Commissione europea

Kit di strumenti per la cibersicurezza nel settore dei trasporti

INTRODUZIONE

La direzione generale della Mobilità e dei trasporti (DG MOVE) della Commissione europea ha stipulato il contratto per l'elaborazione del presente kit di strumenti con l'intento di accrescere la consapevolezza e la preparazione dei portatori di interessi del settore dei trasporti in materia di minacce informatiche. Il contenuto del presente kit offre indicazioni per comprendere le minacce informatiche e per attenuarne l'impatto, oltre a fornire due percorsi di sensibilizzazione corrispondenti a profili diversi:

- tutto il personale dei trasporti (sono forniti orientamenti e informazioni di carattere generale);

- responsabili decisionali del settore dei trasporti per quanto riguarda la cibersicurezza.

I collegamenti ipertestuali connettono le diverse parti che costituiscono il kit di strumenti per supportarne la navigabilità.

Le pratiche elencate nel presente kit di strumenti sono unicamente di natura consultiva. Ciascuna delle raccomandazioni formulate non è né vincolante né obbligatoria. Inoltre il presente kit di strumenti non riflette le posizioni ufficiali della Commissione europea né ha l'intento di fornire mezzi di rispondenza alla normativa dell'UE, vigente o futura.

Profili di interesse per la sensibilizzazione in materia di cibersicurezza

Profilo I: tutto il personale dei trasporti. Il primo percorso è rivolto a tutto il personale delle organizzazioni del settore trasporti e fornisce informazioni che aiutano a comprendere meglio le più comuni minacce informatiche che prendono di mira i trasporti. Offre inoltre approfondimenti su come affrontare potenziali minacce alla cibersicurezza, ad esempio individuandole, segnalandole e attenuandole grazie all'impiego di buone pratiche di cibersicurezza.

Profilo II: responsabili decisionali per la cibersicurezza dei trasporti. Il secondo percorso riguarda il personale con responsabilità decisionali in merito alla cibersicurezza nelle organizzazioni del settore dei trasporti. Il presente percorso evidenzia le buone pratiche rispondenti alle esigenze dei diversi modi di trasporto. Fornisce, nello specifico, buone pratiche per individuare e rilevare le minacce informatiche emergenti che prendono di mira le organizzazioni dei trasporti e per elaborare le misure di protezione e di risposta.

Commissione europea

Kit di strumenti per la cibersicurezza nel settore dei trasporti

Panorama delle minacce ai trasporti

Minacce informatiche emergenti che interessano differenti modi di trasporto

Profili di interesse per la sensibilizzazione in materia di cibersicurezza

Percorsi di sensibilizzazione alternativi corrispondenti a profili diversi nell'ambito dei trasporti

Commissione europea

Panorama delle minacce ai trasporti

Il panorama delle minacce alla cibersicurezza è dinamico e in continua evoluzione. È possibile nondimeno individuare le minacce informatiche a cui sono esposti tutti i modi di trasporto.

Commissione europea

Gli autori delle minacce

Singoli individui oppure organizzazioni potenzialmente in grado di incidere sulla sicurezza e sulla protezione dei servizi e dei sistemi di trasporto.

Minacce informatiche emergenti

Una selezione di minacce informatiche che possono avere conseguenze per la sicurezza e la protezione dei servizi e dei sistemi di trasporto.

Commissione europea

Gli autori delle minacce

Singoli individui oppure organizzazioni possono, deliberatamente o no, mettere in luce e sfruttare vulnerabilità che possono causare incidenti e influire sui servizi di trasporto, per quanto riguarda, tra l'altro, la loro sicurezza e protezione, nonché le attività, le risorse finanziarie e la reputazione dei servizi stessi.

Gli autori di maggior peso di azioni malevole che prendono intenzionalmente di mira le organizzazioni del settore dei trasporti sono i **criminali informatici**, i **soggetti interni**, gli **Stati nazionali** e i **gruppi sponsorizzati da uno Stato**. Soggetti ostili quali i **criminali informatici** conducono massicce campagne di attacchi e agiscono spesso dietro compenso in denaro.

I **soggetti *interni*** conoscono le singolarità delle organizzazioni per le quali lavorano e sono spesso ben consapevoli delle minime vulnerabilità nella sicurezza. I *soggetti interni* possono essere dipendenti scontenti, fornitori e singoli appaltatori.

Con l'intensificarsi di tensioni geopolitiche, **Stati nazionali** e **gruppi sostenuti da uno Stato** perseguono obiettivi strategici a lungo termine, tentando sovente di nascondersi nei meandri dei sistemi delle organizzazioni per raccogliere informazioni sensibili. Una volta consolidata la loro posizione all'interno dei sistemi, gli autori di attacchi appoggiati da uno Stato cercano di guadagnare una posizione in virtù della quale poter creare il maggior danno possibile.

Gli autori di minacce privi di intenzioni malevole sono soggetti **interni** che possono inconsapevolmente o accidentalmente compiere azioni che comportano eventi di cibersicurezza e, nei casi peggiori, incidenti informatici.

Commissione europea

Minacce informatiche emergenti

Sono numerose le minacce informatiche che prendono di mira i trasporti: **attacchi distribuiti di negazione dei servizi**, **negazione dei servizi**, furto di dati, diffusione di **malware**, **phishing**, manipolazione del software, **accesso non autorizzato**, attacchi distruttivi, falsificazione o aggiramento del processo decisionale dell'operatore della sicurezza, mascheramento dell'identità, abuso dei privilegi di accesso, **ingegneria sociale**, defacing, intercettazioni, uso improprio di risorse e manipolazione dell'hardware. Sulla scorta di una ricerca esaustiva nella documentazione disponibile al pubblico e in base alle interviste di esperti, le minacce informatiche emergenti più pressanti che riguardano i trasporti sono: malware, attacchi (distribuiti) di negazione dei servizi, accesso non autorizzato e furto, manipolazione del software.

Commissione europea

Minaccia n. 1: malware

Software maligno che può colpire singoli individui o organizzazioni nell'ambito di tutti i modi di trasporto.

Minaccia n. 2: attacchi (distribuiti) di negazione dei servizi

Attacchi alla cibersicurezza che impediscono ai singoli o alle organizzazioni di accedere ai servizi e alle risorse.

Minaccia n. 3: accesso non autorizzato e furto

Accesso non autorizzato, appropriazione e sfruttamento indebiti di dati critici.

Minaccia n. 4: manipolazione del software

Attacchi alla cibersicurezza diretti al software allo scopo di modificarne il comportamento e che mettono in atto azioni aggressive specifiche.

Minaccia n. 1: malware

Il malware consiste in un software maligno che può comprendere vari tipi di applicazioni software, come virus, trojan, worm, ransomware, minatori di criptovalute, o qualsiasi software che possa avere un impatto potenzialmente negativo sulle organizzazioni o sui singoli soggetti nell'ambito di tutti i modi di trasporto.

Attenuare la diffusione di malware progettati per danneggiare intenzionalmente i computer, i server, i client o le reti, singolarmente o tutti allo stesso tempo, è tra le principali priorità della cibersicurezza nell'ambito di tutti i modi di trasporto. Un tipico vettore di attacco può operare tramite e-mail di phishing indirizzate ai dipendenti. Altri vettori di attacco possono richiedere l'uso di diverse e sofisticate strategie di ingegneria sociale, come l'inserimento di una chiave USB in una porta libera (ad esempio la ricarica del telefono cellulare). Attivando i collegamenti ipertestuali contenuti nelle e-mail sospette o aprendo i file allegati, l'utente può inconsapevolmente installare dei malware.

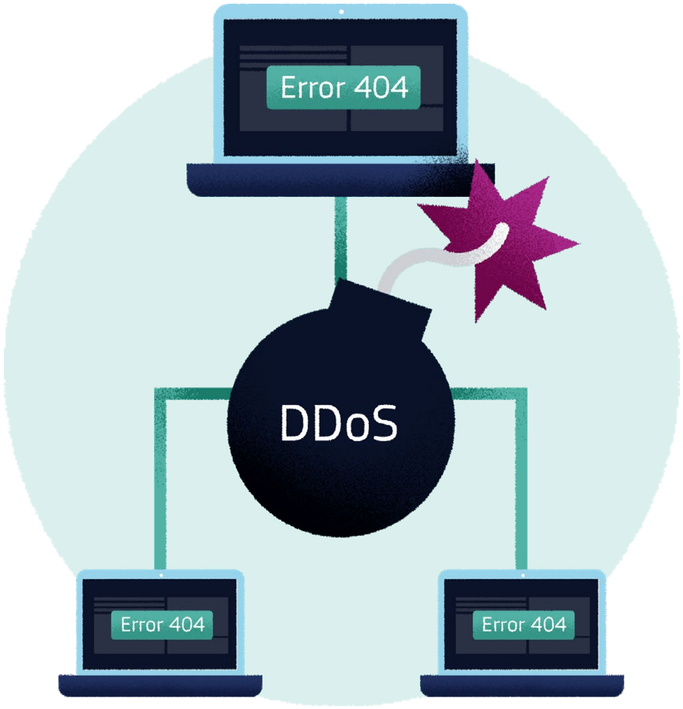
Ad esempio, l'attacco informatico del ransomware WannaCry ha colpito più di 150 paesi, infestando oltre 230 000 sistemi. Tale ransomware viene solitamente diffuso attraverso e-mail di phishing contenenti allegati o collegamenti ipertestuali malevoli. Questo tipo di attacco sfrutta in modo malevolo l'ingegneria sociale per indurre gli utenti del sistema a installare (o ad attivare) uno specifico malware.

Minaccia n. 2: attacchi (distribuiti) di negazione del servizio

Gli attacchi distribuiti di negazione del servizio (*Distributed Denial of Service*, DDoS) e gli attacchi di negazione del servizio (*Denial of Service*, DoS) danneggiano la disponibilità di dati, servizi, sistemi e altre risorse e la relativa accessibilità. Gli attacchi di questo tipo possono differire in base alla durata e possono essere diretti contemporaneamente a più di un servizio o sistema. Gli attacchi DDoS adottano sistemi (o canali di attacco) multipli, allo scopo di sovraccaricare di richieste i servizi o i sistemi presi di mira. Gli attacchi riusciti compromettono la capacità di un servizio o di un sistema di gestire un volume imprevisto di richieste, il che si traduce nella negazione dell'accesso ai servizi e alle risorse.

Occorre osservare che, una volta colpiti, i servizi e i sistemi appartenenti alle organizzazioni dei trasporti possono essere sfruttati per condurre attacchi DDoS e DoS nei confronti di specifici sistemi in esercizio o anche di altre organizzazioni.

Possono ad esempio essere presi di mira sistemi informativi aziendali (come computer e dispositivi personali) per ottenere l'accesso alle tecnologie operative, che potrebbero essere connesse alla rete Internet o ad altre reti ai fini del trasferimento di dati operativi. Le connessioni tra reti e sistemi diversi (quali ad esempio le reti aziendali, le tecnologie operative e gli accessi per la manutenzione da remoto) possono costituire le vulnerabilità sfruttabili per condurre attacchi DDoS o DoS a servizi e sistemi di trasporto critici. Gli attacchi DDoS e DoS possono per esempio sfruttare protocolli comuni di rete e di comunicazione come il *Web Services Dynamic Discovery* (*WS-Discovery*), che i dispositivi IoT possono utilizzare per scoprire in modo automatico tutti i nodi delle reti in area locale (LAN). Se i dispositivi IoT presentano delle vulnerabilità, gli autori di attacchi possono sfruttarle per scoprire altri dispositivi connessi e per condurre attacchi DDoS o DoS.



Minaccia n. 3: accesso non autorizzato e furto

L'intenzione degli autori di minacce può essere quella di ottenere un accesso logico o fisico non autorizzato a una rete, un sistema o un'applicazione, oppure a determinati dati o ad altra risorsa allo scopo di condurre attività malevole, tra cui il furto di dati o risorse sensibili (comprese le risorse fisiche).
Le minacce di accesso non autorizzato e di furto interessano risorse proprietarie e riservate (tra cui dati di identità personale, credenziali di account con privilegi, sistemi e altri tipi di informazioni proprietarie e riservate). Tali minacce possono sfruttare le vulnerabilità dei sistemi nonché singoli individui inconsapevoli che rivelano dati sensibili come le proprie credenziali (ad esempio dati di login, password, ecc.) o dati personali (ad esempio, indirizzo e-mail, numero di identificazione personale, ecc.).

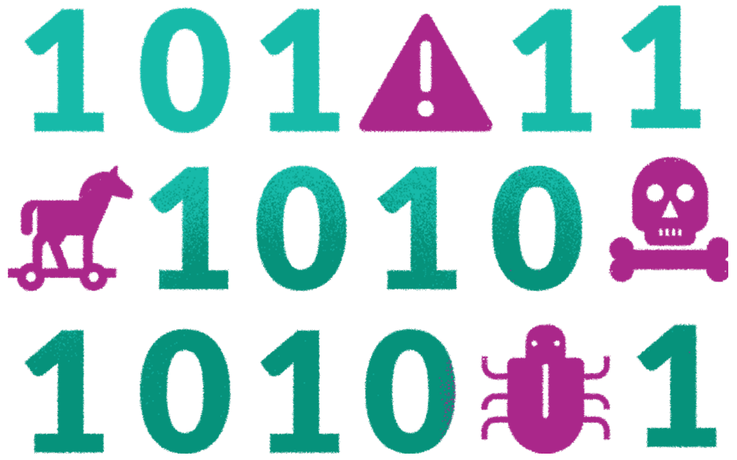
Per quanto riguarda l'accesso non autorizzato, il furto d'identità è l'uso illecito di dati personali o di identificatori unici al fine di impersonare singole persone oppure servizi e sistemi per ottenere l'accesso a risorse private o proprietarie (incluse, per esempio, risorse finanziarie e fisiche). Tali minacce alla cibersicurezza possono riguardare inoltre risorse fisiche nell'ambito di tutti i modi di trasporto.

Commissione europea

Minaccia n. 4: manipolazione del software

Configurazioni errate e manipolazioni del software e dei sistemi correlati o di loro componenti possono avere un'incidenza diretta sulla posizione di sicurezza dei servizi e dei sistemi di trasporto.
Gli attacchi alla cibersicurezza che sfruttano le manipolazioni del software modificano le impostazioni dell'applicazione o intervengono sull'integrità dei dati con l'intento di alterare il comportamento di sistemi e servizi. Gli autori degli attacchi possono manipolare intenzionalmente il software (o parte di esso) al fine di ottenere dei vantaggi in merito a risorse sensibili (ad esempio ottenere un accesso non autorizzato, impedire il legittimo accesso di singoli individui o di sistemi alle risorse richieste, raccogliere informazioni sensibili, modificare il comportamento di talune funzioni, ecc.).

Gli autori degli attacchi possono ad esempio minacciare i canali di comunicazione dei produttori allo scopo di caricare aggiornamenti maligni del software su servizi e sistemi (ivi incluse le tecnologie operative). L'autore di una minaccia utilizza credenziali di autorizzazione compromesse per accedere a un'interfaccia di rete protetta per la manutenzione remota con l'intento di installare un software manipolato e compromettere ulteriormente altri servizi e sistemi accessibili. Detto autore installa software manipolato che compromette in misura ancora maggiore i servizi e i sistemi presi di mira o attacca altri servizi o sistemi connessi.



Commissione europea

Profili di interesse per la sensibilizzazione in materia di cibersicurezza

1

Profilo I: tutto il personale dei trasporti

Il primo percorso è rivolto a tutto il personale delle organizzazioni del settore trasporti, dal personale operativo al personale amministrativo. Il percorso fornisce orientamenti per una maggiore comprensione e consapevolezza delle più comuni minacce informatiche, offrendo inoltre approfondimenti su come affrontare potenziali minacce alla cibersicurezza, ad esempio individuandole, segnalandole e attenuandole. Questo percorso è comune a tutti i modi di trasporto.

2

Profilo II: responsabili decisionali per la cibersicurezza dei trasporti

Il secondo percorso riguarda il personale con responsabilità decisionali in materia di cibersicurezza nelle organizzazioni del settore dei trasporti. Tale percorso fornisce buone pratiche rispondenti alle esigenze dei diversi modi di trasporto al fine di individuare e rilevare le minacce informatiche emergenti che prendono di mira le organizzazioni dei trasporti e per elaborare le misure di protezione e risposta.

Commissione europea

Profilo I: tutto il personale dei trasporti

La presente sezione riguarda tutto il personale delle organizzazioni del settore trasporti, dal personale operativo all'amministrazione, e fornisce orientamenti per una maggiore comprensione e consapevolezza delle più comuni minacce informatiche, offrendo inoltre approfondimenti su come affrontare potenziali minacce alla cibersicurezza, ad esempio individuandole, segnalandole e attenuandole.

In questa sezione sono contenuti consigli utili e pratiche raccomandate che hanno rilevanza per **tutti i modi di trasporto**.

Buone pratiche contro i malware

Ciascuno può contribuire a tutelare la propria organizzazione seguendo buone pratiche atte a **individuare e prevenire la diffusione di malware**, come quelle indicate di seguito.

- ***Seguire politiche di sicurezza*** *quali, tra le altre: effettuare la scansione dei file e dei supporti di conservazione per rilevare la presenza di virus; evitare di aprire e di inviare via e-mail tipi specifici di file (ad esempio file eseguibili con estensioni .exe, .bat, .com, ecc.); installare solo software autorizzato; assicurarsi che il software (incluso l'antivirus) sia aggiornato e funzioni correttamente.*

- *Eseguire regolarmente il* ***backup dei propri dati*** *facendo ricorso a dispositivi o servizi sicuri (e autorizzati) di conservazione dei dati, che dovrebbero supportare meccanismi di crittografia a protezione dei dati a riposo ed essere disponibili per le procedure di ripristino degli stessi dati.*

- *Proteggere con* ***misure di sicurezza*** *adeguate (ad esempio password, crittografia, ecc.) tutti i sistemi, compresi i dispositivi mobili e gli endpoint, oltre a non dimenticare di bloccare in modo sicuro (fisicamente e digitalmente) tutti i sistemi quando rimangono incustoditi.*

- *Evitare di aprire allegati e di attivare collegamenti ipertestuali contenuti in e-mail inattese e in finestre di pop-up del browser web sospette che presentano un corpo di testo insolito o che provengono da mittenti e domini Internet sconosciuti.*

- *Non inserire nel proprio computer* ***dispositivi rimovibili non affidabili o sconosciuti****, come chiavette USB, dischi rigidi e altri dispositivi di conservazione.*

- *Evitare di disabilitare le misure di sicurezza contro i malware (ad esempio, software antivirus, software di filtraggio dei contenuti, firewall, ecc.).*

- ***Aggiornare regolarmente il software installato*** *alle più recenti versioni disponibili (che i responsabili della sicurezza informatica o gli amministratori di sistema possono rilasciare tramite aggiornamenti periodici).*

- *Non usare credenziali e account privilegiati (per esempio a livello di amministratore) per attività e operazioni ordinarie.*

- *Segnalare ai responsabili della sicurezza informatica o agli amministratori di sistema ogni e-mail sospetta o qualsiasi comportamento imprevisto del sistema.*

- *Prestare attenzione alla sicurezza informatica durante il lavoro ordinario quotidiano in modo da riconoscere i problemi a essa legati e reagire di conseguenza.*

Buone pratiche contro gli attacchi (distribuiti) di negazione del servizio

È possibile contribuire alla tutela della propria organizzazione individuando attacchi **distribuiti di negazione del servizio (DDoS)** e attacchi di **negazione del servizio (DoS)**.
È opportuno contattare immediatamente i responsabili della sicurezza e il personale IT dell'organizzazione qualora sia rilevato o constatato uno dei seguenti indicatori di attacchi DDoS e DoS potenzialmente in corso nei confronti dei propri servizi o sistemi:

- *richieste in numero crescente che consumano la capacità della rete (evento percepito in termini di lentezza dei servizi e delle risposte) con conseguenti disfunzioni del servizio o del sistema dovute al sovraccarico;*

- *incremento della domanda di utilizzo delle risorse di memoria senza una ragione evidente;*

- ***comportamenti imprevisti di servizi e sistemi**, crash frequenti e insoliti messaggi di errore causati da consumo malevolo di risorse computazionali o connessioni di rete;*

- ***prestazioni ridotte** dei dispositivi, tempi lunghi per l'esecuzione di compiti banali e attività evidenti (ad esempio, ventola rumorosa mentre il funzionamento dei dispositivi è lento);*

- ***connessioni Internet impreviste o perdita delle connessioni** a servizi e sistemi;*

- *lievi cambiamenti comportamentali dei comandi operativi o delle tecnologie di funzionamento con conseguenti danni fisici;*

- *negazione degli accessi agli account privilegiati o amministrativi intesa a bloccare il recupero tramite procedure di risposta agli incidenti.*

Buone pratiche contro l'accesso non autorizzato e il furto

Per prevenire attacchi che comportano l'accesso non autorizzato e il furto occorre attenersi a principi quali "la necessità di conoscere" e "la sicurezza e la privacy per impostazione predefinita", i quali evidenziano come l'accesso alle risorse sensibili e riservate (tra cui i dati personali e sensibili, i sistemi di trasporto, ecc.) dovrebbe essere concesso solo a coloro che ne hanno diritto per svolgere i propri compiti. È possibile contribuire a tutelare la propria organizzazione seguendo buone pratiche atte a individuare e prevenire l'accesso non autorizzato e il furto, come ad esempio:

- *seguire le politiche di sicurezza dell'organizzazione;*
- *evitare la condivisione e la pubblicazione online di credenziali e dati personali, comprese le immagini che possono contenere tali informazioni;*
- *non utilizzare o trasmettere credenziali e dati personali (e altri dati sensibili) su reti, dispositivi o servizi web inaffidabili e non protetti (ad esempio siti web che utilizzano protocolli o indirizzi non criptati, come http:// invece di protocolli o indirizzi sicuri quali https://);*
- ***non rivelare mai a nessuno le proprie credenziali** (ad esempio login e password) nemmeno via e-mail o per telefono;*
- *proteggere i dati sensibili digitati su tastiera o visualizzati a schermo (anche sui dispositivi mobili) da soggetti non autorizzati, installare filtri privacy per schermi, evitare di lavorare da luoghi pubblici con dispositivi privati e di lasciare qualsiasi dispositivo sprovvisto di blocco e incustodito;*
- ***usare password complesse** (ad esempio password sufficientemente lunghe, che combinano caratteri alfanumerici e caratteri speciali) conformi alle pertinenti politiche di sicurezza dell'organizzazione per impedire l'accesso non autorizzato;*
- ***modificare le password predefinite** dei sistemi e dei dispositivi connessi (ad esempio stampanti, router, videocamere, sistemi Smart Lock, ecc.);*
- *evitare di usare le stesse credenziali (ad esempio login e password) per più servizi e sistemi e non usare le medesime credenziali per servizi e sistemi che richiedono account privilegiati;*
- *inviare le password e le chiavi per attività di trasferimento di file protetti (ad esempio archivi in formato ZIP) solamente tramite un canale fuori banda (ad esempio SMS via GSM e chiamata telefonica) e mai tramite e-mail;*
- ***attivare l'autenticazione a due fattori (2FA)** o l'autenticazione a più fattori (MFA), se possibile.*

Buone pratiche contro la manipolazione del software

È possibile contribuire alla tutela della propria organizzazione seguendo buone pratiche volte a individuare e prevenire la manipolazione del software, come ad esempio:

- *evitare l'installazione di software inaffidabile su sistemi e dispositivi (ivi inclusi personal computer, server, periferiche, dispositivi di rete, smartphone, ecc.);*
- *installare sempre software e aggiornamenti da fonti e siti web ufficiali (ad esempio i produttori, gli archivi aziendali, ecc.);*
- *non scaricare software e applicazioni, né qualsivoglia file, da fonti illegali;*
- *disinstallare il software non indispensabile o non utilizzato di recente e disabilitare le connessioni superflue (ad esempio i protocolli e i servizi di rete) tra cui l'accesso a servizi remoti (ad esempio i servizi di conservazione su cloud);*
- *effettuare la scansione di ogni software o dispositivo di conservazione ricorrendo a un programma antivirus affidabile e aggiornato;*
- *scaricare software industriale sicuro (ad esempio aggiornamenti, patch, nuovi prodotti, ecc.) da fornitori fidati, verificandolo su un apposito dispositivo isolato ("white station");*
- *provvedere all'aggiornamento di tutto il software installato rispettando le politiche e le pratiche in vigore nell'organizzazione.*

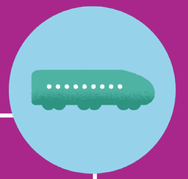
Commissione europea

Profilo II: responsabili decisionali per la cibersicurezza dei trasporti

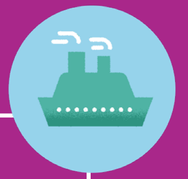
Questa parte è rivolta al personale che ha responsabilità decisionali in materia di cibersicurezza nelle organizzazioni dei trasporti. Il presente percorso evidenzia le buone pratiche rispondenti alle esigenze dei diversi modi di trasporto. Sono fornite, nello specifico, buone pratiche per individuare e rilevare le minacce informatiche emergenti, nonché per elaborare le misure di protezione e di risposta.

Commissione europea

Buone pratiche di cibersicurezza applicabili al trasporto aereo



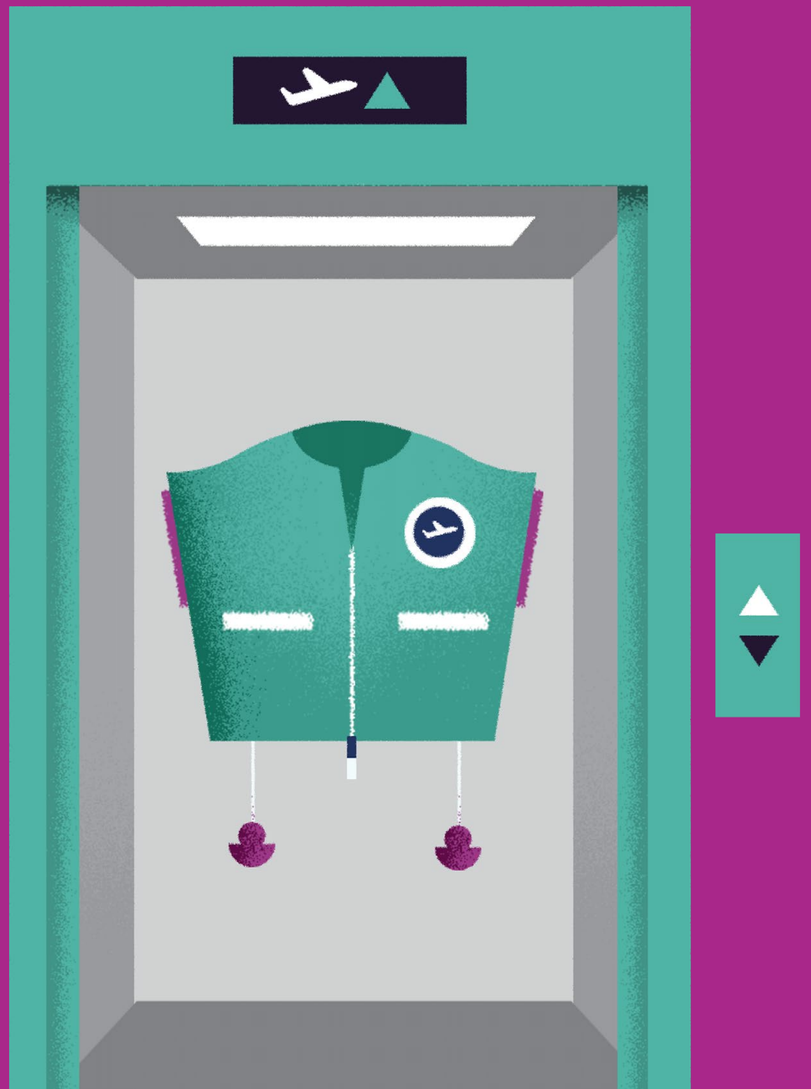
Buone pratiche di cibersicurezza applicabili al trasporto terrestre



Buone pratiche di cibersicurezza applicabili al trasporto marittimo

Commissione europea

Buone pratiche e misure di sicurezza applicabili al trasporto aereo



Governance

Le organizzazioni del trasporto aereo devono comprendere in maniera chiara le minacce emergenti per elaborare le politiche e i processi di gestione intesi a regolare i propri metodi volti ad accrescere la cibersicurezza dei servizi e dei sistemi operativi, tra cui le tecnologie dell'informazione (IT) e le tecnologie operative (OT).

Le buone pratiche per le organizzazioni di qualsiasi dimensione prevedono quanto indicato di seguito.

- Garantire che i problemi legati alla cibersicurezza siano segnalati dagli alti dirigenti agli amministratori delegati e ai consigli direttivi, i quali possono assumere decisioni informate in merito all'assegnazione delle risorse.

- Nominare in un ruolo di primo piano un responsabile della cibersicurezza e della sicurezza fisica, incaricato della gestione globale della sicurezza delle IT e delle OT, senza tuttavia alcun coinvolgimento a livello operativo per prevenire conflitti di interesse.

- Definire chiaramente le responsabilità, le competenze, le autorizzazioni e i ruoli correlati alla sicurezza informatica, oltre a darne comunicazione e a concordarli con il personale interessato, in particolare per quanto riguarda i membri delle squadre di pronto intervento informatico (*Computer Emergency Response Teams*, CERT);

- Garantire la governance della cibersicurezza lungo l'intera catena di fornitura dei servizi per la sicurezza, comprese le interfacce fisiche e digitali, dai produttori e installatori di tecnologia ai garanti della sicurezza.

- Concordare le attività e i controlli, comprese le responsabilità condivise, per la gestione dei rischi connessi alla cibersicurezza, oltre a garantire che tali responsabilità coprano tutto il ciclo di vita delle soluzioni e dei servizi relativi alla sicurezza (ad esempio in virtù di contratti di servizi).

- Definire i meccanismi di governance (ad esempio le politiche) per conformarsi agli obblighi di cui ai regolamenti e alle direttive pertinenti, quali, ad esempio, il regolamento (UE) 2018/1139 recante norme comuni nel settore dell'aviazione civile e il regolamento di esecuzione (UE) 2017/373 della Commissione che stabilisce i requisiti comuni per i fornitori di servizi di gestione del traffico aereo e di navigazione aerea e di altre funzioni della rete di gestione del traffico aereo e per la loro sorveglianza, nonché la direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva NIS).

Esempi di servizi e di sistemi relativi al trasporto aereo: sono esempi di IT le tecnologie accessibili ai dipendenti (ad esempio i personal computer, i telefoni cellulari, le periferiche per ufficio, ecc.) e ai passeggeri (come i router e le connessioni delle reti Wi-Fi pubbliche, ecc.). Sono esempi di OT: i sistemi per il controllo di supervisione e acquisizione dati (SCADA), i sistemi di riscaldamento, ventilazione e condizionamento dell'aria (HVAC), i punti di controllo di sicurezza dei bagagli a mano, i sistemi di gestione dei bagagli, il controllo dell'accesso, il monitoraggio, la sorveglianza, la risposta alle emergenze, la tecnologia di screening, i sistemi di controllo dell'illuminazione aeroportuale, i sistemi e i sensori radar, i sistemi di posizionamento globale (GPS), i sistemi di gestione del traffico aereo (ATM), i sistemi di comunicazione, navigazione e sorveglianza (CNS), i sistemi di informazione aeronautica, i sistemi meteorologici, i sistemi dei centri operativi di sicurezza, i sistemi di bordo delle compagnie aeree, e altri.

Identificare le minacce alla cibersicurezza

La gestione del rischio: le organizzazioni del settore aeronautico devono adottare le misure necessarie per identificare, valutare e comprendere i rischi connessi alla cibersicurezza dei sistemi di rete e dell'informazione che sostengono l'operatività di funzioni essenziali.

Ciò comporta un approccio organizzativo globale alla gestione del rischio, che richiede quanto riportato in appresso.

- *Garantire una chiara visione d'insieme dei vari sistemi hardware e software impiegati per la fornitura di servizi di tipo diverso. Nell'ambito del trasporto aereo, tali sistemi implicano l'uso delle tecnologie dell'informazione (IT) e delle tecnologie operative (OT).*

- *Eseguire valutazioni dei **rischi connessi alla cibersicurezza** che tengano conto delle minacce emergenti, delle vulnerabilità note e dei dati operativi in relazione ai sistemi in questione. Organizzazioni quali le squadre di pronto intervento informatico della rete europea per la gestione del traffico aereo (European Air Traffic Management Computer Emergency Response Team, EATM-CERT) e il centro di analisi e condivisione delle informazioni aeronautiche (Aviation Information Sharing and Analysis Centre, A-ISAC) possono fornire elementi di approfondimento nel campo delle minacce che prendono di mira il trasporto aereo.*

- *Garantire che le valutazioni dei rischi riguardino anche il rischio connesso alle attività quotidiane del personale (ad esempio l'uso dei social media e dei dispositivi personali, il trattamento dei dati, la condivisione delle informazioni, ecc.).*

- *Individuare e porre in atto misure di trattamento del rischio e piani per attenuare i rischi connessi alla cibersicurezza.*

- *Provvedere all'attuazione di un **sistema di gestione della sicurezza delle informazioni** (Information Security Management System, ISMS) e di un **sistema di gestione per la protezione dei dati personali** (Privacy Information Management System, PIMS) allineati agli altri sistemi di gestione. Tali sistemi di gestione (ISMS e PIMS) implicano l'attuazione di controlli sulla sicurezza (nonché su protezione dei dati e privacy) per attenuare e prevenire minacce emergenti contro la sicurezza dei servizi e dei sistemi del trasporto aereo (ivi compresi i relativi dati).*

- *Tenere conto di tutti i vincoli concernenti **la gestione dei beni e la pianificazione delle risorse** (ossia i vincoli che possono influenzare la consegna, la manutenzione e il sostegno di sistemi critici per l'operatività di funzioni essenziali nell'ambito del trasporto aereo).*

Esempi di quadri per la gestione del rischio: esistono diversi quadri che possono orientare e sostenere un approccio mirato per la gestione del rischio nel settore del trasporto aereo, quali ad esempio le norme della famiglia ISO/IEC 27000, il quadro per la cibersicurezza del *National Institute of Standards and Technology* (NIST), il quadro MITRE ATT&CK, la norma BSI IT-Grundschutz, ecc. Organizzazioni internazionali come IATA e ICAO forniscono orientamenti per la valutazione dei rischi connessi alla cibersicurezza. L'Agenzia dell'Unione europea per la cibersicurezza (ENISA), l'Agenzia dell'Unione europea per la sicurezza aerea (AESA), l'Eurocontrol e l'associazione *Airports Council International* (ACI), tra gli altri, danno risalto a buone pratiche per garantire la sicurezza degli aeroporti, dei gestori del traffico aereo e delle altre organizzazioni del settore aeronautico. L'impresa comune SESAR coordina e concentra tutte le attività di ricerca e sviluppo dell'UE sulla gestione del traffico aereo, anche per quanto concerne gli aspetti della protezione e della sicurezza.

Protezione dalle minacce alla cibersicurezza

È opportuno che le organizzazioni del settore del trasporto aereo attuino misure di sicurezza adeguate e proporzionate per salvaguardare dagli attacchi informatici le proprie reti e i propri sistemi informativi, tra cui le tecnologie dell'informazione (IT) e le tecnologie operative (OT). Tali misure di sicurezza comprendono quanto indicato di seguito.

- ***Politiche e processi in materia di sicurezza:*** *elaborare, attuare, comunicare e applicare le politiche e le procedure adeguate a delineare un metodo globale per garantire la sicurezza dei sistemi e dei dati che sostengono l'operatività di funzioni essenziali nel trasporto aereo. Tali politiche per la sicurezza (ad esempio le strategie riguardanti le password e la conservazione) e procedure di sicurezza dovrebbero inoltre contemplare la gestione delle patch e delle vulnerabilità dei sistemi hardware e software (comprese le IT e le OT), la gestione degli incidenti e la protezione del sistema e della rete.*

- ***Gestione dell'accesso e dell'identità:*** *comprendere, documentare e gestire l'accesso alle reti e ai sistemi informativi (comprese le IT e le OT) che sostengono l'operatività di funzioni essenziali nell'ambito del trasporto aereo. Gli utenti (o le funzioni automatizzate) che possono accedere ai dati e ai sistemi sono opportunamente verificati, autenticati e autorizzati, tenendo conto anche delle differenze di ruolo e di responsabilità tra gli account regolari e gli account privilegiati.*

- ***Sicurezza dei dati e dei sistemi:*** *proteggere i dati (conservati e trasmessi elettronicamente), le reti e i sistemi informativi critici (incluse le IT e le OT) dagli attacchi informatici. Tenuto conto di un approccio orientato al rischio, è opportuno che le organizzazioni attuino misure di sicurezza per ridurre efficacemente le possibilità per gli autori degli attacchi di compromettere i dati, le reti e i sistemi. Tali misure di sicurezza dovrebbero prevedere inoltre l'adozione di protocolli di crittografia e di comunicazione sicuri per salvaguardare i dati a riposo e in transito dalle minacce informatiche derivanti da attacchi del tipo "man-in-the-middle". Inoltre è necessario combinare tali misure con misure di sicurezza fisica per tutelare l'accesso ai sistemi (ad esempio, i sistemi dovrebbero essere situati in stanze chiuse con accesso limitato).*

- ***La resilienza delle reti e dei sistemi:*** *costruire la resilienza delle reti e dei sistemi (incluse le IT e le OT) progettando e realizzando reti e sistemi, come pure le relative procedure operative, in modo che possano resistere all'impatto degli attacchi informatici e attenuarne gli effetti. Soluzioni per la progettazione e la realizzazione che migliorano la resilienza sono ad esempio: la verifica formale delle funzioni essenziali, la ridondanza dei sistemi e delle reti, la segregazione delle reti (in particolare la segregazione delle IT e delle OT), le misure di sicurezza a più livelli e molte altre. Occorre osservare che sotto il profilo della sicurezza delle informazioni i domini di protezione che applicano regole di segregazione di reti e sistemi possono fornire adeguate soluzioni di sicurezza. È tuttavia possibile che in base a talune esigenze operative dei sistemi (ad esempio le attività di manutenzione, i trasferimenti di dati, ecc.) sia necessario eludere o connettere domini di protezione diversi (ad esempio le reti e i sistemi segregati), ivi compresa la connessione delle IT e delle OT.*

Rilevare le minacce alla cibersicurezza

È opportuno che le organizzazioni garantiscano che le misure di sicurezza restino efficaci e rilevino ogni evento di cibersicurezza che influisce o può influire sui controlli di sicurezza così come sui servizi e sui sistemi essenziali. Le opportune misure di sicurezza atte a rilevare le minacce alla cibersicurezza sono indicate in appresso.

■ ***Monitoraggio della sicurezza:*** *monitorare lo stato della sicurezza delle reti e dei sistemi informativi, tra cui le tecnologie dell'informazione (IT) e le tecnologie operative (OT), che sostengono l'operatività di funzioni essenziali nei servizi di trasporto aereo. Per contribuire adeguatamente al monitoraggio della sicurezza, occorre prendere in esame, ad esempio, i dati dei file seguenti:*

- *log di sicurezza;*
- *log del rilevamento di virus;*
- *log delle intrusioni;*
- *log di identificazione, autenticazione e autorizzazione;*
- *log di sistema e dei servizi;*
- *log del traffico di rete;*
- *log di trattamento dei dati.*

■ ***Individuazione di eventi legati alla sicurezza:*** *rilevare attività malevole (cioè eventi legati alla sicurezza) che incidono o possono incidere sulla sicurezza delle reti e dei sistemi informativi (comprese le IT e le OT) che sostengono l'operatività di funzioni essenziali nei servizi di trasporto aereo.*

Tali misure possono richiedere l'adozione di tecnologie specifiche (ad esempio il sistema di gestione delle informazioni e degli eventi di sicurezza, il sistema di rilevamento delle intrusioni, il sistema di prevenzione delle intrusioni, ecc.) e la creazione di un centro operativo per la sicurezza o di un mezzo analogo, vale a dire lo sviluppo di strumenti per rilevare e analizzare gli attacchi informatici, nonché per elaborare le relative risposte e le azioni di recupero, a livello locale.

I gruppi nazionali di intervento per la sicurezza informatica in caso di incidente (CSIRT), le squadre di pronto intervento informatico (CERT) di settore (ad esempio l'EATM-CERT di EUROCONTROL), le CERT commerciali delle compagnie aeree e il centro di analisi e condivisione delle informazioni aeronautiche (A-ISAC) possono fornire informazioni in materia di minacce informatiche quale contributo alle attività di monitoraggio e rilevamento ai fini della sicurezza.

Commissione europea

Pianificazione della risposta e del recupero

È opportuno che le organizzazioni definiscano, applichino e testino procedure di gestione degli incidenti intese a garantire la continuità operativa dei servizi e dei sistemi nell'eventualità di incidenti di cibersicurezza. Le misure di attenuazione hanno lo scopo di ridurre o limitare l'impatto degli incidenti informatici.

È opportuno che la pianificazione della risposta e del recupero preveda l'adozione di misure di sicurezza volte ad attenuare l'impatto di specifici attacchi alla cibersicurezza, come le misure seguenti:

- *il coordinamento e la cooperazione con i CSIRT nazionali, con le CERT (pubbliche e commerciali) e con i centri di condivisione e analisi delle informazioni (ISAC); il coordinamento degli incidenti e delle crisi a livello paneuropeo;*

- *la condivisione delle informazioni con altre organizzazioni, ivi inclusi i fornitori nella catena di prestazione dei servizi di trasporto aereo;*

- ***esercitazioni in materia di attacchi informatici** (simulazioni a tavolino sul coordinamento e sugli aspetti tecnici) da effettuarsi periodicamente per valutare le misure e le procedure di sicurezza nonché la resilienza delle organizzazioni nel far fronte a incidenti informatici;*

- *l'accesso a spazi di conservazione di archivio o di backup in caso di compromissione dell'integrità e della disponibilità degli archivi di dati;*

- *l'impiego di **protocolli per la sicurezza** che prevedano procedure dettagliate per gestire gli incidenti di cibersicurezza e per ripristinare le normali condizioni operative di servizi e sistemi;*

- *azioni di reindirizzamento del traffico di rete a servizi ridondanti durante gli attacchi di negazione del servizio;*

- *procedure manuali per operare con servizi e sistemi le cui modalità operative si sono degradate;*

- *la definizione di procedure per affrontare i casi di violazione dei dati, comprese le procedure per far fronte alle violazioni dei dati personali in conformità del regolamento generale sulla protezione dei dati e di ogni altro regolamento o altra direttiva settoriale pertinente;*

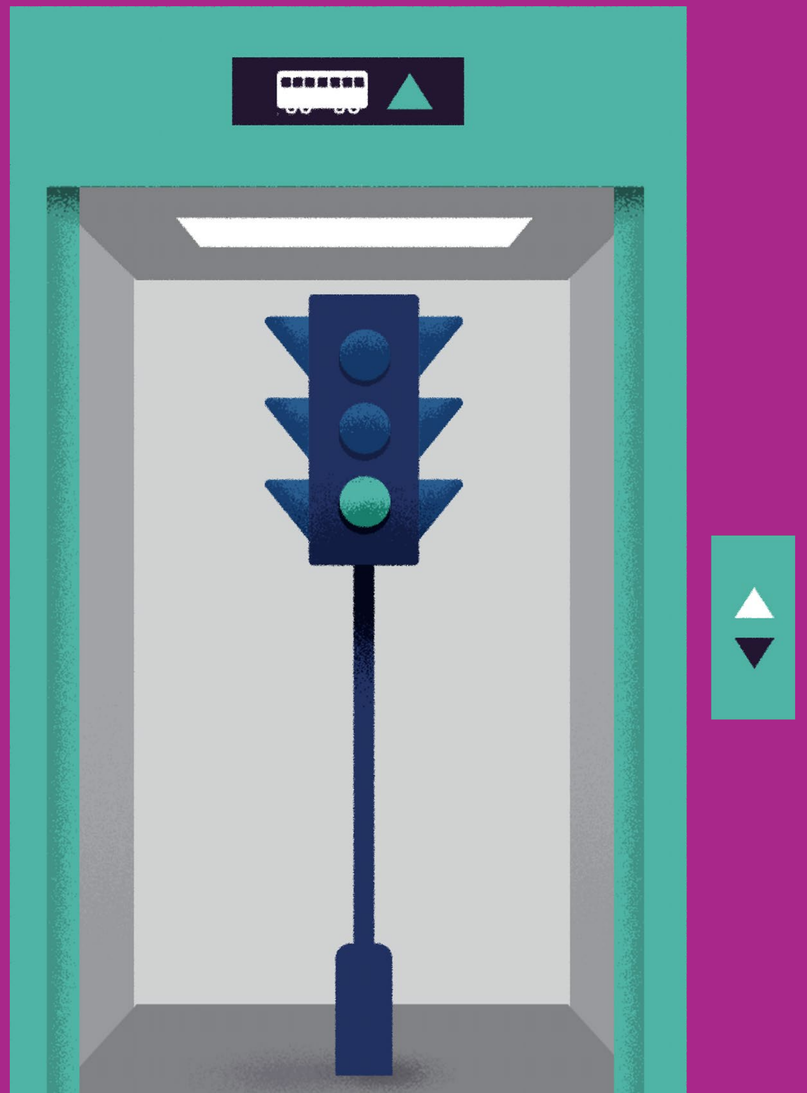
- *la sottoscrizione di un'**assicurazione informatica** per coprire parzialmente il rischio associato agli incidenti gravi di cibersicurezza;*

- *la sottoscrizione con modello "retainer" di contratti per la fornitura di servizi di risposta agli incidenti presso una o più ditte specializzate, onde disporre di ulteriori capacità e competenze;*

- *l'elaborazione di procedure per la condivisione delle **informazioni sugli incidenti di cibersicurezza** con le parti interessate pertinenti, che comprendano le procedure di notifica degli incidenti ai sensi della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva NIS).*

Commissione europea

Buone pratiche e misure di sicurezza applicabili al settore del trasporto terrestre



Commissione europea

Governance

Le organizzazioni del trasporto terrestre devono comprendere in maniera chiara le minacce emergenti per elaborare le politiche e i processi di gestione intesi a regolare i propri metodi volti ad accrescere la cibersicurezza dei servizi e dei sistemi operativi, tra cui le tecnologie dell'informazione (IT) e le tecnologie operative (OT).

Le buone pratiche per le organizzazioni di qualsiasi dimensione prevedono quanto indicato di seguito.

- *Garantire che i problemi legati alla cibersicurezza siano segnalati dagli alti dirigenti agli amministratori delegati e ai consigli direttivi, i quali possono assumere decisioni informate in merito all'assegnazione delle risorse.*

- *Nominare in un ruolo di primo piano un responsabile della cibersicurezza e della sicurezza fisica, incaricato della gestione globale della sicurezza delle IT e delle OT, senza tuttavia alcun coinvolgimento a livello operativo per prevenire conflitti di interesse.*

- *Definire chiaramente le responsabilità, le competenze, le autorizzazioni e i ruoli correlati alla sicurezza informatica, oltre a darne comunicazione e a concordarli con il personale interessato, il che è necessario, in particolare, nei confronti dei membri delle squadre di pronto intervento informatico (CERT).*

- *Garantire la governance della cibersicurezza lungo l'intera catena di fornitura dei servizi per la sicurezza, comprese le interfacce fisiche e digitali, dai produttori e installatori di tecnologia ai garanti della sicurezza.*

- *Concordare le attività e i controlli, comprese le responsabilità condivise, per la gestione dei rischi connessi alla cibersicurezza, oltre a garantire che tali responsabilità coprano tutto il ciclo di vita delle soluzioni e dei servizi relativi alla sicurezza (ad esempio in virtù di contratti di servizi).*

- *Definire i meccanismi di governance (ad esempio le politiche) per conformarsi agli obblighi di cui ai regolamenti e alle direttive pertinenti. Ciò comprende un'ampia serie di politiche che contemplano i modi specifici di trasporto nonché diverse tipologie di portatori di interessi (tra cui ad esempio i produttori di veicoli e sistemi ferroviari) e la direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva NIS).*

Esempi di servizi e di sistemi relativi al trasporto terrestre: sono esempi di IT le tecnologie accessibili ai dipendenti (ad esempio i personal computer, i telefoni cellulari, le periferiche per ufficio, ecc.) e ai passeggeri (come i router e le connessioni delle reti Wi-Fi pubbliche, ecc.). Sono esempi di OT i sistemi per il controllo di supervisione e acquisizione dati (SCADA), i sistemi di riscaldamento, ventilazione e condizionamento dell'aria (HVAC), i sistemi di posizionamento globale (GPS), il controllo dell'accesso, il monitoraggio, la sorveglianza, la risposta alle emergenze, la tecnologia di screening. Sistemi specifici del trasporto ferroviario sono, ad esempio: i sistemi operativi (di controllo-comando) che comprendono i sistemi di segnalamento, il sistema europeo di gestione del traffico ferroviario (ERTMS), i sistemi di bordo, i sistemi di manutenzione, e altri.

Identificare le minacce alla cibersicurezza

La gestione del rischio: le organizzazioni del settore del trasporto terrestre devono adottare le misure necessarie per identificare, valutare e comprendere i rischi connessi alla cibersicurezza dei sistemi di rete e dell'informazione che sostengono l'operatività di funzioni essenziali. Ciò comporta un approccio organizzativo globale alla gestione del rischio, che richiede quanto riportato in appresso.

- *Garantire una chiara visione d'insieme dei vari sistemi hardware e software impiegati per la fornitura di servizi di tipo diverso. Nell'ambito del trasporto terrestre tali sistemi implicano l'uso delle tecnologie dell'informazione (IT) e delle tecnologie operative (OT).*

- *Eseguire valutazioni dei **rischi connessi alla cibersicurezza** che tengano conto delle minacce emergenti, delle vulnerabilità note e dei dati operativi in relazione ai sistemi in questione. Esempi di sistemi nei modi di trasporto terrestre sono: i sistemi di pagamento, i sistemi di rete e di comunicazione (come Internet, le comunicazioni radio, la rete Wi-Fi), le apparecchiature di bordo, i centri di controllo operativo, i sistemi di gestione dell'identità, i sistemi di sicurezza, e altri. Per le infrastrutture ferroviarie, i sistemi sono ad esempio: il materiale rotabile, i sottosistemi "esercizio e gestione del traffico", i sottosistemi "controllo-comando e segnalamento" di bordo e a terra, e altri.*

- *Garantire che le valutazioni dei rischi riguardino anche i rischi connessi alle attività quotidiane del personale (ad esempio l'uso dei social media e dei dispositivi personali, il trattamento dei dati, la condivisione delle informazioni, ecc.).*

- *Individuare e porre in atto misure per il trattamento dei rischi e piani per attenuare i rischi connessi alla cibersicurezza, quali ad esempio un **sistema di gestione della sicurezza delle informazioni** (Information Security Management System, ISMS) e un **sistema di gestione per la protezione dei dati personali** (Privacy Information Management System, PIMS) allineati agli altri sistemi di gestione. Tali sistemi di gestione (ISMS e PIMS) implicano l'attuazione di controlli sulla sicurezza (nonché su protezione dei dati e privacy) per attenuare e prevenire minacce emergenti contro la sicurezza dei servizi e dei sistemi del trasporto terrestre (ivi compresi i relativi dati).*

- *Tenere in considerazione tutti i vincoli che interessano **la gestione dei beni e la pianificazione delle risorse** (ossia i vincoli che possono influenzare la consegna, la manutenzione e il sostegno di sistemi critici per l'operatività di funzioni essenziali del trasporto terrestre).*

Esempi di quadri per la gestione del rischio: esistono diversi quadri che possono orientare e sostenere un approccio mirato per la gestione del rischio nel settore del trasporto su strada e ferroviario, quali ad esempio le norme della famiglia ISO/IEC 27000, il quadro per la cibersicurezza del *National Institute of Standards and Technology*(NIST), il quadro MITRE ATT&CK, la norma BSI IT-Grundschutz, ecc. Organizzazioni come l'ENISA elaborano buone pratiche per la sicurezza informatica delle auto intelligenti e dei trasporti pubblici intelligenti, su cui si basano i costruttori e le associazioni del settore (ad esempio l'associazione europea dei produttori di automobili, ACEA). Nell'ambito del trasporto ferroviario, l'Agenzia dell'Unione europea per le ferrovie (*European Union Agency for Railways*, ERA) definisce le specifiche tecniche di interoperabilità cui va adeguato ogni sottosistema o parte di sottosistema per soddisfare i requisiti essenziali e garantire l'interoperabilità del sistema ferroviario dell'Unione europea. L'impresa comune Shift2Rail è inoltre alla guida di iniziative e progetti di innovazione (in cui è contemplata la cibersicurezza) nel settore ferroviario.

Protezione dalle minacce alla cibersicurezza

È opportuno che le organizzazioni del trasporto terrestre attuino misure di sicurezza adeguate e proporzionate per salvaguardare dagli attacchi informatici le proprie reti e i propri sistemi informativi, tra cui le tecnologie dell'informazione (IT) e le tecnologie operative (OT). Tali misure di sicurezza comprendono quanto indicato di seguito.

- ***Politiche e processi in materia di sicurezza:*** *elaborare, attuare, comunicare e applicare politiche e procedure adeguate a delineare un metodo globale per garantire la sicurezza dei sistemi e dei dati che sostengono l'operatività di funzioni essenziali nei vari modi di trasporto terrestre. Tali politiche per la sicurezza (ad esempio le strategie riguardanti le password e la conservazione) e procedure di sicurezza dovrebbero inoltre contemplare la gestione delle patch e delle vulnerabilità dei sistemi hardware e software (comprese le IT e le OT), la gestione degli incidenti e la protezione del sistema e della rete.*

- ***Gestione dell'accesso e dell'identità:*** *comprendere, documentare e gestire l'accesso alle reti e ai sistemi informativi (comprese le IT e le OT) che sostengono l'operatività di funzioni essenziali per tutti i modi di trasporto terrestre. Gli utenti (o le funzioni automatizzate) che possono accedere ai dati e ai sistemi sono opportunamente verificati, autenticati e autorizzati, tenendo conto anche delle differenze di ruolo e di responsabilità tra gli account regolari e gli account privilegiati.*

- ***Sicurezza dei dati e dei sistemi:*** *proteggere i dati (conservati e trasmessi elettronicamente), le reti e i sistemi informativi critici (incluse le IT e le OT) dagli attacchi informatici. Tenuto conto di un approccio orientato al rischio, è opportuno che le organizzazioni attuino misure di sicurezza per ridurre efficacemente le possibilità per gli autori degli attacchi di compromettere i dati, le reti e i sistemi. Tali misure di sicurezza dovrebbero prevedere inoltre l'adozione di protocolli di crittografia e di comunicazione sicuri per salvaguardare i dati a riposo e in transito dalle minacce informatiche derivanti da attacchi del tipo "man-in-the-middle". Inoltre è necessario combinare tali misure con misure di sicurezza fisica per tutelare l'accesso ai sistemi (ad esempio, i sistemi dovrebbero essere situati in stanze chiuse con accesso limitato). Ciò riveste grande importanza per quei sistemi che incidono sulla sicurezza della vita.*

- ***La resilienza delle reti e dei sistemi:*** *costruire la resilienza delle reti e dei sistemi (incluse le IT e le OT) progettando e realizzando reti e sistemi, come pure le relative procedure operative, in modo che possano resistere all'impatto degli attacchi informatici e attenuarne gli effetti. Soluzioni per la progettazione e la realizzazione che migliorano la resilienza sono ad esempio: la verifica formale delle funzioni essenziali, la ridondanza dei sistemi e delle reti, la segregazione delle reti (in particolare la segregazione delle IT e delle OT), le misure di sicurezza a più livelli e molte altre. Occorre osservare che sotto il profilo della sicurezza delle informazioni i domini di protezione che applicano regole di segregazione di reti e sistemi possono fornire adeguate soluzioni di sicurezza. È tuttavia possibile che in base a talune esigenze operative dei sistemi (ad esempio le attività di manutenzione, i trasferimenti di dati, ecc.) sia necessario eludere o connettere domini di protezione diversi (ad esempio le reti e i sistemi segregati), ivi compresa la connessione delle IT e delle OT.*

Rilevare le minacce alla cibersicurezza

È opportuno che le organizzazioni garantiscano che le misure di sicurezza restino efficaci e rilevino ogni evento di cibersicurezza che influisce o può influire sui controlli di sicurezza così come sui servizi e sui sistemi essenziali. Le opportune misure di sicurezza atte a rilevare le minacce alla cibersicurezza sono indicate in appresso.

■ ***Monitoraggio della sicurezza:*** *monitorare lo stato della sicurezza delle reti e dei sistemi informativi, tra cui le tecnologie dell'informazione (IT) e le tecnologie operative (OT), che sostengono l'operatività di funzioni essenziali per tutti i modi di trasporto terrestre. Ciò è necessario al fine di rilevare potenziali minacce alla sicurezza e di tracciare la continuità dell'efficacia delle misure a salvaguardia della sicurezza. Per contribuire adeguatamente al monitoraggio della sicurezza, occorre prendere in esame, ad esempio, i dati dei file seguenti:*

- *log di sicurezza;*
- *log del rilevamento di virus;*
- *log delle intrusioni;*
- *log di identificazione, autenticazione e autorizzazione;*
- *log di sistema e dei servizi;*
- *log del traffico di rete;*
- *log di trattamento dei dati.*

■ ***Individuazione di eventi legati alla sicurezza:*** *rilevare attività malevole (ossia eventi legati alla sicurezza) che incidono o possono incidere sulla sicurezza delle reti e dei sistemi informativi (comprese le IT e le OT) che sostengono l'operatività di funzioni essenziali.*

Tali misure possono richiedere l'adozione di tecnologie specifiche (ad esempio il sistema di gestione delle informazioni e degli eventi di sicurezza, il sistema di rilevamento delle intrusioni, il sistema di prevenzione delle intrusioni, ecc.) e la creazione di un centro operativo per la sicurezza o di un mezzo analogo, vale a dire lo sviluppo di strumenti per rilevare e analizzare gli attacchi informatici, nonché per elaborare le relative risposte e le azioni di recupero, a livello locale.
I gruppi nazionali di intervento per la sicurezza informatica in caso di incidente (CSIRT), le squadre di pronto intervento informatico (CERT) settoriali e commerciali, gli operatori stradali e ferroviari e il centro di analisi e condivisione delle informazioni riguardanti la rete ferroviaria europea (European Rail Information Sharing and Analysis Centre, ER-ISAC) possono fornire informazioni in materia di minacce informatiche quale contributo alle attività di monitoraggio e rilevamento ai fini della sicurezza.

Pianificazione della risposta e del recupero

È opportuno che le organizzazioni definiscano, applichino e testino procedure di gestione degli incidenti intese a garantire la continuità operativa dei servizi e dei sistemi nell'eventualità di incidenti di cibersicurezza.

È opportuno che la pianificazione della risposta e del recupero preveda l'adozione di misure di sicurezza volte ad attenuare l'impatto di specifici attacchi alla cibersicurezza, come le misure seguenti:

- *il coordinamento e la cooperazione con i CSIRT nazionali (pubblici e commerciali) e con le CERT e i centri ISAC durante gli incidenti informatici, il coordinamento degli incidenti e delle crisi a livello paneuropeo;*

- *la condivisione delle informazioni con altre organizzazioni, tra cui i fornitori nella catena di prestazione dei servizi di trasporto terrestre;*

- ***esercitazioni in materia di attacchi informatici** (simulazioni a tavolino relative al coordinamento e agli aspetti tecnici) da effettuarsi periodicamente per valutare le misure e le procedure di sicurezza oltre alla resilienza delle organizzazioni nel far fronte agli incidenti informatici;*

- *l'accesso a spazi di conservazione di archivio o di backup in caso di compromissione dell'integrità e della disponibilità degli archivi di dati;*

- *l'impiego di **protocolli per la sicurezza** che prevedano procedure dettagliate per gestire gli incidenti di cibersicurezza e per ripristinare le normali condizioni operative di servizi e sistemi;*

- *azioni di reindirizzamento del traffico di rete a servizi ridondanti durante gli attacchi di negazione del servizio;*

- *procedure manuali per operare con servizi e sistemi le cui modalità operative si sono degradate;*

- *la definizione di procedure per affrontare i casi di violazione dei dati, comprese le procedure per far fronte alle violazioni dei dati personali in conformità del regolamento generale sulla protezione dei dati e di ogni altro regolamento o altra direttiva settoriale pertinente;*

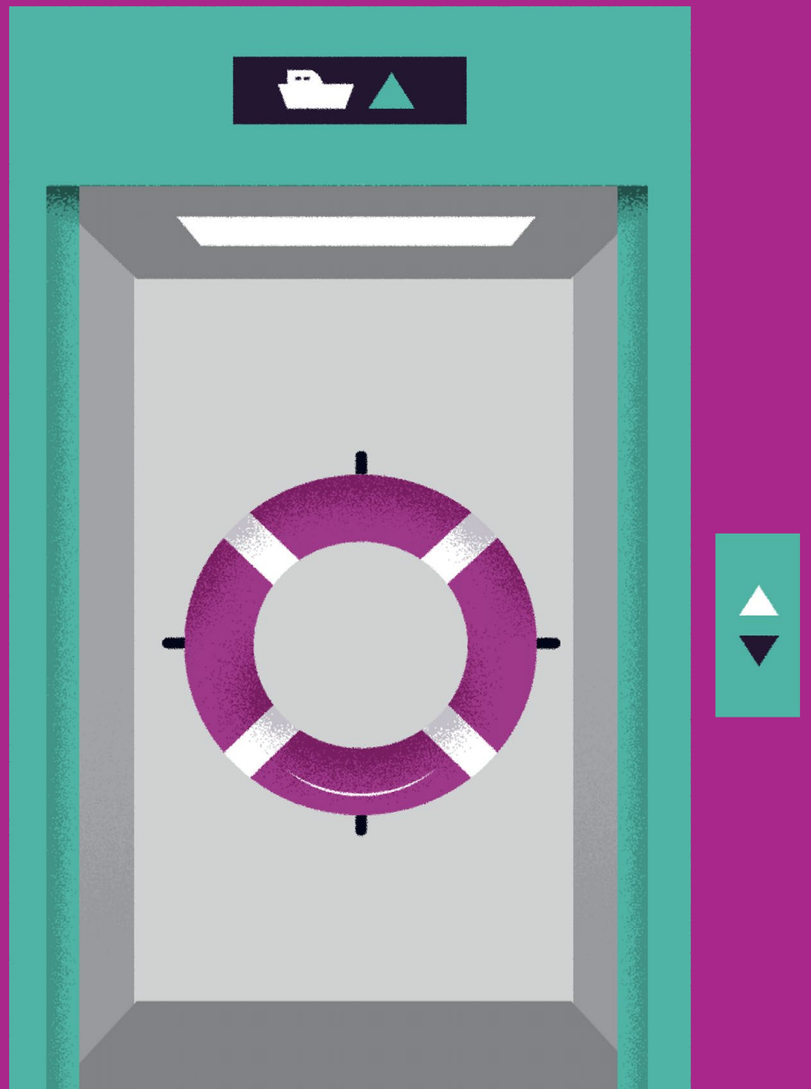
- *la sottoscrizione di un'**assicurazione informatica** per coprire parzialmente il rischio associato agli incidenti gravi di cibersicurezza;*

- *la sottoscrizione con modello "retainer" di contratti per la fornitura di servizi di risposta agli incidenti presso una o più ditte specializzate, onde disporre di ulteriori capacità e competenze;*

- *l'elaborazione di procedure per la condivisione delle informazioni sugli incidenti di cibersicurezza con le parti interessate pertinenti, che comprendano le procedure di notifica degli incidenti ai sensi della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva NIS).*

Commissione europea

Buone pratiche e misure di sicurezza applicabili al settore del trasporto marittimo



Governance

Le organizzazioni del trasporto marittimo devono comprendere in maniera chiara le minacce emergenti per elaborare le politiche e i processi di gestione intesi a regolare i propri metodi volti ad accrescere la cibersicurezza dei servizi e dei sistemi operativi, tra cui le tecnologie dell'informazione (IT) e le tecnologie operative (OT).

Le buone pratiche per le organizzazioni di qualsiasi dimensione prevedono quanto indicato di seguito.

- *Garantire che i problemi legati alla cibersicurezza siano segnalati dagli alti dirigenti agli amministratori delegati e ai consigli direttivi, i quali possono assumere decisioni informate in merito all'assegnazione delle risorse.*

- *Nominare in un ruolo di primo piano un responsabile della gestione globale della sicurezza delle IT e delle OT e le cui funzioni dovrebbero riguardare sia la sicurezza informatica sia la sicurezza fisica.*

- *Definire chiaramente le responsabilità, le competenze, le autorizzazioni e i ruoli correlati alla cibersicurezza, stabilire i livelli di autorità e le linee di comunicazione tra il personale a terra e il personale di bordo e nell'ambito di ciascun organico, oltre a concordare tali aspetti con il personale interessato. Ciò è necessario, in particolare, per i membri delle squadre di pronto intervento informatico (CERT). Il personale che ricopre ruoli correlati alla normativa dell'UE in materia di sicurezza e protezione marittime, come gli agenti di sicurezza degli impianti portuali, gli agenti di sicurezza dei porti o gli agenti di sicurezza della compagnia oppure la persona designata a terra e il comandante a bordo, dovrebbe almeno essere a conoscenza delle misure di cibersicurezza adottate dall'organizzazione.*

- *Garantire la governance della cibersicurezza lungo l'intera catena di fornitura dei servizi per la sicurezza, comprese le interfacce fisiche e digitali, dai produttori e installatori di tecnologia ai garanti della sicurezza.*

- *Concordare le attività e i controlli, comprese le responsabilità condivise, per la gestione dei rischi connessi alla cibersicurezza, oltre a garantire che tali responsabilità coprano tutto il ciclo di vita delle soluzioni e dei servizi relativi alla sicurezza (ad esempio in virtù di contratti di servizi).*

- *Definire i meccanismi di governance (ad esempio le politiche) per conformarsi agli obblighi di cui ai regolamenti e alle direttive pertinenti, quali per esempio: il regolamento (UE) 2019/1239 che istituisce un sistema di interfaccia unica marittima europea, il regolamento (CE) n. 725/2004 relativo al miglioramento della sicurezza delle navi e degli impianti portuali, la direttiva 2005/65/CE relativa al miglioramento della sicurezza dei porti e il regolamento (CE) n. 336/2006 sull'attuazione nella Comunità del codice internazionale di gestione della sicurezza, così come la risoluzione A.741 (18) che sancisce l'adozione del codice internazionale di gestione della sicurezza delle navi e della prevenzione dell'inquinamento (codice ISM). In tale contesto è importante inoltre citare il sistema comune per la condivisione delle informazioni (CISE), un'iniziativa dell'UE che mira a rendere interoperabili i sistemi di sorveglianza europei e degli Stati membri affinché a tutte le autorità interessate sia dato accesso alle informazioni classificate e non classificate di cui le stesse devono disporre per condurre missioni in mare.*

Esempi di servizi e di sistemi relativi al trasporto marittimo: sono esempi di IT le tecnologie accessibili ai dipendenti (ad esempio i personal computer, i telefoni cellulari, le periferiche per ufficio, ecc.) e ai passeggeri (come i router e le connessioni delle reti Wi-Fi pubbliche, ecc.). Sono esempi di OT i sistemi per il controllo di supervisione e acquisizione dati (SCADA), i sistemi di riscaldamento, ventilazione e condizionamento dell'aria (HVAC), i sistemi di posizionamento globale (GPS), il controllo dell'accesso, il monitoraggio, la sorveglianza, la risposta alle emergenze, le tecnologie di controllo,, i sistemi di navigazione di bordo, il sistema SafeSeaNet, i sistemi a ponte, i sistemi di movimentazione e gestione del carico, i sistemi di gestione della propulsione e dei macchinari e di controllo della potenza, i sistemi di controllo degli accessi, i sistemi di assistenza e gestione dei passeggeri, le reti pubbliche destinate ai passeggeri, i sistemi amministrativi e i sistemi riguardanti il benessere degli equipaggi, i sistemi di comunicazione, e altri.

Identificare le minacce alla cibersicurezza

La gestione del rischio: le organizzazioni del settore marittimo devono adottare le misure necessarie per identificare, analizzare, valutare e segnalare i rischi connessi alla cibersicurezza e per assumere, prevenire e trasferire tali rischi o per ridurli ad un livello accettabile. Ciò comporta un approccio organizzativo globale alla gestione del rischio, che richiede quanto riportato in appresso.

- *Garantire una chiara visione d'insieme dei vari sistemi hardware e software impiegati per la fornitura di servizi di tipo diverso. Nell'ambito del trasporto marittimo tali sistemi implicano l'uso delle tecnologie dell'informazione (IT) e delle tecnologie operative (OT) e le modalità di connessione e integrazione dei sistemi stessi con i referenti a terra, tra cui le pubbliche autorità, i terminal marittimi e gli stivatori.*

- *Individuare e valutare le principali operazioni di bordo della nave che risultano vulnerabili a fronte di attacchi informatici ed eseguire valutazioni dei rischi connessi alla cibersicurezza (compresa la valutazione degli eventuali effetti sotto il profilo operativo e la probabilità che questi si verifichino) che dovrebbero tener conto delle minacce emergenti, delle vulnerabilità note e dei dati operativi in relazione ai sistemi in questione. Ove opportuno, stabilire un collegamento con le valutazioni della sicurezza effettuate per le navi, gli impianti portuali e i porti come stabilito dalla normativa dell'UE in materia di sicurezza marittima. Tali valutazioni individuano eventuali minacce alla sicurezza delle infrastrutture portuali e le lacune in materia di sicurezza. Inoltre le organizzazioni marittime quali l'Organizzazione marittima internazionale (IMO) e i centri di condivisione e analisi delle informazioni (ISAC) in ambito marittimo possono fornire informazioni più approfondite sulle minacce che prendono di mira il trasporto marittimo.*

- *Garantire che le valutazioni dei rischi riguardino anche i rischi connessi alle attività quotidiane del personale (ad esempio l'uso dei social media e dei dispositivi personali, il trattamento dei dati, la condivisione delle informazioni, ecc.).*

- *Individuare e porre in atto misure per il trattamento dei rischi e piani per attenuare i rischi connessi alla cibersicurezza. Provvedere, ad esempio, all'attuazione di un sistema di gestione della sicurezza delle informazioni (Information Security Management System, ISMS) e di un sistema di gestione per la protezione dei dati personali (Privacy Information Management System, PIMS), allineati con altri sistemi di gestione come il sistema di gestione della sicurezza in conformità del codice internazionale di gestione della sicurezza delle navi e della prevenzione dell'inquinamento (codice ISM). Tali sistemi di gestione (ISMS e PIMS) implicano l'attuazione di controlli sulla sicurezza (nonché su protezione dei dati e privacy) per attenuare e prevenire minacce emergenti contro la sicurezza dei servizi e dei sistemi del trasporto marittimo (ivi compresi i relativi dati).*

- *Tenere conto di tutti i vincoli concernenti **la gestione dei beni e la pianificazione delle risorse** (ossia i vincoli che possono influenzare la consegna, la manutenzione e il sostegno di sistemi critici per l'operatività di funzioni essenziali nell'ambito del trasporto marittimo). Come nel caso delle valutazioni, stabilire ove opportuno riferimenti incrociati con i requisiti di cui al codice ISM, con i sistemi di gestione della sicurezza e con i piani di sicurezza realizzati ai sensi della normativa dell'UE in materia di sicurezza e protezione marittime.*

Esempi di quadri per la gestione del rischio: esistono diversi quadri che possono orientare e sostenere un approccio mirato per la gestione del rischio nel settore del trasporto marittimo, quali ad esempio le norme della famiglia ISO/IEC 27000, il quadro per la cibersicurezza del *National Institute of Standards and Technology* (NIST), il quadro MITRE ATT&CK, la norma BSI IT-Grundschutz, ecc. Il quadro per la cibersicurezza del NIST è stato anche modulato per far fronte alla sicurezza informatica nel contesto del trasferimento in mare di liquidi alla rinfusa, delle operazioni offshore e delle operazioni delle navi passeggeri. Analogamente, il consiglio marittimo baltico e internazionale (*Baltic and International Maritime Council*, BIMCO) ha emesso le proprie linee guida in materia di cibersicurezza a bordo delle navi (*"The Guidelines on Cyber Security Onboard Ships"*) e l'IMO ha diffuso i propri orientamenti sulla gestione del rischio informatico (*"Guidelines on maritime cyber risk management"*) (MSC-FAL.1/Circ.3). L'Agenzia dell'Unione europea per la cibersicurezza (ENISA) ha condotto numerosi studi riguardanti le buone pratiche per la cibersicurezza nel settore marittimo, in particolare per la sicurezza informatica dei porti. L'Agenzia europea per la sicurezza marittima (EMSA) fornisce servizi alla comunità marittima tra cui formazioni sulla sensibilizzazione in materia di cibersicurezza. Vi sono norme che definiscono anche specifici requisiti di sicurezza in merito ai sistemi e alle reti del trasporto via mare, come ad esempio la norma IEC 61162-460:2018 sulla sicurezza e protezione delle apparecchiature e dei sistemi per la navigazione marittima e le radiocomunicazioni, la norma ISO 16425:2013 in materia di navi e tecnologia marina, la norma IEC 62443-4-1:2018 sulla sicurezza dei sistemi di automazione e controllo industriali, ecc.

Protezione dalle minacce alla cibersicurezza

Le organizzazioni del settore del trasporto marittimo devono attuare misure di sicurezza adeguate e appropriate per salvaguardare le proprie reti e i propri sistemi informativi, incluse le tecnologie dell'informazione (IT) e le tecnologie operative (OT). Tali misure di sicurezza comprendono quanto indicato di seguito.

- ***Politiche e processi in materia di sicurezza:*** *elaborare, attuare, comunicare e applicare le politiche e le procedure adeguate a delineare un metodo globale per garantire la sicurezza dei sistemi e dei dati che sostengono l'operatività di funzioni essenziali nell'ambito del trasporto marittimo. Le misure di sicurezza (tra cui misure di sicurezza informatica e fisica) devono far parte di piani pertinenti quali il sistema di gestione della sicurezza e il piano di sicurezza della nave. Tali politiche per la sicurezza (ad esempio le strategie riguardanti le password e la conservazione) e procedure di sicurezza dovrebbero inoltre contemplare la gestione delle patch e delle vulnerabilità dei sistemi hardware e software (comprese le IT e le OT), la gestione degli incidenti e la protezione del sistema e della rete.*

- ***Gestione dell'accesso e dell'identità:*** *comprendere, documentare e gestire l'accesso alle reti e ai sistemi informativi (comprese le IT e le OT) che sostengono l'operatività di funzioni essenziali nell'ambito del trasporto marittimo. Gli utenti (o le funzioni automatizzate) che possono accedere ai dati e ai sistemi sono opportunamente verificati, autenticati e autorizzati, tenendo conto anche delle differenze di ruolo e di responsabilità tra gli account regolari e gli account privilegiati.*

- ***Sicurezza dei dati e dei sistemi:*** *proteggere i dati (conservati e trasmessi elettronicamente), le reti e i sistemi informativi critici (incluse le IT e le OT) dagli attacchi informatici. Tenuto conto di un approccio orientato al rischio, è opportuno che le organizzazioni attuino misure di sicurezza per ridurre efficacemente le possibilità per gli autori degli attacchi di compromettere dati, reti e sistemi. Tali misure di sicurezza dovrebbero prevedere inoltre l'adozione di protocolli di crittografia e di comunicazione sicuri per salvaguardare i dati a riposo e in transito dalle minacce informatiche derivanti da attacchi del tipo "man-in-the-middle". Inoltre è necessario combinare tali misure con misure di sicurezza fisica per tutelare l'accesso ai sistemi (ad esempio, i sistemi dovrebbero essere situati in stanze chiuse con accesso limitato). Ciò è molto importante per i sistemi che possono avere un impatto sulla sicurezza della vita (ad esempio sistemi di navigazione e di radiocomunicazioni di categoria II e III).*

- ***La resilienza delle reti e dei sistemi:*** *costruire la resilienza delle reti e dei sistemi (incluse le IT e le OT) progettando e realizzando reti e sistemi, come pure le relative procedure operative, in modo che possano resistere all'impatto degli attacchi informatici e attenuarne gli effetti. Soluzioni per la progettazione e la realizzazione che migliorano la resilienza sono ad esempio: la verifica formale delle funzioni essenziali, la ridondanza dei sistemi e delle reti, la segregazione delle reti (in particolare la segregazione delle IT e delle OT), le misure di sicurezza a più livelli e molte altre. Occorre osservare che sotto il profilo della sicurezza delle informazioni i domini di protezione che applicano regole di segregazione di reti e sistemi possono fornire adeguate soluzioni di sicurezza. Tuttavia è possibile che talune esigenze operative dei sistemi (ad esempio le attività di manutenzione, i trasferimenti di dati, ecc.) richiedano di eludere o di collegare domini di sicurezza differenti (ad esempio le reti e i sistemi segregati), ivi compresa la connessione delle IT e delle OT.*

Rilevare le minacce alla cibersicurezza

È opportuno che le organizzazioni garantiscano che le misure di sicurezza restino efficAaci e rilevino ogni evento di cibersicurezza che influisce o può influire sui controlli di sicurezza così come sui servizi e sui sistemi essenziali. Le opportune misure di sicurezza atte a rilevare le minacce alla cibersicurezza sono indicate in appresso.

■ ***Monitoraggio della sicurezza:*** *monitorare lo stato della sicurezza delle reti e dei sistemi informativi, tra cui le tecnologie dell'informazione (IT) e le tecnologie operative (OT), che sostengono l'operatività di funzioni essenziali nell'ambito dei servizi di trasporto marittimo. Ciò è necessario al fine di rilevare potenziali minacce alla sicurezza e di tracciare la continuità dell'efficacia delle misure a salvaguardia della sicurezza. Per contribuire adeguatamente al monitoraggio della sicurezza, occorre prendere in esame, ad esempio, i dati dei file seguenti:*

- *log di sicurezza;*
- *log del rilevamento di virus;*
- *log delle intrusioni;*
- *log di identificazione, autenticazione e autorizzazione;*
- *log di sistema e dei servizi;*
- *log del traffico di rete;*
- *log di trattamento dei dati.*

■ ***Individuazione di eventi legati alla sicurezza:*** *rilevare attività malevole (cioè eventi legati alla sicurezza) che incidono o possono incidere sulla sicurezza delle reti e dei sistemi informativi (comprese le IT e le OT) che sostengono l'operatività di funzioni essenziali nell'ambito dei servizi di trasporto marittimo.*

Tali misure possono richiedere l'adozione di tecnologie specifiche (ad esempio il sistema di gestione delle informazioni e degli eventi di sicurezza, il sistema di rilevamento delle intrusioni, il sistema di prevenzione delle intrusioni, ecc.) e la creazione di un centro operativo per la sicurezza o di un mezzo analogo, ovvero lo sviluppo di strumenti per rilevare e analizzare gli attacchi informatici, nonché per elaborare le relative risposte e le azioni di recupero, a livello locale.

I gruppi nazionali di intervento per la sicurezza informatica in caso di incidente (CSIRT), le squadre per la risposta alle emergenze informatiche (CERT) di settore e commerciali degli operatori marittimi e i centri ISAC in ambito marittimo possono fornire informazioni in materia di minacce informatiche quale contributo alle attività di monitoraggio e rilevamento ai fini della sicurezza.

Pianificazione della risposta e del recupero

È opportuno che le organizzazioni definiscano, applichino e testino procedure di gestione degli incidenti intese a garantire la continuità operativa dei servizi e dei sistemi nell'eventualità di incidenti di cibersicurezza.
È opportuno che la pianificazione della risposta e del recupero preveda l'adozione di misure di sicurezza volte ad attenuare l'impatto di specifici attacchi alla cibersicurezza, come le misure seguenti:

- *azioni di reindirizzamento del traffico di rete a servizi ridondanti durante gli attacchi di negazione del servizio;*

- *procedure manuali per operare con servizi e sistemi le cui modalità operative si sono degradate;*

- *stabilire programmi per esercitazioni e attività di addestramento (ad esempio simulazioni a tavolino relative al coordinamento, agli aspetti tecnici e alla reazione) per reagire agli attacchi informatici e alle situazioni di emergenza, nonché per valutare le misure di sicurezza, le procedure e la resilienza delle organizzazioni nel far fronte agli incidenti informatici.*

- *l'accesso a spazi di conservazione di archivio o di backup in caso di compromissione dell'integrità e della disponibilità degli archivi di dati;*

- *il coordinamento e la cooperazione con i CSIRT nazionali (pubblici e commerciali) e con le CERT e i centri ISAC durante gli incidenti informatici, il coordinamento degli incidenti e delle crisi a livello paneuropeo;*

- *la condivisione delle informazioni con altre organizzazioni, ivi inclusi i fornitori nella catena di prestazione dei servizi di trasporto marittimo;*

- *l'impiego di protocolli per la sicurezza che prevedano procedure dettagliate per gestire gli incidenti di cibersicurezza e per ripristinare le normali condizioni operative di servizi e sistemi;*

- *la definizione di procedure per affrontare i casi di violazione dei dati, comprese le procedure per far fronte alle violazioni dei dati personali in conformità del regolamento generale sulla protezione dei dati e di ogni altro regolamento o altra direttiva settoriale pertinente;*

- *la sottoscrizione di un'**assicurazione informatica** per coprire parzialmente il rischio associato agli incidenti gravi di cibersicurezza;*

- *la sottoscrizione con modello "retainer" di contratti per la fornitura di servizi di risposta agli incidenti presso una o più ditte specializzate, onde disporre di ulteriori capacità e competenze;*

- *l'elaborazione di procedure per la condivisione delle informazioni sugli incidenti di cibersicurezza (tra cui le non conformità, gli incidenti e le situazioni pericolose), che comprendano le procedure di notifica degli incidenti ai sensi della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva NIS).*

Lussemburgo: Ufficio delle pubblicazioni dell'Unione europea, 2021

Print ISBN 978-92-76-40509-2 doi:10.2832/57315 MI-05-21-230-IT-C
PDF ISBN 978-92-76-40504-7 doi:10.2832/390455 MI-05-21-230-IT-N

Ufficio delle pubblicazioni dell'Unione europea