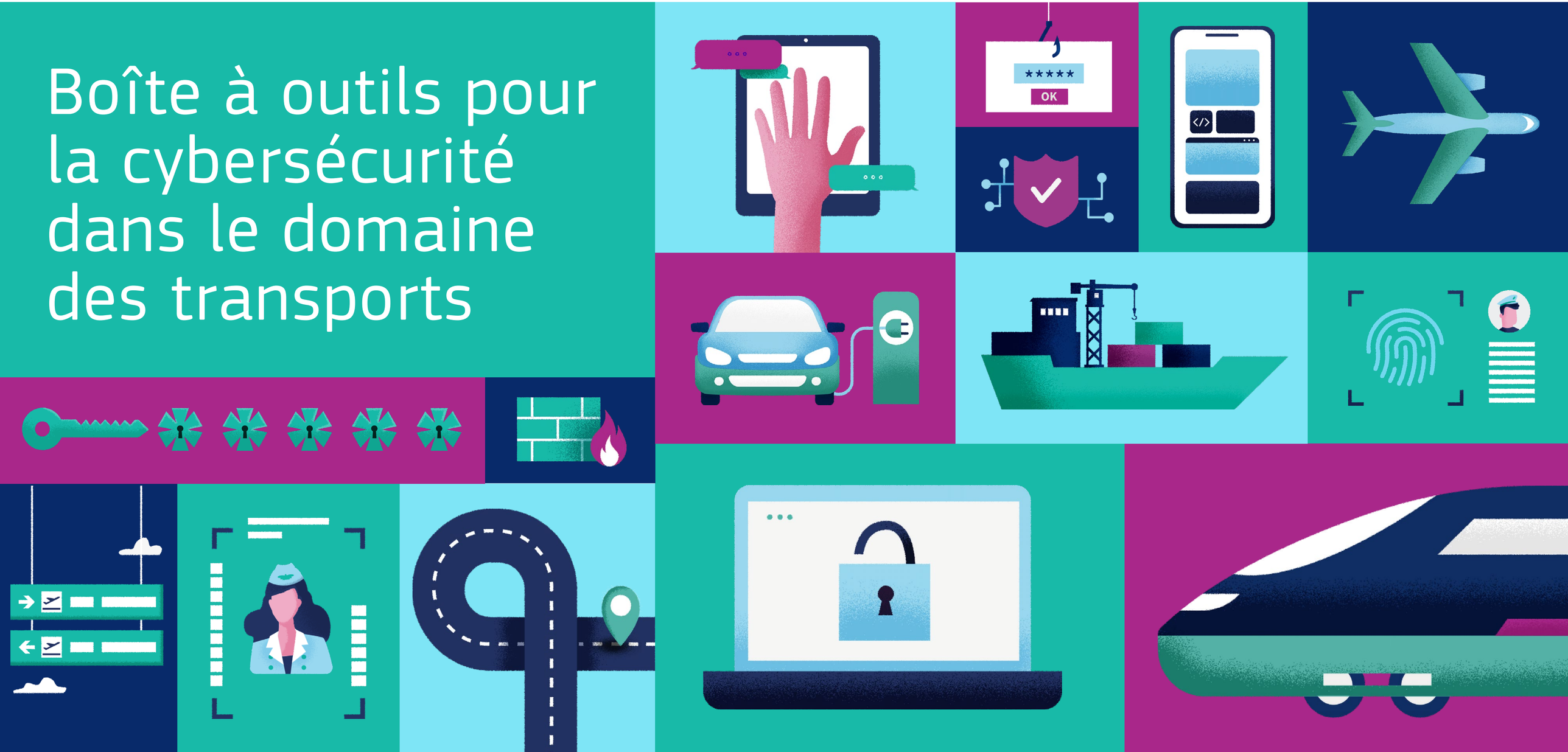
Commission européenne

Boîte à outils pour la cybersécurité dans le domaine des transports



Introduction

La direction générale de la mobilité et des transports de la Commission européenne (DG MOVE) a commandé l'élaboration de la présente boîte à outils en vue de sensibiliser davantage les acteurs du secteur des transports aux cybermenaces et de mieux les préparer face à celles-ci. Elle fournit des informations permettant de comprendre les cybermenaces et d'atténuer leurs conséquences. La présente boîte à outils propose deux parcours de sensibilisation correspondant à des profils différents, à savoir:

- le personnel du secteur des transports dans son ensemble (informations et orientations générales);
- les décideurs du secteur des transports chargés de la cybersécurité pour les différents modes de transport.

Des hyperliens relient les différents éléments de la boîte à outils afin de faciliter la navigation.

Les pratiques énumérées dans la présente boîte à outils ont un caractère purement consultatif. Les recommandations formulées ne sont ni contraignantes ni obligatoires. En outre, la présente boîte à outils ne reflète pas la position officielle de la Commission européenne et elle n'est pas destinée à servir de base pour se conformer aux législations de l'Union en vigueur ou à venir.

Profils à sensibiliser à la cybersécurité

Profil I: le personnel du secteur des transports dans son ensemble. Le premier parcours s'adresse à l'ensemble du personnel travaillant dans les entreprises de transport. Il fournit des informations permettant de mieux comprendre les cybermenaces les plus courantes qui prennent pour cible les transports. En outre, il fournit des informations sur la manière de lutter contre les cybermenaces potentielles, notamment par la détection, la notification et l'atténuation de ces menaces grâce à l'application de bonnes pratiques en matière de cybersécurité.

Profil II: les décideurs dans le domaine de la cybersécurité des transports. Le deuxième parcours s'adresse aux membres du personnel responsables de la prise de décision en matière de cybersécurité dans les organisations de transport. Il décrit de bonnes pratiques adaptées aux différents modes de transport. En particulier, il fournit de bonnes pratiques permettant aux organisations de transport visées de recenser et de détecter les cybermenaces émergentes et de prendre des mesures de protection et de réaction contre celles-ci.

Commission européenne

Boîte à outils pour la cybersécurité dans le domaine des transports

Panorama des menaces pour les transports

Cybermenaces émergentes touchant différents modes de transport

Profils à sensibiliser à la cybersécurité

Des parcours différents de sensibilisation à la cybersécurité correspondant à divers profils dans le secteur des transports

Commission européenne

Panorama des menaces pour les transports

Le panorama des cybermenaces est dynamique et en constante évolution. Néanmoins, il est possible de recenser des cybermenaces qui pèsent sur tous les modes de transport.

Commission européenne

Acteurs de la menace

Individus ou organisations susceptibles d'avoir une incidence sur la sûreté et la sécurité des services et systèmes de transport

Cybermenaces émergentes

Certaines cybermenaces susceptibles d'avoir une incidence sur la sûreté et la sécurité des services et systèmes de transport

Acteurs de la menace

Les individus ou les organisations peuvent, volontairement ou involontairement, mettre en évidence et exploiter des vulnérabilités susceptibles de provoquer des incidents et de perturber les services de transport, ce qui peut nuire à la sûreté, à la sécurité et à la réputation du transport et avoir des répercussions économiques et financières.

Les principaux acteurs malveillants qui prennent délibérément pour cible les organisations de transport sont les **cybercriminels**, les **acteurs internes**, les **États-nations** et les **groupes soutenus par des États**.
Les acteurs hostiles de type **cybercriminel** mènent des campagnes massives de cyberattaques et sont souvent à la recherche de récompenses financières.

Les **acteurs internes** connaissent les particularités des organisations pour lesquelles ils travaillent et sont souvent bien au fait des failles de sécurité subtiles. Ces acteurs internes peuvent être des employés, des fournisseurs et des contractants mécontents.
À mesure que les tensions géopolitiques mondiales s'intensifient, les **États-nations** et les **groupes soutenus par des États** se fixent des objectifs stratégiques à long terme. Ils tentent souvent de se cacher dans la profondeur des systèmes des organisations et de collecter des informations confidentielles. Une fois qu'ils ont trouvé un point d'appui dans les systèmes, les attaquants soutenus par des États cherchent à se mettre dans une position leur permettant de causer le préjudice le plus grave possible.

Les acteurs non malveillants sont des **acteurs internes** qui effectuent des actions non intentionnelles ou accidentelles entraînant des événements compromettant la cybersécurité et, dans les cas les plus graves, des incidents de sécurité informatique portant atteinte à la sûreté et à la sécurité des services de transport.

Cybermenaces émergentes

Il existe un nombre important de cybermenaces visant les transports: **déni de service distribué**, **déni de service**, vol de données, diffusion de **logiciels malveillants**, **hameçonnage**, manipulation du logiciel, **accès non autorisé**, attaques destructrices, falsification ou contournement du processus décisionnel de l'opérateur de sécurité, usurpation d'identité, abus des privilèges d'accès, **ingénierie sociale**, défiguration, écoutes clandestines, utilisation malveillante d'actifs et manipulation du matériel informatique.

À la lumière d'une recherche bibliographique exhaustive de documents accessibles au public et d'entretiens avec des experts, les cybermenaces émergentes les plus préoccupantes pour les transports sont les suivantes: logiciels malveillants, déni de service (distribué), accès non autorisé et vol, et manipulation du logiciel.

Commission européenne

Menace #1: Logiciels malveillants

Logiciels malveillants susceptibles de nuire à des particuliers ou à des organisations pour tous les modes de transport

Menace #2: Déni de service (distribué)

Cyberattaques empêchant des particuliers ou des organisations d'accéder aux services et ressources

Menace #3: Accès non autorisé et vol

Accès non autorisé à des actifs critiques et prise de possession et exploitation de ces actifs

Menace #4: Manipulation du logiciel

Cyberattaques visant un logiciel afin de modifier son comportement et de mener des attaques spécifiques

Menace #1: Logiciel malveillant

Parmi les logiciels malveillants figurent différents types d'applications logicielles tels que les virus, les chevaux de Troie, les vers, les rançongiciels, les mineurs de cryptomonnaies, ainsi que les logiciels susceptibles d'avoir des incidences négatives sur les organisations ou les particuliers pour tous les modes de transport.

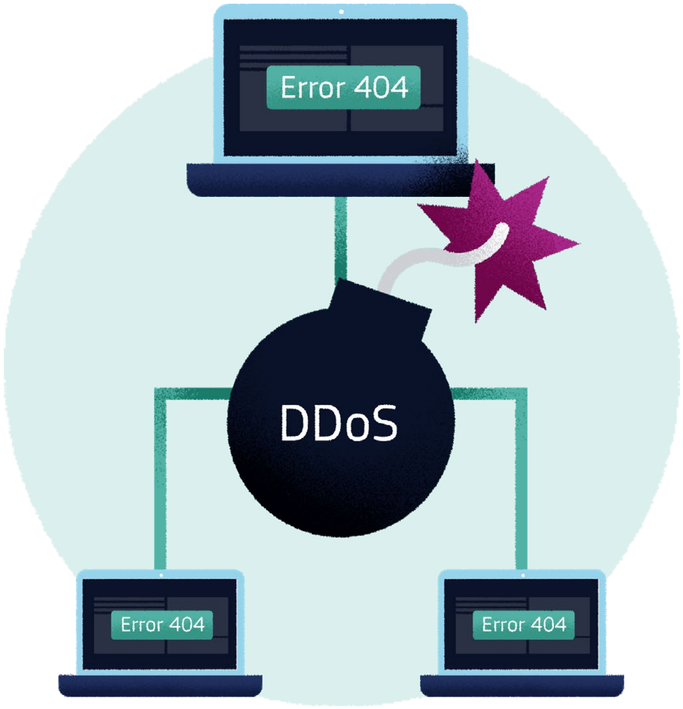
La lutte contre la diffusion de logiciels malveillants conçus pour endommager intentionnellement des ordinateurs, des serveurs, des réseaux ou l'ensemble de ces éléments et pour porter atteinte à des clients figure parmi les grandes priorités en matière de cybersécurité pour tous les modes de transport. Un vecteur d'attaque caractéristique peut consister à hameçonner des employés par courrier électronique. Parmi les autres vecteurs d'attaque figurent différentes stratégies d'ingénierie sociale sophistiquées, telles que la connexion d'une clé USB dans un port libre (dans le port de recharge d'un téléphone portable, par exemple). En cliquant sur des liens hypertextes figurant dans des courriers électroniques suspects ou en ouvrant des pièces jointes, l'utilisateur peut installer des logiciels malveillants à son insu.

Par exemple, la cyberattaque par rançongiciel WannaCry a touché plus de 150 pays et a contaminé plus de 230 000 systèmes. Il s'agissait d'un rançongiciel qui se propageait généralement par courrier électronique d'hameçonnage contenant des pièces jointes ou des liens hypertextes malveillants. Ce type d'attaque repose sur des stratagèmes malveillants d'ingénierie sociale visant à induire les utilisateurs du système en erreur et à les pousser à installer (ou à activer) des logiciels malveillants spécifiques.

Menace #2: Déni de service (distribué)

Les attaques par déni de service distribué (DDoS) et par déni de service (DoS) portent atteinte à la disponibilité et à l'accessibilité des données, des services, des systèmes et d'autres ressources. Ces types d'attaques sont de durée variable et peuvent cibler plus d'un service ou système à la fois. Les attaques DDoS utilisent plusieurs systèmes (ou canaux d'attaque) afin de submerger de demandes des services ou des systèmes pris pour cible. Les attaques menées avec succès compromettent les capacités des services et des systèmes à faire face à un volume anormalement élevé de demandes, ce qui se traduit par un accès refusé aux services et aux ressources.

Il convient de noter que les services et systèmes touchés qui appartiennent à des organisations de transport peuvent être exploités afin de diriger des attaques DDoS et DoS contre des systèmes spécifiques d'exploitation ou contre d'autres organisations.
Par exemple, les systèmes d'information d'une entreprise (les ordinateurs et appareils personnels, par exemple) peuvent être pris pour cible afin d'accéder aux technologies d'exploitation, qui peuvent être connectées à l'internet ou à des réseaux à des fins de transfert de données opérationnelles. Les connexions entre différents systèmes et réseaux (tels que les réseaux d'entreprise, les technologies d'exploitation et les accès de maintenance à distance) peuvent constituer des vulnérabilités qu'il est possible d'exploiter pour mener des attaques DDoS ou DoS contre des services et systèmes de transport essentiels. Par exemple, les attaques DDoS et DoS peuvent exploiter des réseaux communs et des protocoles de communication — le Web Services Dynamic Discovery (WS-Discovery), par exemple — utilisés par les appareils connectés pour découvrir automatiquement chaque nœud sur les réseaux locaux (LAN). Si les appareils connectés présentent des vulnérabilités, les attaquants peuvent exploiter ces failles pour découvrir d'autres appareils connectés et lancer des attaques DDoS ou DoS.



Menace #3: Accès non autorisé et vol

Les acteurs de la menace peuvent chercher à obtenir un accès logique ou physique sans autorisation à un réseau, à un système, à une application, à des données ou à une autre ressource afin de mener des activités malveillantes, telles que le vol de données ou de ressources confidentielles (y compris de ressources physiques). Les menaces de type accès non autorisé et vol prennent pour cible des actifs confidentiels et protégés (y compris des identités personnelles, des identifiants de comptes privilégiés, des systèmes et d'autres types d'informations confidentielles et protégées). Ces menaces peuvent exploiter des vulnérabilités des systèmes ainsi que des personnes qui divulguent par inadvertance des données confidentielles telles que des identifiants (nom d'utilisateur, mot de passe, etc.) ou des données à caractère personnel (adresse électronique, numéro d'identification personnel, etc.).

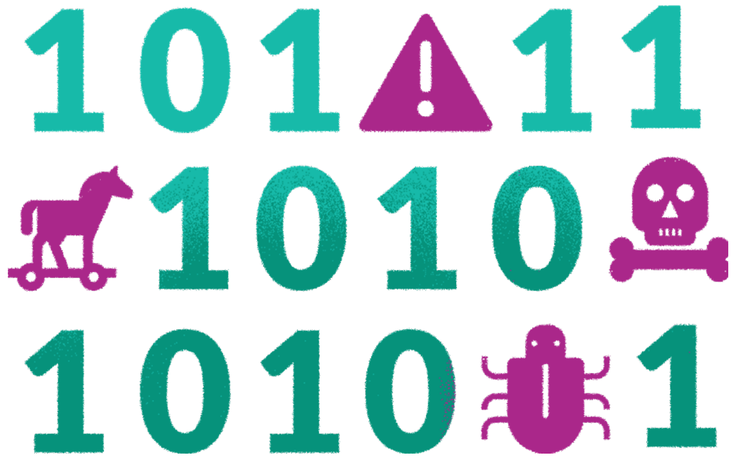
Par opposition à l'accès non autorisé, l'usurpation d'identité est l'utilisation illicite de données à caractère personnel ou d'identifiants uniques dans le but de se faire passer pour des personnes, des services ou des systèmes et d'accéder à des ressources privées ou protégées (y compris des ressources financières et physiques, par exemple). Ces cybermenaces peuvent également prendre pour cible des actifs physiques dans tous les modes de transport.

Commission européenne

Menace #4: Manipulation du logiciel

Le mauvais paramétrage et la manipulation de logiciels et de systèmes ou composants connexes peuvent avoir une incidence directe sur la posture de sécurité des services et systèmes de transport.
Les cyberattaques exploitant des manipulations du logiciel modifient les paramètres d'un logiciel ou compromettent l'intégrité des données en vue de modifier le comportement des systèmes et services. Les attaquants peuvent manipuler intentionnellement un logiciel (ou une partie d'un logiciel) afin d'obtenir des avantages (obtenir un accès non autorisé, empêcher des personnes ou des systèmes autorisés d'accéder aux ressources nécessaires, collecter des informations confidentielles, modifier les comportements fonctionnels, etc.) par une mainmise sur des actifs sensibles.

Par exemple, les attaquants peuvent viser les canaux de communication des fabricants afin de télécharger des mises à jour logicielles malveillantes sur des services et systèmes (y compris sur des technologies d'exploitation). Les agents de la menace utilisent des identifiants d'autorisation compromis pour accéder à une interface réseau sécurisée de maintenance à distance afin d'installer des logiciels manipulés et de compromettre d'autres services et systèmes accessibles. Les logiciels manipulés installés par ces agents ont pour objectif de compromettre davantage les services et systèmes pris pour cible ou d'attaquer d'autres services ou systèmes connectés.



Commission européenne

Profils à sensibiliser à la cybersécurité

Commission européenne

1

Profil I: Personnel des transports dans son ensemble

Le premier parcours s'adresse à l'ensemble du personnel des organisations de transport, allant du personnel chargé des opérations au personnel administratif. Il propose des orientations permettant de mieux comprendre et connaître les cybermenaces les plus courantes. En outre, il contient des informations sur la manière de lutter contre les cybermenaces potentielles, notamment par la détection, la notification et l'atténuation de ces menaces. Ce parcours est commun à tous les modes de transport.

2

Profil II: Décideurs dans le domaine de la cybersécurité des transports

Le deuxième parcours s'adresse aux membres du personnel responsables de la prise de décision en matière de sécurité ou de cybersécurité dans les organisations de transport. Ce parcours décrit de bonnes pratiques adaptées aux différents modes de transport. Il fournit de bonnes pratiques permettant aux organisations de transport visées de recenser et de détecter les cybermenaces émergentes et de prendre des mesures de protection et de réaction contre celles-ci.

Commission européenne

Profil I: Personnel des transports dans son ensemble

La présente section s'adresse à l'ensemble du personnel des organisations de transport, allant du personnel chargé des opérations au personnel administratif. Elle propose des orientations permettant de mieux comprendre et connaître les cybermenaces les plus courantes. En outre, elle contient des informations sur la manière de lutter contre les cybermenaces potentielles, notamment par la détection, la notification et l'atténuation de ces menaces.
La présente section énonce des pratiques recommandées et des conseils utiles, qui s'appliquent à **tous les modes de transport**.

Bonnes pratiques pour se protéger des logiciels malveillants

Vous pouvez contribuer à protéger votre organisation en appliquant les bonnes pratiques énoncées ci-après en matière de **détection et de prévention des tentatives de diffusion de logiciels malveillants**:

- ***suivre les politiques de sécurité**: notamment, analyser les supports de mémoire et les fichiers pour détecter des virus, éviter d'ouvrir et d'envoyer par courrier électronique certains types de fichiers (notamment des fichiers exécutables tels que les fichiers .exe,.bat,.com, etc.), installer uniquement des logiciels autorisés, veiller à ce que les logiciels (y compris les antivirus) soient à jour et fonctionnent correctement, et d'autres actions;*

- *effectuer régulièrement **des copies de sauvegarde de vos données** sur des dispositifs ou services de stockage de données sécurisés (et autorisés), lesquels devraient avoir recours à des mécanismes de chiffrement afin de protéger les données au repos et de garantir leur disponibilité pour les procédures de rétablissement des données;*

- *protéger par des **mesures de sécurité** appropriées (mot de passe, chiffrement, etc.) tous les systèmes, y compris les dispositifs mobiles et les périphériques, sans oublier de verrouiller (physiquement et numériquement) tous les systèmes laissés sans surveillance;*

- *éviter d'ouvrir des pièces jointes et de cliquer sur les liens hypertextes contenus dans des fenêtres intruses de navigateur web ou des courriels inopinés suspects, accompagnés d'un texte étrange ou provenant d'expéditeurs et de domaines internet inconnus;*

- *éviter d'insérer dans un ordinateur des **dispositifs amovibles non sécurisés ou inconnus**, tels que des clés USB, des disques durs et d'autres dispositifs de stockage;*

- *éviter de désactiver les dispositifs de protection contre les logiciels malveillants (antivirus, logiciel de filtrage du contenu, pare-feu, etc.);*

- ***mettre régulièrement à jour les logiciels** en veillant à ce que les dernières versions disponibles (que les agents de sécurité de l'information ou les administrateurs du système peuvent diffuser avec des mises à jour régulières) soient installées;*

- *éviter d'utiliser des comptes et des identifiants privilégiés (de niveau administrateur, par exemple) pour les activités et opérations courantes;*

- *signaler aux agents de sécurité de l'information ou aux administrateurs du système tout courrier électronique suspect ou comportement inhabituel du système;*

- *accorder une attention particulière à la sécurité de l'information dans le cadre de vos activités courantes pour détecter les problèmes en matière de sécurité informatique et être en mesure de réagir de façon appropriée.*

Bonnes pratiques pour se protéger des attaques par déni de service (distribué)

Vous pouvez contribuer à protéger votre organisation en détectant les **attaques par déni de service distribué (DDoS)** et les **attaques par déni de service (DoS)**. Contactez immédiatement vos équipes chargées de la sécurité et des systèmes informatiques si vous détectez ou rencontrez un ou plusieurs indicateurs révélateurs d'une attaque DDoS ou DoS actuellement dirigée contre vos services ou systèmes, notamment:

- *une augmentation des demandes consommant de la capacité de réseau (ce qui se traduit par des services lents et des temps de réponse longs) et entraînant des défaillances du service ou du système en raison de la surcharge;*
- *une augmentation de la demande d'utilisation des ressources de mémoire sans raison évidente;*
- *des **comportements inhabituels des services et systèmes**, tels que des plantages fréquents et des messages d'erreur étranges dus à la consommation malveillante de ressources informatiques ou de connexions réseau;*
- *une **baisse de la performance** des appareils, des temps d'exécution longs pour des tâches banales et des comportements perceptibles (par exemple, ventilateur bruyant lorsque les appareils fonctionnent lentement);*
- *des **connexions internet ou des pertes de connexions inhabituelles** aux services et systèmes;*
- *des modifications subtiles du comportement des fonctions de contrôle ou des technologies d'exploitation entraînant des dommages physiques;*
- *des accès refusés à des comptes privilégiés ou à des comptes administrateur afin de bloquer les procédures d'intervention en cas d'incident.*

Commission européenne

Bonnes pratiques pour se protéger des tentatives d'accès non autorisé et de vol

Pour prévenir les attaques de type accès non autorisé et vol, il est nécessaire de suivre des principes tels que le «besoin d'en connaître» et la «sécurité et le respect de la vie privée par défaut», selon lesquels les actifs sensibles et confidentiels (y compris les données à caractère personnel et confidentiel, les systèmes de transport, etc.) ne devraient être accessibles qu'aux personnes autorisées à y accéder afin d'exercer leurs fonctions. Vous pouvez contribuer à protéger votre organisation en appliquant les bonnes pratiques énoncées ci-après en matière de détection et de prévention des tentatives d'accès non autorisé et de vol:

- *suivre les politiques de votre organisation en matière de sécurité;*

- *éviter de partager et de publier en ligne des identifiants et des données à caractère personnel, y compris des images susceptibles de contenir de telles informations;*

- *éviter d'utiliser ou de transmettre des identifiants et des données à caractère personnel (ou à caractère confidentiel) vers des réseaux, appareils ou services web non fiables et non sécurisés (par exemple, sites web utilisant des protocoles ou adresses non sécurisés: http:// au lieu de https:///);*

- ***ne jamais divulguer des identifiants** (nom d'utilisateur et mot de passe), même par courrier électronique ou par téléphone;*

- *protéger les données confidentielles dactylographiées au clavier ou affichées sur un écran (y compris sur les appareils mobiles) des regards des personnes non autorisées, installer des écrans de protection de la vie privée, éviter de travailler depuis des lieux publics avec des appareils privés et éviter de laisser vos appareils déverrouillés et sans surveillance;*

- ***utiliser des mots de passe complexes** (par exemple, un mot de passe suffisamment long composé de caractères alphanumériques et de caractères spéciaux) respectant les politiques de sécurité en la matière de votre organisation afin d'empêcher tout accès non autorisé;*

- ***modifier les mots de passe par défaut** des systèmes et appareils connectés (imprimantes, routeurs, caméras, serrure intelligente, etc.);*

- *éviter d'utiliser les mêmes identifiants (nom d'utilisateur et mot de passe) pour plusieurs services et systèmes et éviter d'utiliser les mêmes identifiants pour les services et systèmes qui nécessitent des comptes privilégiés;*

- *envoyer vos mots de passe et vos clés protégeant des fichiers transférés (par exemple, des archives ZIP) uniquement par l'intermédiaire d'un canal hors bande (par exemple, SMS depuis un téléphone portable ou appel téléphonique) et jamais par courrier électronique;*

- ***activer l'authentification à deux facteurs (A2F)** ou l'authentification multifactorielle (AMF), si possible.*

Commission européenne

Bonnes pratiques pour se protéger contre la manipulation du logiciel

Vous pouvez contribuer à protéger votre organisation en appliquant les bonnes pratiques énoncées ci-après en matière de détection et de prévention des tentatives de manipulation du logiciel:

- *éviter d'installer des logiciels non fiables sur les systèmes et appareils (y compris sur les ordinateurs personnels, les serveurs, les périphériques, les appareils de réseau, les smartphones, etc.);*
- *installer toujours les logiciels et les mises à jour à partir de sources et de sites web officiels (par exemple, éditeur du logiciel, référentiels d'entreprise, etc.);*
- *éviter de télécharger des logiciels et des applications (et des fichiers divers) à partir de sources illégales;*
- *ne pas installer de logiciels inutiles ou non utilisés dernièrement et désactiver les connexions inutiles (protocoles et services de réseau, par exemple), y compris l'accès aux services à distance (par exemple, les services de stockage en nuage);*
- *analyser tous vos logiciels ou dispositifs de stockage à l'aide d'un antivirus fiable et actualisé;*
- *télécharger des logiciels industriels sûrs (mises à jour, correctifs, nouveaux produits, etc.) auprès de fournisseurs de confiance utilisant le principe de station blanche;*
- *mettre à jour tous les logiciels installés conformément aux politiques et pratiques de votre organisation.*

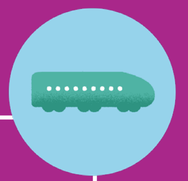
Commission européenne

Profil II: Décideurs dans le domaine de la cybersécurité des transports

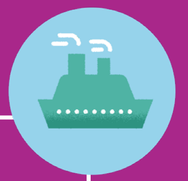
La présente partie s'adresse aux membres du personnel responsables de la prise de décision en matière de sécurité ou de cybersécurité dans les organisations de transport. Elle décrit de bonnes pratiques adaptées aux différents modes de transport. En particulier, elle contient de bonnes pratiques permettant de recenser et de détecter les cybermenaces émergentes et de prendre des mesures de protection et de réaction contre celles-ci.

Commission européenne

Bonnes pratiques en matière de cybersécurité adaptées au transport aérien



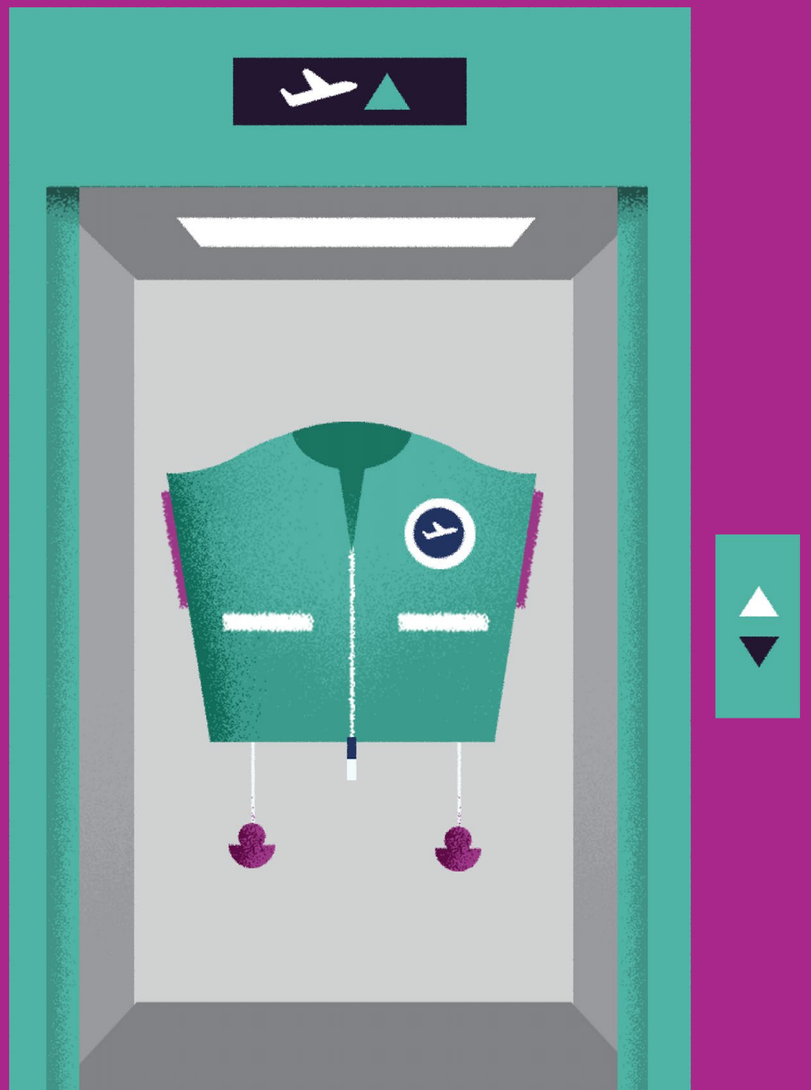
Bonnes pratiques en matière de cybersécurité adaptées au transport terrestre



Bonnes pratiques en matière de cybersécurité adaptées au transport maritime

Commission européenne

Bonnes pratiques et mesures de sécurité adaptées au transport aérien



Commission européenne

Gouvernance

Les organisations du secteur de l'aviation doivent comprendre clairement les menaces émergentes afin de définir les stratégies et les processus de gestion régissant leurs approches et d'améliorer la cybersécurité des services et systèmes d'exploitation, y compris des technologies de l'information et des technologies opérationnelles.

Les bonnes pratiques applicables aux organisations de toute taille sont les suivantes:

- veiller à ce que le personnel d'encadrement supérieur signale les enjeux en matière de cybersécurité aux instances dirigeantes et aux conseils d'administration afin que ceux-ci puissent prendre des décisions éclairées concernant l'allocation des ressources;

- nommer un haut responsable de la cybersécurité et de la sécurité physique, chargé de la gestion générale de la sécurité des technologies de l'information et des technologies opérationnelles, mais ne participant pas à l'exploitation afin d'éviter les conflits d'intérêts;

- définir clairement les rôles, les responsabilités, les compétences et les habilitations en matière de cybersécurité, en concertation et en accord avec le personnel concerné, en particulier avec le personnel des centres de réponse aux urgences informatiques (CERT);

- garantir la bonne gouvernance en matière de cybersécurité tout au long de la chaîne d'approvisionnement en services de sécurité, pour les interfaces aussi bien physiques que numériques, depuis les fabricants et les installateurs de technologies jusqu'aux fournisseurs de services de sécurité;

- convenir des activités et des contrôles, y compris des responsabilités partagées, à mettre en place pour gérer les risques en matière de cybersécurité, et veiller à ce que ces responsabilités soient maintenues (par exemple, par des accords de service) tant que les solutions et services de sécurité sont utilisés;

- définir des mécanismes de gouvernance (par exemple, des politiques) afin de se conformer aux obligations découlant des règlements et directives en matière de cybersécurité, tels que, par exemple, le règlement (UE) 2018/1139 concernant des règles communes dans le domaine de l'aviation civile et le règlement d'exécution (UE) 2017/373 de la Commission établissant des exigences communes relatives aux prestataires de services de gestion du trafic aérien et de services de navigation aérienne ainsi que des autres fonctions de réseau de la gestion du trafic aérien, et à leur supervision, ainsi que la directive SRI [directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information].

Exemples de services et de systèmes dans le transport aérien: les technologies de l'information sont, par exemple, les appareils accessibles aux employés (ordinateurs personnels, téléphones portables, périphériques de bureau, etc.) ainsi qu'aux passagers (connexions Wi-Fi publiques, etc.). Parmi les exemples de technologies opérationnelles figurent les systèmes d'acquisition et de contrôle des données (SCADA), les systèmes de chauffage, de ventilation et de climatisation (CVC), les postes de contrôle de sécurité pour les bagages de cabine, les systèmes de manutention des bagages (BHS), le contrôle d'accès, le suivi, la surveillance, la réaction aux alarmes, la technologie de filtrage, les systèmes d'éclairage d'approche, les systèmes radar et les capteurs, les systèmes de localisation GPS, les systèmes de gestion du trafic aérien (GTA), les systèmes de communication, navigation et surveillance (CNS), les systèmes d'information aéronautique, les systèmes d'information météorologique, les systèmes des centres d'opérations de sécurité et les instruments de bord.

Commission européenne

Identifier les cybermenaces

Gestion des risques: les organisations du secteur de l'aviation doivent prendre les mesures appropriées afin d'identifier, d'évaluer et de comprendre les risques en matière de cybersécurité pour le réseau et les systèmes d'information qui sous-tendent l'exploitation des fonctions essentielles.

Pour ce faire, elles doivent adopter une approche organisationnelle globale de la gestion des risques, en menant notamment les actions suivantes:

- *avoir une vue d'ensemble claire des différents systèmes matériels et logiciels déployés pour fournir différents services. Dans le contexte de l'aviation, ces systèmes font intervenir des technologies de l'information ainsi que des technologies opérationnelles;*

- *réaliser des **évaluations des risques en matière de cybersécurité**, qui tiennent compte des menaces émergentes, des vulnérabilités connues et des données opérationnelles relatives aux systèmes évalués. Des organisations telles que le centre de réponse aux urgences informatiques pour la gestion du trafic aérien européen (EATM-CERT) et le centre d'échange et d'analyse d'informations sur l'aviation (A-ISAC) peuvent fournir des informations sur les menaces pesant sur le transport aérien;*

- *veiller à ce que les évaluations des risques portent aussi sur les risques liés aux activités quotidiennes du personnel (utilisation des médias sociaux, utilisation des appareils personnels, traitement des données, partage d'informations, etc.);*

- *élaborer et mettre en œuvre des mesures et des plans de traitement des risques pour atténuer les risques en matière de cybersécurité;*

- *mettre en œuvre un **système de gestion de la sécurité de l'information** (SGSI) et un **système de gestion des informations personnelles** (SGIP) complets en harmonie avec d'autres systèmes de gestion. Ces systèmes de gestion (c'est-à-dire les SGSI et les SGIP) nécessitent la mise en œuvre de contrôles de sécurité (ainsi que de protection des données et de la vie privée) afin d'atténuer et de prévenir les menaces émergentes nuisant à la sécurité des services et systèmes aéronautiques (et à celle des données connexes);*

- *tenir compte de toutes les contraintes liées à la **gestion des actifs et à la planification des ressources** (c'est-à-dire les contraintes susceptibles de peser sur le fonctionnement, la maintenance et le soutien de systèmes critiques pour l'exploitation des fonctions essentielles dans le transport aérien).*

Exemples de cadres de gestion des risques: différents cadres (normes de la famille ISO/CEI 27000, cadre de cybersécurité NIST, cadre MITRE ATT&CK et BSI IT-Grundschutz, entre autres) peuvent étayer et sous-tendre une approche de gestion des risques adaptée au transport aérien. Des organisations internationales telles que l'IATA et l'OACI fournissent des orientations pour l'évaluation des risques en matière de cybersécurité. L'ENISA, l'AESA, Eurocontrol et le Conseil international des aéroports (ACI) mettent notamment en évidence les bonnes pratiques en matière de protection des aéroports, des prestataires de services de gestion du trafic aérien et d'autres organisations du secteur de l'aviation. L'entreprise commune SESAR coordonne et concentre toutes les activités de recherche et de développement (R&D) de l'UE dans le domaine de la gestion du trafic aérien, y compris celles portant sur des aspects liés à la sûreté et à la sécurité.

Se protéger contre les cybermenaces

Les organisations de transport aérien devraient mettre en œuvre des mesures de sécurité adéquates et proportionnées afin de protéger leurs réseaux et systèmes d'information — y compris les technologies de l'information et les technologies opérationnelles — contre les cyberattaques. Les mesures de sécurité à prendre sont notamment les suivantes:

- ***politiques et processus de sécurité:*** *définir, mettre en œuvre, communiquer et faire appliquer des stratégies et des processus appropriés, qui façonnent une approche globale de la protection des systèmes et des données à l'appui de l'exploitation des fonctions essentielles dans le secteur de l'aviation. Ces stratégies et procédures de sécurité (par exemple, les politiques en matière de mots de passe et de stockage) devraient également porter sur les correctifs et la gestion des vulnérabilités des systèmes matériels et logiciels (y compris des technologies de l'information et des technologies opérationnelles), sur la gestion des incidents et sur la protection des systèmes et des réseaux;*

- ***gestion des identités et des accès:*** *comprendre, documenter et gérer l'accès aux réseaux et systèmes d'information (y compris aux technologies de l'information et aux technologies opérationnelles) qui sous-tendent l'exploitation des fonctions essentielles dans le transport aérien. Les utilisateurs (ou les fonctions automatisées) qui peuvent accéder à des données ou à des systèmes sont dûment vérifiés, authentifiés et autorisés. Cette mesure devrait également tenir compte des différentes fonctions et responsabilités associées aux comptes ordinaires et aux comptes privilégiés;*

- ***sécurité des données et des systèmes:*** *protéger les données (stockées et transmises par voie électronique), les réseaux critiques et les systèmes d'information (y compris les technologies de l'information et les technologies opérationnelles) contre les cyberattaques. Selon une approche axée sur les risques, les organisations devraient mettre en œuvre des mesures de sécurité afin de limiter efficacement les possibilités pour les attaquants de compromettre les données, les réseaux et les systèmes. Ces mesures de sécurité devraient aussi inclure l'adoption de protocoles de chiffrement et de communication sécurisée afin de protéger les données au repos et en transit contre les cybermenaces qui se traduisent par des attaques de l'homme du milieu. En outre, il convient de combiner ces mesures avec des mesures de sécurité physique afin de protéger l'accès aux systèmes (par exemple, les systèmes devraient être situés dans des locaux fermés à accès restreint);*

- ***résilience des réseaux et des systèmes:*** *renforcer la résilience des réseaux et des systèmes (y compris des technologies de l'information et des technologies opérationnelles) en pensant leur conception et leur mise en œuvre (ainsi que leurs procédures opérationnelles) de façon à diminuer et à atténuer l'incidence des cyberattaques. Les solutions de conception et de mise en œuvre permettant de renforcer la résilience sont, par exemple: les fonctions critiques formellement vérifiées, la redondance des systèmes et des réseaux, la séparation des réseaux (en particulier, la séparation des technologies de l'information et des technologies opérationnelles) et les mesures de sécurité à plusieurs niveaux. Il convient de noter que du point de vue de la sécurité de l'information, les domaines de sécurité mettant en œuvre la séparation des réseaux et des systèmes peuvent fournir des solutions de sécurité appropriées. Toutefois, les besoins opérationnels (les activités de maintenance, les transferts de données, etc.) des systèmes peuvent entraîner la nécessité de contourner ou de connecter différents domaines de sécurité (par exemple, systèmes et réseaux séparés), y compris de connecter des technologies de l'information et des technologies opérationnelles.*

Détecter les cybermenaces

Les organisations devraient veiller à ce que les mesures de sécurité restent efficaces et détecter tous les événements compromettant la cybersécurité qui touchent ou sont susceptibles de toucher les contrôles de sécurité, ainsi que les services et systèmes essentiels. Les mesures de sécurité pertinentes en matière de détection des cybermenaces sont les suivantes:

■ ***surveillance de la sécurité:*** *surveiller l'état de sécurité des réseaux et des systèmes d'information — y compris des technologies de l'information et des technologies opérationnelles — qui sous-tendent l'exploitation des fonctions essentielles dans les services de transport aérien. Afin de faciliter la surveillance de la sécurité, les données prises en considération sont, par exemple:*

- *les journaux de sécurité;*
- *les journaux de détection des virus;*
- *les journaux de détection des intrusions;*
- *les journaux d'identification, d'authentification et d'autorisation;*
- *les journaux des systèmes et des services;*
- *les journaux du trafic réseau;*
- *les journaux de traitement des données;*

■ ***découverte d'événements compromettant la sécurité de l'information:*** *détecter les activités malveillantes (c'est-à-dire les événements compromettant la sécurité) qui menacent ou sont susceptibles de menacer la sécurité des réseaux et des systèmes d'information (y compris des technologies de l'information et des technologies opérationnelles) qui sous-tendent l'exploitation des fonctions essentielles dans les services de transport aérien.*

Ces mesures peuvent nécessiter l'adoption de technologies spécifiques (gestion de la sécurité de l'information et gestion des événements compromettant la sécurité, système de détection des intrusions, système de prévention des intrusions, etc.) et la mise en place d'un centre d'opérations de sécurité (SOC) ou d'un organisme équivalent. Il s'agit donc de mettre en place des moyens de détection, d'analyse, de réponse et de rétablissement face aux cyberattaques à l'échelle locale.

Les centres de réponse aux incidents de sécurité informatique (CSIRT), les CERT sectoriels [parmi lesquels le centre de réponse aux urgences informatiques pour la gestion du trafic aérien européen (EATM-CERT)], les CERT privés des compagnies aériennes et le centre d'échange et d'analyse d'informations sur l'aviation (A-ISAC) peuvent fournir des services de renseignement sur les cybermenaces pour éclairer les activités de surveillance de la sécurité et de détection.

Commission européenne

Planification de la réponse et du rétablissement

Les organisations devraient définir, mettre en œuvre et mettre à l'essai des procédures de gestion des incidents visant à assurer la continuité des activités des services et systèmes en cas d'incident de cybersécurité. Les mesures d'atténuation ont pour objectif de freiner ou limiter les conséquences des incidents de sécurité informatique.

La planification de la réponse et du rétablissement devrait tenir compte des mesures de sécurité visant à atténuer l'incidence de cyberattaques spécifiques, telles que:

- *la coordination et la collaboration avec les CSIRT nationaux, les CERT (publics et privés) et les ISAC pendant les incidents de sécurité informatique, et la coordination au niveau paneuropéen en situation d'incident et de crise;*

- *le partage d'informations avec d'autres organisations, y compris avec des prestataires situés dans la chaîne d'approvisionnement des services aéronautiques;*

- *la réalisation périodique d'**exercices de cyberattaques** (coordination sur table et exercices techniques) pour évaluer les mesures et procédures de sécurité ainsi que la résilience de l'organisation pour faire face aux incidents de sécurité informatique;*

- *l'accès aux sites de stockage archivés ou de sauvegarde lorsque l'intégrité et la disponibilité des espaces de stockage de données sont compromises;*

- *l'élaboration de **manuels de sécurité** comportant des procédures détaillées pour gérer les incidents de sécurité informatique et ramener les services et les systèmes dans des conditions opérationnelles normales;*

- *la réorientation du trafic réseau vers des services redondants lors d'attaques par déni de service;*

- *les procédures manuelles pour l'exploitation des services et des systèmes dans des modes d'exploitation diminués;*

- *la définition de procédures pour lutter contre les violations de données, y compris de procédures de lutte contre les violations de données portant sur des données à caractère personnel, conformément au règlement général sur la protection des données (RGPD) et à tout autre règlement ou directive sectorielle en la matière;*

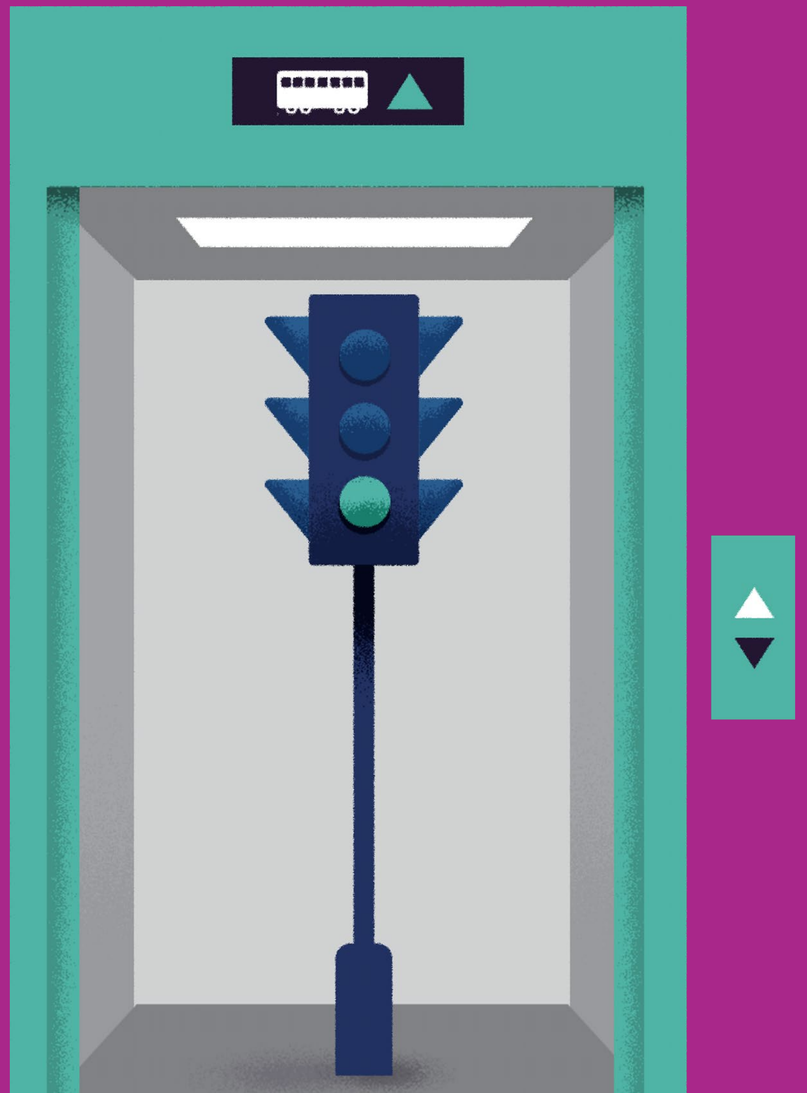
- *la souscription d'une **assurance face aux risques informatiques** afin d'atténuer partiellement le risque associé aux incidents de sécurité informatique graves;*

- *le versement de paiements de disponibilité à une ou plusieurs firmes spécialisées dans les interventions en cas d'incident pour disposer de capacités et de compétences supplémentaires;*

- *la définition de procédures pour le **partage d'informations sur les incidents de sécurité informatique** avec les parties prenantes concernées, y compris de procédures de notification des incidents conformes à la directive SRI [directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union].*

Commission européenne

Bonnes pratiques et mesures de sécurité adaptées au transport terrestre



Gouvernance

Les organisations du secteur du transport terrestre (ferroviaire et routier) doivent comprendre clairement les menaces émergentes afin de définir des stratégies et des processus de gestion régissant leurs approches et d'améliorer la cybersécurité des services et systèmes d'exploitation, y compris des technologies de l'information et des technologies opérationnelles.

Les bonnes pratiques applicables aux organisations de toute taille sont les suivantes:

- *veiller à ce que le personnel d'encadrement supérieur signale les enjeux en matière de cybersécurité aux instances dirigeantes et aux conseils d'administration afin que ceux-ci puissent prendre des décisions éclairées concernant l'allocation des ressources;*

- *nommer un haut responsable de la cybersécurité et de la sécurité physique, chargé de la gestion générale de la sécurité des technologies de l'information et des technologies opérationnelles, mais ne participant pas à l'exploitation afin d'éviter les conflits d'intérêts;*

- *définir clairement les rôles, les responsabilités, les compétences et les habilitations en matière de cybersécurité, en concertation et en accord avec le personnel concerné, en particulier avec le personnel des centres de réponse aux urgences informatiques (CERT);*

- *garantir la bonne gouvernance en matière de cybersécurité tout au long de la chaîne d'approvisionnement en services de sécurité, pour les interfaces aussi bien physiques que numériques, depuis les fabricants et les installateurs de technologies jusqu'aux fournisseurs de services de sécurité;*

- *convenir des activités et des contrôles, y compris des responsabilités partagées, à mettre en place pour gérer les risques en matière de cybersécurité, et veiller à ce que ces responsabilités soient maintenues (par exemple, par des accords de service) tant que les solutions et services de sécurité sont utilisés;*

- *définir des mécanismes de gouvernance (par exemple, des politiques) afin de se conformer aux obligations découlant des règlements et directives en matière de cybersécurité. Ce point englobe un large éventail de politiques portant sur les différents modes de transport, ainsi que différentes catégories de parties prenantes (par exemple, les constructeurs de véhicules et de systèmes ferroviaires), ainsi que la directive SRI [directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information].*

Commission européenne

Exemples de services et de systèmes dans le transport terrestre: les technologies de l'information sont, par exemple, les appareils accessibles aux employés (ordinateurs personnels, téléphones portables, périphériques de bureau, etc.) ainsi qu'aux passagers (connexions Wi-Fi publiques, etc.). Parmi les exemples de technologies opérationnelles figurent les systèmes d'acquisition et de contrôle des données (SCADA), les systèmes de chauffage, de ventilation et de climatisation (CVC), les systèmes de localisation GPS, le contrôle d'accès, le suivi, la surveillance, la réaction aux alarmes et la technologie de filtrage. Parmi les systèmes spécifiques au transport ferroviaire figurent notamment les systèmes d'exploitation (systèmes de contrôle-commande), y compris les systèmes de signalisation, le système européen de gestion du trafic ferroviaire (ERTMS), les systèmes ferroviaires embarqués, les systèmes de maintenance, etc.

Commission européenne

Identifier les cybermenaces

Gestion des risques: les organisations du secteur du transport terrestre doivent prendre les mesures appropriées afin d'identifier, d'évaluer et de comprendre les risques en matière de cybersécurité pour le réseau et les systèmes d'information qui sous-tendent l'exploitation des fonctions essentielles. Pour ce faire, elles doivent adopter une approche organisationnelle globale de la gestion des risques, en menant notamment les actions suivantes:

- *avoir une vue d'ensemble claire des différents systèmes matériels et logiciels déployés pour fournir différents services. Dans le contexte du transport terrestre, ces systèmes font intervenir des technologies de l'information ainsi que des technologies opérationnelles;*

- *réaliser des **évaluations des risques en matière de cybersécurité**, qui devraient tenir compte des menaces émergentes, des vulnérabilités connues et des données opérationnelles relatives aux systèmes évalués. Parmi les exemples de systèmes dans les modes de transport terrestre figurent: les systèmes de paiement, les systèmes de réseaux et de communication (internet, radiocommunication, Wi-Fi, etc.), les équipements embarqués, les centres de contrôle opérationnels, les systèmes de gestion de l'identité, les systèmes de sécurité, etc. Les systèmes des infrastructures ferroviaires sont, par exemple: le matériel roulant, les sous-systèmes d'exploitation et de gestion du trafic, les systèmes de contrôle-commande, les sous-systèmes de signalisation à bord et en bordure des voies, etc.;*

- *veiller à ce que les évaluations des risques portent aussi sur les risques liés aux activités quotidiennes du personnel (utilisation des médias sociaux, utilisation des appareils personnels, traitement des données, partage d'informations, etc.);*

- *élaborer et mettre en œuvre des mesures et des plans de traitement des risques pour atténuer les risques en matière de cybersécurité; par exemple, mettre en œuvre un **système de gestion de la sécurité de l'information** (SGSI) et un **système de gestion des informations personnelles** (SGIP) complets en harmonie avec d'autres systèmes de gestion. Ces systèmes de gestion (c'est-à-dire les SGSI et les SGIP) nécessitent la mise en œuvre de contrôles de sécurité (ainsi que de protection des données et de la vie privée) afin d'atténuer et de prévenir les menaces émergentes nuisant à la sécurité des services et systèmes de transport terrestre (et à celle des données connexes);*

- *tenir compte de toutes les contraintes liées à la **gestion des actifs et à la planification des ressources** (c'est-à-dire les contraintes susceptibles de peser sur le fonctionnement, la maintenance et le soutien de systèmes critiques pour l'exploitation des fonctions essentielles dans le transport terrestre).*

Exemples de cadres de gestion des risques: différents cadres (normes de la famille ISO/CEI 27000, cadre de cybersécurité NIST, cadre MITRE ATT&CK et BSI IT-Grundschutz, entre autres) peuvent étayer et sous-tendre une approche de gestion des risques adaptée au transport routier et ferroviaire. Des organisations telles que l'ENISA définissent des bonnes pratiques en matière de cybersécurité pour les voitures intelligentes et des transports publics intelligents, destinés aux constructeurs et aux associations du secteur (par exemple, l'Association des constructeurs européens d'automobiles — ACEA). Dans le domaine du transport ferroviaire, l'Agence de l'Union européenne pour les chemins de fer (ERA) définit des spécifications techniques d'interopérabilité (STI) auxquelles chaque sous-système ou partie de sous-système doit se conformer pour satisfaire aux exigences essentielles et assurer l'interopérabilité du système ferroviaire de l'Union européenne. L'entreprise commune Shift2Rail est également le moteur d'initiatives et de projets innovants dans le domaine du transport ferroviaire (y compris en matière de cybersécurité).

Se protéger contre les cybermenaces

Les organisations de transport terrestre devraient mettre en œuvre des mesures de sécurité adéquates et proportionnées afin de protéger leurs réseaux et systèmes d'information — y compris les technologies de l'information et les technologies opérationnelles — contre les cyberattaques. Les mesures de sécurité à prendre sont notamment les suivantes:

- ***politiques et processus de sécurité:*** *définir, mettre en œuvre, communiquer et faire appliquer des stratégies et des processus appropriés, qui façonnent une approche globale de la protection des systèmes et des données à l'appui de l'exploitation des fonctions essentielles dans les modes transport terrestre. Ces stratégies et procédures de sécurité (par exemple, les politiques en matière de mots de passe et de stockage) devraient également porter sur les correctifs et la gestion des vulnérabilités des systèmes matériels et logiciels (y compris des technologies de l'information et des technologies opérationnelles), sur la gestion des incidents et sur la protection des systèmes et des réseaux;*

- ***gestion des identités et des accès:*** *comprendre, documenter et gérer l'accès aux réseaux et systèmes d'information (y compris aux technologies de l'information et aux technologies opérationnelles) qui sous-tendent l'exploitation des fonctions essentielles dans les modes transport terrestre. Les utilisateurs (ou les fonctions automatisées) qui peuvent accéder à des données ou à des systèmes sont dûment vérifiés, authentifiés et autorisés. Cette mesure devrait également tenir compte des différentes fonctions et responsabilités associées aux comptes ordinaires et aux comptes privilégiés;*

- ***sécurité des données et des systèmes:*** *protéger les données (stockées et transmises par voie électronique), les réseaux critiques et les systèmes d'information (y compris les technologies de l'information et les technologies opérationnelles) contre les cyberattaques. Selon une approche axée sur les risques, les organisations devraient mettre en œuvre des mesures de sécurité afin de limiter efficacement les possibilités pour les attaquants de compromettre les données, les réseaux et les systèmes. Ces mesures de sécurité devraient aussi inclure l'adoption de protocoles de chiffrement et de communication sécurisée afin de protéger les données au repos et en transit contre les cybermenaces qui se traduisent par des attaques de l'homme du milieu. En outre, il convient de combiner ces mesures avec des mesures de sécurité physique afin de protéger l'accès aux systèmes (par exemple, les systèmes devraient être situés dans des locaux fermés à accès restreint). Ce point est très important pour les systèmes susceptibles d'avoir une incidence sur la sécurité de la vie humaine;*

- ***résilience des réseaux et des systèmes:*** *renforcer la résilience des réseaux et des systèmes (y compris des technologies de l'information et des technologies opérationnelles) en pensant leur conception et leur mise en œuvre (ainsi que leurs procédures opérationnelles) de façon à diminuer et à atténuer l'incidence des cyberattaques. Les solutions de conception et de mise en œuvre permettant de renforcer la résilience sont, par exemple: les fonctions critiques formellement vérifiées, la redondance des systèmes et des réseaux, la séparation des réseaux (en particulier, la séparation des technologies de l'information et des technologies opérationnelles) et les mesures de sécurité à plusieurs niveaux. Il convient de noter que du point de vue de la sécurité de l'information, les domaines de sécurité mettant en œuvre la séparation des réseaux et des systèmes peuvent fournir des solutions de sécurité appropriées. Toutefois, les besoins opérationnels (les activités de maintenance, les transferts de données, etc.) des systèmes peuvent entraîner la nécessité de contourner ou de connecter différents domaines de sécurité (par exemple, systèmes et réseaux séparés), y compris de connecter des technologies de l'information et des technologies opérationnelles.*

Détecter les cybermenaces

Les organisations devraient veiller à ce que les mesures de sécurité restent efficaces et détecter tous les événements compromettant la cybersécurité qui touchent ou sont susceptibles de toucher les contrôles de sécurité, ainsi que les services et systèmes essentiels. Les mesures de sécurité pertinentes en matière de détection des cybermenaces sont les suivantes:

- ***surveillance de la sécurité:*** *surveiller l'état de sécurité des réseaux et des systèmes d'information — y compris des technologies de l'information et des technologies opérationnelles — qui sous-tendent l'exploitation des fonctions essentielles dans les modes transport terrestre. Cette mesure est nécessaire afin de détecter les menaces potentielles pour la sécurité et de surveiller l'efficacité des mesures de sécurité et de protection dans la durée. Afin de faciliter la surveillance de la sécurité, les données prises en considération sont, par exemple:*

  - *les journaux de sécurité;*
  - *les journaux de détection des virus;*
  - *les journaux de détection des intrusions;*
  - *les journaux d'identification, d'authentification et d'autorisation;*
  - *les journaux des systèmes et des services;*
  - *les journaux du trafic réseau;*
  - *les journaux de traitement des données;*

- ***découverte d'événements compromettant la sécurité de l'information:*** *détecter les activités malveillantes (c'est-à-dire les événements compromettant la sécurité) qui menacent ou sont susceptibles de menacer la sécurité des réseaux et des systèmes d'information (y compris des technologies de l'information et des technologies opérationnelles) qui sous-tendent l'exploitation des fonctions essentielles.*

Ces mesures peuvent nécessiter l'adoption de technologies spécifiques (gestion de la sécurité de l'information et gestion des événements compromettant la sécurité, système de détection des intrusions, système de prévention des intrusions, etc.) et la mise en place d'un centre d'opérations de sécurité (SOC) ou d'un organisme équivalent. Il s'agit donc de mettre en place des moyens de détection, d'analyse, de réponse et de rétablissement face aux cyberattaques à l'échelle locale.
Les centres de réponse aux incidents de sécurité informatique (CSIRT), les CERT sectoriels et privés, les opérateurs routiers et ferroviaires et le centre d'échange et d'analyse d'informations pour le rail européen (ER-ISAC) peuvent fournir des services de renseignement sur les cybermenaces pour informer les activités de surveillance de la sécurité et de détection.

Commission européenne

Planification de la réponse et du rétablissement

Les organisations devraient définir, mettre en œuvre et mettre à l'essai des procédures de gestion des incidents visant à assurer la continuité des activités des services et systèmes en cas d'incident de cybersécurité.

La planification de la réponse et du rétablissement devrait tenir compte des mesures de sécurité visant à atténuer l'incidence de cyberattaques spécifiques, telles que:

- *la coordination et la collaboration avec les CSIRT nationaux, les CERT (publics et privés) et les ISAC pendant les incidents de sécurité informatique, et la coordination au niveau paneuropéen en situation d'incident et de crise;*

- *le partage d'informations avec d'autres organisations, y compris avec des prestataires situés dans la chaîne d'approvisionnement des services de transport terrestre;*

- *la réalisation périodique d'**exercices de cyberattaques** (coordination sur table et exercices techniques) pour évaluer les mesures et procédures de sécurité ainsi que la résilience de l'organisation pour faire face aux incidents de sécurité informatique;*

- *l'accès aux sites de stockage archivés ou de sauvegarde lorsque l'intégrité et la disponibilité des espaces de stockage de données sont compromises;*

- *l'élaboration de **manuels de sécurité** comportant des procédures détaillées pour gérer les incidents de sécurité informatique et ramener les services et les systèmes dans des conditions opérationnelles normales;*

- *la réorientation du trafic réseau vers des services redondants lors d'attaques par déni de service;*

- *les procédures manuelles pour l'exploitation des services et des systèmes dans des modes d'exploitation diminués;*

- *la définition de procédures pour lutter contre les violations de données, y compris de procédures de lutte contre les violations de données portant sur des données à caractère personnel, conformément au règlement général sur la protection des données (RGPD) et à tout autre règlement ou directive sectorielle en la matière;*

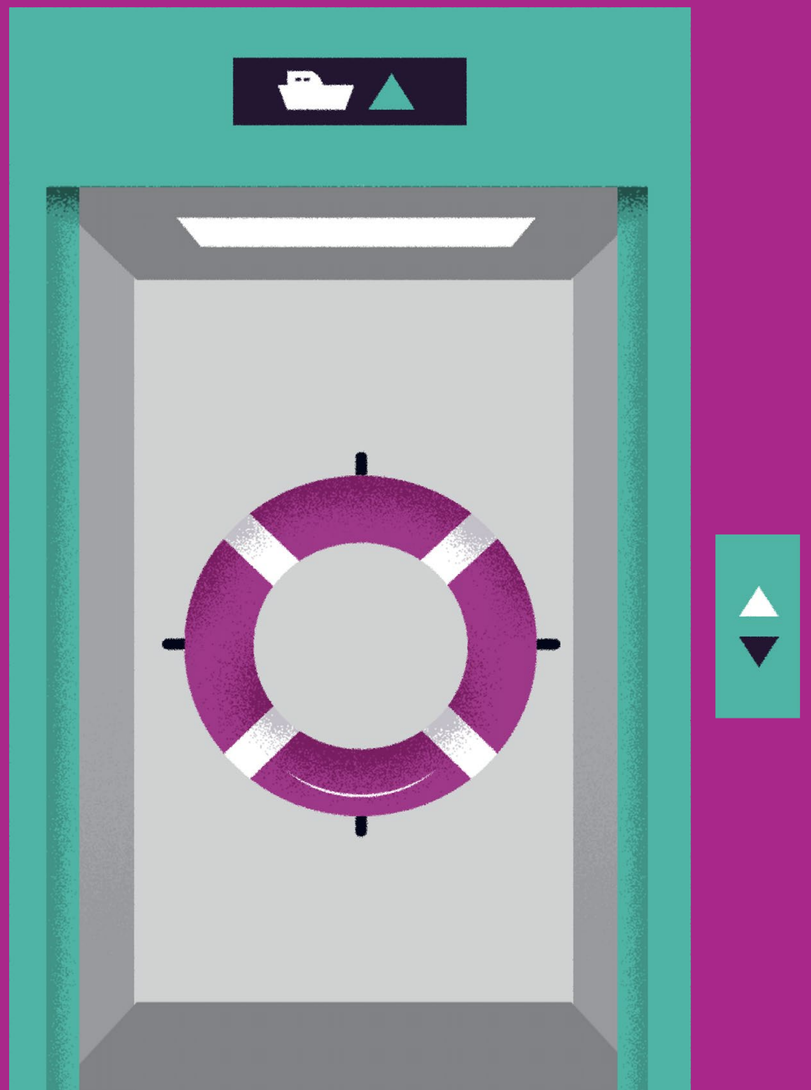
- *la souscription d'une **assurance face aux risques informatiques** afin d'atténuer partiellement le risque associé aux incidents de sécurité informatique graves;*

- *le versement de paiements de disponibilité à une ou plusieurs firmes spécialisées dans les interventions en cas d'incident pour disposer de capacités et de compétences supplémentaires;*

- *la définition de procédures pour le partage d'informations sur les incidents de sécurité informatique avec les parties prenantes concernées, y compris de procédures de notification des incidents conformes à la directive SRI [directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union].*

Commission européenne

Bonnes pratiques et mesures de sécurité adaptées au transport maritime



Commission européenne

Gouvernance

Les organisations du secteur du transport maritime doivent comprendre clairement les menaces émergentes afin de définir les politiques et les processus de gestion régissant leurs approches et d'améliorer la cybersécurité des services et systèmes d'exploitation, y compris des technologies de l'information et des technologies opérationnelles.

Les bonnes pratiques applicables aux organisations de toute taille sont les suivantes:

- *veiller à ce que le personnel d'encadrement supérieur signale les enjeux en matière de cybersécurité aux instances dirigeantes et aux conseils d'administration afin que ceux-ci puissent prendre des décisions éclairées concernant l'allocation des ressources;*

- *nommer un haut responsable chargé de la gestion générale de la sécurité des technologies de l'information et des technologies opérationnelles. Cette personne devrait être responsable de la cybersécurité et de la sécurité physique;*

- *définir clairement les rôles, les responsabilités, les compétences et les habilitations en matière de cybersécurité, et définir les niveaux d'autorité et les lignes de communication pour et entre le personnel à terre et le personnel à bord, en concertation et en accord avec le personnel concerné, en particulier avec le personnel des centres de réponse aux urgences informatiques (CERT). Les membres du personnel ayant des fonctions liées à la législation de l'UE en matière de sécurité et de sûreté maritimes, tels que les agents de sûreté des installations portuaires, les agents de sûreté portuaire, les responsables de la sûreté au sein des compagnies, la personne désignée à terre et le capitaine devraient au moins posséder une bonne connaissance des mesures de cybersécurité prises par l'organisation;*

- *garantir la bonne gouvernance en matière de cybersécurité tout au long de la chaîne d'approvisionnement en services de sécurité, pour les interfaces aussi bien physiques que numériques, depuis les fabricants et les installateurs de technologies jusqu'aux fournisseurs de services de sécurité;*

- *convenir des activités et des contrôles, y compris des responsabilités partagées, à mettre en place pour gérer les risques en matière de cybersécurité, et veiller à ce que ces responsabilités soient maintenues (par exemple, par des accords de service) tant que les solutions et services de sécurité sont utilisés;*

- *définir des mécanismes de gouvernance (par exemple, des politiques) afin de se conformer aux obligations découlant des règlements et directives en matière de cybersécurité, par exemple du règlement (UE) 2019/1239 établissant un système de guichet unique maritime européen (EMSWe), du règlement (CE) nº 725/2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires, de la directive 2005/65/CE relative à l'amélioration de la sûreté des ports, du règlement (CE) nº 336/2006 relatif à l'application du code international de gestion de la sécurité (ISM) et la résolution A.741(18) adoptant le code ISM pour la sécurité de l'exploitation des navires et la prévention de la pollution. Dans ce contexte, il convient également de mentionner l'environnement commun de partage de l'information (CISE), une initiative de l'UE qui a pour objectif de rendre les systèmes de surveillance de l'Union et des États membres interopérables afin de permettre à toutes les autorités concernées d'accéder aux informations classifiées et non classifiées dont elles ont besoin pour effectuer des missions en mer.*

Commission européenne

Exemples de services et de systèmes dans le transport maritime: les technologies de l'information sont, par exemple, les appareils accessibles aux employés (ordinateurs personnels, téléphones portables, périphériques de bureau, etc.) ainsi qu'aux passagers (connexions Wi-Fi publiques, etc.). Parmi les exemples de technologies opérationnelles figurent les systèmes d'acquisition et de contrôle des données (SCADA), les systèmes de chauffage, de ventilation et de climatisation (CVC), les systèmes de localisation GPS, le contrôle d'accès, le suivi, la surveillance, la réaction aux alarmes, la technologie de filtrage, les systèmes de navigation embarqués, SafeSeaNet, les systèmes de pont, les systèmes de manutention et de gestion du fret, les systèmes de gestion de la propulsion et des machines et les commandes de puissance, les systèmes de contrôle d'accès, les systèmes de service et de gestion à l'intention des passagers, les réseaux publics à l'intention des passagers, les systèmes d'administration et de bien-être de l'équipage, les systèmes de communication, etc.

Commission européenne

Identifier les cybermenaces

Gestion des risques: les organisations maritimes doivent prendre des mesures appropriées afin d'identifier, d'analyser, d'évaluer et de communiquer les risques en matière de cybersécurité, ainsi que pour les accepter, les éviter, les transférer ou les réduire à un niveau acceptable. Pour ce faire, elles doivent adopter une approche organisationnelle globale de la gestion des risques, en menant notamment les actions suivantes:

- *avoir une vue d'ensemble claire des différents systèmes matériels et logiciels déployés pour fournir différents services. Dans le contexte du transport maritime, ces systèmes font intervenir des technologies de l'information et des technologies opérationnelles, et la manière dont ces systèmes se connectent et s'intègrent avec les acteurs à terre, notamment avec les autorités, les terminaux maritimes et les manutentionnaires;*

- *recenser et évaluer les principales opérations à bord des navires qui sont vulnérables aux cyberattaques, et réaliser des évaluations des risques en matière de cybersécurité (y compris des évaluations des incidences opérationnelles potentielles et de la probabilité d'occurrence), lesquelles devraient tenir compte des menaces émergentes, des vulnérabilités connues et des données opérationnelles relatives aux systèmes évalués. Le cas échéant, il convient de faire le lien avec les évaluations de sûreté effectuées pour les navires (SSA), les installations portuaires (PFSA) et les ports (PSA), conformément à la législation de l'UE en matière de sûreté maritime. Ces évaluations recensent les éventuelles menaces pesant sur la sûreté des infrastructures portuaires et les faiblesses en matière de sûreté. En outre, des organisations maritimes telles que l'Organisation maritime internationale (OMI) et les ISAC maritimes peuvent fournir des informations sur les menaces ciblant le transport maritime;*

- *veiller à ce que les évaluations des risques portent aussi sur les risques liés aux activités quotidiennes du personnel (utilisation des médias sociaux, utilisation des appareils personnels, traitement des données, partage d'informations, etc.);*

- *élaborer et mettre en œuvre des mesures et des plans de traitement des risques pour atténuer les risques en matière de cybersécurité. Par exemple, mettre en œuvre un système de gestion de la sécurité de l'information (SGSI) et un système de gestion des informations personnelles (SGIP) complets en harmonie avec d'autres systèmes de gestion tels que les systèmes de gestion de la sécurité (SGS), conformément au code international de gestion de la sécurité (ISM). Ces systèmes de gestion (c'est-à-dire les SGSI et les SGIP) nécessitent la mise en œuvre de contrôles de sécurité (ainsi que de protection des données et de la vie privée) afin d'atténuer et de prévenir les menaces émergentes nuisant à la sécurité des services et systèmes maritimes (et à celle des données connexes);*

- *tenir compte de toutes les contraintes liées à la **gestion des actifs et à la planification des ressources** (c'est-à-dire les contraintes susceptibles de peser sur le fonctionnement, la maintenance et le soutien de systèmes critiques pour l'exploitation des fonctions essentielles dans le transport maritime). En ce qui concerne les évaluations, il convient de faire référence, le cas échéant, aux exigences du code ISM, des systèmes de gestion de la sécurité (SGS) et des plans de sécurité mis en œuvre conformément à la législation de l'UE en matière de sûreté et de sécurité maritimes.*

Exemples de cadres de gestion des risques: différents cadres (code ISM ou normes de la famille ISO/CEI 27000, cadre de cybersécurité NIST, cadre MITRE ATT&CK et BSI IT-Grundschutz, entre autres) peuvent étayer et sous-tendre une approche de gestion des risques adaptée au transport maritime. Le cadre de cybersécurité NIST a aussi été adapté pour s'appliquer à la cybersécurité des transferts maritimes de liquides en vrac, des opérations en mer et de l'exploitation des navires à passagers. De même, le Conseil maritime baltique et international (BIMCO) a publié des *«directives sur la cybersécurité à bord des navires»* et l'Organisation maritime internationale (OMI) a publié des *«directives sur la gestion des cyber-risques maritimes»* (MSC-FAL.1/Circ.3). L'ENISA a mené plusieurs études portant sur les bonnes pratiques en matière de cybersécurité maritime, en particulier sur la cybersécurité portuaire. L'AESM fournit des services à la communauté maritime, y compris des formations de sensibilisation à la cybersécurité. Des normes (la norme CEI 61162-460:2018 sur la sûreté et la sécurité des matériels et systèmes de navigation et de radiocommunication maritimes, la norme ISO 16425:2013 sur les navires et les technologies maritimes, la norme CEI 62443-4-1:2018 sur la sécurité des automatismes industriels et des systèmes de commande industriels, etc.) définissent aussi des exigences spécifiques en matière de sécurité et de sûreté pour les systèmes et réseaux de transport maritime.

Se protéger contre les cybermenaces

Les organisations de transport maritime devraient mettre en œuvre des mesures de sécurité adéquates et proportionnées afin de protéger leurs réseaux et systèmes d'information — y compris les technologies de l'information et les technologies opérationnelles. Les mesures de sécurité à prendre sont notamment les suivantes:

- ***politiques et processus de sécurité:*** *définir, mettre en œuvre, communiquer et faire appliquer des stratégies et des processus appropriés, qui façonnent une approche globale de la protection des systèmes et des données à l'appui de l'exploitation des fonctions essentielles dans le transport maritime. Des mesures de sécurité (y compris des mesures de sécurité informatique et de sécurité physique) devraient être incluses dans les plans pertinents, notamment dans le système de gestion de la sécurité (SGS) et le plan de sûreté du navire (SSP). Ces stratégies et procédures de sécurité (par exemple, les politiques en matière de mots de passe et de stockage) devraient également porter sur les correctifs et la gestion des vulnérabilités des systèmes matériels et logiciels (y compris des technologies de l'information et des technologies opérationnelles), sur la gestion des incidents et sur la protection des systèmes et des réseaux;*

- ***gestion des identités et des accès:*** *comprendre, documenter et gérer l'accès aux réseaux et systèmes d'information (y compris aux technologies de l'information et aux technologies opérationnelles) qui sous-tendent l'exploitation des fonctions essentielles dans le transport maritime. Les utilisateurs (ou les fonctions automatisées) qui peuvent accéder à des données ou à des systèmes sont dûment vérifiés, authentifiés et autorisés. Cette mesure devrait également tenir compte des différentes fonctions et responsabilités associées aux comptes ordinaires et aux comptes privilégiés;*

- ***sécurité des données et des systèmes:*** *protéger les données (stockées et transmises par voie électronique), les réseaux critiques et les systèmes d'information (y compris les technologies de l'information et les technologies opérationnelles) contre les cyberattaques. Selon une approche axée sur les risques, les organisations devraient mettre en œuvre des mesures de sécurité afin de limiter efficacement les possibilités pour les attaquants de compromettre les données, les réseaux et les systèmes. Ces mesures de sécurité devraient aussi inclure l'adoption de protocoles de chiffrement et de communication sécurisée afin de protéger les données au repos et en transit contre les cybermenaces qui se traduisent par des attaques de l'homme du milieu. En outre, il convient de combiner ces mesures avec des mesures de sécurité physique afin de protéger l'accès aux systèmes (par exemple, les systèmes devraient être situés dans des locaux fermés à accès restreint). Ce point est très important pour les systèmes susceptibles d'avoir une incidence sur la sécurité de la vie humaine (par exemple, les systèmes de navigation et de radiocommunication des catégories II et III);*

- ***résilience des réseaux et des systèmes:*** *renforcer la résilience des réseaux et des systèmes (y compris des technologies de l'information et des technologies opérationnelles) en pensant leur conception et leur mise en œuvre (ainsi que leurs procédures opérationnelles) de façon à diminuer et à atténuer l'incidence des cyberattaques. Les solutions de conception et de mise en œuvre permettant de renforcer la résilience sont, par exemple: les fonctions critiques formellement vérifiées, la redondance des systèmes et des réseaux, la séparation des réseaux (en particulier, la séparation des technologies de l'information et des technologies opérationnelles) et les mesures de sécurité à plusieurs niveaux. Il convient de noter que du point de vue de la sécurité de l'information, les domaines de sécurité mettant en œuvre la séparation des réseaux et des systèmes peuvent fournir des solutions de sécurité appropriées. Toutefois, les besoins (les activités de maintenance, les transferts de données, etc.) des systèmes (par exemple, des navires autonomes maritimes de surface — MASS) peuvent entraîner la nécessité de contourner ou de connecter différents domaines de sécurité (par exemple, systèmes et réseaux séparés), y compris de connecter des technologies de l'information et des technologies opérationnelles.*

Commission européenne

Détecter les cybermenaces

Les organisations devraient veiller à ce que les mesures de sécurité restent efficaces et détecter tous les événements compromettant la cybersécurité qui touchent ou sont susceptibles de toucher les contrôles de sécurité, ainsi que les services et systèmes essentiels. Les mesures de sécurité pertinentes en matière de détection des cybermenaces sont les suivantes:

■ ***surveillance de la sécurité:*** *surveiller l'état de sécurité des réseaux et des systèmes d'information — y compris des technologies de l'information et des technologies opérationnelles — qui sous-tendent l'exploitation des fonctions essentielles dans les services de transport maritime. Cette mesure est nécessaire afin de détecter les menaces potentielles pour la sécurité et de surveiller l'efficacité des mesures de sécurité et de protection dans la durée. Afin de faciliter la surveillance de la sécurité, les données prises en considération sont, par exemple:*

- *les journaux de sécurité;*
- *les journaux de détection des virus;*
- *les journaux de détection des intrusions;*
- *les journaux d'identification, d'authentification et d'autorisation;*
- *les journaux des systèmes et des services;*
- *les journaux du trafic réseau;*
- *les journaux de traitement des données;*

■ ***découverte d'événements compromettant la sécurité de l'information:*** *détecter les activités malveillantes (c'est-à-dire les événements compromettant la sécurité) qui menacent ou sont susceptibles de menacer la sécurité des réseaux et des systèmes d'information (y compris des technologies de l'information et des technologies opérationnelles) qui sous-tendent l'exploitation des fonctions essentielles dans les services de transport maritime.*

Ces mesures peuvent nécessiter l'adoption de technologies spécifiques (gestion de la sécurité de l'information et gestion des événements compromettant la sécurité, système de détection des intrusions, système de prévention des intrusions, etc.) et la mise en place d'un centre d'opérations de sécurité (SOC) ou d'un organisme équivalent. Il s'agit donc de développer des moyens de détection, d'analyse, de réponse et de rétablissement face aux cyberattaques à l'échelon local.

Les centres de réponse aux incidents de sécurité informatique (CSIRT), les CERT sectoriels et les CERT privés d'opérateurs maritimes et les ISAC maritimes peuvent fournir des services de renseignement sur les cybermenaces pour informer les activités de surveillance de la sécurité et de détection.

Commission européenne

Planification de la réponse et du rétablissement

Les organisations devraient définir, mettre en œuvre et mettre à l'essai des procédures de gestion des incidents visant à assurer la continuité des activités des services et systèmes en cas d'incident de cybersécurité.
La planification de la réponse et du rétablissement devrait tenir compte des mesures de sécurité visant à atténuer l'incidence de cyberattaques spécifiques, telles que:

- *la réorientation du trafic réseau vers des services redondants lors d'attaques par déni de service;*

- *les procédures manuelles pour l'exploitation des services et des systèmes dans des modes d'exploitation diminués;*

- *l'établissement de programmes pour les entraînements et les exercices (par exemple, exercices de coordination sur table, exercices techniques et de réaction) afin de se préparer à répondre aux cyberattaques et aux situations d'urgence et d'évaluer les mesures de sécurité, les procédures et la résilience de l'organisation pour faire face aux incidents de sécurité informatique;*

- *l'accès aux sites de stockage archivés ou de sauvegarde lorsque l'intégrité et la disponibilité des espaces de stockage de données sont compromises;*

- *la coordination et la collaboration avec les CSIRT nationaux, les CERT (publics et privés) et les ISAC pendant les incidents de sécurité informatique, et la coordination au niveau paneuropéen en situation d'incident et de crise;*

- *le partage d'informations avec d'autres organisations, y compris avec des prestataires situés dans la chaîne d'approvisionnement des services du transport maritime;*

- *l'élaboration de manuels de sécurité comportant des procédures détaillées pour gérer les incidents de sécurité informatique et ramener les services et les systèmes dans des conditions opérationnelles normales;*

- *la définition de procédures pour lutter contre les violations de données, y compris de procédures de lutte contre les violations de données portant sur des données à caractère personnel, conformément au règlement général sur la protection des données (RGPD) et à tout autre règlement ou directive sectorielle en la matière;*

- *la souscription d'une assurance face aux risques informatiques afin d'atténuer partiellement le risque associé aux incidents de sécurité informatique graves;*

- *le versement de paiements de disponibilité à une ou plusieurs firmes spécialisées dans les interventions en cas d'incident pour disposer de capacités et de compétences supplémentaires;*

- *la définition de procédures pour le partage d'informations sur les incidents de sécurité informatique (y compris sur les non-conformités, les accidents et les situations dangereuses) avec les parties prenantes concernées, y compris de procédures de notification des incidents conformes à la directive SRI [directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union].*

Luxembourg: Office des publications de l'Union européenne, 2021

Print	ISBN 978-92-76-40472-9	doi:10.2832/398308	MI-05-21-230-FR-C
PDF	ISBN 978-92-76-40468-2	doi:10.2832/034	MI-05-21-230-FR-N

Office des publications de l'Union européenne