Komisja Europejska

Zestaw narzędzi służących zapewnieniu cyberbezpieczeństwa w transporcie

Wprowadzenie

Dyrekcja Generalna ds. Mobilności i Transportu Komisji Europejskiej (DG MOVE) zleciła opracowanie niniejszego zestawu narzędzi w celu podniesienia świadomości i poprawy gotowości zainteresowanych stron z sektora transportu w zakresie zagrożeń dla cyberbezpieczeństwa. Zestaw ten zawiera informacje umożliwiające zrozumienie zagrożeń dla cyberbezpieczeństwa i łagodzenie ich wpływu. Niniejszy zestaw narzędzi obejmuje dwie ścieżki podnoszenia świadomości odpowiadające różnym profilom:

- wszystkich pracowników sektora transportu (ogólne informacje i wytyczne);
- decydenci w zakresie cyberbezpieczeństwa w sektorze transportu.

Poszczególne części składające się na zestaw narzędzi połączone są hiperłączami w celu zapewnienia możliwości nawigowania.

Praktyki wymienione w niniejszym zestawie narzędzi mają charakter wyłącznie doradczy. Żadne ze sformułowanych zaleceń nie jest wiążące ani obowiązkowe. Ponadto w niniejszym zestawie narzędzi nie przedstawiono oficjalnego stanowiska Komisji Europejskiej i nie ma on na celu wprowadzenia środków zapewnienia zgodności z obowiązującymi lub przyszłymi przepisami UE.

Profile świadomości w zakresie cyberbezpieczeństwa

Profil I: wszyscy pracownicy sektora transportu. Pierwsza ścieżka dotyczy wszystkich pracowników organizacji transportowych. W ramach tej ścieżki przedstawiono informacje umożliwiające zrozumienie najbardziej powszechnych zagrożeń dla cyberbezpieczeństwa dotyczących transportu. Ponadto zawarto tu informacje na temat sposobów radzenia sobie z potencjalnymi zagrożeniami dla cyberbezpieczeństwa, w tym ich identyfikacji, sprawozdawczości w ich zakresie i ich łagodzenia dzięki stosowaniu dobrych praktyk w zakresie cyberbezpieczeństwa.

Profil II: decydenci w zakresie cyberbezpieczeństwa w sektorze transportu. Druga ścieżka dotyczy pracowników odpowiedzialnych za podejmowanie decyzji w zakresie cyberbezpieczeństwa w organizacjach transportowych. W ramach tej ścieżki przedstawiono dobre praktyki dostosowane do poszczególnych rodzajów transportu. W szczególności uwzględniono w niej dobre praktyki dotyczące identyfikacji i wykrywania pojawiających się zagrożeń dla cyberbezpieczeństwa organizacji transportowych, ochrony przed tymi zagrożeniami i reagowania na nie.

Komisja Europejska

Zestaw narzędzi służących zapewnieniu cyberbezpieczeństwa w transporcie

Krajobraz zagrożeń w sektorze transportu

Pojawiające się zagrożenia dla cyberbezpieczeństwa mające wpływ na różne rodzaje transportu

Profile świadomości w zakresie cyberbezpieczeństwa

Alternatywne ścieżki podnoszenia świadomości osób zatrudnionych w sektorze transportu, charakteryzujących się różnymi profilami

Komisja Europejska

Krajobraz zagrożeń w sektorze transportu

Krajobraz zagrożeń dla cyberbezpieczeństwa jest dynamiczny i stale się zmienia. Można jednak zidentyfikować zagrożenia dla cyberbezpieczeństwa, z którymi mierzą się wszystkie rodzaje transportu.

Komisja Europejska

Agresorzy

Osoby lub organizacje, które mogą potencjalnie wpływać na bezpieczeństwo i ochronę usług oraz systemów transportu

Pojawiające się zagrożenia dla cyber-bezpieczeństwa

Wybrane zagrożenia dla cyberbezpieczeństwa, które mogą wpływać na bezpieczeństwo i ochronę usług oraz systemów transportu

Komisja Europejska

Agresorzy

Osoby lub organizacje mogą umyślnie lub nieumyślnie ujawniać lub wykorzystywać podatności, co może prowadzić do incydentów i wpływać negatywnie na usługi transportu, w tym ich bezpieczeństwo, ochronę, działalność w ich zakresie, kwestie finansowe i ich reputację.

Do najważniejszych podmiotów działających w złych zamiarach, które celowo działają na szkodę organizacji transportowych, należą **cyberprzestępcy**, **osoby mające dostęp do informacji wewnętrznych**, **państwa narodowe** oraz **grupy finansowane przez państwo**. Przeciwnicy tacy jak **cyberprzestępcy** prowadzą na masową skalę kampanie mające na celu atak i często konkurują o nagrody pieniężne.

Osoby mające dostęp do informacji wewnętrznych znają specyfikę organizacji, w których pracują, i często są świadome nieznacznych luk w zakresie ochrony. Takimi osobami mającymi dostęp do informacji wewnętrznych mogą być rozczarowani pracownicy, dostawcy i indywidualni wykonawcy.

W miarę jak geopolityczne napięcia przybierają na sile, **państwa narodowe** oraz **grupy finansowane przez państwo** dążą do osiągnięcia długoterminowych celów strategicznych. Często próbują się zaszyć w głębokich strukturach organizacji i gromadzić informacje szczególnie chronione. Gdy już uda im się osiągnąć stabilną pozycję w strukturach, sprawcy ataków finansowani przez państwo dążą do uzyskania takiego stanowiska, dzięki któremu będą mogli wyrządzić największą możliwą szkodę.

Innymi niezłośliwymi agresorami są **osoby mające dostęp do informacji wewnętrznych**, które mogą nieumyślnie lub przypadkowo podjąć czynności prowadzące do zdarzeń związanych z cyberbezpieczeństwem, a w najgorszym przypadku do cyberincydentów mających negatywny wpływ na bezpieczeństwo i ochronę usług transportu.

Komisja Europejska

Pojawiające się zagrożenia dla cyberbezpieczeństwa

Istnieje wiele zagrożeń dla cyberbezpieczeństwa transportu: **rozproszony atak typu „odmowa usługi”**, **atak typu „odmowa usługi”**, kradzież danych, rozpowszechnienie **złośliwego oprogramowania**, **phishing**, manipulacja oprogramowaniem komputerowym, **dostęp podmiotów nieuprawnionych**, szkodliwe ataki, sfałszowanie lub obejście procesu decyzyjnego podmiotu zapewniającego ochronę, maskarada (podszywanie się pod inną osobę), nadużycie uprawnień dostępu, **inżynieria społeczna**, atak typu defacement, podsłuch sieciowy, niewłaściwe wykorzystanie aktywów oraz manipulacja sprzętem.
Na podstawie kompleksowego badania literatury obejmującego ogólnodostępne dokumenty oraz wywiadów z ekspertami można wyodrębnić następujące najistotniejsze zagrożenia dla cyberbezpieczeństwa transportu: złośliwe oprogramowanie, (rozproszony) atak typu „odmowa usługi”, dostęp podmiotów nieuprawnionych i kradzież, a także manipulacja oprogramowaniem komputerowym.

Komisja Europejska

Zagrożenie nr 1: złośliwe oprogramowanie

Złośliwe oprogramowanie, które może mieć negatywny wpływ na osoby lub organizacje prowadzące działalność w różnych rodzajach transportu

Zagrożenie nr 2: (rozproszony) atak typu „odmowa usługi”

Ataki na cyberbezpieczeństwo uniemożliwiające osobom lub organizacjom uzyskanie dostępu do usług i zasobów

Zagrożenie nr 3: dostęp podmiotów nieuprawnionych i kradzież

Dostęp podmiotów nieuprawnionych, przywłaszczenie i wykorzystanie aktywów krytycznych

Zagrożenie nr 4: manipulacja oprogramowaniem komputerowym

Ataki na cyberbezpieczeństwo oprogramowania komputerowego mające na celu zmianę jego zachowania i przeprowadzenie konkretnych ataków

Komisja Europejska

Zagrożenie nr 1: złośliwe oprogramowanie

Złośliwe oprogramowanie oznacza takie oprogramowanie, które może obejmować różne rodzaje aplikacji stosowanych z oprogramowaniem komputerowym, takich jak wirusy, trojany, robaki, oprogramowania typu ransomware, kopalnie kryptowalut lub każde oprogramowanie, które może mieć negatywny wpływ na organizacje lub osoby korzystające z różnych rodzajów transportu.

Ograniczenie rozpowszechniania się złośliwego oprogramowania opracowanego, aby umyślnie wyrządzać szkodę komputerom, serwerom, klientom, sieciom lub wszystkim tym elementom lub podmiotom, stanowi jeden z priorytetów cyberbezpieczeństwa we wszystkich rodzajach transportu. Typowy wektor ataku może obejmować skierowany przeciw pracownikom phishing wiadomości e-mail. Inne wektory ataku mogą obejmować różne wyszukane strategie inżynierii społecznej, takie jak podłączenie pamięci USB do wolnego portu (np. służącego do ładowania telefonu komórkowego). Klikając w hiperłącza przesłane w podejrzanych wiadomościach e-mail lub otwierając załączone pliki, użytkownik może nieświadomie zainstalować złośliwe oprogramowanie.

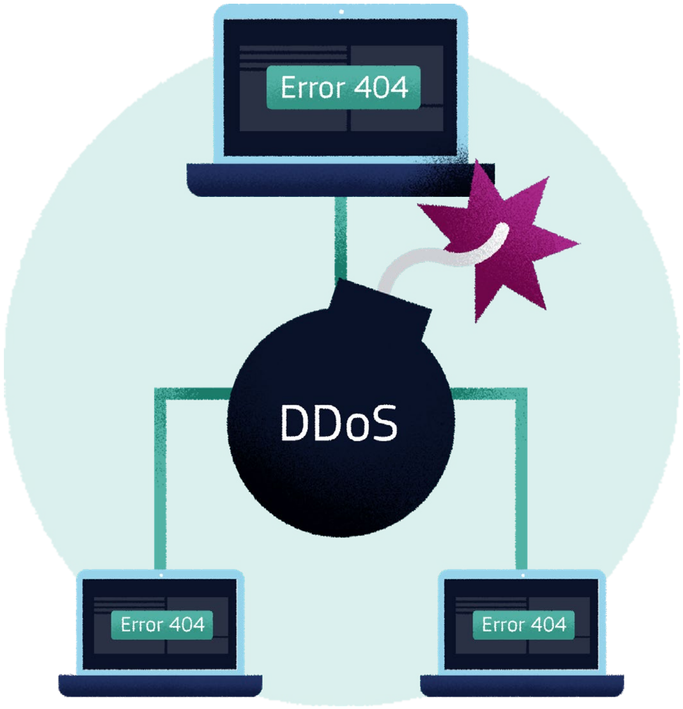
Na przykład cyberatak z użyciem oprogramowania typu ransomware WannaCry obejmował zasięgiem ponad 150 państw, a w jego wyniku zainfekowanych zostało ponad 230 000 systemów. Wykorzystano do niego oprogramowanie typu ransomware, które zazwyczaj rozprzestrzenia się za pośrednictwem phishingu wiadomości e-mail zawierających złośliwe załączniki lub hiperłącza. W tego typu ataku w złym zamiarze wykorzystuje się inżynierię społeczną, aby wprowadzić użytkowników systemu w błąd i doprowadzić do zainstalowania (lub aktywowania) przez nich konkretnego złośliwego oprogramowania.

Zagrożenie nr 2: (rozproszony) atak typu „odmowa usługi”

Rozproszony atak typu „odmowa usługi” (atak typu DDoS) oraz atak typu „odmowa usługi” (atak typu DoS) wpływają na dostępność danych, usług, systemów oraz innych zasobów. Tego rodzaju ataki mogą się różnić czasem trwania i mogą być jednocześnie skierowane przeciwko kilku usługom lub systemom. W atakach typu DDoS wykorzystuje się wiele systemów (lub kanałów ataku), aby przeciążyć żądaniami usługi lub systemy będące celem ataku. Udane ataki wpływają na zdolność usług i systemów do przetwarzania niespodziewanie wysokiej liczby żądań. Prowadzi to do odmowy dostępu do usług i zasobów.

Należy zauważyć, że zaatakowane usługi i systemy należące do organizacji transportowych mogą być wykorzystane do przeprowadzenia ataków typu DDoS i DoS skierowanych przeciwko konkretnym systemom będącym w eksploatacji lub innym organizacjom.

Na przykład agresorzy mogą zaatakować instytucjonalne systemy informatyczne (takie jak komputery i urządzenia przenośne), aby uzyskać dostęp do technologii operacyjnych, które mogą być podłączone do internetu lub sieci dostępu w celu przesyłania danych operacyjnych. Powiązania między różnymi systemami i sieciami (takimi jak sieci korporacyjne, technologie operacyjne i dostęp do obsługi na odległość) mogą stanowić podatne elementy, które można wykorzystać do przeprowadzenia ataków typu DDoS lub DoS na kluczowe usługi i systemy transportu. Na przykład w atakach typu DDoS i DoS można wykorzystać popularne protokoły sieciowe i komunikacyjne, takie jak Web Services Dynamic Discovery (WS-Discovery), z których urządzenia IoT mogą korzystać w celu automatycznego wykrycia każdego węzła w lokalnej sieci komputerowej (LAN). Jeżeli urządzenia IoT zawierają podatne elementy, sprawcy ataków mogą je wykorzystać do wykrycia innych połączonych urządzeń i przeprowadzenia ataków typu DDoS lub DoS.



Komisja Europejska

Zagrożenie nr 3: dostęp podmiotów nieuprawnionych i kradzież

Agresorzy mogą dążyć do uzyskania nieuprawnionego logicznego lub fizycznego dostępu do sieci, systemu, aplikacji, danych lub innego zasobu w celu przeprowadzenia złośliwych działań, w tym dokonania kradzieży wrażliwych danych lub zasobów (w tym zasobów fizycznych).
Zagrożenie w postaci nieuprawnionego dostępu i kradzieży dotyczy aktywów poufnych i własnościowych (w tym tożsamości osób, danych dostępu do kont uprzywilejowanych, systemów i innych rodzajów informacji poufnych i zastrzeżonych). Zagrożenia te mogą się wiązać z wykorzystaniem podatności systemów, a także ujawnieniem danych wrażliwych, takich jak dane dostępu (np. login, hasło itp.) lub dane osobowe (np. adres e-mail, osobisty numer identyfikacyjny itp.), przez niczego nieświadome osoby.

W kontekście dostępu podmiotów nieuprawnionych kradzież tożsamości stanowi nielegalne wykorzystanie danych osobowych lub unikalnego identyfikatora w celu podszycia się pod osoby lub usługi i systemy, aby uzyskać dostęp do prywatnych lub własnościowych zasobów (np. zasobów finansowych i fizycznych). Takie zagrożenia dla cyberbezpieczeństwa mogą dotyczyć także aktywów fizycznych we wszystkich rodzajach transportu.

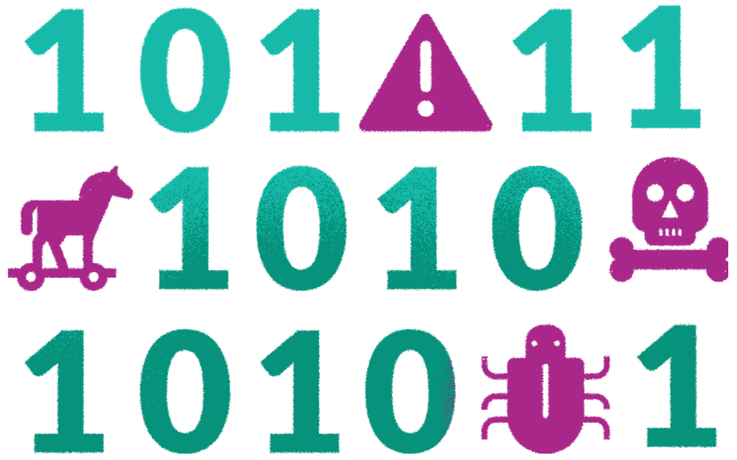
Komisja Europejska

Zagrożenie nr 4: manipulacja oprogramowaniem komputerowym

Nieprawidłowe konfiguracje oprogramowania i powiązanych systemów lub podzespołów i manipulacja nimi mogą w bezpośrednio wpływać na stan bezpieczeństwa usług i systemów transportu.

Ataki na cyberbezpieczeństwo obejmujące manipulacje oprogramowaniem polegają na zmianie ustawień oprogramowania lub osłabieniu integralności danych w celu zmiany zachowań systemów i usług. Sprawcy ataków mogą celowo manipulować oprogramowaniem (lub jego częścią) w celu uzyskania korzyści (np. uzyskanie nieuprawnionego dostępu, uniemożliwienie uprawnionym osobom lub systemom dostępu do niezbędnych zasobów, gromadzenie informacji szczególnie chronionych, zmiana zachowań funkcjonalnych itp.) w odniesieniu do aktywów wrażliwych.

Sprawcy ataków mogą na przykład wziąć na cel kanały komunikacyjne producentów w celu załadowania aktualizacji ze złośliwym oprogramowaniem do usług i systemów (w tym technologii operacyjnych). Agresor wykorzystuje dane uwierzytelniające, których bezpieczeństwo zostało naruszone, do uzyskania dostępu do zabezpieczonego interfejsu sieci zdalnej obsługi technicznej, aby zainstalować oprogramowanie poddane manipulacji i naruszyć bezpieczeństwo innych dostępnych usług i systemów. Agresor instaluje oprogramowanie poddane manipulacji, które w większym stopniu narusza bezpieczeństwo docelowych usług lub systemów lub atakuje inne podłączone usługi lub systemy.



Komisja Europejska

Profile świadomości w zakresie cyberbezpieczeństwa

Komisja Europejska

1

Profil I: wszyscy pracownicy sektora transportu

Pierwsza ścieżka dotyczy wszystkich pracowników organizacji transportowych, od pracowników operacyjnych po personel administracyjny. W ramach tej ścieżki przedstawiono wytyczne, których celem jest poprawa zrozumienia i podniesienie świadomości najbardziej powszechnych zagrożeń dla cyberbezpieczeństwa. Zawarto tu też informacje na temat sposobów radzenia sobie z potencjalnymi zagrożeniami dla cyberbezpieczeństwa, w tym ich identyfikacji, zgłaszania i łagodzenia ich skutków. Ścieżka ta jest wspólna dla wszystkich rodzajów transportu.

2

Profil II: decydenci w zakresie cyberbezpieczeństwa w sektorze transportu

Druga ścieżka dotyczy pracowników odpowiedzialnych za podejmowanie decyzji w zakresie bezpieczeństwa lub cyberbezpieczeństwa w organizacjach transportowych. Przedstawiono w jej ramach dobre praktyki dostosowane do poszczególnych rodzajów transportu. Uwzględniono w niej dobre praktyki dotyczące identyfikacji i wykrywania pojawiających się zagrożeń dla cyberbezpieczeństwa organizacji transportowych, ochrony przed tymi zagrożeniami i reagowania na nie.

Komisja Europejska

Profil I: wszyscy pracownicy sektora transportu

Ścieżka ta dotyczy wszystkich pracowników organizacji transportowych, od pracowników operacyjnych po personel administracyjny. W jej ramach przedstawiono wytyczne, których celem jest poprawa zrozumienia i podniesienie świadomości najbardziej powszechnych zagrożeń dla cyberbezpieczeństwa. Zawarto tu też informacje na temat sposobów radzenia sobie z potencjalnymi zagrożeniami dla cyberbezpieczeństwa, w tym ich identyfikacji, zgłaszania i łagodzenia ich skutków.
Część ta obejmuje zalecane praktyki i przydatne wskazówki adekwatne **do wszystkich rodzajów transportu**.

Komisja Europejska

Dobre praktyki dotyczące złośliwego oprogramowania

Możesz pomóc chronić swoją organizację dzięki stosowaniu dobrych praktyk w zakresie **identyfikacji złośliwego oprogramowania i uniemożliwiania jego działania**, takich jak:

- ***przestrzeganie polityki bezpieczeństwa**, na przykład w drodze skanowania nośników danych i plików pod kątem wirusów, unikania otwierania i wysyłania pocztą elektroniczną określonych rodzajów plików (np. plików wykonywalnych, takich jak .exe, .bat, .com itp.), instalowania wyłącznie autoryzowanego oprogramowania, dbania o aktualność i właściwe funkcjonowanie oprogramowania (w tym antywirusowego), a także innych polityk;*

- ***regularnie wykonywanie kopii zapasowych danych** na bezpiecznych (i autoryzowanych) urządzeniach pamięciowych lub w bezpiecznych (i autoryzowanych) usługach przechowywania danych, które to kopie powinny obsługiwać mechanizmy szyfrowania w celu ochrony nieużywanych danych i być dostępne na potrzeby procedur przywracania danych;*

- *ochrona, przy użyciu odpowiednich **środków bezpieczeństwa** (np. hasła, szyfrowania itp.), wszystkich systemów, w tym urządzeń mobilnych i końcowych, oraz zabezpieczone blokowanie (fizycznie i cyfrowo) wszystkich niewykorzystywanych w danym czasie systemów;*

- *unikanie otwierania załączników i klikania w hiperłącza zawarte w nieoczekiwanych wiadomościach e-mail i oknach podręcznych przeglądarki internetowej z nietypową treścią lub od nieznanych nadawców i z nieznanych domen internetowych;*

- *unikanie podłączania do komputera **niezaufanych lub nieznanych urządzeń przenośnych**, takich jak pamięć USB, dyski twarde i inne urządzenia pamięciowe;*

- *unikanie wyłączania środków bezpieczeństwa chroniących przed złośliwym oprogramowaniem (np. oprogramowania antywirusowego, oprogramowania filtrującego treści, zapory sieciowej itp.);*

- ***przeprowadzanie regularnych aktualizacji zainstalowanego oprogramowania** do najnowszych dostępnych wersji (które specjaliści ds. bezpieczeństwa informacji lub administratorzy systemów mogą udostępniać);*

- *unikanie korzystania z kont uprzywilejowanych i danych uwierzytelniających (np. na poziomie administratora) w odniesieniu do standardowych działań i operacji;*

- *zgłaszanie specjalistom ds. bezpieczeństwa informacji lub administratorom systemów wszelkich podejrzanych wiadomości e-mail lub nieoczekiwanych zachowań systemów.*

- *Należy poświęcić uwagę bezpieczeństwu informacji w codziennej pracy, aby identyfikować problemy związane z bezpieczeństwem informatycznym i odpowiednio na nie reagować.*

Komisja Europejska

Dobre praktyki dotyczące (rozproszonego) ataku typu „odmowa usługi”

Możesz pomóc chronić swoją organizację dzięki identyfikowaniu **rozproszonych ataków typu „odmowa usługi” (ataków typu DDoS)** oraz ataków **typu „odmowa usługi” (DoS).** W przypadku wykrycia lub stwierdzenia któregokolwiek z następujących wskaźników potencjalnie trwających ataków typu DDoS i DoS w usługach lub systemach organizacji należy niezwłocznie skontaktować się z zespołem ds. bezpieczeństwa i zespołem informatycznym:

- *rosnąca liczba żądań obciążających przepustowość sieci (przejawiająca się jako powolność usług i odpowiedzi) skutkująca awarią usługi lub systemu z powodu przeciążenia;*

- *rosnące zapotrzebowanie na korzystanie z zasobów pamięci bez oczywistego powodu;*

- ***nieoczekiwane zachowanie usług i systemów**, częste awarie i nietypowe komunikaty o błędach spowodowane złośliwym wykorzystaniem zasobów obliczeniowych lub połączeń sieciowych;*

- ***obniżona sprawność urządzeń**, długie wykonywanie trywialnych zadań i zauważalne oznaki sprzętowe (np. głośno działający wentylator przy jednoczesnej powolnej pracy urządzeń);*

- ***nieoczekiwane połączenia internetowe lub utrata połączeń** z usługami i systemami;*

- *subtelne zmiany działania dotyczące kontroli operacji lub technologii, powodujące fizyczne szkody.*

- *Odmowy dostępu do kont uprzywilejowanych lub administracyjnych w celu uniemożliwienia przywrócenia prawidłowego działania procedur reagowania na incydenty.*

Dobre praktyki dotyczące nieuprawnionego dostępu i kradzieży

Aby zapobiec atakom związanym z nieuprawnionym dostępem i kradzieżą, konieczne jest przestrzeganie zasad takich jak zasada ograniczonego dostępu i zasada domyślnego bezpieczeństwa i prywatności, w których podkreśla się, że aktywa wrażliwe i poufne (w tym dane osobowe i wrażliwe, systemy transportowe itp.) powinny być dostępne tylko dla osób, które mają prawo dostępu do nich ze względu na wykonywane przez siebie obowiązki. Możesz pomóc chronić swoją organizację dzięki stosowaniu dobrych praktyk w zakresie identyfikacji nieuprawnionego dostępu i zapobiegania mu, takich jak:

- *przestrzeganie organizacyjnej polityki bezpieczeństwa;*
- *unikanie udostępniania i publikowania danych uwierzytelniających i danych osobowych w internecie, w tym zdjęć, które mogą zawierać takie informacje;*
- *unikanie wykorzystywania lub przekazywania danych uwierzytelniających i danych osobowych (i innych danych wrażliwych) do niezaufanych i niezabezpieczonych sieci, urządzeń lub usług sieciowych (np. strony internetowe wykorzystujące inne niż bezpieczne protokoły lub adresy http:// zamiast bezpiecznych https://);*
- ***nieujawnianie w żadnym wypadku danych uwierzytelniających** (np. loginu i hasła), nawet za pośrednictwem poczty elektronicznej lub telefonu;*
- *zapewnienie ochrony danych wrażliwych wpisywanych na klawiaturze lub wyświetlanych na ekranie (w tym na urządzeniach mobilnych) przed osobami nieuprawnionymi, zainstalowanie ekranów prywatności i unikanie pracy z miejsc publicznych przy użyciu urządzeń prywatnych oraz unikanie pozostawiania jakichkolwiek urządzeń odblokowanych i bez nadzoru;*
- ***używanie złożonych haseł** (np. wystarczająco długie hasło zawierające znaki alfanumeryczne i specjalne) zgodne z odpowiednimi zasadami bezpieczeństwa organizacji, aby zapobiec nieuprawnionemu dostępowi;*
- ***zmiana haseł domyślnych** podłączonych systemów i urządzeń (np. drukarki, routery, kamery, inteligentne zamki itp.);*
- *unikanie stosowania tych samych danych uwierzytelniających (np. loginu i hasła) w odniesieniu do wielu usług i systemów oraz unikanie wykorzystywania tych samych danych uwierzytelniających w odniesieniu do usług i systemów wymagających kont uprzywilejowanych;*
- *wysyłanie haseł i kluczy do przekazywanych plików chronionych (np. archiwów ZIP) wyłącznie za pośrednictwem kanału poza pasmem (np. w krótkiej wiadomości tekstowej (SMS) przez telefon komórkowy w ramach systemu GSM lub w rozmowie telefonicznej), nie poczty elektronicznej;*
- ***aktywowanie**, w miarę możliwości, **uwierzytelniania dwuskładnikowego** lub wieloskładnikowego.*

Komisja Europejska

Dobre praktyki dotyczące manipulacji oprogramowaniem komputerowym

Możesz pomóc chronić swoją organizację dzięki stosowaniu dobrych praktyk w zakresie identyfikacji manipulowania oprogramowaniem komputerowym i zapobiegania mu, takich jak:

- *unikanie instalowania niewiarygodnego oprogramowania w systemach i na urządzeniach (w tym komputerach osobistych, serwerach, urządzeniach peryferyjnych, urządzeniach sieciowych, smartfonach itp.);*
- *instalowanie wyłącznie oprogramowania i aktualizacji z oficjalnych źródeł i stron internetowych (np. producentów, repozytoriów korporacyjnych itp.);*
- *unikanie pobierania oprogramowania i aplikacji (oraz wszelkich plików) z nielegalnych źródeł;*
- *odinstalowanie zbędnego lub dawno nieużywanego oprogramowania oraz wyłączenie niepotrzebnych połączeń (np. protokołów i usług sieciowych), w tym dostępu do usług zdalnych (np. usług przechowywania w chmurze);*
- *skanowanie wszelkiego oprogramowania lub urządzeń pamięciowych wiarygodnym i aktualnym oprogramowaniem antywirusowym;*
- *pobieranie bezpiecznego oprogramowania przemysłowego (np. aktualizacji, łatek, nowych produktów itp.) od zaufanych dostawców, z wykorzystaniem odpowiedniego systemu unieszkodliwiającego;*
- *aktualizowanie całego zainstalowanego oprogramowania zgodnie z polityką i praktykami organizacyjnymi.*

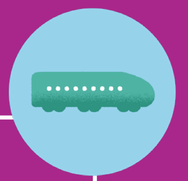
Komisja Europejska

Profil II: decydenci w zakresie cyberbezpieczeństwa w sektorze transportu

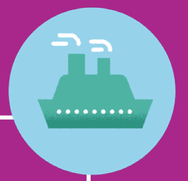
Ta część dotyczy pracowników odpowiedzialnych za podejmowanie decyzji w zakresie bezpieczeństwa lub cyberbezpieczeństwa w organizacjach transportowych. W ramach tej ścieżki przedstawiono dobre praktyki dostosowane do poszczególnych rodzajów transportu. W szczególności uwzględniono w niej dobre praktyki dotyczące identyfikacji i wykrywania pojawiających się zagrożeń dla cyberbezpieczeństwa, ochrony przed tymi zagrożeniami i reagowania na nie.

Komisja Europejska

Dobre praktyki w zakresie cyber-bezpieczeństwa dostosowane do transportu lotniczego



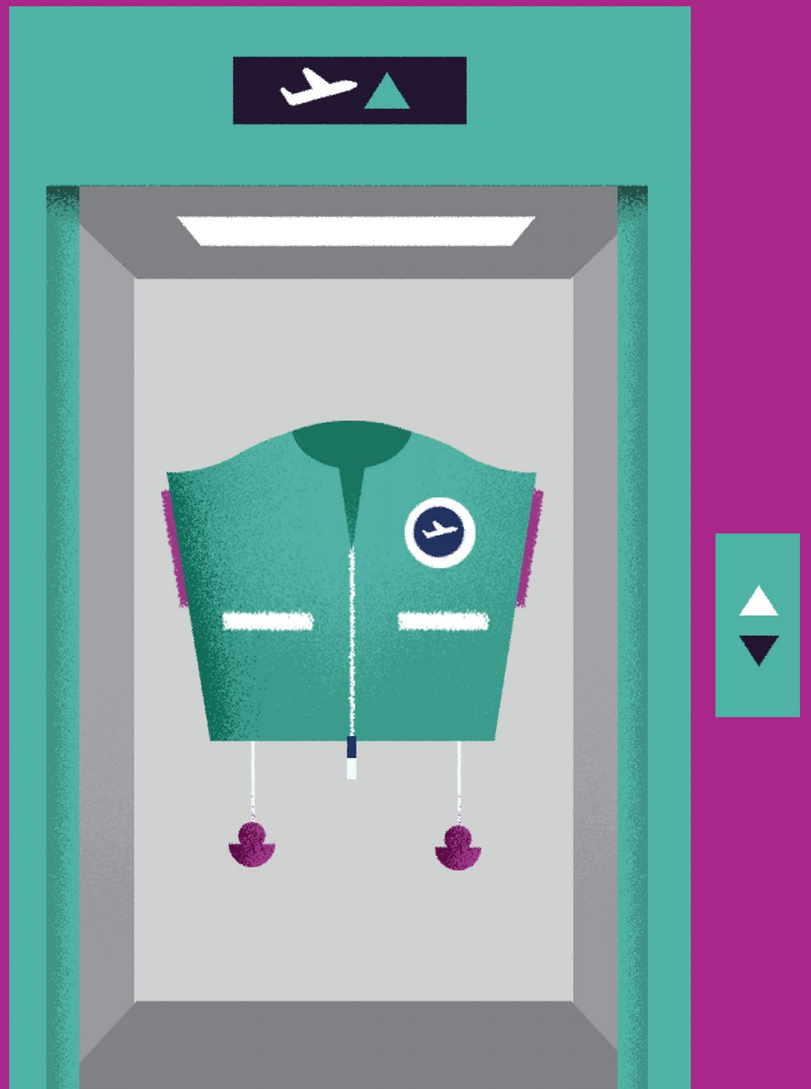
Dobre praktyki w zakresie cyber-bezpieczeństwa dostosowane do transportu lądowego



Dobre praktyki w zakresie cyber-bezpieczeństwa dostosowane do transportu morskiego

Komisja Europejska

Dobre praktyki i środki bezpieczeństwa dostosowane do transportu lotniczego



Zarządzanie

Organizacje w transporcie lotniczym potrzebują jasnego zrozumienia pojawiających się zagrożeń, aby określić politykę zarządzania i procesy służące uregulowaniu ich podejść w celu wzmocnienia cyberbezpieczeństwa usług i systemów w ramach operacji, w tym technologii informacyjnej (IT) i technologii operacyjnej (OT).

Dobre praktyki dla organizacji dowolnej wielkości obejmują:

- zapewnienie, aby kierownictwo najwyższego szczebla zgłaszało problemy związane z cyberbezpieczeństwem kadrom zarządzającym i zarządom, które dzięki temu mogą podejmować świadome decyzje dotyczące alokacji zasobów;

- wyznaczenie osoby na wysokim stanowisku, odpowiedzialnej za cyberbezpieczeństwo i bezpieczeństwo fizyczne, z ogólną odpowiedzialnością za zarządzanie bezpieczeństwem technologii informacyjnej (IT) i technologii operacyjnej (OT), ale bez angażowania się w operacje, aby uniknąć konfliktu interesów;

- wyraźne określenie ról, obowiązków, kompetencji i uprawnień związanych z cyberbezpieczeństwem oraz informowanie o nich odpowiedniego personelu i uzgadnianie ich z nim, w szczególności w przypadku członków zespołów reagowania na incydenty komputerowe (CERT);

- zapewnienie zarządzania cyberbezpieczeństwem w całym łańcuchu dostaw usług w zakresie bezpieczeństwa, w tym zarówno interfejsów fizycznych, jak i cyfrowych, od producentów technologii i instalatorów po dostawców usług w zakresie bezpieczeństwa;

- uzgodnienie działań i kontroli, w tym podziału obowiązków, w celu zarządzania ryzykiem w cyberprzestrzeni oraz zapewnienie, aby obowiązki te utrzymywano przez cały okres użytkowania (np. na mocy umów o świadczenie usług) rozwiązań i usług w zakresie bezpieczeństwa;

- określenie mechanizmów zarządzania (np. polityki) w celu wypełnienia zobowiązań wynikających z odpowiednich rozporządzeń i dyrektyw, takich jak np. rozporządzenie (UE) 2018/1139 w sprawie wspólnych zasad w dziedzinie lotnictwa cywilnego i rozporządzenie wykonawcze Komisji (UE) 2017/373 ustanawiające wspólne wymogi dotyczące instytucji zapewniających zarządzanie ruchem lotniczym/służby żeglugi powietrznej i inne funkcje sieciowe zarządzania ruchem lotniczym oraz nadzór nad nimi, a także dyrektywa w sprawie bezpieczeństwa sieci i informacji (dyrektywa (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych).

Przykłady usług i systemów w transporcie lotniczym:
Przykładami technologii informacyjnych są technologie, do których mają dostęp pracownicy (np. komputery osobiste, telefony komórkowe, biurowe urządzenia peryferyjne itp.), jak również pasażerowie (np. publiczne routery i połączenia Wi-Fi itp.). Przykładami technologii operacyjnych są systemy kontroli i gromadzenia danych (SCADA), systemy ogrzewania, wentylacji i klimatyzacji (HVAC), punkty kontroli bezpieczeństwa bagażu podręcznego, systemy obsługi bagażu, technologia kontroli dostępu, monitorowania, nadzoru, reagowania na alarmy oraz kontroli bezpieczeństwa, systemy sterowania oświetleniem lotniska, systemy i czujniki radarowe, globalne systemy pozycjonowania (GPS), systemy zarządzania ruchem lotniczym (ATM), systemy łączności, nawigacji i dozorowania, lotnicze systemy informacyjne, systemy meteorologiczne, systemy centrum monitorowania bezpieczeństwa, systemy pokładowe linii lotniczych i inne technologie.

Komisja Europejska

Identyfikacja zagrożeń dla cyberbezpieczeństwa

Zarządzanie ryzykiem: Organizacje transportu lotniczego muszą podjąć odpowiednie działania w celu identyfikacji, oceny i zrozumienia ryzyka w cyberprzestrzeni dla sieci i systemów informacyjnych wspomagających działanie podstawowych funkcji.

Wymaga to ogólnego podejścia organizacyjnego w zakresie zarządzania ryzykiem, obejmującego:

- *zapewnienie jasnego przeglądu poszczególnych systemów sprzętowych i programowych wdrożonych w celu świadczenia różnych usług. W kontekście transportu lotniczego systemy takie obejmują technologię informacyjną (IT) oraz technologie operacyjne (OT);*

- *przeprowadzanie **ocen ryzyka w cyberprzestrzeni**, w których uwzględnia się pojawiające się zagrożenia, znane podatności oraz dane operacyjne w odniesieniu do systemów objętych oceną. Organizacje takie jak europejski zespół reagowania na incydenty komputerowe w zarządzaniu ruchem lotniczym oraz ośrodek wymiany i analizy informacji o lotnictwie (A-ISAC) mogą dostarczać informacji na temat zagrożeń dla transportu lotniczego;*

- *zapewnienie, aby oceny ryzyka obejmowały również ryzyko związane z codziennymi czynnościami personelu (np. korzystanie z mediów społecznościowych, korzystanie z urządzeń osobistych, przetwarzanie danych, wymiana informacji itp.);*

- *określanie i wdrażanie środków i planów odnoszących się do postępowania w przypadku ryzyka w celu ograniczenia ryzyka w cyberprzestrzeni;*

- *wdrożenie kompleksowego **systemu zarządzania bezpieczeństwem informacji** (SZBI) oraz **systemu zarządzania danymi osobowymi** (PIMS), dostosowanych do innych systemów zarządzania. Takie systemy zarządzania (tj. SZBI i PIMS) obejmują wdrażanie kontroli bezpieczeństwa (jak również ochrony danych i prywatności) w celu ograniczania pojawiających się zagrożeń mających wpływ na bezpieczeństwo usług i systemów transportu lotniczego (w tym ich danych) oraz zapobiegania takim zagrożeniom;*

- *uwzględnianie wszelkich ograniczeń związanych z **zarządzaniem aktywami i planowaniem zasobów** (tj. ograniczeń, które mogą wpływać na dostawę, utrzymanie i obsługę systemów krytycznych dla działania podstawowych funkcji w transporcie lotniczym).*

Komisja Europejska

Przykłady ram zarządzania ryzykiem: Różne ramy (np. normy z serii ISO/IEC 27000, ramy cyberbezpieczeństwa NIST, ramy MITRE ATT&CK, BSI IT-Grundschutz itp.) mogą stanowić źródło informacji i podstawę dostosowanego podejścia do zarządzania ryzykiem w transporcie lotniczym. Organizacje międzynarodowe, takie jak IATA i ICAO, zapewniają wytyczne dotyczące oceny ryzyka w cyberprzestrzeni. ENISA, EASA, Eurocontrol i Międzynarodowa Rada Portów Lotniczych propagują między innymi dobre praktyki w zakresie zabezpieczania portów lotniczych, dostawców usług zarządzających ruchem lotniczym i innych organizacji lotniczych. Wspólne Przedsięwzięcie SESAR koordynuje i koncentruje wszystkie działania UE w dziedzinie badań i rozwoju dotyczące zarządzania ruchem lotniczym, obejmujące również aspekty bezpieczeństwa i ochrony.

Komisja Europejska

Ochrona przed zagrożeniami dla cyberbezpieczeństwa

Organizacje w transporcie lotniczym powinny wdrożyć odpowiednie i proporcjonalne środki bezpieczeństwa w celu ochrony swoich sieci i systemów informacyjnych, w tym technologii informacyjnej (IT) i technologii operacyjnej (OT), przed cyberatakami. Środki bezpieczeństwa obejmują:

- ***polityki i procesy bezpieczeństwa:*** *określanie, wdrażanie i egzekwowanie odpowiednich polityk i procesów oraz informowanie o nich, w których to politykach i procesach określono ogólne podejście do zabezpieczania systemów i danych wspomagających działanie podstawowych funkcji w transporcie lotniczym. Takie polityki (np. polityka w zakresie haseł i przechowywania) oraz procedury bezpieczeństwa powinny również obejmować łatki i zarządzanie podatnościami w systemach sprzętowych i programowych (w tym IT i OT), zarządzanie incydentami oraz ochronę systemu i sieci;*

- ***zarządzanie tożsamością i dostępem:*** *zrozumienie i dokumentowanie dostępu do sieci i systemów informacyjnych (w tym IT i OT) wspomagających działanie podstawowych funkcji w transporcie lotniczym oraz zarządzanie tym dostępem. Użytkownicy (lub automatyczne funkcje) mający możliwość uzyskania dostępu do danych lub systemów są odpowiednio weryfikowani, uwierzytelniani i autoryzowani. Należy w tym także uwzględniać poszczególne role i obowiązki w odniesieniu do kont zwykłych i uprzywilejowanych;*

- ***bezpieczeństwo danych i systemów:*** *ochrona danych (przechowywanych i przekazywanych elektronicznie), krytycznych sieci i systemów informacyjnych (w tym IT i OT) przed cyberatakami. Biorąc pod uwagę podejście oparte na ryzyku, organizacje powinny wdrożyć środki bezpieczeństwa w celu skutecznego ograniczenia możliwości zagrożenia danym, sieciom i systemom przez sprawców ataków. Wspomniane środki bezpieczeństwa powinny również obejmować wprowadzenie szyfrowania i bezpiecznych protokołów komunikacyjnych w celu ochrony danych odłożonych i przekazywanych przed zagrożeniami dla cyberbezpieczeństwa, których skutkiem są ataki przez powtórzenie. Ponadto konieczne jest połączenie takich środków ze środkami bezpieczeństwa fizycznego w celu ochrony dostępu do systemów (np. systemy należy umieścić w zamkniętych pomieszczeniach o ograniczonym dostępie);*

- ***odporność sieci i systemów:*** *budowanie odporności sieci i systemów (w tym IT i OT) poprzez ich projektowanie i wdrażanie (wraz z odnośnymi procedurami operacyjnymi) z myślą o odporności na cyberataki oraz łagodzeniu skutków takich ataków. Przykłady rozwiązań projektowych i wdrożeniowych zwiększających odporność obejmują: formalnie zweryfikowane funkcje krytyczne, zapewnianie dodatkowych systemów i sieci, segregację sieci (w szczególności segregację IT i OT), wielowarstwowe środki bezpieczeństwa i wiele innych. Należy zauważyć, że z punktu widzenia bezpieczeństwa informacji domeny bezpieczeństwa, w których wdraża się segregację sieci i systemów, mogą stanowić odpowiednie rozwiązanie w zakresie bezpieczeństwa. Potrzeby operacyjne (np. czynności konserwacyjne, transfery danych itp.) systemów mogą jednak wymagać obejścia lub połączenia różnych domen bezpieczeństwa (np. odseparowanych systemów i sieci), w tym połączenia IT i OT.*

Komisja Europejska

Wykrywanie zagrożeń dla cyberbezpieczeństwa

Organizacje powinny zapewnić, aby środki bezpieczeństwa pozostawały skuteczne, i wykrywać wszelkie zdarzenia związane z cyberbezpieczeństwem mające wpływ lub mogące mieć wpływ na kontrole bezpieczeństwa, jak również na podstawowe usługi i systemy. Odpowiednie środki bezpieczeństwa służące wykrywaniu zagrożeń dla cyberbezpieczeństwa obejmują:

- ***monitorowanie bezpieczeństwa:*** *monitorowanie stanu bezpieczeństwa sieci i systemów informacyjnych – w tym technologii informacyjnej (IT) i technologii operacyjnej (OT) – wspomagających działanie podstawowych funkcji w usługach transportu lotniczego. Aby wspierać monitorowanie bezpieczeństwa, uwzględnia się przykładowo następujące dane:*

  - *dzienniki bezpieczeństwa;*
  - *dzienniki wykrywania wirusów;*
  - *dzienniki wykrywania włamań;*
  - *dzienniki identyfikacji, uwierzytelniania i autoryzacji;*
  - *dzienniki systemowe i serwisowe;*
  - *dzienniki ruchu sieciowego;*
  - *dzienniki przetwarzania danych.*

- ***wykrycie zdarzenia związanego z bezpieczeństwem informacji:*** *wykrywanie szkodliwych działań (tj. zdarzeń związanych z bezpieczeństwem informacji) mających wpływ lub mogących wpłynąć na bezpieczeństwo sieci i systemów informacyjnych (w tym IT i OT) wspomagających działanie podstawowych funkcji w usługach transportu lotniczego.*

Środki te mogą wymagać wdrożenia określonych technologii (np. zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem informacji, systemu wykrywania włamań, systemu zapobiegania włamaniom itp.) oraz ustanowienia SOC (centrum monitorowania bezpieczeństwa) lub równoważnego rozwiązania. Oznacza to opracowanie środków służących do wykrywania i analizowania cyberataków, reagowania na nie oraz przywracania normalnego stanu po takich atakach na poziomie lokalnym.

Krajowe zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), sektorowe zespoły CERT (np. europejski zespół reagowania na incydenty komputerowe w zarządzaniu ruchem lotniczym (EATM-CERT) Europejskiej Organizacji ds. Bezpieczeństwa Żeglugi Powietrznej), komercyjne zespoły CERT linii lotniczych oraz ośrodek wymiany i analizy informacji o lotnictwie (A-ISAC) mogą zapewniać analizę cyberzagrożeń na potrzeby monitorowania i wykrywania zagrożeń dla bezpieczeństwa.

Komisja Europejska

Planowanie reakcji i przywracania normalnego stanu

Organizacje powinny określić, wdrożyć i przetestować procedury zarządzania incydentami służące zapewnieniu ciągłości świadczenia usług i działania systemów w przypadku cyberincydentów. Środki łagodzące są przeznaczone do przeciwdziałania skutkom cyberincydentów lub ich ograniczenia.

W planowaniu reakcji i przywracania normalnego stanu należy uwzględnić środki bezpieczeństwa łagodzące skutki określonych ataków na cyberbezpieczeństwo, takie jak:

- *koordynacja i współpraca z krajowymi zespołami CSIRT, (publicznymi i komercyjnymi) zespołami CERT i ośrodkami wymiany i analizy informacji podczas cyberincydentów, koordynacja incydentów i kryzysów na poziomie ogólnoeuropejskim;*

- *wymiana informacji z innymi organizacjami, w tym z dostawcami w łańcuchu dostaw usług transportu lotniczego;*

- *przeprowadzanie okresowych **ćwiczeń w zakresie cyberataków** (koordynacyjne i techniczne ćwiczenia symulacyjne) w celu oceny środków i procedur bezpieczeństwa, a także odporności organizacji na cyberincydenty;*

- *dostęp do zarchiwizowanych lub zapasowych miejsc przechowywania w przypadku naruszenia integralności i dostępności magazynów danych;*

- ***podręczniki dotyczące bezpieczeństwa** zawierające szczegółowe procedury zarządzania cyberincydentami oraz przywracania normalnych warunków operacyjnych usług i systemów;*

- *przekierowania ruchu sieciowego do nadmiarowych usług podczas ataków typu „odmowa usługi”;*

- *procedury ręczne umożliwiające działanie z usługami i systemami w trybie pracy podczas awarii;*

- *określenie procedur postępowania w przypadku naruszeń ochrony danych, w tym procedur postępowania w przypadku naruszeń ochrony danych mających wpływ na dane osobowe zgodnie z ogólnym rozporządzeniem o ochronie danych (RODO) oraz wszelkimi innymi odpowiednimi rozporządzeniami lub dyrektywami sektorowymi;*

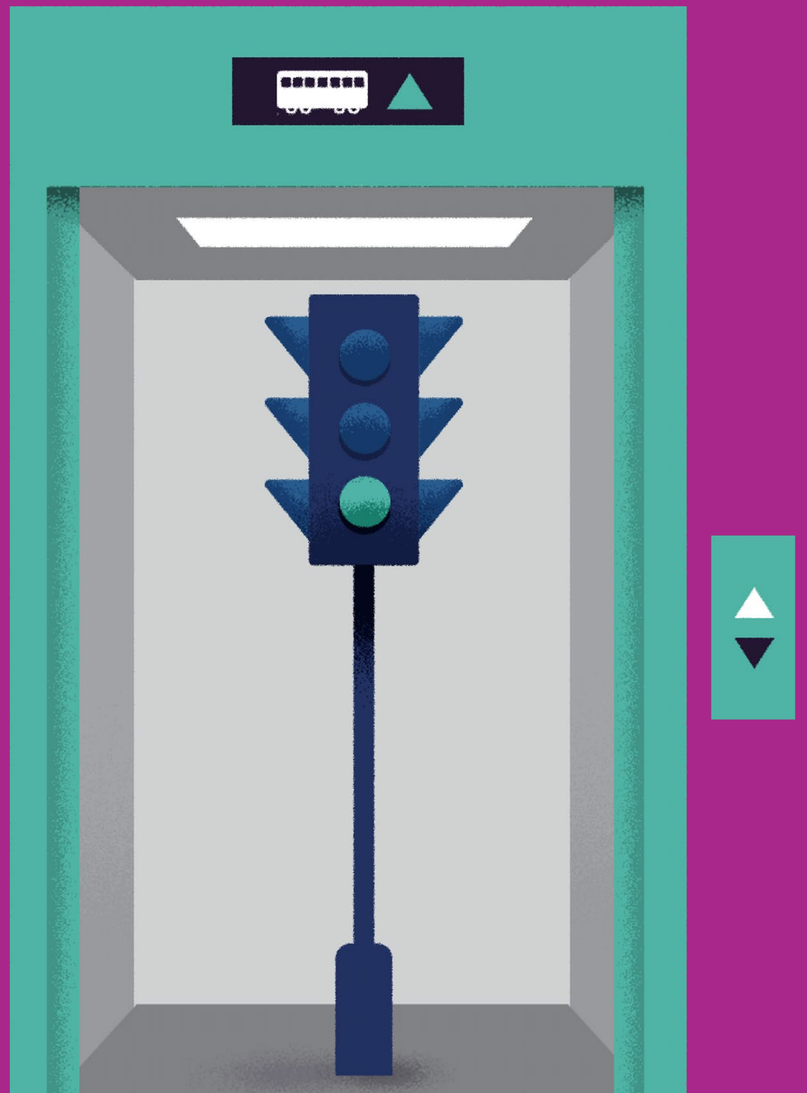
- *zakup **cyberubezpieczenia** w celu częściowego zrównoważenia ryzyka związanego z poważnymi cyberincydentami;*

- *zawarcie umowy dotyczącej reagowania na incydenty z co najmniej jedną wyspecjalizowaną firmą w celu uzyskania dodatkowych możliwości i wiedzy fachowej;*

- *określenie procedur **wymiany informacji o cyberincydentach** z odpowiednimi zainteresowanymi stronami, w tym procedur zgłaszania incydentów zgodnie z dyrektywą dotyczącą cyberbezpieczeństwa (dyrektywa (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii).*

Komisja Europejska

Dobre praktyki i środki bezpieczeństwa dostosowane do transportu lądowego



Zarządzanie

Organizacje w transporcie lądowym (kolejowym i drogowym) potrzebują jasnego zrozumienia pojawiających się zagrożeń, aby określić politykę zarządzania i procesy służące uregulowaniu ich podejść w celu zwiększenia cyberbezpieczeństwa usług i systemów w ramach operacji, w tym technologii informacyjnej (IT) i technologii operacyjnej (OT).

Dobre praktyki dla organizacji dowolnej wielkości obejmują:

- *zapewnienie, aby kierownictwo najwyższego szczebla zgłaszało problemy związane z cyberbezpieczeństwem kadrom zarządzającym i zarządom, które dzięki temu mogą podejmować świadome decyzje dotyczące alokacji zasobów;*

- *wyznaczenie osoby na wysokim stanowisku, odpowiedzialnej za cyberbezpieczeństwo i bezpieczeństwo fizyczne, z ogólną odpowiedzialnością za zarządzanie bezpieczeństwem technologii informacyjnej (IT) i technologii operacyjnej (OT), ale bez angażowania się w operacje, aby uniknąć konfliktu interesów;*

- *wyraźne określenie ról, obowiązków, kompetencji i uprawnień związanych z cyberbezpieczeństwem oraz informowanie o nich odpowiedniego personelu i uzgadnianie ich z nim. Jest to konieczne w szczególności w przypadku członków zespołów reagowania na incydenty komputerowe (CERT);*

- *zapewnienie zarządzania cyberbezpieczeństwem w całym łańcuchu dostaw usług w zakresie bezpieczeństwa, w tym zarówno interfejsów fizycznych, jak i cyfrowych, od producentów technologii i instalatorów po dostawców usług w zakresie bezpieczeństwa;*

- *uzgodnienie działań i kontroli, w tym podziału obowiązków, w celu zarządzania ryzykiem w cyberprzestrzeni oraz zapewnienie, aby obowiązki te utrzymywano przez cały okres użytkowania (np. na mocy umów o świadczenie usług) rozwiązań i usług w zakresie bezpieczeństwa;*

- *określenie mechanizmów zarządzania (np. polityki) w celu wypełnienia obowiązków wynikających z odpowiednich rozporządzeń i dyrektyw. Odnosi się to do to szerokiego zestawu polityk obejmujących poszczególne rodzaje transportu, a także różnego rodzaju zainteresowane strony (np. producentów pojazdów i systemów kolejowych), jak również dyrektywy dotyczącej cyberbezpieczeństwa (dyrektywa (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii).*

Przykłady usług i systemów w transporcie lądowym: Przykładami technologii informacyjnych są technologie, do których mają dostęp pracownicy (np. komputery osobiste, telefony komórkowe, biurowe urządzenia peryferyjne itp.), jak również pasażerowie (np. publiczne routery i połączenia Wi-Fi itp.). Przykładami technologii operacyjnych są systemy kontroli i gromadzenia danych (SCADA), systemy ogrzewania, wentylacji i klimatyzacji (HVAC), globalne systemy pozycjonowania (GPS), technologia kontroli dostępu, monitorowania, nadzoru, reagowania na alarmy oraz kontroli bezpieczeństwa. Systemy specyficzne dla transportu kolejowego to np.: systemy operacyjne (systemy kontrolno-decyzyjne), w tym systemy sygnalizacyjne, europejski system zarządzania ruchem kolejowym (ERTMS), systemy pokładowe, systemy obsługi technicznej i inne.

Komisja Europejska

Identyfikacja zagrożeń dla cyberbezpieczeństwa

Zarządzanie ryzykiem: Organizacje transportu lądowego muszą podjąć odpowiednie działania w celu identyfikacji, oceny i zrozumienia ryzyka w cyberprzestrzeni dla sieci i systemów informacyjnych wspomagających działanie podstawowych funkcji. Wymaga to ogólnego podejścia organizacyjnego w zakresie zarządzania ryzykiem, obejmującego:

- *zapewnienie jasnego przeglądu poszczególnych systemów sprzętowych i programowych wdrożonych w celu świadczenia różnych usług. W kontekście transportu lądowego systemy takie obejmują technologię informacyjną (IT) oraz technologie operacyjne (OT);*

- *przeprowadzanie **ocen ryzyka w cyberprzestrzeni**, w których należy uwzględnić pojawiające się zagrożenia, znane podatności oraz dane operacyjne w odniesieniu do systemów objętych oceną. Przykładami systemów w rodzajach transportu lądowego są: systemy płatności, systemy sieciowe i komunikacyjne (np. internet, łączność radiowa, Wi-Fi itp.), urządzenia pokładowe, centra kontroli operacyjnej, systemy zarządzania tożsamością, systemy bezpieczeństwa i inne. W odniesieniu do infrastruktur kolejowych przykłady systemów to: tabor, podsystemy „Ruch kolejowy", podsystemy kontrolno-decyzyjne, sterowanie ruchem kolejowym, a także podsystemy pokładowe i przytorowe oraz inne;*

- *zapewnienie, aby oceny ryzyka obejmowały również ryzyko związane z codziennymi czynnościami personelu (np. korzystanie z mediów społecznościowych, korzystanie z urządzeń osobistych, przetwarzanie danych, wymiana informacji itp.);*

- *określanie i wdrażanie środków i planów odnoszących się do postępowania w przypadku ryzyka w celu ograniczenia ryzyka w cyberprzestrzeni, między innymi wdrożenie kompleksowego **systemu zarządzania bezpieczeństwem informacji** (SZBI) oraz **systemu zarządzania danymi osobowymi** (PIMS), dostosowanych do innych systemów zarządzania. Takie systemy zarządzania (tj. SZBI i PIMS) obejmują wdrażanie kontroli bezpieczeństwa (jak również ochrony danych i prywatności) w celu ograniczania pojawiających się zagrożeń mających wpływ na bezpieczeństwo usług i systemów transportu lądowego (w tym ich danych) oraz zapobiegania takim zagrożeniom;*

- *uwzględnianie wszelkich ograniczeń związanych z **zarządzaniem aktywami i planowaniem zasobów** (tj. ograniczeń, które mogą wpływać na dostawę, utrzymanie i obsługę systemów krytycznych dla działania podstawowych funkcji w transporcie lądowym).*

Przykłady ram zarządzania ryzykiem: Różne ramy (np. normy z serii ISO/IEC 27000, ramy cyberbezpieczeństwa NIST, ramy MITRE ATT&CK, BSI IT-Grundschutz itp.) mogą stanowić źródło informacji i podstawę dostosowanego podejścia do zarządzania ryzykiem w transporcie drogowym i kolejowym. Organizacje takie jak ENISA określają dobre praktyki w zakresie cyberbezpieczeństwa inteligentnych samochodów i inteligentnego transportu publicznego, stanowiące źródło informacji dla producentów i stowarzyszeń branżowych (np. dla Europejskiego Stowarzyszenia Producentów Samochodów – ACEA).
W transporcie kolejowym Agencja Kolejowa Unii Europejskiej (ERA) określa techniczne specyfikacje interoperacyjności (TSI), z którymi musi być zgodny każdy podsystem lub każda część podsystemu w celu spełnienia zasadniczych wymagań i zapewnienia interoperacyjności systemu kolejowego Unii Europejskiej. Wspólne Przedsięwzięcie Shift2Rail także przyczynia się do opracowywania innowacyjnych inicjatyw i projektów (w tym dotyczących cyberbezpieczeństwa) dla transportu kolejowego.

Komisja Europejska

Ochrona przed zagrożeniami dla cyberbezpieczeństwa

Organizacje w transporcie lądowym powinny wdrożyć odpowiednie i proporcjonalne środki bezpieczeństwa w celu ochrony swoich sieci i systemów informacyjnych, w tym technologii informacyjnej (IT) i technologii operacyjnej (OT), przed cyberatakami. Środki bezpieczeństwa obejmują:

- ***polityki i procesy bezpieczeństwa:*** *określanie, wdrażanie i egzekwowanie odpowiednich polityk i procesów oraz informowanie o nich, w których to politykach i procesach określono ogólne podejście do zabezpieczania systemów i danych wspomagających działanie podstawowych funkcji w rodzajach transportu lądowego. Takie polityki (np. polityka w zakresie haseł i przechowywania) oraz procedury bezpieczeństwa powinny również obejmować łatki i zarządzanie podatnościami w systemach sprzętowych i programowych (w tym IT i OT), zarządzanie incydentami oraz ochronę systemu i sieci;*

- ***zarządzanie tożsamością i dostępem:*** *zrozumienie i dokumentowanie dostępu do sieci i systemów informacyjnych (w tym IT i OT) wspomagających działanie podstawowych funkcji w rodzajach transportu lądowego oraz zarządzanie tym dostępem. Użytkownicy (lub automatyczne funkcje) mający możliwość uzyskania dostępu do danych lub systemów są odpowiednio weryfikowani, uwierzytelniani i autoryzowani. Należy w tym także uwzględniać poszczególne role i obowiązki w odniesieniu do kont zwykłych i uprzywilejowanych;*

- ***bezpieczeństwo danych i systemów:*** *ochrona danych (przechowywanych i przekazywanych elektronicznie), krytycznych sieci i systemów informacyjnych (w tym IT i OT) przed cyberatakami. Biorąc pod uwagę podejście oparte na ryzyku, organizacje powinny wdrożyć środki bezpieczeństwa w celu skutecznego ograniczenia możliwości zagrożenia danym, sieciom i systemom przez sprawców ataków. Wspomniane środki bezpieczeństwa powinny również obejmować wprowadzenie szyfrowania i bezpiecznych protokołów komunikacyjnych w celu ochrony danych odłożonych i przekazywanych przed zagrożeniami dla cyberbezpieczeństwa, których skutkiem są ataki przez powtórzenie. Ponadto konieczne jest połączenie takich środków ze środkami bezpieczeństwa fizycznego w celu ochrony dostępu do systemów (np. systemy należy umieścić w zamkniętych pomieszczeniach o ograniczonym dostępie). Jest to bardzo ważne w przypadku tych systemów, które mogą mieć wpływ na bezpieczeństwo życia;*

- ***odporność sieci i systemów:*** *budowanie odporności sieci i systemów (w tym IT i OT) poprzez ich projektowanie i wdrażanie (wraz z odnośnymi procedurami operacyjnymi) z myślą o odporności na cyberataki oraz łagodzeniu skutków takich ataków. Przykłady rozwiązań projektowych i wdrożeniowych zwiększających odporność obejmują: formalnie zweryfikowane funkcje krytyczne, zapewnianie dodatkowych systemów i sieci, segregację sieci (w szczególności segregację IT i OT), wielowarstwowe środki bezpieczeństwa i wiele innych. Należy zauważyć, że z punktu widzenia bezpieczeństwa informacji domeny bezpieczeństwa, w których wdraża się segregację sieci i systemów, mogą stanowić odpowiednie rozwiązanie w zakresie bezpieczeństwa. Potrzeby operacyjne (np. czynności konserwacyjne, transfery danych itp.) systemów mogą jednak wymagać obejścia lub połączenia różnych domen bezpieczeństwa (np. odseparowanych systemów i sieci), w tym połączenia IT i OT.*

Komisja Europejska

Wykrywanie zagrożeń dla cyberbezpieczeństwa

Organizacje powinny zapewnić, aby środki bezpieczeństwa pozostawały skuteczne, i wykrywać wszelkie zdarzenia związane z cyberbezpieczeństwem mające wpływ lub mogące mieć wpływ na kontrole bezpieczeństwa, jak również na podstawowe usługi i systemy. Odpowiednie środki bezpieczeństwa służące wykrywaniu zagrożeń dla cyberbezpieczeństwa obejmują:

- ***monitorowanie bezpieczeństwa:*** *monitorowanie stanu bezpieczeństwa sieci i systemów informacyjnych – w tym technologii informacyjnej (IT) i technologii operacyjnej (OT) – wspomagających działanie podstawowych funkcji w rodzajach transportu lądowego. Jest to konieczne do wykrywania potencjalnych zagrożeń dla bezpieczeństwa oraz śledzenia bieżącej skuteczności środków ochrony bezpieczeństwa. Aby wspierać monitorowanie bezpieczeństwa, uwzględnia się przykładowo następujące dane:*

  - *dzienniki bezpieczeństwa;*
  - *dzienniki wykrywania wirusów;*
  - *dzienniki wykrywania włamań;*
  - *dzienniki identyfikacji, uwierzytelniania i autoryzacji;*
  - *dzienniki systemowe i serwisowe;*
  - *dzienniki ruchu sieciowego;*
  - *dzienniki przetwarzania danych.*

- ***wykrycie zdarzenia związanego z bezpieczeństwem informacji:*** *wykrywanie szkodliwych działań (tj. zdarzeń związanych z bezpieczeństwem informacji) mających wpływ lub mogących wpłynąć na bezpieczeństwo sieci i systemów informacyjnych (w tym IT i OT) wspomagających działanie podstawowych funkcji.*

Środki te mogą wymagać wdrożenia określonych technologii (np. zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem informacji, systemu wykrywania włamań, systemu zapobiegania włamaniom itp.) oraz ustanowienia SOC (centrum monitorowania bezpieczeństwa) lub równoważnego rozwiązania. Oznacza to opracowanie środków służących do wykrywania i analizowania cyberataków, reagowania na nie oraz przywracania normalnego stanu po takich atakach na poziomie lokalnym. Krajowe zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), sektorowe i komercyjne zespoły CERT lub operatorzy drogowi i kolejowi oraz europejski ośrodek wymiany i analizy informacji o kolejach (ER-ISAC) mogą zapewniać analizę cyberzagrożeń na potrzeby monitorowania i wykrywania zagrożeń dla bezpieczeństwa.

Komisja Europejska

Planowanie reakcji i przywracania normalnego stanu

Organizacje powinny określić, wdrożyć i przetestować procedury zarządzania incydentami służące zapewnieniu ciągłości świadczenia usług i działania systemów w przypadku cyberincydentów.

W planowaniu reakcji i przywracania normalnego stanu należy uwzględnić środki bezpieczeństwa łagodzące skutki określonych ataków na cyberbezpieczeństwo, takie jak:

- *koordynacja i współpraca z krajowymi zespołami CSIRT, (publicznymi i komercyjnymi) zespołami CERT i ośrodkami wymiany i analizy informacji podczas cyberincydentów, koordynacja incydentów i kryzysów na poziomie ogólnoeuropejskim;*

- *wymiana informacji z innymi organizacjami, w tym z dostawcami w łańcuchu dostaw usług transportu lądowego;*

- *przeprowadzanie okresowych **ćwiczeń w zakresie cyberataków** (koordynacyjne i techniczne ćwiczenia symulacyjne) w celu oceny środków i procedur bezpieczeństwa, a także odporności organizacji na cyberincydenty;*

- *dostęp do zarchiwizowanych lub zapasowych miejsc przechowywania w przypadku naruszenia integralności i dostępności magazynów danych;*

- ***podręczniki dotyczące bezpieczeństwa** zawierające szczegółowe procedury zarządzania cyberincydentami oraz przywracania normalnych warunków operacyjnych usług i systemów;*

- *przekierowania ruchu sieciowego do nadmiarowych usług podczas ataków typu „odmowa usługi”;*

- *procedury ręczne umożliwiające działanie z usługami i systemami w trybie pracy podczas awarii;*

- *określenie procedur postępowania w przypadku naruszeń ochrony danych, w tym procedur postępowania w przypadku naruszeń ochrony danych mających wpływ na dane osobowe zgodnie z ogólnym rozporządzeniem o ochronie danych (RODO) oraz wszelkimi innymi odpowiednimi rozporządzeniami lub dyrektywami sektorowymi;*

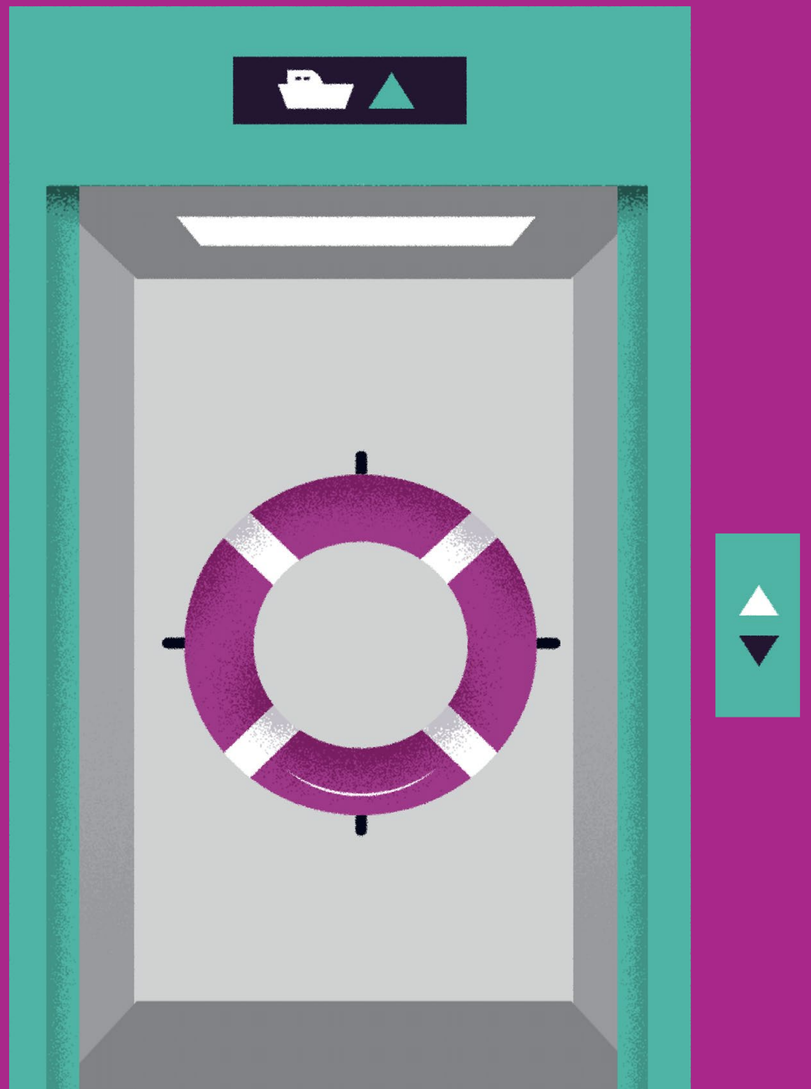
- *zakup **cyberubezpieczenia** w celu częściowego zrównoważenia ryzyka związanego z poważnymi cyberincydentami;*

- *zawarcie umowy dotyczącej reagowania na incydenty z co najmniej jedną wyspecjalizowaną firmą w celu uzyskania dodatkowych możliwości i wiedzy fachowej;*

- *określenie procedur wymiany informacji o cyberincydentach z odpowiednimi zainteresowanymi stronami, w tym procedur zgłaszania incydentów zgodnie z dyrektywą dotyczącą cyberbezpieczeństwa (dyrektywa (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii).*

Komisja Europejska

Dobre praktyki i środki bezpieczeństwa dostosowane do transportu morskiego



Komisja Europejska

Zarządzanie

Organizacje w transporcie morskim potrzebują jasnego zrozumienia pojawiających się zagrożeń, aby określić politykę zarządzania i procesy służące uregulowaniu ich podejść w celu zwiększenia cyberbezpieczeństwa usług i systemów w ramach operacji, w tym technologii informacyjnej (IT) i technologii operacyjnej (OT).

Dobre praktyki dla organizacji dowolnej wielkości obejmują:

- *zapewnienie, aby kierownictwo najwyższego szczebla zgłaszało problemy związane z cyberbezpieczeństwem kadrom zarządzającym i zarządom, które dzięki temu mogą podejmować świadome decyzje dotyczące alokacji zasobów;*

- *wyznaczenie osoby na wysokim stanowisku z ogólną odpowiedzialnością za zarządzanie bezpieczeństwem technologii informacyjnej (IT) i technologii operacyjnej (OT). Osoba na tym stanowisku powinna odpowiadać za cyberbezpieczeństwo, jak również bezpieczeństwo fizyczne;*

- *wyraźne określenie ról, obowiązków, kompetencji i uprawnień związanych z cyberbezpieczeństwem, zdefiniowanie poziomów uprawnień i kanałów komunikacji personelu na lądzie i na statku oraz między nimi, a także uzgodnienie ich z odpowiednim personelem. Jest to konieczne w szczególności w przypadku członków zespołów reagowania na incydenty komputerowe (CERT). Członkowie personelu na stanowiskach związanych z prawodawstwem UE w zakresie bezpieczeństwa i ochrony na morzu, np. oficerowie ochrony obiektu portowego, oficerowie ochrony portu, oficerowie ochrony armatora lub wyznaczona osoba na lądzie oraz kapitan na statku, powinni znać co najmniej środki cyberbezpieczeństwa wdrażane przez organizację;*

- *zapewnienie zarządzania cyberbezpieczeństwem w całym łańcuchu dostaw usług w zakresie bezpieczeństwa, w tym zarówno interfejsów fizycznych, jak i cyfrowych, od producentów technologii i instalatorów po dostawców usług w zakresie bezpieczeństwa;*

- *uzgodnienie działań i kontroli, w tym podziału obowiązków, w celu zarządzania ryzykiem w cyberprzestrzeni oraz zapewnienie, aby obowiązki te utrzymywano przez cały okres użytkowania (np. na mocy umów o świadczenie usług) rozwiązań i usług w zakresie bezpieczeństwa;*

- *określenie mechanizmów zarządzania (np. polityki) w celu wypełnienia zobowiązań wynikających z odpowiednich rozporządzeń i dyrektyw, np. rozporządzenia (UE) 2019/1239 ustanawiającego europejski system morskich pojedynczych punktów kontaktowych, rozporządzenia (WE) nr 725/2004 w sprawie wzmocnienia ochrony statków i obiektów portowych, dyrektywy 2005/65/WE w sprawie wzmocnienia ochrony portów, rozporządzenia (WE) nr 336/2006 w sprawie wdrożenia we Wspólnocie Międzynarodowego kodeksu zarządzania bezpieczeństwem oraz rezolucji A.741 (18), w której przyjęto Międzynarodowy kodeks zarządzania bezpieczną eksploatacją statków i zapobieganiem zanieczyszczaniu. W tym kontekście należy również wspomnieć o wspólnym mechanizmie wymiany informacji (CISE), inicjatywie UE, która ma na celu zapewnienie interoperacyjności systemów nadzoruj w Europie i państwach członkowskich, aby umożliwić wszystkim zainteresowanym organom dostęp do informacji niejawnych i jawnych, których potrzebują do prowadzenia misji na morzu.*

Komisja Europejska

Przykłady usług i systemów w transporcie morskim:
Przykładami technologii informacyjnych są technologie, do których mają dostęp pracownicy (np. komputery osobiste, telefony komórkowe, biurowe urządzenia peryferyjne itp.), jak również pasażerowie (np. publiczne routery i połączenia Wi-Fi itp.). Przykładami technologii operacyjnych są systemy kontroli i gromadzenia danych (SCADA), systemy ogrzewania, wentylacji i klimatyzacji (HVAC), globalne systemy pozycjonowania (GPS), technologia kontroli dostępu, monitorowania, nadzoru, reagowania na alarmy oraz kontroli bezpieczeństwa, pokładowe systemy nawigacyjne, SafeSeaNet, systemy mostka, systemy obsługi ładunku i zarządzania nim, systemy zarządzania napędem i maszynami oraz systemy kontroli mocy, systemy kontroli dostępu, systemy obsługi pasażerów i zarządzania nimi, sieci publiczne skierowane do pasażerów, systemy administracyjne i systemy opieki społecznej dla załogi, systemy łączności i inne.

Komisja Europejska

Identyfikacja zagrożeń dla cyberbezpieczeństwa

Zarządzanie ryzykiem: Organizacje morskie muszą podjąć odpowiednie działania w zakresie określenia, analizy i oceny ryzyka w cyberprzestrzeni oraz informowania o nim, a także akceptowania, unikania, przenoszenia tego ryzyka lub ograniczania go do dopuszczalnego poziomu. Wymaga to ogólnego podejścia organizacyjnego w zakresie zarządzania ryzykiem, obejmującego:

- *zapewnienie jasnego przeglądu poszczególnych systemów sprzętowych i programowych wdrożonych w celu świadczenia różnych usług. W kontekście transportu morskiego systemy takie obejmują technologię informacyjną (IT) oraz technologie operacyjne (OT), a także sposoby łączenia i integracji tych systemów z systemami lądowymi, w tym z organami publicznymi, terminalami morskimi i sztauerami;*

- *określenie i ocenę kluczowych operacji na statku, które są narażone na cyberataki, oraz przeprowadzenie ocen ryzyka w cyberprzestrzeni (w tym ocena potencjalnych skutków operacyjnych i prawdopodobieństwa wystąpienia), w których należy uwzględnić pojawiające się zagrożenia, znane podatności oraz dane operacyjne w odniesieniu do systemów objętych oceną. W stosownych przypadkach obejmuje to też powiązanie z ocenami stanu ochrony przeprowadzanymi dla statków, obiektów portowych i portów, jak określono w prawodawstwie UE dotyczącym bezpieczeństwa morskiego. W ramach tych ocen określa się możliwe zagrożenia dla bezpieczeństwa infrastruktury portowej oraz słabe punkty zabezpieczeń. Ponadto organizacje morskie, takie jak Międzynarodowa Organizacja Morska (IMO) i morskie ośrodki wymiany i analizy informacji, mogą dostarczać informacji na temat zagrożeń dla transportu morskiego;*

- *zapewnienie, aby oceny ryzyka obejmowały również ryzyko związane z codziennymi czynnościami personelu (np. korzystanie z mediów społecznościowych, korzystanie z urządzeń osobistych, przetwarzanie danych, wymiana informacji itp.);*

- *określanie i wdrażanie środków i planów odnoszących się do postępowania w przypadku ryzyka w celu ograniczenia ryzyka w cyberprzestrzeni. Na przykład wdrożenie kompleksowego systemu zarządzania bezpieczeństwem informacji (SZBI) oraz systemu zarządzania danymi osobowymi (PIMS), dostosowanych do innych systemów zarządzania, takich jak systemy zarządzania bezpieczeństwem, zgodnie z międzynarodowym kodeksem zarządzania bezpieczeństwem (kodeksem ISM). Takie systemy zarządzania (tj. SZBI i PIMS) obejmują wdrażanie kontroli bezpieczeństwa (jak również ochrony danych i prywatności) w celu ograniczania pojawiających się zagrożeń mających wpływ na bezpieczeństwo usług i systemów transportu morskiego (w tym ich danych) oraz zapobiegania takim zagrożeniom;*

- *uwzględnianie wszelkich ograniczeń związanych z **zarządzaniem aktywami i planowaniem zasobów** (tj. ograniczeń, które mogą wpływać na dostawę, utrzymanie i obsługę systemów krytycznych dla działania podstawowych funkcji w transporcie morskim). Jeżeli chodzi o oceny, w stosownych przypadkach należy dokonać odniesienia do wymogów kodeksu ISM, systemów zarządzania bezpieczeństwem oraz planów ochrony opracowanych zgodnie z prawodawstwem UE w zakresie bezpieczeństwa i ochrony na morzu.*

Przykłady ram zarządzania ryzykiem: Różne ramy (np. kodeks ISM lub normy z serii ISO/IEC 27000, ramy cyberbezpieczeństwa NIST, ramy MITRE ATT&CK, BSI IT-Grundschutz itp.) mogą stanowić źródło informacji i podstawę dostosowanego podejścia do zarządzania ryzykiem w transporcie morskim. Ramy cyberbezpieczeństwa NIST również dostosowano do kwestii cyberbezpieczeństwa morskiego transportu płynnych towarów luzem, operacji morskich oraz operacji na statkach pasażerskich. Podobnie Bałtycka i Międzynarodowa Rada Morska (BIMCO) wydała „The Guidelines on Cyber Security Onboard Ships" [„Wytyczne dotyczące cyberbezpieczeństwa na statkach"], a Międzynarodowa Organizacja Morska (IMO) wydała specjalny dokument „Guidelines on maritime cyber risk management" [„Wytyczne dotyczące zarządzania ryzykiem w cyberprzestrzeni na morzu"] (MSC-FAL.1/Circ.3). Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) przeprowadziła szereg badań dotyczących dobrych praktyk w zakresie cyberbezpieczeństwa na morzu, w szczególności cyberbezpieczeństwa portów. Europejska Agencja Bezpieczeństwa Morskiego (EMSA) świadczy usługi na rzecz społeczności morskiej, w tym oferuje szkolenia podnoszące świadomość w zakresie cyberbezpieczeństwa. W normach (tj. w normie IEC 61162-460:2018 dotyczącej bezpieczeństwa i ochrony urządzeń i systemów nawigacji i radiokomunikacji morskiej, ISO 16425:2013 dotyczącej statków i technologii morskich, IEC 62443-4-1:2018 dotyczącej bezpieczeństwa w systemach sterowania i automatyki przemysłowej itp.) określono ponadto szczegółowe wymagania dotyczące bezpieczeństwa i ochrony systemów i sieci w transporcie morskim.

Komisja Europejska

Ochrona przed zagrożeniami dla cyberbezpieczeństwa

Organizacje w transporcie morskim powinny wdrożyć odpowiednie i proporcjonalne środki bezpieczeństwa w celu ochrony swoich sieci i systemów informacyjnych, w tym technologii informacyjnej (IT) i operacyjnej. Środki bezpieczeństwa obejmują:

- ***polityki i procesy bezpieczeństwa:*** *określanie, wdrażanie i egzekwowanie odpowiednich polityk i procesów oraz informowanie o nich, w których to politykach i procesach określono ogólne podejście do zabezpieczania systemów i danych wspomagających działanie podstawowych funkcji w transporcie morskim. Środki bezpieczeństwa (w tym środki cyberbezpieczeństwa i bezpieczeństwa fizycznego) należy uwzględnić w odpowiednich planach, takich jak system zarządzania bezpieczeństwem oraz plan ochrony statku. Takie polityki (np. polityka w zakresie haseł i przechowywania) oraz procedury bezpieczeństwa powinny również obejmować łatki i zarządzanie podatnościami w systemach sprzętowych i programowych (w tym IT i OT), zarządzanie incydentami oraz ochronę systemu i sieci;*

- ***zarządzanie tożsamością i dostępem:*** *zrozumienie i dokumentowanie dostępu do sieci i systemów informacyjnych (w tym IT i OT) wspomagających działanie podstawowych funkcji w transporcie morskim oraz zarządzanie tym dostępem. Użytkownicy (lub automatyczne funkcje) mający możliwość uzyskania dostępu do danych lub systemów są odpowiednio weryfikowani, uwierzytelniani i autoryzowani. Należy w tym także uwzględniać poszczególne role i obowiązki w odniesieniu do kont zwykłych i uprzywilejowanych;*

- ***bezpieczeństwo danych i systemów:*** *ochrona danych (przechowywanych i przekazywanych elektronicznie), krytycznych sieci i systemów informacyjnych (w tym IT i OT) przed cyberatakami. Biorąc pod uwagę podejście oparte na ryzyku, organizacje powinny wdrożyć środki bezpieczeństwa w celu efektywnego ograniczenia możliwości zagrożenia danym, sieciom i systemom przez sprawców ataków. Wspomniane środki bezpieczeństwa powinny również obejmować wprowadzenie szyfrowania i bezpiecznych protokołów komunikacyjnych w celu ochrony danych odłożonych i przekazywanych przed zagrożeniami dla cyberbezpieczeństwa, których skutkiem są ataki przez powtórzenie. Ponadto konieczne jest połączenie takich środków ze środkami bezpieczeństwa fizycznego w celu ochrony dostępu do systemów (np. systemy należy umieścić w zamkniętych pomieszczeniach o ograniczonym dostępie). Jest to bardzo ważne w przypadku tych systemów, które mogą mieć wpływ na bezpieczeństwo życia (np. systemy nawigacji i łączności radiowej kategorii II i III);*

- ***odporność sieci i systemów:*** *budowanie odporności sieci i systemów (w tym IT i OT) poprzez ich projektowanie i wdrażanie (wraz z odnośnymi procedurami operacyjnymi) z myślą o odporności na cyberataki oraz łagodzeniu skutków takich ataków. Przykłady rozwiązań projektowych i wdrożeniowych zwiększających odporność obejmują: formalnie zweryfikowane funkcje krytyczne, zapewnianie dodatkowych systemów i sieci, segregację sieci (w szczególności segregację IT i OT), wielowarstwowe środki bezpieczeństwa i wiele innych. Należy zauważyć, że z punktu widzenia bezpieczeństwa informacji domeny bezpieczeństwa, w których wdraża się segregację sieci i systemów, mogą stanowić odpowiednie rozwiązanie w zakresie bezpieczeństwa. Potrzeby (np. czynności konserwacyjne, transfery danych itp.) systemów (np. autonomiczne nawodne statki morskie – MASS) mogą jednak wymagać obejścia lub połączenia różnych domen bezpieczeństwa (np. odseparowanych systemów i sieci), w tym połączenia IT i OT.*

Wykrywanie zagrożeń dla cyberbezpieczeństwa

Organizacje powinny zapewnić, aby środki bezpieczeństwa pozostawały skuteczne, i wykrywać wszelkie zdarzenia związane z cyberbezpieczeństwem mające wpływ lub mogące mieć wpływ na kontrole bezpieczeństwa, jak również na podstawowe usługi i systemy. Odpowiednie środki bezpieczeństwa służące wykrywaniu zagrożeń dla cyberbezpieczeństwa obejmują:

■ ***monitorowanie bezpieczeństwa:*** *monitorowanie stanu bezpieczeństwa sieci i systemów informacyjnych – w tym technologii informacyjnej (IT) i technologii operacyjnej (OT) – wspomagających działanie podstawowych funkcji w transporcie morskim. Jest to konieczne do wykrywania potencjalnych zagrożeń dla bezpieczeństwa oraz śledzenia bieżącej skuteczności środków ochrony bezpieczeństwa. Aby wspierać monitorowanie bezpieczeństwa, uwzględnia się przykładowo następujące dane:*

- *dzienniki bezpieczeństwa;*
- *dzienniki wykrywania wirusów;*
- *dzienniki wykrywania włamań;*
- *dzienniki identyfikacji, uwierzytelniania i autoryzacji;*
- *dzienniki systemowe i serwisowe;*
- *dzienniki ruchu sieciowego;*
- *dzienniki przetwarzania danych;*

■ ***wykrycie zdarzenia związanego z bezpieczeństwem informacji:*** *wykrywanie szkodliwych działań (tj. zdarzeń związanych z bezpieczeństwem informacji) mających wpływ lub mogących mieć wpływ na bezpieczeństwo sieci i systemów informacyjnych (w tym IT i OT) wspomagających działanie podstawowych funkcji w usługach transportu morskiego.*

Środki te mogą wymagać wdrożenia określonych technologii (np. zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem informacji, systemu wykrywania włamań, systemu zapobiegania włamaniom itp.) oraz ustanowienia SOC (centrum monitorowania bezpieczeństwa) lub równoważnego rozwiązania. Oznacza to opracowanie środków służących do wykrywania i analizowania cyberataków, reagowania na nie oraz przywracania normalnego stanu po takich atakach na poziomie lokalnym.

Krajowe zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), sektorowe i komercyjne zespoły CERT operatorów morskich oraz morskie ośrodki wymiany i analizy informacji mogą zapewniać analizę cyberzagrożeń na potrzeby monitorowania i wykrywania zagrożeń dla bezpieczeństwa.

Komisja Europejska

Planowanie reakcji i przywracania normalnego stanu

Organizacje powinny określić, wdrożyć i przetestować procedury zarządzania incydentami służące zapewnieniu ciągłości świadczenia usług i działania systemów w przypadku cyberincydentów.
W planowaniu reakcji i przywracania normalnego stanu należy uwzględnić środki bezpieczeństwa łagodzące skutki określonych ataków na cyberbezpieczeństwo, takie jak:

- *przekierowania ruchu sieciowego do nadmiarowych usług podczas ataków typu „odmowa usługi”;*
- *procedury ręczne umożliwiające działanie z usługami i systemami w trybie pracy podczas awarii;*
- *opracowanie programów ćwiczeń i testów (np. koordynacyjne i techniczne ćwiczenia symulacyjne oraz ćwiczenia reagowania) z myślą o reagowaniu na cyberataki i sytuacje nadzwyczajne, a także w celu oceny środków i procedur bezpieczeństwa, a także odporności organizacji na cyberincydenty;*
- *dostęp do zarchiwizowanych lub zapasowych miejsc przechowywania w przypadku naruszenia integralności i dostępności magazynów danych;*
- *koordynacja i współpraca z krajowymi zespołami CSIRT, (publicznymi i komercyjnymi) zespołami CERT i ośrodkami wymiany i analizy informacji podczas cyberincydentów, koordynacja incydentów i kryzysów na poziomie ogólnoeuropejskim;*
- *wymiana informacji z innymi organizacjami, w tym z dostawcami w łańcuchu dostaw usług w transporcie morskim;*
- *podręczniki dotyczące bezpieczeństwa zawierające szczegółowe procedury zarządzania cyberincydentami oraz przywracania normalnych warunków operacyjnych usług i systemów;*
- *określenie procedur postępowania w przypadku naruszeń ochrony danych, w tym procedur postępowania w przypadku naruszeń ochrony danych mających wpływ na dane osobowe zgodnie z ogólnym rozporządzeniem o ochronie danych (RODO) oraz wszelkimi innymi odpowiednimi rozporządzeniami lub dyrektywami sektorowymi;*
- *zakup cyberubezpieczenia w celu częściowego zrównoważenia ryzyka związanego z poważnymi cyberincydentami;*
- *zawarcie umowy dotyczącej reagowania na incydenty z co najmniej jedną wyspecjalizowaną firmą w celu uzyskania dodatkowych możliwości i wiedzy fachowej;*
- *określenie procedur wymiany informacji o cyberincydentach (w tym o niezgodnościach, wypadkach i sytuacjach niebezpiecznych) z odpowiednimi zainteresowanymi stronami, w tym procedur zgłaszania incydentów zgodnie z dyrektywą dotyczącą cyberbezpieczeństwa (dyrektywa (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii).*

Luksemburg: Urząd Publikacji Unii Europejskiej, 2021

Print ISBN 978-92-76-40467-5 doi:10.2832/68980 MI-05-21-230-PL-C
PDF ISBN 978-92-76-40471-2 doi:10.2832/294700 MI-05-21-230-PL-N