IT și OT) care sprijină operațiunile desfășurate de persoanele cu funcții esențiale din sectorul

transporturilor terestre. Utilizatorii (sau funcțiile automate) care pot accesa date sau sisteme sunt verificați, autentificați și autorizați în mod corespunzător. Acest lucru ar trebui să țină seama, de asemenea, de diferitele roluri și responsabilități ale conturilor obișnuite și ale celor privilegiate.

- **Securitatea datelor și a sistemelor:** protecția datelor (stocate și transmise în format electronic), a rețelelor și a sistemelor informatice critice (inclusiv IT și OT) împotriva atacurilor cibernetice. Ținând seama de o abordare bazată pe riscuri, organizațiile ar trebui să pună în aplicare măsuri de securitate pentru a limita în mod eficient posibilitățile atacatorilor de a compromite date, rețele și sisteme. Aceste măsuri de securitate ar trebui să includă, de asemenea, adoptarea de protocoale de criptare și de comunicații securizate pentru a proteja datele inactive și datele în tranzit împotriva amenințărilor la adresa securității cibernetice generate de atacuri de tip „man-in-the-middle”. În plus, este necesar ca aceste măsuri să fie combinate cu măsuri de securitate fizică pentru a proteja accesul la sisteme (de exemplu, sistemele ar

trebui amplasate în încăperi închise cu acces restricționat). Acest lucru este foarte important pentru sistemele care pot avea un impact asupra siguranței vieții.

- **Reziliența rețelelor și a sistemelor:** consolidarea rezilienței rețelelor și a sistemelor (inclusiv IT și OT) prin conceperea și implementarea acestora (și a procedurilor operaționale ale acestora) pentru a rezista la atacuri cibernetice și pentru a atenua impactul respectivelor atacuri. Exemple de soluții de proiectare și implementare care cresc gradul de reziliență: funcțiile critice verificate în mod oficial, redundanța sistemelor și a rețelelor, segregarea rețelelor (în special, segregarea IT și OT), măsuri de securitate pe mai multe niveluri etc. Trebuie remarcat faptul că, din punctul de vedere al securității informațiilor, domeniile de securitate care implementează segregări de rețea și de sistem pot oferi soluții de securitate adecvate. Cu toate acestea, nevoile operaționale (de exemplu, activități de întreținere, transferuri de date etc.) ale sistemelor pot implica ocolirea sau conectarea unor domenii de securitate diferite (de exemplu, sisteme și rețele separate), inclusiv conectarea IT și OT.

Detectarea amenințărilor la adresa securității cibernetice

Organizațiile ar trebui să se asigure că măsurile de securitate sunt în continuare eficace și să detecteze orice eveniment de securitate cibernetică care afectează sau poate afecta controalele de securitate, precum și serviciile și sistemele esențiale. În scopul detectării amenințărilor la adresa securității cibernetice, măsurile de securitate relevante sunt următoarele:

■ **Monitorizarea securității:** monitorizarea stării securității rețelor și sistemelor informatice – inclusiv tehnologia informației (IT) și tehnologia operațională (OT) – care sprijină operațiunile desfășurate de persoanele cu funcții esențiale din sectorul transporturilor terestre. Acest lucru este necesar pentru a detecta potențialele amenințări la adresa securității și pentru a monitoriza permanent eficacitatea a măsurilor de protecție și de securitate. Pentru a sprijini activitatea de monitorizare a securității, datele luate în considerare sunt, de exemplu:

- jurnale de securitate
- jurnale privind activitățile de detectare a virușilor
- jurnale privind activitățile de detectare a intruziunilor
- jurnale privind activitățile de identificare, de autentificare și de autorizare
- jurnale privind sistemele și serviciile

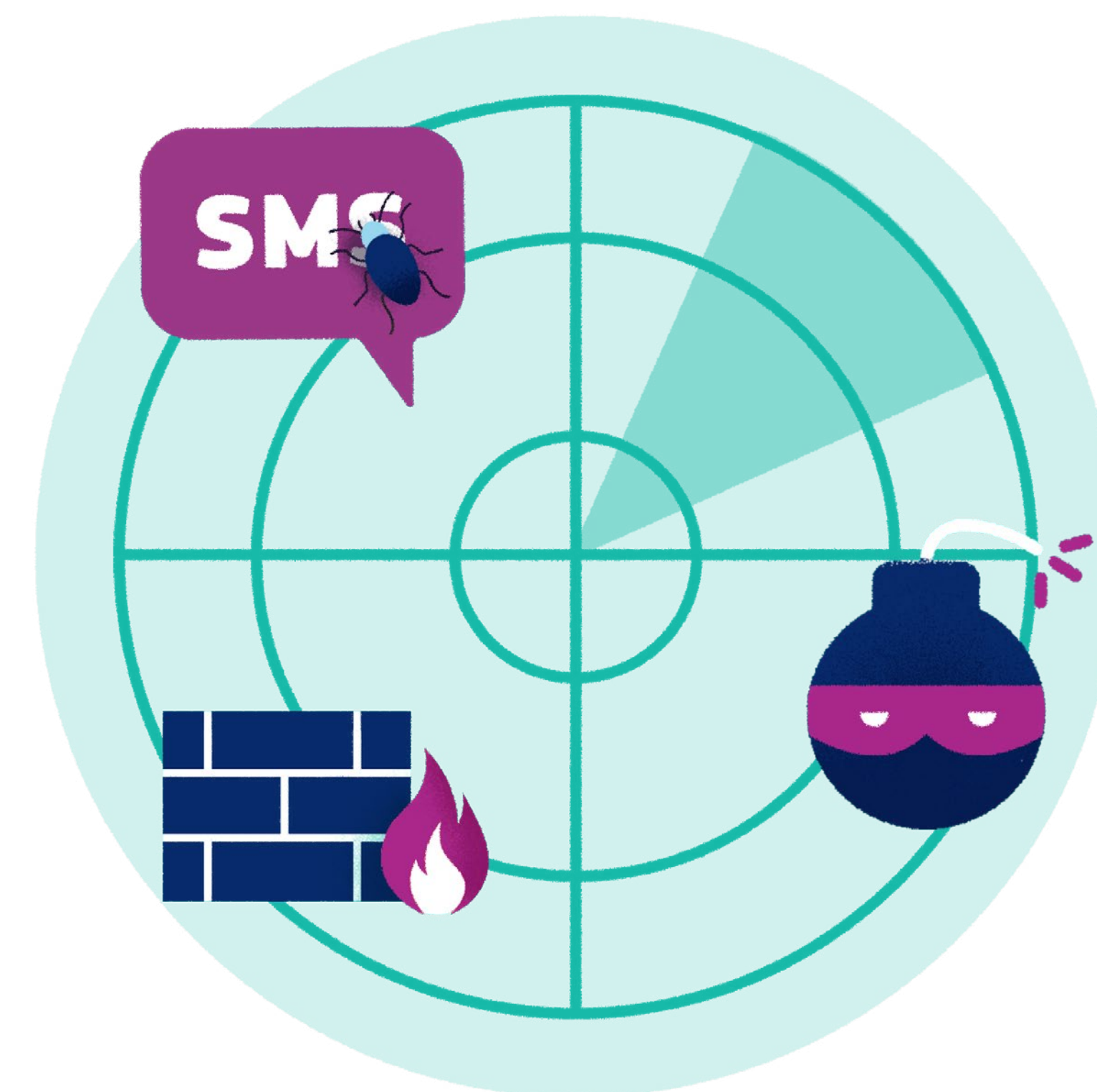
- jurnale privind traficul în rețea
- jurnale privind activitățile de prelucrare a datelor

■ **Descoperirea unui eveniment de securitate:**

detectarea activităților răuvoitoare (și anume, evenimente de securitate) care afectează sau au potențialul de a afecta securitatea rețelor și a sistemelor informatice (inclusiv IT și OT) care sprijină operațiunile desfășurate de persoanele cu funcții esențiale.

Aceste măsuri pot implica adoptarea unor tehnologii specifice (de exemplu, gestionarea informațiilor și a evenimentelor de securitate, sistemul de detectare a intruziunilor, sistemul de prevenire a intruziunilor etc.) și înființarea unui centru de operațiuni de securitate (SOC) sau a unui centru echivalent, și anume, dezvoltarea de mijloace de detectare, analiză, răspuns și redresare în urma atacurilor cibernetice la nivel local.

Echipele naționale de intervenție în caz de incidente de securitate informatică (CSIRT), echipele CERT sectoriale și comerciale sau operatorii rutieri și feroviari și Centrul european de schimb și analiză de informații în sectorul feroviar (ER-ISAC) pot furniza informații în materie de amenințări cibernetice care includ informații cu privire la activitățile de monitorizare și de identificare a evenimentelor de securitate.



Planificarea acțiunilor de răspuns și de redresare

Organizațiile ar trebui să definească, să instituie și să testeze proceduri de gestionare a incidentelor, în scopul asigurării continuității activităților serviciilor și sistemelor în cazul unor incidente de securitate cibernetică.

Planificarea acțiunilor de răspuns și de redresare ar trebui să țină seama de măsurile de securitate care atenuează impactul atacurilor specifice de securitate cibernetică, cum ar fi:

- *Coordonarea și colaborarea cu echipele CSIRT naționale, echipele CERT (publice și comerciale) și centrele ISAC în timpul incidentelor de securitate cibernetică, al activităților de coordonare a incidentelor și al crizelor de securitate cibernetică la nivel paneuropean*

- *Schimbul de informații cu alte organizații, inclusiv cu furnizori din cadrul lanțului de aprovizionare al serviciilor din sectorul transporturilor terestre*

- *Efectuarea de **exerciții periodice de simulare de atacuri cibernetice** (exerciții de coordonare teoretice, dar și tehnice) pentru evaluarea măsurilor și a procedurilor de securitate, precum și a rezilienței organizațiilor în ceea ce privește gestionarea incidentelor cibernetice*

- *Accesul la locațiile de stocare a datelor arhivate sau de rezervă în caz de compromitere a integrității și disponibilității datelor stocate*

- **Manuale de proceduri de securitate** care includ proceduri detaliate privind gestionarea incidentelor de securitate cibernetică și restabilirea condițiilor normale de funcționare a serviciilor și a sistemelor

- *Redirecționarea traficului de rețea către servicii redundante în timpul atacurilor de tip „blocare a serviciului”*

- *Proceduri manuale de operare cu servicii și sisteme în moduri de funcționare în condiții de avarie*

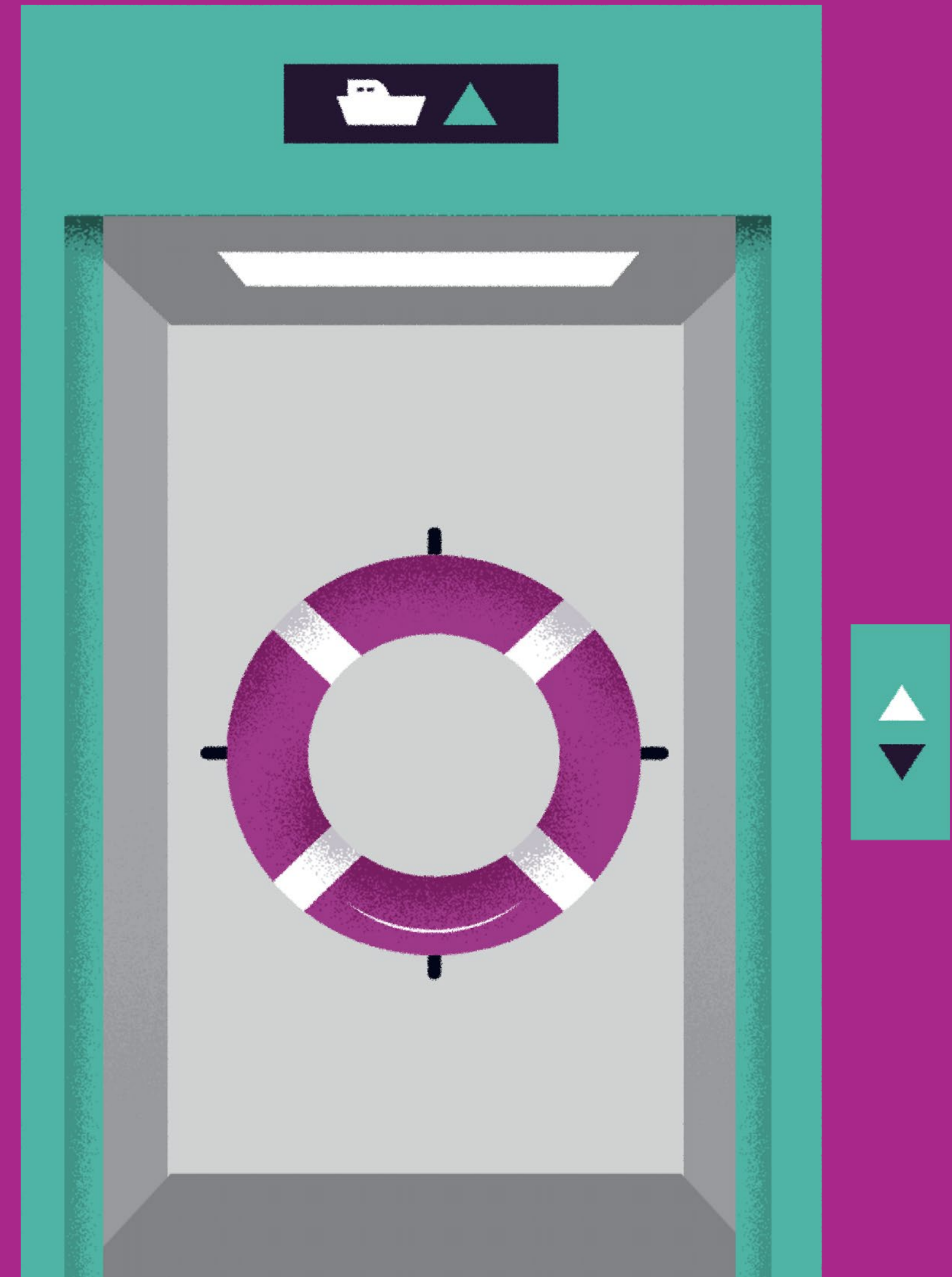
- *Definirea procedurilor pentru tratarea cazurilor de încălcare a securității datelor, inclusiv a procedurilor de abordare a situațiilor de încălcare a securității datelor care afectează date cu caracter personal, în conformitate cu Regulamentul general privind protecția datelor (RGPD) și cu orice alt regulament/altă directivă sectorial(ă) relevant(ă)*

- *Achiziționarea de **polițe de asigurare împotriva atacurilor cibernetice** pentru a acoperi parțial riscul asociat incidentelor cibernetice grave*

- *Încheierea unui contract tip abonament de servicii de răspuns la incidente cu una sau mai multe firme specializate pentru capacități și expertiză suplimentare*

- *Definirea procedurilor pentru schimbul de informații privind incidentele de securitate cibernetică cu părțile interesate relevante, inclusiv a procedurilor de notificare a incidentelor în conformitate cu Directiva NIS [Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune].*

Bune practici și măsuri de securitate adaptate la transportul maritim



Guvernanță

Organizațiile din sectorul transportului maritim au nevoie de o înțelegere clară a amenințărilor emergente pentru a elabora politici și procese de management care să le reglementeze abordările în vederea consolidării securității cibernetice a serviciilor și sistemelor în cadrul operațiunilor, inclusiv a tehnologiei informației (IT) și a tehnologiei operaționale (OT).

Bunele practici pentru organizațiile de orice dimensiune includ:

- *Asigurarea faptului că nivelurile de conducere de nivel superior raportează preocupările legate de securitatea cibernetică cadrelor de conducere și consiliilor de administrație, care pot lua decizii în cunoștință de cauză cu privire la alocarea resurselor*
- *Numirea unei persoane cu funcție de conducere de nivel superior cu responsabilități generale de conducere în domeniul securității tehnologiei informației (IT) și a tehnologiei operaționale (OT). Această persoană ar trebui să fie responsabilă atât pentru securitatea cibernetică, cât și pentru securitatea fizică.*

- *Definirea clară a rolurilor, a responsabilităților, a competențelor și a autorizărilor legate de securitatea cibernetică, definirea nivelurilor ierarhice de autoritate și a canalelor de comunicare între personalul de la țărm și cel de la bord și convenirea acestora împreună cu personalul competent. Acest lucru este necesar, în special, pentru membrii echipelor de răspuns la incidente de securitate cibernetică (CERT). Personalul cu roluri legate de legislația UE în materie de securitate și siguranță maritimă, cum ar fi agenții de securitate ai instalațiilor portuare, agenții de securitate portuară sau agenții de securitate ai companiilor sau persoana desemnată de pe uscat și comandantul de navă ar trebui să cunoască cel puțin măsurile de securitate cibernetică luate de organizație.*

- *Asigurarea guvernanței în materie de securitate cibernetică de-a lungul întregului lanț de servicii de securitate, inclusiv interfețe fizice și digitale, de la producătorii și instalatorii de tehnologii la furnizorii de servicii de securitate*

- *Convenirea asupra activităților și controalelor, inclusiv asupra responsabilităților partajate, pentru gestionarea riscurilor în materie de securitate cibernetică și asigurarea menținerii*

acestor responsabilități pe toată durata ciclului de viață (de exemplu, prin acorduri de servicii) a soluțiilor și serviciilor de securitate

- *Definirea mecanismelor de guvernanță (de exemplu, politici) în vederea respectării obligațiilor care decurg din regulamentele și directivele relevante, de exemplu, Regulamentul (UE) 2019/1239 de stabilire a unui mediu aferent ghișeului unic european în domeniul maritim (EMSWe), Regulamentul (CE) nr. 725/2004 privind consolidarea securității navelor și a instalațiilor portuare, Directiva 2005/65/CE privind consolidarea securității portuare și Regulamentul (CE) nr. 336/2006 privind aplicarea Codului Internațional de Management al Siguranței (ISM) și Rezoluția A.741(18) de adoptare a Codului ISM pentru exploatarea în siguranță a navelor și prevenirea poluării. În acest context, este relevant, de asemenea, să se menționeze Mediul comun pentru schimbul de informații (CISE), o inițiativă a UE care urmărește asigurarea interoperabilității sistemelor de supraveghere europene și a statelor membre pentru a oferi tuturor autorităților în cauză acces la informațiile clasificate și neclasificate de care au nevoie pentru a desfășura misiuni pe mare.*

Exemple de servicii și sisteme de din sectorul

transportului maritim: exemple în domeniul IT: serviciile și sistemele accesibile angajaților (de exemplu, computere portabile, telefoane mobile, periferice de birou etc.), precum și pasagerilor (de exemplu, routere și conexiuni Wi-Fi publice etc.). Exemple în domeniul OT: sistemele de monitorizare, control și achiziții de date (SCADA), sistemele de încălzire, de ventilare și de climatizare (HVAC), sistemele de poziționare globală (GPS), sistemele de control al accesului, sistemele de monitorizare, sistemele de supraveghere, sistemele de reacție în caz de alarmă și tehnologia de verificare, sistemele de navigație de la bord, SafeSeaNet, sistemele podurilor, sistemele de manipulare și de gestionare a mărfurilor, sisteme de propulsie și de gestionare a mașinilor și de reglaj al puterii, sistemele de control al accesului, sistemele de deservire și de gestionare pentru pasageri, rețelele publice destinate pasagerilor, sistemele administrative și de asigurare a bunăstării echipajului, sistemele de comunicații etc.



Identificarea amenințărilor la adresa securității cibernetice

Gestionarea riscurilor: Organizațiile din sectorul maritim trebuie să ia măsurile adecvate pentru identificarea, analizarea, evaluarea și comunicarea riscurilor în materie de securitate cibernetică, precum și pentru acceptarea, evitarea, transferul sau reducerea acestora la un nivel acceptabil. Acest lucru necesită o abordare organizațională globală a gestionării riscurilor, care implică:

- Asigurarea unei imagini de ansamblu clare asupra diferitelor sisteme hardware și software utilizate pentru furnizarea diferitelor servicii. În cadrul sectorului transportului maritim, astfel de sisteme implică tehnologia informației (IT), precum și tehnologiile operaționale (OT) și modul în care aceste sisteme sunt conectate și integrate la țărm, inclusiv cu autoritățile publice, terminalele maritime și operatorii portuari.

- Identificarea și evaluarea principalelor operațiuni de la bordul navelor vulnerabile la atacuri cibernetice, și efectuarea de evaluări ale riscurilor în materie de securitate cibernetică (inclusiv evaluarea impactului operațional potențial și a probabilității de apariție a unor evenimente), care ar trebui să țină seama de amenințările emergente, de vulnerabilitățile

cunoscute și de datele operaționale în legătură cu sistemele vizate. După caz, stabilirea legăturii cu evaluările de securitate efectuate pentru nave (SSA), instalații portuare (PFSA) și porturi (PSA), astfel cum se prevede în legislația UE în materie de securitate maritimă. Acestea identifică posibilele amenințări la adresa securității infrastructurii portuare și deficiențele în materie de securitate. În plus, organizațiile maritime precum Organizația Maritimă Internațională (OMI) și centrele ISAC din sectorul maritim pot oferi informații cu privire la amenințările care vizează sectorul transportului maritim.

- Asigurarea faptului că evaluările riscurilor acoperă, de asemenea, riscurile legate de activitățile zilnice ale personalului (de exemplu, utilizarea platformelor de comunicare socială, utilizarea de dispozitive portabile, prelucrarea datelor, schimbul de informații etc.)

- Identificarea și punerea în aplicare de măsuri de gestionare a riscurilor și de planuri de atenuare a riscurilor în materie de securitate cibernetică. De exemplu, instituirea unui sistem cuprinzător de management al securității informațiilor (ISMS) și a unui sistem de management al informațiilor confidențiale,

corelate cu alte sisteme de management, cum ar fi sistemele de management al siguranței (SMS), în conformitate cu Codul internațional de management al siguranței (ISM). Astfel de sisteme de gestionare (și anume, ISMS și PIMS) implică efectuarea unor controale de securitate (precum și în ceea ce privește protecția și confidențialitatea datelor) pentru a atenua și a preveni amenințările emergente care afectează securitatea serviciilor și a sistemelor din sectorul transportului maritim (inclusiv a datelor acestora)

- Luarea în considerare a oricăror constrângeri legate de **gestionarea activelor și planificarea resurselor** (și anume, constrângerile care pot afecta furnizarea, întreținerea și sprijinirea sistemelor strategice pentru operațiunile desfășurate de persoanele cu funcții esențiale din sectorul transportului maritim). În ceea ce privește evaluările, se face o trimitere încrucișată, după caz, la cerințele Codului ISM, ale sistemelor de management al siguranței (SMS) și ale planurilor de securitate realizate în conformitate cu legislația UE în materie de siguranță și securitate maritimă.

Exemple de cadre de gestionare a riscurilor: Diferite cadre (de exemplu, Codul ISM sau standardele din categoria ISO/IEC 27000, cadrul de securitate cibernetică NIST, cadrul MITRE ATT&CK, BSI IT-Grundschutz etc.) pot furniza informații și pot sprijini o abordare adaptată de gestionare a riscurilor pentru transportul maritim. Cadrul de securitate cibernetică al NIST a fost, de asemenea, adaptat pentru a aborda securitatea cibernetică a transportului maritim de lichide în vrac (Maritime Bulk Liquids Transfer - MBLT), a operațiunilor deasupra mării și a operațiunilor navelor de pasageri. În mod similar, Consiliul Maritim Baltic și Internațional (Baltic and International Maritime Council - BIMCO) a publicat orientările intitulate *The Guidelines on Cyber Security Onboard Ships* („Orientările privind securitatea cibernetică la bordul navelor”), iar Organizația Maritimă Internațională (OMI) a publicat orientările specifice intitulate *Guidelines on maritime cyber risk management* („Orientări privind gestionarea riscurilor ciberneticice din sectorul maritim”) (MSC-FAL.1/Circ.3). ENISA a realizat mai multe studii privind bunele practici în materie de securitate cibernetică în sectorul maritim, în special securitatea cibernetică a porturilor. EMSA oferă servicii comunității maritime, inclusiv cursuri de formare pentru conștientizarea securității ciberneticice. Standardele (de exemplu, IEC 61162-460:2018 privind siguranța și securitatea echipamentelor și sistemelor de navigație și radiocomunicații maritime, ISO 16425:2013 privind navele și tehnologia marină, IEC 62443-4-1:2018 privind securitatea sistemelor industriale de automatizare și control etc.) definesc, de asemenea, cerințe specifice de securitate și de siguranță pentru sistemele și rețelele din sectorul transportului maritim.



Protecția împotriva amenințărilor la adresa securității cibernetice

Organizațiile din sectorul transportului maritim ar trebui să pună în aplicare măsuri de securitate adecvate și proporționale pentru a-și proteja rețelele și sistemele informatice – inclusiv tehnologia informației (IT) și tehnologia operațională (OT) împotriva atacurilor cibernetice. Măsurile de securitate includ:

■ **Politici și procese de securitate:** definirea, punerea în aplicare, comunicarea și asigurarea respectării unor politici și procese adecvate, care definesc o abordare globală pentru securizarea sistemelor și a datelor care sprijină operațiunile desfășurate de persoanele cu funcții esențiale din sectorul transportului maritim. Măsurile de securitate (inclusiv măsurile de securitate cibernetică și fizică) ar trebui incluse în planurile relevante, cum ar fi sistemul de management al siguranței (SMS) și Planul de securitate al navei (SSP). Astfel de politici și de proceduri de securitate (de exemplu, politici privind parolele și stocarea) ar trebui să acopere, de asemenea, corecții și gestionarea vulnerabilităților sistemelor hardware și software (inclusiv IT și OT), gestionarea incidentelor, protecția sistemelor și a rețelelor.

■ **Gestionarea identității și a accesului:** înțelegerea, documentarea și gestionarea accesului la rețele și sisteme

informatice (inclusiv IT și OT) care sprijină operațiunile desfășurate de persoanele cu funcții esențiale din sectorul transportului maritim. Utilizatorii (sau funcțiile automate) care pot accesa date sau sisteme sunt verificați, autentificați și autorizați în mod corespunzător. Acest lucru ar trebui să țină seama, de asemenea, de diferitele roluri și responsabilități ale conturilor obișnuite și ale celor privilegiate.

■ **Securitatea datelor și a sistemelor:** protecția datelor (stocate și transmise în format electronic), a rețelelor și a sistemelor informatice critice (inclusiv IT și OT) împotriva atacurilor cibernetice. Ținând seama de o abordare bazată pe riscuri, organizațiile ar trebui să pună în aplicare măsuri de securitate pentru a limita în mod eficient posibilitățile atacatorilor de a compromite date, rețele și sisteme. Aceste măsuri de securitate ar trebui să includă, de asemenea, adoptarea de protocoale de criptare și de comunicații securizate pentru a proteja datele inactive și datele în tranzit împotriva amenințărilor la adresa securității cibernetice generate de atacuri de tip „man-in-the-middle”. În plus, este necesar ca aceste măsuri să fie combinate cu măsuri de securitate fizică pentru a proteja accesul la sisteme (de exemplu, sistemele ar trebui amplasate în încăperi închise cu acces restricționat).

Acest lucru este foarte important pentru sistemele care pot avea un impact asupra siguranței vieții (de exemplu, sistemele de navigație și radiocomunicații de categoriile II și III).

■ **Reziliența rețelelor și sistemelor:** consolidarea rezilienței rețelelor și a sistemelor (inclusiv IT și OT) prin conceperea și implementarea acestora (și a procedurilor operaționale ale acestora) pentru a rezista la atacuri cibernetice și pentru a atenua impactul respectivelor atacuri. Exemple de soluții de proiectare și implementare care cresc gradul de reziliență: funcțiile critice verificate în mod oficial, redundanța sistemelor și a rețelelor, segregarea rețelelor (în special, segregarea IT și OT), măsuri de securitate pe mai multe niveluri etc. Trebuie remarcat faptul că, din punctul de vedere al securității informațiilor, domeniile de securitate care implementează segregări de rețea și de sistem pot oferi soluții de securitate adecvate. Cu toate acestea, nevoile (de exemplu, activități de întreținere, transferuri de date etc.) sistemelor (de exemplu, Maritime Autonomous Surface Ships – MASS) pot implica ocolirea sau conectarea unor domenii de securitate diferite (de exemplu, sisteme și rețele separate), inclusiv conectarea IT și OT.

Detectarea amenințărilor la adresa securității cibernetice

Organizațiile ar trebui să se asigure că măsurile de securitate sunt în continuare eficace și să detecteze orice eveniment de securitate cibernetică care afectează sau poate afecta controalele de securitate, precum și serviciile și sistemele esențiale. În scopul detectării amenințărilor la adresa securității cibernetice, măsurile de securitate relevante sunt următoarele:

■ **Monitorizarea securității:** monitorizarea stării securității rețelelor și sistemelor informatice – inclusiv tehnologia informației (IT) și tehnologia operațională (OT) – care sprijină operațiunile desfășurate de persoanele cu funcții esențiale din sectorul serviciilor de transport maritim. Acest lucru este necesar pentru a detecta potențialele amenințări la adresa securității și pentru a monitoriza permanent eficacitatea a măsurilor de protecție și de securitate. Pentru a sprijini activitatea de monitorizare a securității, datele luate în considerare sunt, de exemplu:

- *jurnale de securitate*
- *jurnale privind activitățile de detectare a virusilor*

- *jurnale privind activitățile de detectare a intruziunilor*
- *jurnale privind activitățile de identificare, de autentificare și de autorizare*
- *jurnale privind sistemele și serviciile*
- *jurnale privind traficul în rețea*
- *jurnale privind activitățile de prelucrare a datelor*

■ **Descoperirea unui eveniment de securitate:** detectarea activităților răuvoitoare (și anume, evenimente de securitate) care afectează sau au potențialul de a afecta securitatea rețelelor și a sistemelor informatice (inclusiv IT și OT) care sprijină operațiunile desfășurate de persoanele cu funcții esențiale din sectorul serviciilor de transport maritim.

Aceste măsuri pot implica adoptarea unor tehnologii specifice (de exemplu, gestionarea informațiilor și a evenimentelor de securitate, sistemul de detectare a intruziunilor, sistemul de prevenire a intruziunilor etc.) și înființarea unui centru de operațiuni de securitate (SOC) sau a unui centru echivalent, și anume, dezvoltarea de mijloace de detectare, analiză,

răspuns și redresare în urma atacurilor cibernetice la nivel local.

Echipele naționale de intervenție în caz de incidente de securitate informatică (CSIRT), echipele CERT sectoriale și echipele CERT comerciale ale operatorilor maritimi, centrele ISAC maritime pot furniza informații în materie de amenințări cibernetice care includ informații cu privire la activitățile de monitorizare și de identificare a evenimentelor de securitate.

Planificarea acțiunilor de răspuns și de redresare

Organizațiile ar trebui să definească, să instituie și să testeze proceduri de gestionare a incidentelor, în scopul asigurării continuității activităților serviciilor și sistemelor în cazul unor incidente de securitate cibernetică.

Planificarea acțiunilor de răspuns și de redresare ar trebui să țină seama de măsurile de securitate care atenuează impactul atacurilor specifice de securitate cibernetică, cum ar fi:

- *Redirecționarea traficului de rețea către servicii redundante în timpul atacurilor de tip „blocare a serviciului”*
- *Proceduri manuale de operare cu servicii și sisteme în moduri de funcționare în condiții de avarie*
- *Stabilirea de programe de antrenamente și exerciții (de exemplu, exerciții de coordonare teoretice, tehnice și de intervenție) pentru a răspunde atacurilor cibernetice și situațiilor de urgență, precum și pentru a evalua măsurile de securitate, procedurile și reziliența organizațională necesare pentru a face față incidentelor cibernetice*

■ *Accesul la locațiile de stocare a datelor arhivate sau de rezervă în caz de compromitere a integrității și disponibilității datelor stocate*

■ *Coordonarea și colaborarea cu echipele CSIRT naționale, echipele CERT (publice și comerciale) și centrele ISAC în timpul incidentelor de securitate cibernetică, al activităților de coordonare a incidentelor și al crizelor de securitate cibernetică la nivel paneuropean*

■ *Schimbul de informații cu alte organizații, inclusiv cu furnizori din cadrul lanțului de aprovizionare al serviciilor din sectorul transportului maritim*

■ *Manuale de proceduri de securitate care includ proceduri detaliate privind gestionarea incidentelor de securitate cibernetică și restabilirea condițiilor normale de funcționare a serviciilor și a sistemelor*

■ *Definirea procedurilor pentru tratarea cazurilor de încălcare a securității datelor, inclusiv a procedurilor de abordare*

a situațiilor de încălcare a securității datelor care afectează date cu caracter personal, în conformitate cu Regulamentul general privind protecția datelor (RGPD) și cu orice alt regulament/altă directivă sectorial(ă) relevant(ă)

■ *Achiziționarea de polițe de asigurare împotriva atacurilor cibernetice pentru a acoperi parțial riscul asociat incidentelor cibernetice grave*

■ *Încheierea unui contract tip abonament de servicii de răspuns la incidente cu una sau mai multe firme specializate pentru capacități și expertiză suplimentare*

■ *Definirea procedurilor pentru schimbul de informații privind incidentele de securitate cibernetică (inclusiv neconformități, accidente și situație periculoase) cu părțile interesate relevante, inclusiv a procedurilor de notificare a incidentelor în conformitate cu Directiva NIS [Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune].*

Informațiile și opiniile prezentate în acest raport aparțin autorului (autorilor) și nu reflectă în mod necesar opinia oficială a Comisiei. Comisia nu garantează precizia datelor incluse în prezentul raport. Nici Comisia Europeană, nici persoanele care acționează în numele Comisiei nu pot fi considerate răspunzătoare pentru modul în care ar putea fi utilizate informațiile cuprinse în prezenta publicație.

Luxemburg: Oficiul pentru Publicații al Uniunii Europene, 2021

© Uniunea Europeană, 2021

Reutilizarea textului este autorizată cu condiția menționării sursei și a păstrării nealterate a sensului sau a mesajului original al acestui document. Comisia Europeană nu este responsabilă pentru modul în care ar putea fi reutilizată prezenta publicație. Politica de reutilizare a documentelor Comisiei Europene este reglementată prin Decizia 2011/833/UE a Comisiei din 12 decembrie 2011 privind reutilizarea documentelor Comisiei (JO L 330, 14.12.2011, p. 39).

Pentru orice utilizare sau reproducere a unor elemente care nu sunt deținute de Uniunea Europeană, este posibil să fie necesară solicitarea permisiunii direct de la titularii drepturilor respective.

Print	ISBN 978-92-76-40494-1	doi:10.2832/106559	MI-05-21-230-RO-C
PDF	ISBN 978-92-76-40493-4	doi:10.2832/296520	MI-05-21-230-RO-N



Oficiul pentru Publicații
al Uniunii Europene