Európska komisia

Súbor nástrojov pre kybernetickú bezpečnosť v oblasti dopravy

Úvod

Generálne riaditeľstvo pre mobilitu a dopravu Európskej komisie (GR MOVE) zadalo zákazku na vypracovanie tohto súboru nástrojov na zvyšovanie povedomia a pripravenosti zainteresovaných strán v oblasti dopravy o kybernetických hrozbách. Súbor poskytuje poznatky na pochopenie kybernetických hrozieb a zmiernenie ich vplyvu na služby, systémy a činnosti v oblasti dopravy. Tento súbor nástrojov poskytuje alternatívne postupy na zvyšovanie povedomia, ktoré sa zameriavajú na rôzne profily v oblasti dopravy:

- Všetci zamestnanci v doprave (poskytovanie všeobecných informácií a usmernení)

- Dopravné subjekty s rozhodovacími právomocami v oblasti kybernetickej bezpečnosti v rámci rozličných druhov dopravy.

Hypertextové odkazy prepájajú rozličné časti, čím vytvárajú súbor nástrojov s cieľom podporovať prehliadateľnosť postupov na zvyšovanie povedomia prispôsobených konkrétnym profilom v oblasti dopravy.

Postupy uvedené v tomto súbore nástrojov majú len poradný charakter. Žiadne z formulovaných odporúčaní nie je záväzné ani povinné. Tento súbor navyše nepredstavuje formálne stanoviská Európskej komisie a jeho cieľom nie je poskytovať prostriedky dosiahnutia súladu s existujúcimi alebo budúcimi právnymi predpismi EÚ.

Profily v oblasti povedomia o kybernetickej bezpečnosti

Profil I: Všetci zamestnanci v doprave Prvý postup sa zameriava na všetkých zamestnancov dopravných organizácií, od zamestnancov v oblasti dopravných služieb po zamestnancov v oblasti administratívy. Poskytuje usmernenia smerom k zvýšenému porozumeniu a povedomiu týkajúcich sa najbežnejších kybernetických hrozieb, ktorých cieľom sú dopravné služby a systémy. Súbor okrem toho poskytuje poznatky o spôsoboch riešenia možných kybernetických hrozieb, a to vrátane ich identifikácie, nahlasovania a zmierňovania prostredníctvom osvedčených postupov v oblasti kybernetickej bezpečnosti.

Profil II: Dopravné subjekty s rozhodovacími právomocami v oblasti kybernetickej bezpečnosti. Druhý postup sa zameriava na zamestnancov v dopravných organizáciách s rozhodovacími právomocami v oblasti kybernetickej bezpečnosti. Tento postup zdôrazňuje osvedčené postupy prispôsobené rôznym druhom dopravy na zlepšovanie stavu kybernetickej bezpečnosti dopravných organizácií. Poskytujú sa v ňom najmä osvedčené postupy s cieľom identifikovať vznikajúce kybernetické hrozby namierené proti dopravným organizáciám, odhaľovať ich, chrániť pred nimi a reagovať na ne.

Európska komisia

Súbor nástrojov pre kybernetickú bezpečnosť v oblasti dopravy

Panoráma hrozieb v oblasti dopravy

Nové kybernetické hrozby ovplyvňujúce rozličné druhy dopravy

Profily v oblasti povedomia o kybernetickej bezpečnosti

Alternatívne postupy na zvyšovanie povedomia o kybernetickej bezpečnosti, ktoré sa zameriavajú na rôzne profily v oblasti dopravy

Európska komisia

Panoráma hrozieb v oblasti dopravy

Panoráma kybernetických hrozieb je dynamická a neprestajne sa vyvíja. Napriek tomu je možné identifikovať kybernetické hrozby, ktorým čelia všetky druhy dopravy pri prevádzke služieb a systémov.

Európska komisia

Aktéri hrozby

Jednotlivci alebo organizácie, ktoré majú potenciál vplývať na bezpečnosť a ochranu dopravných služieb a systémov

Nové kybernetické hrozby

Vybrané kybernetické hrozby, ktoré môžu eventuálne predstavovať vektory útoku, ktorý má vplyv na bezpečnosť a ochranu dopravných služieb a systémov

Európska komisia

Aktéri hrozby

Jednotlivci alebo organizácie môžu úmyselne alebo neúmyselne odhaliť a zneužiť zraniteľnosti, ktoré majú potenciál spôsobiť incidenty a vplývať na dopravné služby vrátane ich bezpečnosti, ochrany, podnikania, financií a dobrého mena. Medzi aktérov hrozby patria okrem iných štátom sponzorované skupiny, páchatelia kybernetickej trestnej činnosti, kybernetickí teroristi, hacktivisti, hackeri (vrátane script kiddies) a insideri (vrátane vysoko postavených insiderov).

Najvýznamnejšími škodlivými aktérmi, ktorí sa úmyselne zameriavajú na dopravné organizácie, sú **páchatelia kybernetickej trestnej činnosti**, **insideri**, **národné štáty** a **štátom sponzorované skupiny**.
Protivníci, ako sú **páchatelia kybernetickej trestnej činnosti**, vedú masívne útočné kampane a ich motiváciou je často finančné obohatenie.

Insideri poznajú jedinečnosti organizácií, pre ktoré pracujú, a často sú dobre oboznámení s citlivými bezpečnostnými zraniteľnosťami. Medzi aktérov vnútornej hrozby patria nespokojní zamestnanci, dodávatelia a zmluvní dodávatelia. So zintenzívňujúcim sa geopolitickým napätím sa **národné štáty** a **štátom sponzorované skupiny** zameriavajú na strategické dlhodobé ciele. Často sa snažia skrývať hlboko v systémoch organizácie a zhromažďovať citlivé informácie. Po vytvorení pevného miesta v systémoch si štátom sponzorovaní útočníci snažia vytvoriť pozíciu, z ktorej majú potenciál spôsobiť čo najhoršie škody. Ich cieľom môžu byť napríklad systémy iných organizácií využitím sieťového prepojenia organizácií.

K ďalším aktérom hrozieb patria **insideri**, ktorí môžu neúmyselne alebo náhodne vykonávať činnosti vedúce k udalostiam v oblasti kybernetickej bezpečnosti a v najhorších prípadoch ku kybernetickým incidentom, ktoré majú vplyv na bezpečnosť a ochranu dopravných služieb.

Európska komisia

Nové kybernetické hrozby

V oblasti dopravy existuje značný počet kybernetických hrozieb namierených proti doprave: **distribuované vyradenie služby**, **vyradenie služby**, krádež údajov, šírenie **malvéru**, **phishing**, manipulácia so softvérom, **neoprávnený prístup**, deštruktívne útoky, falšovanie alebo obchádzanie rozhodovacieho procesu prevádzkovateľa bezpečnosti, predstieranie identity, zneužitie prístupových oprávnení, **sociálne inžinierstvo**, pozmeňovanie vzhľadu, odpočúvanie, zneužitie majetku a manipulácia s hardvérom. Podľa komplexného výskumu dostupných dokumentov a rozhovorov s expertmi najnaliehavejšími novými kybernetickými hrozbami vplývajúcimi na dopravu sú: malvér, (distribuované) vyradenie služby, neoprávnený prístup a krádež, ako aj manipulácia so softvérom.

Európska komisia

Hrozba č. 1: Malvér

Škodlivý softvér, ktorý môže mať potenciálny vplyv na jednotlivcov alebo organizácie v rámci rôznych druhov dopravy.

Hrozba č. 2: (Distribuované) vyradenie služby

Kybernetické útoky, ktoré jednotlivcom alebo organizácii zabraňujú v prístupe k príslušným dopravným službám a zdrojom.

Hrozba č. 3: Neoprávnený prístup a krádež

Neoprávnený prístup, privlastnenie a zneužitie kritických aktív.

Hrozba č. 4: Manipulácia so softvérom

Kybernetické útoky namierené proti softvéru s cieľom upraviť jeho správanie a vykonávajúce špecifické útoky.

Hrozba č. 1: Malvér

Malvér tvorí škodlivý softvér, ktorý môže zahŕňať rôzne druhy softvérových aplikácií, ako sú vírusy, trójske kone, (počítačové) červy, ransomware, ťažiče kryptomeny alebo akýkoľvek softvér, ktorý môže mať potenciálne nepriaznivý vplyv na organizácie alebo jednotlivcov v rámci rôznych druhov dopravy.

Zmierňovanie šírenia malvéru určeného na úmyselné poškodenie počítačov, serverov, klientov, sietí alebo všetkých uvedených častí patrí medzi hlavné priority kybernetickej bezpečnosti v rámci všetkých druhov dopravy. Typický vektor útoku môže zahŕňať e-maily využívajúce phishing, ktoré sú zacielené na zamestnancov. Medzi ďalšie vektory útoku môžu patriť rozličné a sofistikované stratégie sociálneho inžinierstva, ako je zapojenie USB kľúča do voľného portu (napr. nabíjanie mobilného telefónu). Kliknutím na hypertextové odkazy v podozrivých e-mailoch alebo otvorením súborov v prílohách môže používateľ nevedome nainštalovať softvér alebo vedome ohroziť dopravné služby a zdroje.

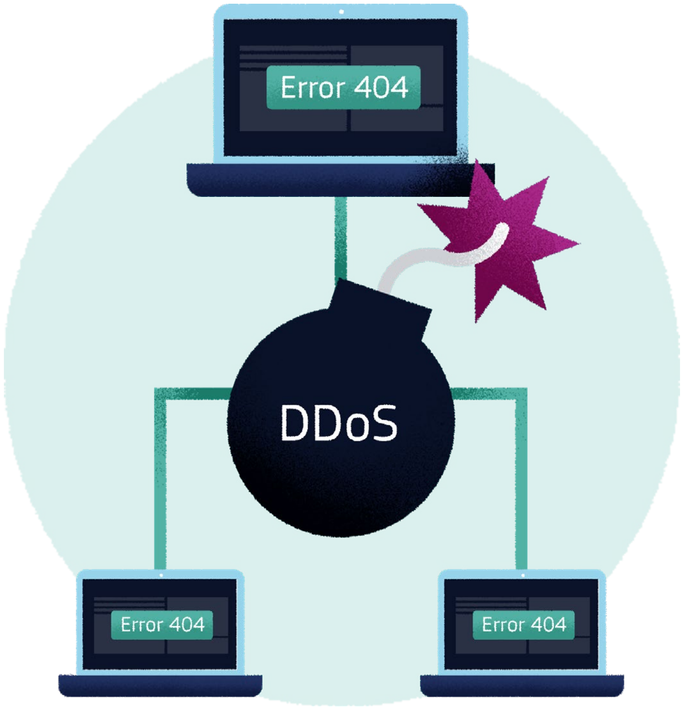
Napríklad, kybernetické napadnutie ransomwarom známym ako WannaCry malo vplyv na viac ako 150 krajín a nakazilo sa ním viac ako 230 000 systémov. Súčasťou útoku bol ransomware, ktorý sa bežne šíri prostredníctvom e-mailov využívajúcich phishing, ktoré obsahujú škodlivé prílohy alebo hypertextové odkazy. Pri tomto druhu útoku sa zneužíva sociálne inžinierstvo s cieľom nabádať používateľov systému, aby si nainštalovali (alebo aktivovali) konkrétny malvér.

Hrozba č. 2: (Distribuované) vyradenie služby

Distribuované útoky typu „vyradenie služby“ (DDoS) a útoky typu „vyradenie služby“ (DoS) majú vplyv na dostupnosť a prístupnosť údajov, služieb, systémov a ďalších zdrojov. Tieto druhy útokov sa môžu líšiť dĺžkou trvania a môžu byť zacielené súčasne na viac ako jednu službu alebo systém. Útoky DDoS využívajú viaceré systémy (alebo kanály útoku) s cieľom preťažiť požiadavkami cieľové služby alebo systémy. Úspešné útoky vplývajú na schopnosť služby a systému zvládnuť neočakávaný objem požiadaviek. Dôsledkom je zamietnutie prístupu k službám a zdrojom.

Je potrebné poznamenať, že zasiahnuté služby a systémy patriace dopravným organizáciám možno zneužiť na vykonávanie útokov DDoS a DoS, ktoré sú zamerané na špecifické systémy v prevádzkových činnostiach alebo aj v iných organizáciách.

Napríklad, podnikové informačné systémy (ako sú osobné počítače a zariadenia) môžu byť cieľom útokov na získanie prístupu k prevádzkovým technológiám, ktoré môžu byť pripojené k internetu alebo ktoré môžu mať prístup k sieťam na účely prenosu prevádzkových údajov. Prepojenia medzi rozličnými systémami a sieťami (ako sú podnikové siete, prevádzkové technológie a prístupy na účely diaľkovej údržby) môžu predstavovať zraniteľnosti, ktoré sa dajú zneužiť na vykonanie útokov DDoS alebo útokov DoS zameraných na kritické dopravné služby a systémy. Napríklad, útoky DDoS a útoky DoS môžu využívať bežné sieťové a komunikačné protokoly, ako sú Web Services Dynamic Discovery (WS-Discovery), ktoré môžu zariadenia internetu vecí používať na automatické vyhľadanie každého uzla v miestnych sieťach (LAN). Ak zariadenia internetu vecí obsahujú zraniteľnosti, útočníci ich môžu zneužiť na vyhľadanie iných pripojených zariadení a vykonať útoky DDoS alebo útoky DoS.



Európska komisia

Hrozba č. 3: Neoprávnený prístup a krádež

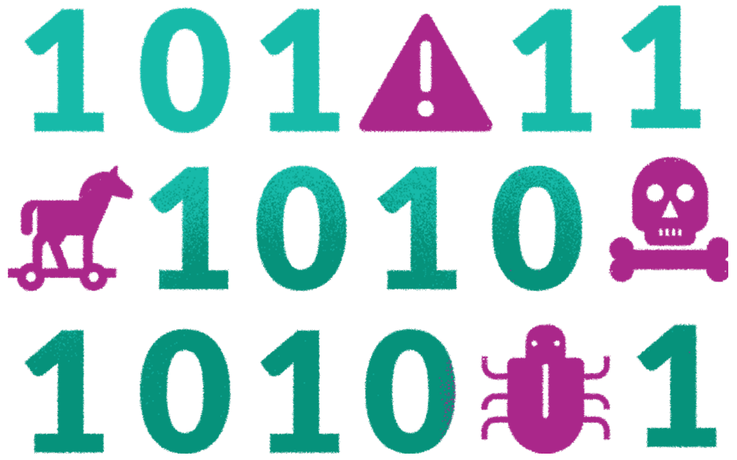
Aktéri hrozby môžu chcieť získať neoprávnený logický alebo fyzický prístup k sieti, systému, aplikácii, údajom alebo inému zdroju s cieľom vykonávať škodlivé činnosti, a to vrátane krádeže citlivých údajov alebo zdrojov (vrátane fyzických zdrojov).
Cieľom hrozieb neoprávneného prístupu a krádeže sú dôverné a chránené aktíva (vrátane osobných identít, prístupových údajov privilegovaných účtov, systémov a iných druhov dôverných a chránených informácií). Tieto hrozby môžu využívať zraniteľnosti systémov, ako a netušiacich jednotlivcov odhaľujúcich citlivé údaje, ako sú prístupové údaje (napr. prihlasovacie meno, heslo atď.) alebo osobné údaje (napr. e-mailová adresa, osobné identifikačné číslo atď.).

Krádež totožnosti v súvislosti s neoprávneným prístupom predstavuje nezákonné použitie osobných údajov alebo jedinečných identifikátorov s cieľom predstierať identitu osôb alebo služieb a systémov na získanie prístupu k súkromným alebo chráneným zdrojom (napr. finančným a fyzickým zdrojom). Cieľom takýchto kybernetických hrozieb môžu byť aj fyzické aktíva v rámci rôznych druhov dopravy.

Hrozba č. 4: Manipulácia so softvérom

Nesprávne nastavenia softvéru a príslušných systémov alebo komponentov a manipulácia s nimi môžu mať priamy vplyv na stav bezpečnosti dopravných služieb a systémov. Kybernetické útoky využívajúce manipuláciu so softvérom upravujú softvérové nastavenia alebo majú vplyv na integritu údajov s cieľom zmeniť správanie systémov a služieb. Útočníci môžu úmyselne manipulovať so softvérom (alebo jeho časťou) s cieľom získať kontrolu (napr. získanie neoprávneného prístupu, zabraňovanie prístupu oprávneným používateľom alebo systémom k nevyhnutným zdrojom, zhromažďovanie citlivých informácií, zmenu funkčného správania atď.) nad citlivými aktívami.

Útočníci sa napríklad môžu zamerať na komunikačné kanály výrobcov s cieľom nahrať aktualizácie škodlivého softvéru do prevádzkovaných služieb a systémov (vrátane prevádzkových technológií). Agent hrozby používa zneužité autorizačné údaje na prístup k sieťovému rozhraniu vzdialenej údržby s cieľom nainštalovať zmanipulovaný softvér a ďalej narúšať iné prístupné služby a systémy. Agent hrozby inštaluje zmanipulovaný softvér, ktorý ďalej narúša cieľové služby a systémy, prípadne útočí na iné prepojené služby alebo systémy.



Európska komisia

Profily v oblasti povedomia o kybernetickej bezpečnosti

Európska komisia

1

Profil I: Všetci zamestnanci v doprave

Prvý postup sa zameriava na všetkých zamestnancov dopravných organizácií, od prevádzkových zamestnancov po zamestnancov v oblasti administratívy. Poskytuje usmernenia smerom k zvýšenému porozumeniu a povedomiu v súvislosti s najbežnejšími kybernetickými hrozbami, ktorých cieľom sú dopravné služby. Okrem toho poskytuje poznatky o spôsoboch riešenia možných kybernetických hrozieb, a to vrátane ich identifikácie, nahlasovania a zmierňovania prostredníctvom postupov v oblasti kybernetickej bezpečnosti. Tento postup je spoločný pre všetky druhy dopravy.

2

Profil II: Subjekty s rozhodovacími právomocami v oblasti kybernetickej bezpečnosti dopravy

Druhý postup sa zameriava na zamestnancov v dopravných organizáciách s rozhodovacími právomocami v oblasti bezpečnosti alebo kybernetickej bezpečnosti. Tento postup poskytuje osvedčené postupy prispôsobené rôznym druhom dopravy. Poskytujú sa v ňom osvedčené postupy s cieľom identifikovať vznikajúce kybernetické hrozby namierené proti dopravným organizáciám, odhaľovať ich, chrániť pred nimi a reagovať na ne.

Európska komisia

Profil I: Všetci zamestnanci v doprave

Táto časť sa zameriava na všetkých zamestnancov dopravných organizácií, od prevádzkových zamestnancov po zamestnancov v oblasti administratívy. Poskytujú sa v nej usmernenia smerom k zvýšenému porozumeniu a povedomiu v súvislosti s najbežnejšími kybernetickými hrozbami, ktorých cieľom sú dopravné služby. Okrem toho poskytuje poznatky o spôsoboch riešenia možných kybernetických hrozieb, a to vrátane ich identifikácie, nahlasovania a zmierňovania prostredníctvom postupov v oblasti kybernetickej bezpečnosti.
V tejto časti sa poskytujú odporúčané postupy a užitočné tipy, ktoré sú relevantné pre **všetky druhy dopravy**.

Osvedčené postupy ochrany pred malvérom

Vašu organizáciu môžete pomôcť chrániť dodržiavaním osvedčených postupov na **identifikáciu malvéru a zabraňovanie jeho šírenia**, ako sú:

- ***Dodržiavanie bezpečnostných politík**, ako sú kontrola pamäťových médií a súborov na účely odhalenia vírusov, neotváranie konkrétnych druhov súborov a ich zasielanie e-mailom (napr. spustiteľné súbory, ako sú súbory s príponou .exe, .bat, .com atď.), inštalácia len autorizovaného softvéru, zabezpečenie aktualizácie softvéru (vrátane antivírusového programu) a jeho správnej funkcie, ako aj ďalších bezpečnostných politík.*

- *Pravidelné **zálohovanie údajov** na zabezpečené (a autorizované) pamäťové dátové zariadenia alebo služby, ktoré by mali podporovať šifrovacie mechanizmy na ochranu údajov v pokoji a ktoré majú dostupné procesy na obnovu údajov.*

- *Ochrana všetkých systémov vrátane mobilných a koncových zariadení vhodnými **bezpečnostnými opatreniami** (napr. heslo, šifrovanie atď.) a bezpečné uzamknutie (fyzické a digitálne) všetkých systémov v prípade ich nepoužívania.*

- *Neotváranie príloh a neklikanie na hypertextové odkazy v neočakávaných e-mailoch a na podozrivých kontextových oknách internetového prehliadača, ktoré obsahujú zvláštny text alebo ktoré pochádzajú od neznámych odosielateľov a internetových domén.*

- *Nepripájanie **nedôveryhodných alebo neznámych odnímateľných zariadení**, ako sú USB kľúče, pevné disky a iné pamäťové zariadenia, k vášmu počítaču.*

- *Nedeaktivácia bezpečnostných opatrení týkajúcich sa malvéru (napr. antivírusový softvér, softvér na filtrovanie obsahu, firewall atď.).*

- *Pravidelná **aktualizácia nainštalovaného softvéru** na najnovšiu dostupnú verziu (ktorú môžu pracovníci v oblasti informačnej bezpečnosti alebo správcovia systému vydávať s pravidelnými aktualizáciami).*

- *Nepoužívanie privilegovaných (napr. administrátorských) účtov a prístupových údajov pri výkone bežných činností a úkonov.*

- *Nahlasovanie každého podozrivého e-mailu alebo neočakávaného správania systému pracovníkom informačnej bezpečnosti alebo správcom systému.*

- *Venovanie pozornosti informačnej bezpečnosti v rámci rutinnej každodennej práce s cieľom rozpoznať problémy s bezpečnosťou v oblasti IT a primerane na ne reagovať.*

Európska komisia

Osvedčené postupy proti (distribuovanému) vyradeniu služby

Vašu organizáciu môžete pomôcť chrániť identifikovaním **útokov typu „distribuované vyradenie služby“ (DDoS)** a útokov **typu „vyradenie služby“ (DoS)**. Vaše bezpečnostné a IT tímy by ste mali bezodkladne kontaktovať, keď odhalíte alebo zaznamenáte ktorýkoľvek z týchto náznakov potenciálne prebiehajúceho útoku DDoS a útoku DoS na vaše služby alebo systémy:

- *Zvyšujúce sa požiadavky pohlcujúce kapacitu siete (pociťované ako pomalosť služieb a odpovedí), čo vedie k zlyhaniu služby alebo siete v dôsledku preťaženia.*

- *Zvyšujúce sa požiadavky na využitie pamäťových zdrojov bez zjavného dôvodu.*

- ***Neočakávané správanie služieb alebo systémov**, časté zlyhania a zvláštne chybové správy v dôsledku škodlivej spotreby výpočtových zdrojov alebo sieťových pripojení.*

- ***Zhoršenie výkonu** zariadení, dlhý čas vykonávania bežných úloh a pozorovateľné činnosti (napr. hlučný ventilátor pri spomalenom výkone zariadení).*

- ***Neočakávané internetové pripojenia alebo strata pripojení** k službám a systémom.*

- *Jemné zmeny v správaní prevádzkových kontrol alebo technológií, ktorých výsledkom je fyzické poškodenie.*

- *Neposkytnutie prístupu k privilegovaným alebo administrátorským účtom s cieľom zabrániť, aby postupy reakcie na incident obnovili prístup.*

Osvedčené postupy proti neoprávnenému prístupu a krádeži

Aby sa zabránilo útokom týkajúcim sa neoprávneného prístupu a krádeže, je nevyhnutné dodržiavať zásady, akými sú *„potreba poznať“* a *„štandardná bezpečnosť a ochrana súkromia“*, ktoré zdôrazňujú to, že citlivé a dôverné aktíva (vrátane osobných a citlivých údajov, dopravných systémov atď.) by mali byť prístupné len osobám, ktoré majú právo na prístup k nim s cieľom vykonávať svoje povinnosti. Vašu organizáciu môžete pomôcť chrániť dodržiavaním osvedčených postupov na identifikáciu neoprávneného prístupu a krádeže a ich zabraňovanie, ako sú:

- *Dodržiavanie bezpečnostných politík organizácie.*

- *Nezdieľanie a nezverejňovanie prístupových údajov a osobných údajov na internete, a to vrátane obrázkov, ktoré môžu takého informácie obsahovať.*

- *Nepoužívanie prístupových údajov a osobných údajov (ako aj iných citlivých údajov) a ich neposielanie na nedôveryhodné a nezabezpečené siete, zariadenia alebo internetové služby (napr. webové sídla, ktoré používajú nezabezpečené protokoly alebo adresy http:// a nie zabezpečené https:///).*

- ***Neodhaľovanie** – nikomu a za žiadnych okolností – **svojich prístupových údajov** (napr. prihlasovacie meno a heslo), a to ani prostredníctvom e-mailu alebo telefonicky.*

- *Ochrana citlivých údajov zadávaných na klávesnici alebo zobrazovaných na obrazovke (vrátane mobilných zariadení) pred neoprávnenými osobami, inštalácia privátnych filtrov na obrazovky a vyhýbanie sa práci na verejných miestach a so súkromnými zariadeniami, ako aj vyhýbanie sa ponechaniu akéhokoľvek zariadenia v neuzamknutom stave a bez dozoru.*

- ***Používanie zložitých hesiel** (napr. dostatočne dlhé heslo s kombináciou alfanumerických a špeciálnych znakov), ktoré sú v súlade s príslušnými bezpečnostnými politikami organizácie, s cieľom zabrániť neoprávnenému prístupu.*

- ***Zmena predvolených hesiel** prepojených systémov a zariadení (napr. tlačiarní, routerov, kamier, inteligentného zámku atď.).*

- *Nepoužívanie rovnakých prístupových údajov (napr. prihlasovacie meno a heslo) v rámci viacerých služieb a systémov, ako aj nepoužívanie rovnakých prístupových údajov v rámci služieb a systémov, ktoré si vyžadujú privilegované účty.*

- *Posielanie hesiel a kľúčov pre prenášané chránené súbory (napr. archívy vo formáte ZIP) len prostredníctvom mimopásmového kanálu (napr. SMS prostredníctvom GSM a telefonátu) a nikdy nie prostredníctvom e-mailu.*

- ***Aktivácia dvojstupňovej autentifikácie (2FA)** alebo viacstupňovej autentifikácie (MFA), ak je to možné.*

Európska komisia

Osvedčené postupy proti manipulácii so softvérom

Vašu organizáciu môžete pomôcť chrániť dodržiavaním osvedčených postupov na identifikáciu manipulácie so softvérom a jej zabraňovanie, ako sú:

- *Neinštalovanie nespoľahlivého softvéru na systémoch a zariadeniach (vrátane osobných počítačov, serverov, periférnych zariadení, sieťových zriadení, smartfónov atď.).*
- *Inštalácia softvéru a aktualizácií výlučne z oficiálnych zdrojov a webových stránok (napr. výrobcovia, podnikové úložiská atď.).*
- *Nesťahovanie softvéru a aplikácií (ako aj akýchkoľvek súborov) z nelegálnych zdrojov.*
- *Odinštalovanie nepotrebného alebo v poslednom období nevyužívaného softvéru, ako aj deaktivácia nepotrebných pripojení (napr. sieťových protokolov a služieb) vrátane prístupu k vzdialeným službám (napr. cloudové úložiská).*
- *Kontrola každého softvéru alebo pamäťových zariadení prostredníctvom spoľahlivého a aktualizovaného antivírusového programu.*
- *Sťahovanie bezpečného priemyselného softvéru (napr. aktualizácií, softvérových záplat, nových produktov atď.) od dôveryhodných dodávateľov pri dodržiavaní zásady „bielej stanice“ (white station principle).*
- *Aktualizácia všetkých nainštalovaných softvérových programov v súlade s politikami a postupmi organizácie.*

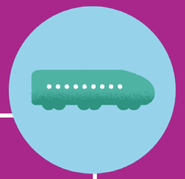
Európska komisia

Profil II: Subjekty s rozhodovacími právomocami v oblasti kybernetickej bezpečnosti dopravy

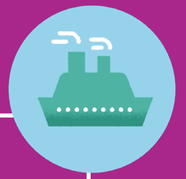
Táto časť sa zameriava na zamestnancov v dopravných organizáciách s rozhodovacími právomocami v oblasti bezpečnosti alebo kybernetickej bezpečnosti. Tento postup zdôrazňuje osvedčené postupy prispôsobené rôznym druhom dopravy. Poskytujú sa v ňom najmä osvedčené postupy s cieľom identifikovať vznikajúce kybernetické hrozby, odhaľovať ich, chrániť pred nimi a reagovať na ne.

Európska komisia

Osvedčené postupy v oblasti kybernetickej bezpečnosti prispôsobené leteckej doprave



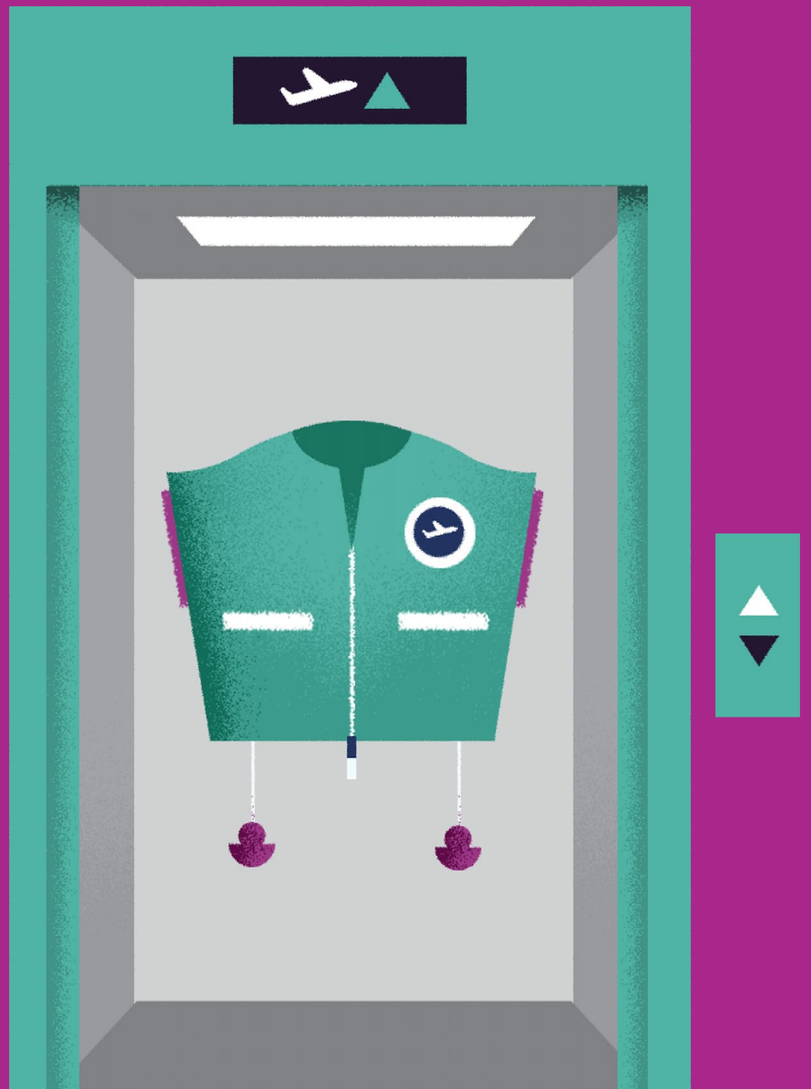
Osvedčené postupy v oblasti kybernetickej bezpečnosti prispôsobené pozemnej doprave



Osvedčené postupy v oblasti kybernetickej bezpečnosti prispôsobené námornej doprave

Európska komisia

Osvedčené postupy a bezpečnostné opatrenia prispôsobené leteckej doprave



Riadenie

Organizácie leteckej dopravy potrebujú jasne pochopiť nové hrozby s cieľom vymedziť politiky a procesy riadenia na riadenie svojich koncepcií s cieľom zvýšiť kybernetickú bezpečnosť prevádzkovaných služieb a systémov, a to vrátane informačných technológií (IT) a prevádzkových technológií (PT).

Medzi osvedčené postupy organizácií, bez ohľadu na ich veľkosť, patria:

- Zabezpečenie, že úrovne vyššieho manažmentu nahlasujú obavy v oblasti kybernetickej bezpečnosti riadiacim pracovníkom a predstavenstvu, ktorí môžu prijať informované rozhodnutia o pridelení zdrojov.

- Stanovenie riadiacej pozície, ktorá je zodpovedná za kybernetickú bezpečnosť, ako aj za fyzickú bezpečnosť, so zodpovednosťou za celkové riadenie, pokiaľ ide o bezpečnosť informačných technológií (IT) a prevádzkových technológií (PT), avšak bez zapojenia do prevádzkových činností na zabránenie konfliktu záujmov.

- Jasné vymedzenie úloh, zodpovedností, právomocí a oprávnení týkajúcich sa kybernetickej bezpečnosti a ich oznamovanie a dohoda o nich s príslušnými zamestnancami, najmä pokiaľ ide o členov tímov reakcie na núdzové počítačové situácie (CERT).

- Zabezpečenie riadenia kybernetickej bezpečnosti v celom dodávateľskom reťazci bezpečnostných služieb, a to vrátane fyzických aj digitálnych rozhraní, od výrobcov technológií a montážnych technikov po poskytovateľov bezpečnostných služieb.

- Dohoda o činnostiach a kontrolách vrátane spoločných zodpovedností na riadenie rizík v oblasti kybernetickej bezpečnosti a zabezpečenie, že tieto zodpovednosti sú udržiavané počas celého životného cyklu (napr. dohodami o službách) bezpečnostných riešení a služieb.

- Vymedzenie mechanizmov riadenia (napr. politík) s cieľom dodržiavať povinnosti vyplývajúce z príslušných nariadení a smerníc, akými sú nariadenie 2018/1139 o spoločných pravidlách v oblasti civilného letectva a vykonávacie nariadenie Komisie 2017/373, ktorým sa stanovujú spoločné požiadavky na poskytovateľov manažmentu letovej prevádzky/leteckých navigačných služieb a na ostatné funkcie siete manažmentu letovej prevádzky a dohľad nad nimi, ako aj smernica NIS (smernica EÚ 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov).

Príklady služieb a systémov v leteckej doprave:
Príkladmi informačných technológií sú tie, ktoré sú prístupné tak zamestnancom (napr. osobné počítače, mobilné telefóny, periférne kancelárske zariadenia atď.), ako aj cestujúcim (napr. verejné routre a pripojenia Wi-Fi atď.). Príkladmi prevádzkových technológií sú systémy kontrolného riadenia a zberu údajov (SCADA), systémy vykurovania, vetrania a klimatizácie (HVAC), kontrolné miesta bezpečnostnej ochrany pre príručnú batožinu, systémy na obsluhu batožiny (BHS), kontrola prístupu, monitorovanie, dohľad, systémy spustenia alarmu, technológie detekčnej kontroly, systémy na kontrolu osvetlenia plochy letiska, radarové zariadenia a snímače, globálne polohové systémy (GPS), systémy manažmentu letovej prevádzky (ATM), spojovacie, navigačné a sledovacie systémy (CNS), letecké informačné systémy, meteorologické systémy, systémy strediska pre bezpečnostné operácie, letecké palubné systémy a iné.

Identifikácia kybernetických hrozieb

Riadenie rizík: Organizácie v oblasti letectva musia prijať primerané kroky na identifikáciu, posúdenie a pochopenie kybernetických rizík pre sieť a informačné systémy, ktoré podporujú prevádzku základných funkcií.

Vyžaduje si to celkový organizačný prístup k riadeniu rizík, ktorého súčasťou sú:

- *Zabezpečenie jasného prehľadu o rozličných hardvérových a softvérových systémoch zavedených na poskytovanie rôznych služieb. Takéto systémy v súvislosti s leteckou dopravou zahŕňajú informačné technológie (IT), ako aj prevádzkové technológie (PT).*

- *Vykonávanie **posúdení kybernetických rizík**, v ktorých sa zohľadňujú nové hrozby, známe zraniteľnosti a prevádzkové údaje vo vzťahu k dotknutým systémom. Organizácie, akými sú Tím reakcie na núdzové počítačové situácie v rámci európskeho manažmentu letovej prevádzky (EATM-CERT) a Stredisko pre výmenu a analýzu informácií v oblasti leteckej dopravy (A-ISAC), môžu poskytnúť poznatky o hrozbách, ktorých cieľom je letecká doprava.*

- *Zabezpečenie, aby sa posúdenia rizík vzťahovali aj na riziká týkajúce sa každodennej činnosti zamestnancov (napr. používanie sociálnych médií, používanie osobných zariadení, spracúvanie osobných údajov, výmena informácií atď.).*

- *Určovanie a vykonávanie opatrení a plánov na riešenie rizík s cieľom zmierňovať kybernetické riziká.*

- *Zavedenie komplexného **systému riadenia informačnej bezpečnosti** (ISMS) a **systému riadenia ochrany osobných údajov** (PIMS), ktoré sú zosúladené s inými systémami riadenia. Takéto systémy riadenia (t. j. ISMS a PIMS) zahŕňajú vykonávanie bezpečnostných kontrol (ako aj kontrol v oblasti ochrany údajov a súkromia) s cieľom zmierňovať vznikajúce hrozby, ktoré majú vplyv na bezpečnosť služieb a systémov leteckej dopravy (vrátane ich údajov), a zabraňovať ich vzniku.*

- *Zohľadnenie všetkých obmedzení týkajúcich sa **správy aktív a plánovania zdrojov** (t. j. obmedzení, ktoré môžu mať vplyv na dodanie, údržbu a podporu kritických systémov pre prevádzku základných funkcií v leteckej doprave).*

Európska komisia

Príklady rámcov riadenia rizík: Východiskom a základom prístupu k riadeniu rizík prispôsobeného pre leteckú dopravu môžu byť rozličné rámce (napr. normy v rámci skupiny ISO/IEC 27000, rámec kybernetickej bezpečnosti NIST, rámec MITRE ATT&CK, BSI IT-Grundschutz atď.). Medzinárodné organizácie, ako sú IATA a ICAO, poskytujú usmernenia pre posudzovanie kybernetického rizika. Organizácie ENISA, EASA, EUROCONTROL a Medzinárodná rada letísk okrem iného vyzdvihujú osvedčené postupy na zabezpečenie letísk, poskytovateľov manažmentu letovej prevádzky a iných organizácií v oblasti leteckej dopravy. Spoločný podnik SESAR koordinuje a sústreďuje všetky výskumné a vývojové činnosti EÚ v oblasti manažmentu letovej prevádzky, ktoré sa vzťahujú na aspekty bezpečnosti, ako aj bezpečnostnej ochrany.

Európska komisia

Ochrana pred kybernetickými hrozbami

Organizácie v oblasti leteckej dopravy by mali vykonávať vhodné a primerané bezpečnostné opatrenia na ochranu svojich sietí a informačných systémov, a to vrátane informačných technológií (IT) a prevádzkových technológií (PT), pred kybernetickým napadnutím. Medzi bezpečnostné opatrenia patria:

- ***Bezpečnostné politiky a postupy:*** *vymedzenie, vykonávanie, oznamovanie a presadzovanie primeraných politík a postupov, v rámci ktorých sa vymedzuje celkový prístup k zabezpečeniu systémov a údajov, ktoré podporujú prevádzku základných funkcií v leteckej doprave. Tieto bezpečnostné politiky (napr. politiky v oblasti hesiel a uchovávania) a postupy by sa mali zároveň vzťahovať na softvérové záplaty a riadenie zraniteľností hardvérových a softvérových systémov (vrátane IT a PT), riadenie incidentov, ako aj na ochranu siete a systému.*

- ***Riadenie identity a prístupu:*** *pochopenie, zdokumentovanie a riadenie prístupu k sieťam a informačným systémom (vrátane IT a PT), ktoré podporujú prevádzku základných funkcií v leteckej doprave. Používatelia (alebo automatizované funkcie), ktoré majú možnosť prístupu k údajom alebo systémom, sa primeraným spôsobom overujú, autentifikujú a autorizujú. Zároveň by sa v rámci toho mali zohľadniť rozdielne úlohy a zodpovednosti, pokiaľ ide o bežné a privilegované účty.*

- ***Zabezpečenie údajov a systému:*** *ochrana údajov (uchovávaných a elektronicky prenášaných), kritických sietí a informačných systémov (vrátane IT a PT) pred kybernetickými útokmi. Organizácie by so zreteľom na prístup založený na rizikách mali vykonávať bezpečnostné opatrenia na účinné obmedzenie príležitostí pre útočníkov na to, aby ohrozili údaje, siete a systémy. Medzi tieto bezpečnostné opatrenia by malo patriť aj zavedenie protokolov šifrovania a chránenej komunikácie s cieľom chrániť údaje v pokoji a prenášané údaje pred kybernetickými hrozbami, ktorých dôsledkom sú útoky technikou „man-in-the-middle“. Okrem toho je nevyhnutné na ochranu prístupu k systémom skombinovať takéto opatrenia s opatreniami v oblasti fyzickej bezpečnosti (napr. systémy by sa mali nachádzať vo vyhradenom priestore s obmedzeným prístupom).*

- ***Odolnosť sietí a systémov:*** *budovanie odolnosti sietí a systémov (vrátane IT a PT) ich koncipovaním a zavádzaním (ako aj ich prevádzkových postupov) tak, aby odolávali vplyvu kybernetických útokov a zmierňovali ho. Príkladmi koncepcie a vykonávania riešení na zvýšenie odolnosti sú: formálne overené kritické funkcie, redundancia systémov a sietí, oddelenie sietí (najmä oddelenie IT a PT), viacvrstvové bezpečnostné opatrenia a mnohé ďalšie. Treba poznamenať, že z hľadiska informačnej bezpečnosti môžu vhodné bezpečnostné riešenia poskytnúť bezpečnostné domény, ktoré zavádzajú oddelenie siete a systému. Prevádzkové potreby (napr. činnosti údržby, prenosy údajov atď.) systému si však môžu vyžadovať obchádzanie alebo pripájanie k odlišným bezpečnostným doménam (napr. oddelené systémy a siete) vrátane pripojenia k IT a PT.*

Odhaľovanie kybernetických hrozieb

Organizácie by mali zabezpečiť, že bezpečnostné opatrenia zostanú účinné a odhalia všetky kybernetické incidenty, ktoré vplývajú alebo ktoré majú potenciál ovplyvniť bezpečnostné kontroly, ako aj základné služby a systémy. Relevantnými bezpečnostnými opatreniami na odhaľovanie kybernetických hrozieb sú:

- ***Monitorovanie bezpečnosti:*** *monitorovanie stavu bezpečnosti sietí a informačných systémov vrátane informačných technológií (IT) a prevádzkových technológií (PT), ktoré podporujú prevádzku základných funkcií v rámci služieb leteckej dopravy. Medzi údaje, ktoré sa zohľadňujú na podporu monitorovania bezpečnosti, patria napríklad:*

  - *záznamy o bezpečnosti*
  - *záznamy o detekcii vírusov*
  - *záznamy o detekcii narušenia*
  - *záznamy o identifikácii, autentifikácii a autorizácii*
  - *systémové záznamy a servisné záznamy*
  - *záznamy o sieťovej prevádzke*
  - *záznamy o spracovaní údajov*

- ***Objavovanie bezpečnostných incidentov:*** *odhaľovanie škodlivých činností (t. j. bezpečnostných incidentov), ktoré majú vplyv alebo ktoré majú potenciál vplývať na bezpečnosť sietí a informačných systémov (vrátane IT a PT) podporujúcich prevádzku základných funkcií v rámci služieb leteckej dopravy.*

Tieto opatrenia si môžu vyžadovať zavedenie konkrétnych technológií (napr. riadenie informačnej bezpečnosti a bezpečnostných incidentov, systém detekcie prienikov, systém prevencie prienikov atď.) a vytvorenie centra bezpečnostných operácií alebo jeho ekvivalentu. Znamená to vytvorenie prostriedkov na lokálne odhaľovanie kybernetických útokov, ich analýzu, reakciu na ne a ich prekonanie.

Spravodajské informácie o kybernetických hrozbách, na ktorých je založené monitorovanie bezpečnosti a odhaľovanie, môžu poskytnúť národné jednotky pre riešenie počítačových bezpečnostných incidentov (CSIRT), sektorové tímy reakcie na núdzové počítačové situácie (CERT) [napr. tím reakcie na núdzové počítačové situácie v rámci európskeho manažmentu letovej prevádzky (EATM-CERT) agentúry EUROCONTROL], komerčné tímy leteckých spoločností na núdzové počítačové situácie a Stredisko pre výmenu a analýzu informácií v oblasti leteckej dopravy (A-ISAC).

Plánovanie reakcie a obnovy

Organizácia by mala vymedziť, vykonať a otestovať postupy riadenia incidentov, ktorých cieľom je zabezpečiť kontinuitu činností služieb a systémov v prípade kybernetických incidentov. Cieľom zmierňujúcich opatrení je zadržať alebo obmedziť vplyv kybernetických incidentov.

V rámci plánovania reakcie a obnovy by sa mali zohľadniť bezpečnostné opatrenia, ktoré zmierňujú vplyv konkrétnych kybernetických napadnutí, ako sú:

- *koordinácia a spolupráca s národnými jednotkami CSIRT, (verejnými a komerčnými) tímami CERT a strediskami ISAC počas kybernetických incidentov, koordinácia incidentov a kríz na celoeurópskej úrovni.*

- *Výmena informácií s inými organizáciami vrátane poskytovateľov v dodávateľskom reťazci služieb leteckej dopravy.*

- *Vykonávanie pravidelných **kybernetickobezpečnostných cvičení** (simulačná koordinácia, ako aj technické cvičenia) na posúdenie bezpečnostných opatrení a postupov, ako aj odolnosti organizácie čeliť kybernetickým incidentom.*

- *Prístup k archivovaným alebo záložným úložiskám v prípade narušenej integrity a dostupnosti dátových úložísk.*

- ***Bezpečnostné operačné protokoly**, ktoré obsahujú podrobné postupy na riadenie kybernetických incidentov a návrat služieb a systémov do bežných prevádzkových podmienok.*

- *Presmerovania sieťovej prevádzky na redundantné služby počas útokov typu „vyradenie služby“.*

- *Manuálne postupy pre režimy prevádzky služieb a systémov za mimoriadnych okolností.*

- *Vymedzenie postupov s cieľom riešiť porušenia ochrany údajov vrátane postupov na riešenie porušení ochrany údajov, ktoré majú vplyv na osobné údaje v súlade so všeobecným nariadením o ochrane údajov a akýmkoľvek iným príslušným sektorovým nariadením alebo smernicou.*

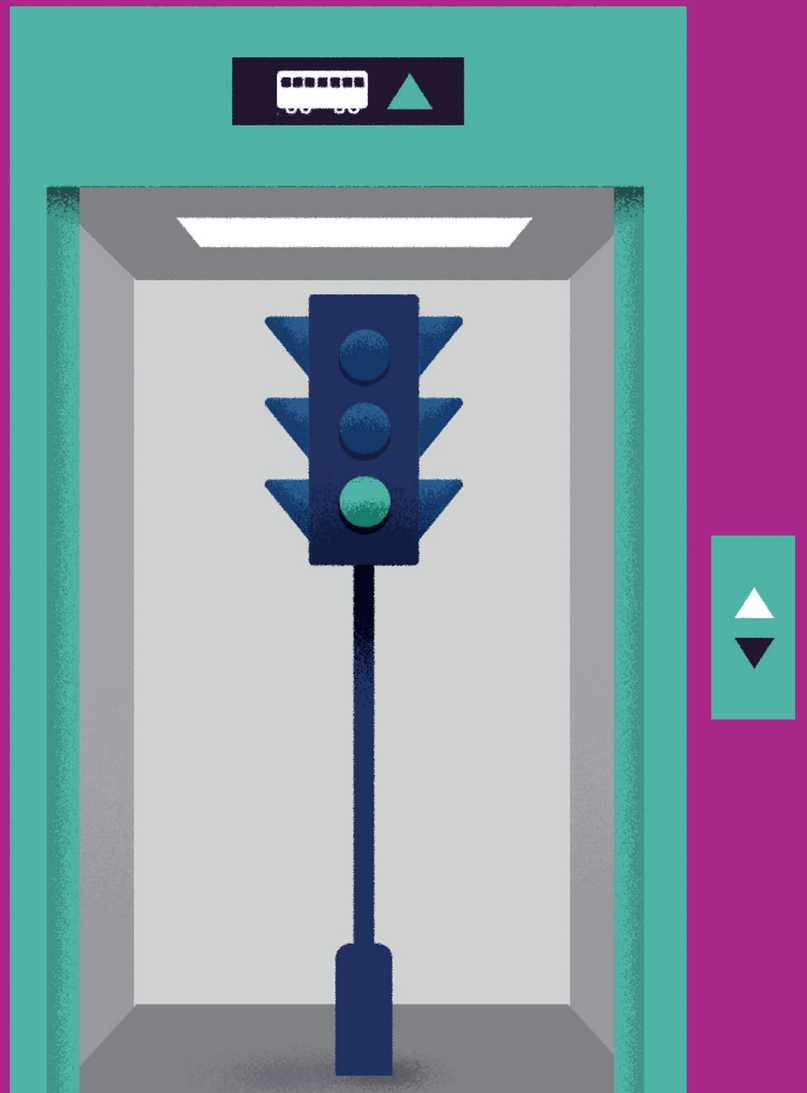
- *Zaobstarať si **kybernetické poistenie** s cieľom čiastočne vykompenzovať riziko späté so závažnými kybernetickými incidentmi.*

- *Na zvýšenie kapacity a odbornosti uzavrieť zmluvu o honorári za reakciu na incident s jednou alebo viacerými špecializovanými firmami.*

- *Vymedziť postupy **výmeny informácií o kybernetických incidentoch** s relevantnými zainteresovanými stranami, a to vrátane postupov na nahlasovanie incidentov v súlade so smernicou NIS (smernica EÚ 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii).*

Európska komisia

Osvedčené postupy a bezpečnostné opatrenia prispôsobené pozemnej doprave



Riadenie

Organizácie pozemnej dopravy (železničná a cestná doprava) potrebujú jasne pochopiť vznikajúce hrozby s cieľom vymedziť politiky a procesy riadenia na riadenie svojich prístupov s cieľom zvýšiť kybernetickú bezpečnosť služieb a systémov v prevádzke, a to vrátane informačných technológií (IT) a prevádzkových technológií (PT).

Medzi osvedčené postupy organizácií, bez ohľadu na ich veľkosť, patria:

- *Zabezpečenie, že úrovne vyššieho manažmentu nahlasujú obavy v oblasti kybernetickej bezpečnosti riadiacim pracovníkom a predstavenstvu, ktorí môžu prijať informované rozhodnutia o pridelení zdrojov.*

- *Stanovenie riadiacej pozície, ktorá je zodpovedná za kybernetickú bezpečnosť, ako aj za fyzickú bezpečnosť, so zodpovednosťou za celkové riadenie, pokiaľ ide o bezpečnosť informačných technológií (IT) a prevádzkových technológií (PT), avšak bez zapojenia do prevádzkových činností na zabránenie konfliktu záujmov.*

- *Jasné vymedzenie úloh, zodpovedností, právomocí a oprávnení týkajúcich sa kybernetickej bezpečnosti a ich oznamovanie a dohoda o nich s dotknutými zamestnancami. Potrebné je to, najmä pokiaľ ide o členov tímov reakcie na núdzové počítačové situácie (CERT).*

- *Zabezpečenie riadenia kybernetickej bezpečnosti v celom dodávateľskom reťazci bezpečnostných služieb, a to vrátane fyzických aj digitálnych rozhraní, od výrobcov technológií a montážnych technikov po poskytovateľov bezpečnostných služieb.*

- *Dohoda o činnostiach a kontrolách vrátane spoločných zodpovedností na riadenie rizík v oblasti kybernetickej bezpečnosti a zabezpečenie, že tieto zodpovednosti sú udržiavané počas celého životného cyklu (napr. dohodami o službách) bezpečnostných riešení a služieb.*

- *Vymedzenie mechanizmov riadenia (napr. politiky) s cieľom dodržiavať povinnosti vyplývajúce z príslušných nariadení a smerníc. Týka sa to širokého súboru politík, ktoré sa vzťahujú na konkrétne druhy dopravy a na rôzne druhy zainteresovaných strán (napr. výrobcov vozidiel a železničných systémov), ako aj smernice NIS (smernica EÚ 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov).*

Príklady služieb a systémov v pozemnej doprave:
Príkladmi informačných technológií sú tie, ktoré sú prístupné tak zamestnancom (napr. osobné počítače, mobilné telefóny, periférne kancelárske zariadenia atď.), ako aj cestujúcim (napr. verejné routre a pripojenia Wi-Fi atď.). Príkladmi prevádzkových technológií sú systémy kontrolného riadenia a zberu údajov (SCADA), systémy vykurovania, vetrania a klimatizácie (HVAC), globálne polohové systémy (GPS), kontrola vstupu, monitorovanie, dohľad, systémy spustenia alarmu a technológie na detekčnú kontrolu. Špecifickými systémami železničnej dopravy sú napríklad: prevádzkové systémy (systémy riadenia-zabezpečenia) vrátane návestných systémov, európsky systém riadenia železničnej dopravy (ERTMS), palubné vlakové systémy, systémy údržby a iné.

Identifikácia kybernetických hrozieb

Riadenie rizík: Organizácie pozemnej dopravy musia prijať primerané kroky na identifikáciu, posúdenie a pochopenie kybernetických rizík pre sieť a informačné systémy, ktoré podporujú prevádzku základných funkcií. Vyžaduje si to celkový organizačný prístup k riadeniu rizík, ktorého súčasťou sú:

- *Zabezpečenie jasného prehľadu o rozličných hardvérových a softvérových systémoch zavedených na poskytovanie rôznych služieb. Takéto systémy v súvislosti s pozemnou dopravou zahŕňajú informačné technológie (IT), ako aj prevádzkové technológie (PT).*

- *Vykonávanie **posúdení kybernetických rizík**, v ktorých by sa mali zohľadniť nové hrozby, známe zraniteľnosti a prevádzkové údaje vo vzťahu k dotknutým systémom.*

Príkladmi systémov v druhoch pozemnej dopravy sú: platobné systémy, sieťové a komunikačné systémy (napr. internet, rádiové spojenie, siete Wi-Fi atď.), vozidlové vybavenie, strediská riadenia prevádzky, systémy riadenia identity, bezpečnostné systémy a iné. Príkladmi systémov železničnej infraštruktúry sú: železničné koľajové vozidlá, subsystémy prevádzky a riadenia dopravy, subsystémy traťového a vozidlového riadenia-zabezpečenia a návestenia, a iné.

- *Zabezpečenie, aby sa posúdenia rizík vzťahovali aj na riziká týkajúce sa každodennej činnosti zamestnancov (napr. používanie sociálnych médií, používanie osobných zariadení, spracúvanie osobných údajov, výmena informácií atď.).*

- *Určovanie a vykonávanie opatrení a plánov na riešenie rizík s cieľom zmierňovať kybernetické riziká. Napríklad ide o zavedenie komplexného **systému riadenia informačnej bezpečnosti** (ISMS) a **systému riadenia ochrany osobných údajov** (PIMS), ktoré sú zosúladené s inými systémami riadenia. Takéto systémy riadenia (t. j. ISMS a PIMS) zahŕňajú vykonávanie bezpečnostných kontrol (ako aj kontrol v oblasti ochrany údajov a súkromia) s cieľom zmierňovať vznikajúce hrozby, ktoré majú vplyv na služby a systémy pozemnej dopravy (vrátane ich údajov), a zabraňovať ich vzniku.*

- *Zohľadnenie všetkých obmedzení týkajúcich sa **správy aktív a plánovania zdrojov** (t. j. obmedzení, ktoré môžu mať vplyv na dodanie, údržbu a podporu kritických systémov pre prevádzku základných funkcií v pozemnej doprave).*

Príklady rámcov riadenia rizík: Východiskom a základom prístupu k riadeniu rizík prispôsobeného pre pozemnú dopravu môžu byť rozličné rámce (napr. normy v rámci skupiny ISO/IEC 27000, rámec kybernetickej bezpečnosti NIST, rámec MITRE ATT&CK, BSI IT-Grundschutz atď.). Organizácie, akou je ENISA, vymedzujú osvedčené postupy v oblasti kybernetickej bezpečnosti inteligentných vozidiel a inteligentnej verejnej dopravy, ktoré sú východiskom pre priemyselných výrobcov a združenia (napr. Európske združenie výrobcov automobilov – ACEA). Železničná agentúra Európskej únie (ERA) vymedzuje v rámci železničnej dopravy technické špecifikácie interoperability (TSI), ktoré musí dodržiavať každý subsystém alebo jeho časť s cieľom spĺňať základné požiadavky a zabezpečiť interoperabilitu železničného systému Európskej únie. Spoločný podnik Shift2Rail takisto podporuje inovačné iniciatívy a projekty (a to aj v oblasti kybernetickej bezpečnosti) v oblasti železničnej dopravy.

Ochrana pred kybernetickými hrozbami

Organizácie v oblasti pozemnej dopravy by mali vykonávať vhodné a primerané bezpečnostné opatrenia na ochranu svojich sietí a informačných systémov, a to vrátane informačných technológií (IT) a prevádzkových technológií (PT), pred kybernetickými útokmi. Medzi bezpečnostné opatrenia patria:

- ***Bezpečnostné politiky a postupy:*** *vymedzenie, vykonávanie, oznamovanie a presadzovanie primeraných politík a postupov, v rámci ktorých sa vymedzuje celkový prístup k zabezpečeniu systémov a údajov, ktoré podporujú prevádzku základných funkcií v pozemnej doprave. Tieto bezpečnostné politiky (napr. politiky v oblasti hesiel a uchovávania) a postupy by sa mali zároveň vzťahovať na softvérové záplaty a riadenie zraniteľností hardvérových a softvérových systémov (vrátane IT a PT), riadenie incidentov, ako aj na ochranu siete a systému.*

- ***Riadenie identity a prístupu:*** *pochopenie, zdokumentovanie a riadenie prístupu k sieťam a informačným systémom (vrátane IT a PT), ktoré podporujú prevádzku základných funkcií v druhoch pozemnej dopravy. Používatelia (alebo automatizované funkcie), ktoré majú možnosť prístupu k údajom alebo systémom, sa primeraným spôsobom overujú, autentifikujú a autorizujú. Zároveň by sa v rámci toho mali zohľadniť rozdielne úlohy a zodpovednosti, pokiaľ ide o bežné a privilegované účty.*

- ***Zabezpečenie údajov a systému:*** *ochrana údajov (uchovávaných a elektronicky prenášaných), kritických sietí a informačných systémov (vrátane IT a PT) pred kybernetickými útokmi. Organizácie by so zreteľom na prístup založený na rizikách mali vykonávať bezpečnostné opatrenia na účinné obmedzenie príležitostí pre útočníkov na to, aby ohrozili údaje, siete a systémy. Medzi tieto bezpečnostné opatrenia by malo patriť aj zavedenie protokolov šifrovania a chránenej komunikácie s cieľom chrániť údaje v pokoji a prenášané údaje pred kybernetickými hrozbami, ktorých dôsledkom sú útoky technikou „man-in-the-middle“. Okrem toho je nevyhnutné na ochranu prístupu k systémom skombinovať takéto opatrenia s opatreniami v oblasti fyzickej bezpečnosti (napr. systémy by sa mali nachádzať vo vyhradenom priestore s obmedzeným prístupom). Mimoriadny význam to má v prípade tých systémov, ktoré môžu mať vplyv na bezpečnosť ľudského života.*

- ***Odolnosť sietí a systémov:*** *budovanie odolnosti sietí a systémov (vrátane IT a PT) ich koncipovaním a zavádzaním (ako aj ich prevádzkových postupov) tak, aby odolávali vplyvu kybernetických útokov a zmierňovali ho. Príkladmi koncepcie a vykonávania riešení na zvýšenie odolnosti sú: formálne overené kritické funkcie, redundancia systémov a sietí, oddelenie sietí (najmä oddelenie IT a PT), viacvrstvové bezpečnostné opatrenia a mnohé ďalšie. Treba poznamenať, že z hľadiska informačnej bezpečnosti môžu vhodné bezpečnostné riešenia poskytnúť bezpečnostné domény, ktoré zavádzajú oddelenie siete a systému. Prevádzkové potreby (napr. činnosti údržby, prenosy údajov atď.) systému si však môžu vyžadovať obchádzanie alebo pripájanie k odlišným bezpečnostným doménam (napr. oddelené systémy a siete) vrátane pripojenia k IT a PT.*

Európska komisia

Odhaľovanie kybernetických hrozieb

Organizácie by mali zabezpečiť, že bezpečnostné opatrenia zostanú účinné a odhalia všetky kybernetické incidenty, ktoré vplývajú alebo ktoré majú potenciál ovplyvniť bezpečnostné kontroly, ako aj základné služby a systémy. Relevantnými bezpečnostnými opatreniami na odhaľovanie kybernetických hrozieb sú:

- ***Monitorovanie bezpečnosti:*** *monitorovanie stavu bezpečnosti sietí a informačných systémov vrátane informačných technológií (IT) a prevádzkových technológií (PT), ktoré podporujú prevádzku základných funkcií v rámci druhov pozemnej dopravy. Je to nevyhnutné na odhaľovanie potenciálnych bezpečnostných hrozieb a sledovanie priebežnej účinnosti ochranných bezpečnostných opatrení. Medzi údaje, ktoré sa zohľadňujú na podporu monitorovania bezpečnosti, patria napríklad:*

  - *záznamy o bezpečnosti*
  - *záznamy o detekcii vírusov*
  - *záznamy o detekcii narušenia*
  - *záznamy o identifikácii, autentifikácii a autorizácii*
  - *systémové záznamy a servisné záznamy*
  - *záznamy o sieťovej prevádzke*
  - *záznamy o spracovaní údajov*

- ***Objavovanie bezpečnostných incidentov:*** *odhaľovanie škodlivých činností (t. j. bezpečnostných incidentov), ktoré majú vplyv alebo ktoré majú potenciál vplývať na bezpečnosť sietí a informačných systémov (vrátane IT a PT) podporujúcich prevádzku základných funkcií.*

Tieto opatrenia si môžu vyžadovať zavedenie konkrétnych technológií (napr. riadenie informačnej bezpečnosti a bezpečnostných incidentov, systém detekcie prienikov, systém prevencie prienikov atď.) a vytvorenie centra bezpečnostných operácií alebo jeho ekvivalentu. Znamená to vytvorenie prostriedkov na lokálne odhaľovanie kybernetických útokov, ich analýzu, reakciu na ne a ich prekonanie.
Spravodajské informácie o kybernetických hrozbách, na ktorých je založené monitorovanie bezpečnosti a odhaľovanie, môžu poskytnúť národné jednotky pre riešenie počítačových bezpečnostných incidentov (CSIRT), sektorové a komerčné tímy CERT alebo prevádzkovatelia v oblasti cestnej a železničnej dopravy a Stredisko pre výmenu a analýzu informácií v oblasti európskej železničnej dopravy (ER-ISAC).

Plánovanie reakcie a obnovy

Organizácia by mala vymedziť, vykonať a otestovať postupy riadenia incidentov, ktorých cieľom je zabezpečiť kontinuitu činností služieb a systémov v prípade kybernetických incidentov.

V rámci plánovania reakcie a obnovy by sa mali zohľadniť bezpečnostné opatrenia, ktoré zmierňujú vplyv konkrétnych kybernetických napadnutí, ako sú:

- *koordinácia a spolupráca s národnými jednotkami CSIRT, (verejnými a komerčnými) tímami CERT a strediskami ISAC počas kybernetických incidentov, koordinácia incidentov a kríz na celoeurópskej úrovni.*

- *Výmena informácií s inými organizáciami vrátane poskytovateľov v dodávateľskom reťazci služieb pozemnej dopravy.*

- *Vykonávanie pravidelných **kybernetickobezpečnostných cvičení** (simulačná koordinácia, ako aj technické cvičenia) na posúdenie bezpečnostných opatrení a postupov, ako aj odolnosti organizácií čeliť kybernetickým incidentom.*

- *Prístup k archivovaným alebo záložným úložiskám v prípade narušenej integrity a dostupnosti dátových úložísk.*

- ***Bezpečnostné operačné protokoly**, ktoré obsahujú podrobné postupy na riadenie kybernetických incidentov a návrat služieb a systémov do bežných prevádzkových podmienok.*

- *Presmerovania sieťovej prevádzky na redundantné služby počas útokov typu „vyradenie služby“.*

- *Manuálne postupy pre režimy prevádzky služieb a systémov za mimoriadnych okolností.*

- *Vymedzenie postupov s cieľom riešiť porušenia ochrany údajov vrátane postupov na riešenie porušení ochrany údajov, ktoré majú vplyv na osobné údaje v súlade so všeobecným nariadením o ochrane údajov a akýmkoľvek iným príslušným sektorovým nariadením alebo smernicou.*

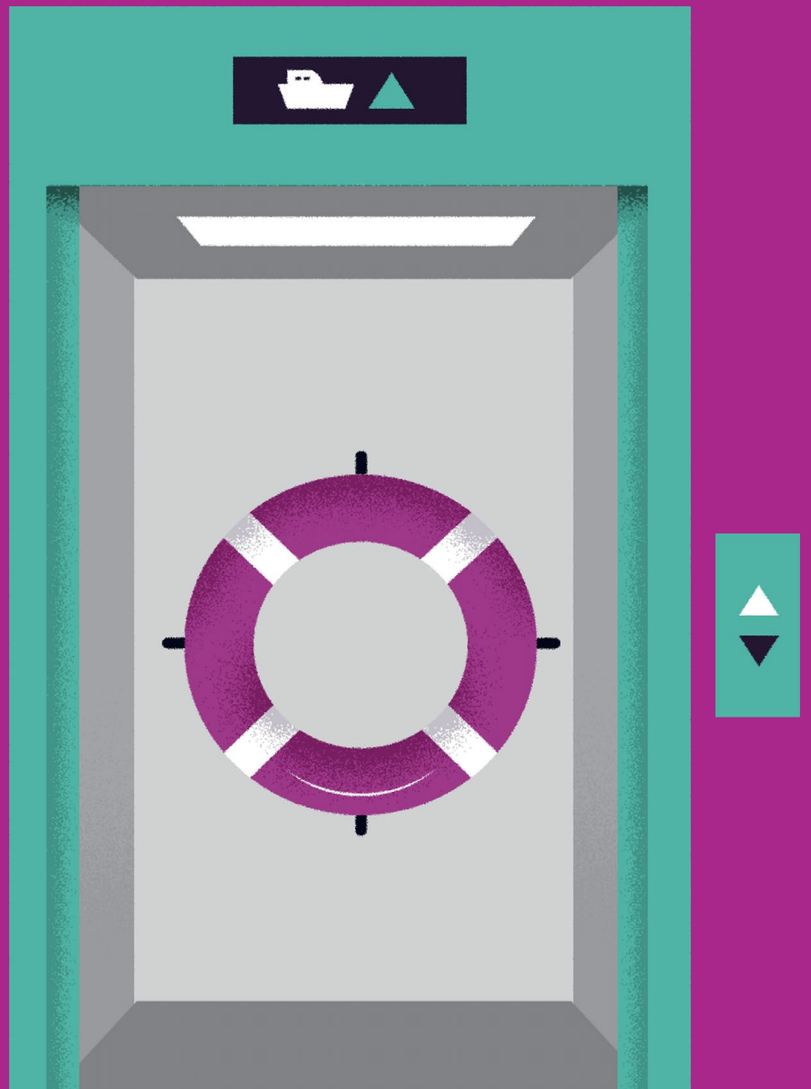
- *Zaobstarať si **kybernetické poistenie** s cieľom čiastočne vykompenzovať riziko späté so závažnými kybernetickými incidentmi.*

- *Na zvýšenie kapacity a odbornosti uzavrieť zmluvu o honorári za reakciu na incident s jednou alebo viacerými špecializovanými firmami.*

- *Vymedziť postupy výmeny informácií o kybernetických incidentoch s relevantnými zainteresovanými stranami, a to vrátane postupov na nahlasovanie incidentov v súlade so smernicou NIS (smernica EÚ 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii).*

Európska komisia

Osvedčené postupy a bezpečnostné opatrenia prispôsobené námornej doprave



Európska komisia

Riadenie

Organizácie námornej dopravy potrebujú jasne pochopiť nové hrozby s cieľom vymedziť politiky a procesy riadenia na riadenie svojich prístupov s cieľom zvýšiť kybernetickú bezpečnosť služieb a systémov v prevádzkových činnostiach, a to vrátane informačných technológií (IT) a prevádzkových technológií (PT).

Medzi osvedčené postupy organizácií, bez ohľadu na ich veľkosť, patria:

- *Zabezpečenie, že úrovne vyššieho manažmentu nahlasujú obavy v oblasti kybernetickej bezpečnosti riadiacim pracovníkom a predstavenstvu, ktorí môžu prijať informované rozhodnutia o pridelení zdrojov.*

- *Stanovenie riadiacej pozície, ktorá je zodpovedná za celkové riadenie, pokiaľ ide o bezpečnosť informačných technológií (IT) a prevádzkových technológií (PT). Táto pozícia by mala byť zodpovedná tak za kybernetickú bezpečnosť, ako aj za fyzickú bezpečnosť.*

- *Jasné vymedzenie úloh, zodpovedností, právomocí a oprávnení týkajúcich sa kybernetickej bezpečnosti, vymedzenie úrovní právomocí a komunikačných spojení medzi pobrežným personálom a personálom lode a navzájom medzi sebou, a dohoda o nich s dotknutými zamestnancami. Potrebné je to, najmä pokiaľ ide o členov tímov reakcie na núdzové počítačové situácie (CERT). Pracovníci s úlohami týkajúcimi sa právnych predpisov EÚ v oblasti námornej bezpečnosti a ochrany, ako sú bezpečnostní dôstojníci prístavných zariadení, bezpečnostní dôstojníci prístavov, bezpečnostní dôstojníci obchodných spoločností, určená osoba na súši (DPA) alebo kapitán na palube, by mali byť oboznámení aspoň s opatreniami v oblasti kybernetickej bezpečnosti, ktoré prijala organizácia.*

- *Zabezpečenie riadenia kybernetickej bezpečnosti v celom dodávateľskom reťazci bezpečnostných služieb, a to vrátane fyzických aj digitálnych rozhraní, od výrobcov technológií a montážnych technikov po poskytovateľov bezpečnostných služieb.*

- *Dohoda o činnostiach a kontrolách vrátane spoločných zodpovedností na riadenie rizík v oblasti kybernetickej bezpečnosti a zabezpečenie, že tieto zodpovednosti sú udržiavané počas celého životného cyklu (napr. dohodami o službách) bezpečnostných riešení a služieb.*

- *Vymedzenie mechanizmov riadenia (napr. politiky) s cieľom dodržiavať povinnosti vyplývajúce z príslušných nariadení a smerníc, akými sú nariadenie 2019/1239, ktorým sa zriaďuje európske prostredie jednotnej námornej platformy (EMSWe), nariadenie 725/2004 o zvýšení bezpečnosti lodí a prístavných zariadení, smernica 2005/65/ES o zvýšení bezpečnosti prístavov a nariadenie (ES) č. 336/2006 o vykonávaní Medzinárodného kódexu pre bezpečnostný manažment, ako aj rezolúcia A.741(18), ktorou sa prijíma medzinárodný kódex pre bezpečnostný manažment lodí a ochranu pred znečistením. V tejto súvislosti za zmienku tiež stojí iniciatíva EÚ Spoločné prostredie na zdieľanie informácií (CISE), ktorej cieľom je urobiť európske systémy dozoru a systémy dozoru členských štátov interoperabilnými tak, aby sa všetkým príslušným orgánom poskytol prístup k utajovaným a neutajovaným informáciám, ktoré potrebujú na vykonávanie misií na mori.*

Príklady služieb a systémov v námornej doprave:
Príkladmi informačných technológií sú tie, ktoré sú prístupné tak zamestnancom (napr. osobné počítače, mobilné telefóny, periférne kancelárske zariadenia atď.), ako aj cestujúcim (napr. verejné routre a pripojenia Wi-Fi atď.). Príkladmi prevádzkových technológií sú systémy kontrolného riadenia a zberu údajov (SCADA), systémy vykurovania, vetrania a klimatizácie (HVAC), globálne polohové systémy (GPS), kontrola vstupu, monitorovanie, dohľad, systémy spustenia alarmu, technológie na detekčnú kontrolu, palubné navigačné systémy, systém SafeSeaNet, mostíkové systémy, systémy na riadenie nákladu a na manipuláciu s ním, systémy riadenia hnacích a strojných zariadení a systémy ovládania výkonu, systémy kontroly prístupu, systémy riadenia a obsluhy cestujúcich, verejné siete určené pre cestujúcich, administratívne systémy a systémy určené na zabezpečenie dobrých životných podmienok posádky, komunikačné systémy a iné.

Identifikácia kybernetických hrozieb

Riadenie rizík: Organizácie námornej dopravy musia prijať primerané kroky na identifikáciu, analýzu, posúdenie a oznamovanie kybernetických rizík, ako aj na ich prijímanie, zabraňovanie im, ich prevádzanie alebo zmierňovanie na prijateľnú úroveň. Vyžaduje si to celkový organizačný prístup k riadeniu rizík, ktorého súčasťou sú:

- *Zabezpečenie jasného prehľadu o rozličných hardvérových a softvérových systémoch zavedených na poskytovanie rôznych služieb. Takéto systémy v súvislosti s námornou dopravou zahŕňajú informačné technológie (IT) a prevádzkové technológie (PT), ako aj spôsob ich prepojenia a integrácie s pobrežím, a to vrátane verejných orgánov, námorných terminálov a dokárskych spoločností.*

- *Identifikácia a hodnotenie kľúčových operácií na palube lode, ktoré sú citlivé na kybernetické útoky, ako aj vykonávanie posúdení kybernetických rizík (vrátane posúdenia možných prevádzkových vplyvov a pravdepodobnosti výskytu), v ktorých by sa mali zohľadniť nové hrozby, známe zraniteľnosti a prevádzkové údaje vo vzťahu k dotknutým systémom. V relevantných prípadoch vytvorenie prepojenia na posúdenia bezpečnosti vykonávané pre lode, prístavné zariadenia a prístavy, ako sa stanovuje v právnych predpisoch EÚ o námornej bezpečnosti. Uvedené posúdenia identifikujú možné bezpečnostné hrozby namierené voči infraštruktúre prístavu a bezpečnostné nedostatky. Organizácie v oblasti námornej dopravy, ako sú Medzinárodná námorná organizácia (IMO) a námorné strediská ISAC, môžu okrem toho poskytnúť poznatky o hrozbách namierených proti námornej doprave.*

- *Zabezpečenie, aby sa posúdenia rizík vzťahovali aj na riziká týkajúce sa každodennej činnosti zamestnancov (napr. používanie sociálnych médií, používanie osobných zariadení, spracúvanie osobných údajov, výmena informácií atď.).*

- *Určovanie a vykonávanie opatrení a plánov na riešenie rizík s cieľom zmierňovať kybernetické riziká. Napríklad, zavedenie komplexného systému riadenia informačnej bezpečnosti (ISMS) a systému riadenia ochrany osobných údajov (PIMS), ktoré sú zosúladené s inými systémami riadenia, ako sú systémy manažmentu bezpečnosti (SMS) v súlade s Medzinárodným kódexom pre bezpečnostný manažment. Takéto systémy riadenia (t. j. ISMS a PIMS) zahŕňajú vykonávanie bezpečnostných kontrol (ako aj kontrol v oblasti ochrany údajov a súkromia) s cieľom zmierňovať nové hrozby, ktoré majú vplyv na služby a systémy námornej dopravy (vrátane ich údajov), a zabraňovať ich vzniku.*

- *Zohľadnenie všetkých obmedzení týkajúcich sa **správy aktív a plánovania zdrojov** (t. j. obmedzení, ktoré môžu mať vplyv na dodanie, údržbu a podporu kritických systémov pre prevádzku základných funkcií v námornej doprave). Pokiaľ ide o posúdenia, v relevantných prípadoch vytvorenie krížového odkazu na požiadavky Medzinárodného kódexu pre bezpečnostný manažment, systémy manažmentu bezpečnosti (SMS) a bezpečnostné plány vykonávané podľa právnych predpisov EÚ o námornej ochrane a bezpečnosti.*

Príklady rámcov riadenia rizík: Východiskom a základom prístupu k riadeniu rizík prispôsobeného pre námornú dopravu môžu byť rozličné rámce (napr. Medzinárodný kódex pre bezpečnostný manažment alebo normy v rámci skupiny ISO/IEC 27000, rámec kybernetickej bezpečnosti NIST, rámec MITRE ATT&CK, BSI IT-Grundschutz atď.). Rámec kybernetickej bezpečnosti NIST bol takisto prispôsobený tak, aby sa vzťahoval na kybernetickú bezpečnosť námornej prepravy tekutého voľne loženého nákladu, prevádzky mimo pobrežia a prevádzky osobných lodí. Baltská a medzinárodná námorná rada (BIMCO) rovnako vydala *„Usmernenia o kybernetickej bezpečnosti na palube lodí“* a Medzinárodná námorná organizácia (IMO) vydala konkrétne *„Usmernenia o riadení námorných kybernetických rizík“* (MSC-FAL.1/Circ.3). Agentúra ENISA vykonala viacero štúdií v súvislosti s osvedčenými postupmi v oblasti námornej kybernetickej bezpečnosti, a najmä kybernetickej bezpečnosti prístavov. Agentúra EMSA poskytuje služby námornému spoločenstvu vrátane odbornej prípravy v oblasti povedomia o kybernetickej bezpečnosti. V normách (napr. IEC 61162-460:2018 o ochrane a bezpečnosti námorného navigačného a rádiokomunikačného zariadenia a systémov, ISO 16425:2013 o lodiach a námorných technológiách, IEC 62443-4-1:2018 o bezpečnosti systémov kontroly a priemyselnej automatizácie atď.) sa zároveň vymedzujú konkrétne požiadavky na bezpečnosť a ochranu, pokiaľ ide o systémy a siete v oblasti námornej dopravy.

Ochrana pred kybernetickými hrozbami

Organizácie v oblasti námornej dopravy by mali vykonávať vhodné a primerané bezpečnostné opatrenia na ochranu svojich sietí a informačných systémov, a to vrátane informačných technológií (IT). Medzi opatrenia na bezpečnosť prevádzky patria:

- ***Bezpečnostné politiky a postupy:*** *vymedzenie, vykonávanie, oznamovanie a presadzovanie primeraných politík a postupov, v rámci ktorých sa vymedzuje celkový prístup k zabezpečeniu systémov a údajov, ktoré podporujú prevádzku základných funkcií v námornej doprave. Bezpečnostné opatrenia (vrátane opatrení v oblasti kybernetickej a fyzickej bezpečnosti) by mali byť súčasťou príslušných plánov, ako je systém manažmentu bezpečnosti, ako aj v bezpečnostnom pláne lode. Tieto bezpečnostné politiky (napr. politiky v oblasti hesiel a uchovávania) a postupy by sa mali zároveň vzťahovať na softvérové záplaty a riadenie zraniteľností hardvérových a softvérových systémov (vrátane IT a PT), riadenie incidentov, ako aj na ochranu siete a systému.*

- ***Riadenie identity a prístupu:*** *pochopenie, zdokumentovanie a riadenie prístupu k sieťam a informačným systémom (vrátane IT a PT), ktoré podporujú prevádzku základných funkcií v námornej doprave. Používatelia (alebo automatizované funkcie), ktoré majú možnosť prístupu k údajom alebo systémom, sa primeraným spôsobom overujú, autentifikujú a autorizujú. Zároveň by sa v rámci toho mali zohľadniť rozdielne úlohy a zodpovednosti, pokiaľ ide o bežné a privilegované účty.*

- ***Zabezpečenie údajov a systému:*** *ochrana údajov (uchovávaných a elektronicky prenášaných), kritických sietí a informačných systémov (vrátane IT a PT) pred kybernetickými útokmi. Organizácie by so zreteľom na prístup založený na rizikách mali vykonávať bezpečnostné opatrenia na účinné obmedzenie príležitostí pre útočníkov na to, aby ohrozili údaje, siete a systémy. Medzi tieto bezpečnostné opatrenia by malo patriť aj zavedenie protokolov šifrovania a chránenej komunikácie s cieľom chrániť údaje v pokoji a prenášané údaje pred kybernetickými hrozbami, ktorých dôsledkom sú útoky technikou „man-in-the-middle“. Okrem toho je nevyhnutné na ochranu prístupu k systémom skombinovať takéto opatrenia s opatreniami v oblasti fyzickej bezpečnosti (napr. systémy by sa mali nachádzať vo vyhradenom priestore s obmedzeným prístupom). Mimoriadny význam to má v prípade tých systémov, ktoré môžu mať vplyv na bezpečnosť ľudského života (napr. navigačné a rádiové komunikačné systémy kategórie II a III).*

- ***Odolnosť sietí a systémov:*** *budovanie odolnosti sietí a systémov (vrátane IT a PT) ich koncipovaním a zavádzaním (ako aj ich prevádzkových postupov) tak, aby odolávali vplyvu kybernetických útokov a zmierňovali ho. Príkladmi koncepcie a vykonávania riešení na zvýšenie odolnosti sú: formálne overené kritické funkcie, redundancia systémov a sietí, oddelenie sietí (najmä oddelenie IT a PT), viacvrstvové bezpečnostné opatrenia a mnohé ďalšie. Treba poznamenať, že z hľadiska informačnej bezpečnosti môžu vhodné bezpečnostné riešenia poskytnúť bezpečnostné domény, ktoré zavádzajú oddelenie siete a systému. Potreby (napr. činnosti údržby, prenosy údajov atď.) systémov (napr. námorné samoriadiace hladinové lode – MASS) si však môžu vyžadovať obchádzanie alebo pripájanie k odlišným bezpečnostným doménam (napr. oddelené systémy a siete) vrátane pripojenia k IT a PT.*

Odhaľovanie kybernetických hrozieb

Organizácie by mali zabezpečiť, že bezpečnostné opatrenia zostanú účinné a odhalia všetky kybernetické incidenty, ktoré vplývajú alebo ktoré majú potenciál ovplyvniť bezpečnostné kontroly, ako aj základné služby a systémy. Relevantnými bezpečnostnými opatreniami na odhaľovanie kybernetických hrozieb sú:

- ***Monitorovanie bezpečnosti:*** *monitorovanie stavu bezpečnosti sietí a informačných systémov vrátane informačných technológií (IT) a prevádzkových technológií (PT), ktoré podporujú prevádzku základných funkcií v rámci služieb námornej dopravy. Je to nevyhnutné na odhaľovanie potenciálnych bezpečnostných hrozieb a sledovanie priebežnej účinnosti ochranných bezpečnostných opatrení. Medzi údaje, ktoré sa zohľadňujú na podporu monitorovania bezpečnosti, patria napríklad:*

  - *záznamy o bezpečnosti*
  - *záznamy o detekcii vírusov*
  - *záznamy o detekcii narušenia*
  - *záznamy o identifikácii, autentifikácii a autorizácii*
  - *systémové záznamy a servisné záznamy*
  - *záznamy o sieťovej prevádzke*
  - *záznamy o spracovaní údajov*

- ***Objavovanie bezpečnostných incidentov:*** *odhaľovanie škodlivých činností (t. j. bezpečnostných incidentov), ktoré majú vplyv alebo ktoré majú potenciál vplývať na bezpečnosť sietí a informačných systémov (vrátane IT a PT) podporujúcich prevádzku základných funkcií v rámci služieb námornej dopravy.*

Tieto opatrenia si môžu vyžadovať zavedenie konkrétnych technológií (napr. riadenie informačnej bezpečnosti a bezpečnostných incidentov, systém detekcie prienikov, systém prevencie prienikov atď.) a vytvorenie centra bezpečnostných operácií alebo jeho ekvivalentu. Znamená to vytvorenie prostriedkov na lokálne odhaľovanie kybernetických napadnutí, ich analýzu, reakciu na ne a ich prekonanie.

Spravodajské informácie o kybernetických hrozbách, na ktorých je založené monitorovanie bezpečnosti a odhaľovanie, môžu poskytnúť národné jednotky pre riešenie počítačových bezpečnostných incidentov (CSIRT), sektorové tímy CERT prevádzkovateľov námornej dopravy a námorné strediská ISAC.

Európska komisia

Plánovanie reakcie a obnovy

Organizácia by mala vymedziť, vykonať a otestovať postupy riadenia incidentov, ktorých cieľom je zabezpečiť kontinuitu činností služieb a systémov v prípade kybernetických incidentov.
V rámci plánovania reakcie a obnovy by sa mali zohľadniť bezpečnostné opatrenia, ktoré zmierňujú vplyv konkrétnych kybernetických napadnutí, ako sú:

- *Presmerovania sieťovej prevádzky na redundantné služby počas útokov typu „vyradenie služby“.*

- *Manuálne postupy pre režimy prevádzky služieb a systémov za mimoriadnych okolností.*

- *Vytvorenie programov nácvikov a cvičení (simulačná koordinácia, technické cvičenia a nácviky reakcie) na reakciu na kybernetické napadnutia a núdzové situácie, ako aj na posúdenie bezpečnostných opatrení, postupov a odolnosti organizácií čeliť kybernetickým incidentom.*

- *Prístup k archivovaným alebo záložným úložiskám v prípade narušenej integrity a dostupnosti dátových úložísk.*

- *koordinácia a spolupráca s národnými jednotkami CSIRT, (verejnými a komerčnými) tímami CERT a strediskami ISAC počas kybernetických incidentov, koordinácia incidentov a kríz na celoeurópskej úrovni.*

- *Výmena informácií s inými organizáciami vrátane poskytovateľov v dodávateľskom reťazci služieb námornej dopravy.*

- *Bezpečnostné operačné protokoly, ktoré obsahujú podrobné postupy na riadenie kybernetických incidentov a návrat služieb a systémov do bežných prevádzkových podmienok.*

- *Vymedzenie postupov s cieľom riešiť porušenia ochrany údajov vrátane postupov na riešenie porušení ochrany údajov, ktoré majú vplyv na osobné údaje v súlade so všeobecným nariadením o ochrane údajov a akýmkoľvek iným príslušným sektorovým nariadením alebo smernicou.*

- *Zaobstarať si kybernetické poistenie s cieľom čiastočne vykompenzovať riziko späté so závažnými kybernetickými incidentmi.*

- *Na zvýšenie kapacity a odbornosti uzavrieť zmluvu o honorári za reakciu na incident s jednou alebo viacerými špecializovanými firmami.*

- *Vymedziť postupy výmeny informácií o kybernetických incidentoch (vrátane nezrovnalostí, nehôd a nebezpečných situácií) s relevantnými zainteresovanými stranami, a to vrátane postupov na nahlasovanie incidentov v súlade so smernicou NIS (smernica EÚ 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii).*

Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2021

Print ISBN 978-92-76-40484-2 doi:10.2832/60114 MI-05-21-230-SK-C
PDF ISBN 978-92-76-40505-4 doi:10.2832/155627 MI-05-21-230-SK-N

Úrad pre vydávanie publikácií
Európskej únie