QBS
SOFTWARE
DELIVERY PLATFORM

Guide de cybersécurité pour le secteur MARITIME

Table des matières

Guide de cybersécurité

Les navires utilisent de plus en plus de systèmes qui reposent sur la numérisation, la digitalisation, l'intégration et l'automatisation, ce qui nécessite une gestion des cyber-risques à bord. À mesure que la technologie se développe, les technologies de l'information (TI) et les technologies opérationnelles (TO) à bord des navires sont de plus en plus connectées à l'internet.

Le risque d'accès non autorisé ou d'attaques malveillantes aux systèmes et réseaux des navires s'en trouve accru. Les risques peuvent également provenir du personnel accédant aux systèmes à bord, par exemple en introduisant des logiciels malveillants via des supports amovibles.

Incidents de cybersécurité

Les incidents de cybersécurité peuvent survenir à la suite de :

- un incident de cybersécurité qui affecte la disponibilité et l'intégrité des TO, par exemple la corruption des données cartographiques contenues dans un système de visualisation des cartes électroniques et d'information (ECDIS)
- une panne survenant lors de la maintenance et de l'installation de correctifs dans les logiciels
- la perte ou la manipulation de données de capteurs externes, essentielles au fonctionnement d'un navire, notamment les systèmes mondiaux de navigation par satellite (GNSS).

Les navires sont de plus en plus intégrés aux opérations à terre, car la communication numérique est utilisée pour faire du business, gérer les opérations et garder le contact avec le siège social.

En outre, les systèmes critiques des navires, essentiels à la sécurité de la navigation, à l'alimentation électrique et à la gestion de la cargaison, sont toujours davantage numérisés et connectés à l'internet pour remplir une grande variété de fonctions légitimes telles que :

- le contrôle des performances du moteur
- la maintenance et la gestion des pièces de rechange
- la gestion de la cargaison, du chargement et du déchargement, des grues, des pompes et la planification de l'arrimage
- le suivi des performances du voyage

La liste ci-dessus fournit des exemples de cette interface et n'est pas exhaustive.
Les systèmes ci-dessus fournissent des données qui peuvent être intéressantes à exploiter pour les cybercriminels.

Gestion du risque cybernétique

La gestion du risque cybernétique doit :

- identifier les rôles et responsabilités des utilisateurs, du personnel clé et de la direction à terre et à bord
- identifier les systèmes, les actifs, les données et les capacités qui, s'ils sont perturbés, pourraient présenter des risques pour les opérations et la sécurité du navire
- mettre en œuvre des mesures techniques et procédurales pour se protéger contre un cyber-incident et assurer la continuité des opérations
- mettre en œuvre des activités de préparation et d'intervention en cas de cyber-incident

Différence entre les systèmes TI et TO

Catégorie	Système de TI	Système de TO
Exigences de performance	♦ En temps non réel ♦ La réponse doit être cohérente ♦ Interaction d'urgence moins critique ♦ Un contrôle d'accès strictement limité peut être mis en œuvre dans la mesure nécessaire à la sécurité	♦ En temps réel ♦ La réponse est critique en termes de temps ♦ Interaction d'urgence critique ♦ L'accès doit être strictement contrôlé, mais ne doit pas gêner ou interférer avec l'interaction homme-machine
Exigences de disponibilité / fiabilité	♦ Les réponses telles que le redémarrage sont acceptables ♦ Les déficiences de disponibilité peuvent être tolérées, en fonction des exigences opérationnelles du système	♦ Les réponses telles que le redémarrage peuvent ne pas être acceptables en raison des exigences opérationnelles ♦ Les exigences de disponibilité peuvent nécessiter des systèmes de secours
Exigences en matière de gestion des risques	♦ Gestion des données ♦ La confidentialité et l'intégrité des données sont primordiales ♦ La tolérance aux pannes peut être moins importante ♦ Les impacts du risque peuvent entraîner un retard dans le dédouanement du navire, le début du chargement/ déchargement ou des opérations commerciales et d'affaires	♦ Contrôle du monde physique ♦ La sécurité est primordiale, suivie par la protection du processus ♦ La tolérance aux pannes est essentielle, même un temps d'arrêt momentané peut être inacceptable ♦ Les impacts du risque sont la non-conformité réglementaire, ainsi que les dommages causés au personnel à bord, à l'environnement, aux équipements et/ou à la cargaison

Vulnérabilités courantes

Les points suivants sont des vulnérabilités cybernétiques courantes que l'on peut trouver à bord des navires existants et de certains navires nouvellement construits :

- systèmes d'exploitation obsolètes et non pris en charge
- logiciels antivirus et protection contre les logiciels malveillants obsolètes ou manquants
- des configurations de sécurité et des « best practices » inadéquats, notamment une gestion inefficace du réseau et l'utilisation de comptes d'administrateur et de mots de passe par défaut
- les réseaux informatiques de bord, qui manquent de mesures de protection des limites et de segmentation des réseaux
- des équipements ou des systèmes essentiels à la sécurité toujours connectés à la partie terrestre
- des contrôles d'accès inadéquats pour les tiers, y compris les entrepreneurs et les prestataires de services.

Défense

Il est important de protéger les systèmes et les données critiques à l'aide de plusieurs couches de mesures de protection, qui tiennent compte du rôle du personnel, des procédures et de la technologie pour :

- augmenter la probabilité qu'un cyber-incident soit détecté
- augmenter l'effort et les ressources nécessaires pour protéger les informations, les données ou la disponibilité des systèmes informatiques et OT

Les systèmes OT connectés à bord devraient nécessiter plus d'une mesure de protection technique et/ou procédurale. Les défenses périmétriques telles que les pare-feu sont importantes pour empêcher toute entrée non souhaitée dans les systèmes, mais cela peut ne pas être suffisant pour faire face aux menaces internes. Cette approche de défense en profondeur encourage la combinaison des éléments suivants :

- sécurité physique du navire, conformément au plan de sûreté du navire (SSP)
- protection des réseaux, y compris une segmentation efficace
- détection des intrusions
- analyse et test périodique des vulnérabilités
- liste blanche des logiciels

- contrôles des accès et des utilisateurs
- procédures appropriées concernant l'utilisation des supports amovibles et des politiques de mots de passe
- sensibilisation du personnel au risque et sa connaissance des procédures appropriées

Mesures de protection technique

Les exemples de CSC mentionnés ci-dessous ont été sélectionnés comme étant particulièrement pertinents pour les équipements et les données à bord des navires :

- Limitation et contrôle des ports, protocoles et services du réseau
- Configuration des dispositifs de réseau tels que les pare-feu, les routeurs et les commutateurs
- Sécurité physique
- Détection, blocage et alertes
- Communication par satellite et radio
- Contrôle d'accès sans fil
- Détection des logiciels malveillants
- Configuration sécurisée de matériel et logiciels
- Protection du courrier électronique et du navigateur web
- Capacité de récupération des données
- Sécurité des logiciels d'application (gestion des correctifs)

Solutions proposées par QBS en collaboration avec GFI Software

KerioControl

Agit comme un routeur et un pare-feu permettant des fonctionnalités VPN sécurisées et un contrôle granulaire des communications entrantes et sortantes.

Comme la bande passante sur les navires peut être limitée, ce produit permet également la gestion de la bande passante pour s'assurer que les services critiques ne sont pas interrompus par une utilisation moins importante comme les médias sociaux et les services de streaming vidéo.

Exinda NetworkOrchestrator

Permet de surveiller le réseau en temps réel pour s'assurer que les applications critiques fonctionnent comme prévu.

Grâce à un tableau de bord intuitif, il permet d'identifier tout problème relatif à une application, un utilisateur, un appareil ou un emplacement.

Ce produit permet également de contrôler le trafic réseau et les applications afin de donner une priorité plus élevée aux services critiques en fonction du service, de l'heure de la journée et/ou des utilisateurs.

LanGuard

Analyse votre réseau pour s'assurer qu'il n'y a pas de correctifs de sécurité manquants qui pourraient ouvrir une vulnérabilité à une partie potentiellement malveillante.

Il analyse le réseau pour trouver les correctifs manquants et identifier les vulnérabilités des systèmes d'exploitation Microsoft, MacOS et Linux, ainsi que des navigateurs web et des logiciels tiers de plus de 60 grands fournisseurs, dont Google, Adobe et Java.