NOTE DE SENSIBILISATION

JANVIER 2025

DÉCIDEURS DE COMPAGNIES MARITIMES

CYBERATTAQUES : ÊTES-VOUS PRÉPARÉS ?

Avec le soutien de la Direction Générale des Affaires Maritimes, de la Pêche et de l'Aquaculture
Avec le soutien de l'Agence Nationale de la Sécurité des Systèmes d'Information

FRANCE CYBER MARITIME

Armateurs de France

Ces quatre dernières années, dans le monde entier, 35 compagnies maritimes ont publiquement reconnu avoir été victimes de cyberattaques[1]. Ces incidents, médiatisés ou non, ont des impacts financiers, opérationnels, réputationnels et assurantiels importants sur le secteur du transport et des services maritimes, dont le fonctionnement opérationnel dépend de plus en plus des systèmes numériques. Les entités avec lesquelles les compagnies maritimes interagissent sont elles aussi largement victimes de telles attaques, qu'il s'agisse des ports, des acteurs de la logistique, des chantiers navals, des équipementiers, des fournisseurs de services numériques, ou encore des sociétés de classification ou des organismes publics. Dans un contexte où le nombre d'exigences réglementaires augmente et où la situation géopolitique internationale est particulièrement incertaine et se dégrade, comment se protéger efficacement ?

1. Source : France Cyber Maritime / ADMIRAL : **https://www.m-cert.fr/admiral/Shipowner.html**

QUELQUES EXEMPLES RÉCENTS D'INCIDENTS CYBER DANS LE SECTEUR MARITIME

- **En novembre 2023**, un opérateur de terminaux portuaires en Australie est victime d'une cyberattaque qui le contraint à suspendre les activités de ses terminaux durant plusieurs jours.

- **En juin 2023**, un équipementier majeur du secteur maritime est victime d'une attaque par rançongiciel, dont l'impact global est estimé à 85 millions de dollars.

- **En janvier 2023**, un fournisseur de plateforme de Safety Management System (SMS) est victime d'une attaque par rançongiciel. Cette attaque impacte plus de 70 clients et 1 000 navires dans le monde entier, perturbant l'utilisation du SMS à terre et à bord.

- **En mars 2022**, le site Internet d'un armateur allemand est contrefait pour mener des opérations de *phishing* (hameçonnage) dans le secteur maritime en usurpant son identité, impactant son image de marque.

- **En mai 2021**, une arnaque au Faux Ordre de Virement (FOVI) à l'encontre d'un armateur allemand entraîne le virement de 1,679 millions de dollars vers le compte bancaire d'un cybercriminel.

- **Enfin**, les actions offensives d'interdiction d'accès au GPS deviennent permanentes dans de nombreuses zones maritimes, de la de la mer Baltique au canal de Suez, avec des impacts directs sur la sécurité de la navigation, mais aussi sur les systèmes informatiques ou de télécommunication qui en dépendent.

QUI PEUT EN VOULOIR AUX ARMATEURS ?

Les armateurs peuvent être les victimes d'attaques :

- Ciblées, provenant d'**acteurs étatique**s visant spécifiquement le secteur en raison de son caractère stratégique : souvent plus difficiles à détecter, leurs conséquences peuvent également être plus destructrices. Les capacités, parfois militaires, utilisées comme dans le cadre du brouillage et du leurrage GPS, sont particulièrement importantes ;

- Opportunistes ou ciblées, par des **acteurs cybercriminels** qui cherchent à exploiter des fragilités des systèmes exposés sur Internet pour mener, par exemple, des attaques par rançongiciel. Ils sont également spécialisés dans le vol et la revente d'informations personnelles en utilisant des techniques de *phishing* et dans les escroqueries de type « Faux ordre de virement ». Certains groupes se sont spécialisés dans le maritime ; d'autres peuvent bénéficier d'un soutien voire d'une certaine bienveillance d'Etats à la législation permissive ou concurrents ;

- Ciblées, par des **hacktivistes** qui inondent des serveurs du secteur maritime et portuaire d'un très grand nombre de requêtes (attaques dites en « déni de service distribué »), qui visent à paralyser, par exemple, le site Internet d'un armateur ou d'un port pendant une durée déterminée et à revendiquer l'attaque sur les réseaux sociaux. Au-delà de l'impact réputationnel, ce type d'attaque peut également avoir des conséquences financières importantes.

À QUEL SCÉNARIO SEREZ-VOUS CONFRONTÉS ?

Paralysie de vos applications de réservation et de votre bureautique suite à une attaque par rançongiciel

21 heures, un vendredi soir. Votre équipe commerciale vous informe que les applications de réservations sont paralysées et qu'aucune nouvelle réservation ne peut être enregistrée. Les applications de gestion de la flotte et de suivi des navires fonctionnent de manière très dégradée. Vos équipes informatiques ne parviennent pas à identifier l'origine de l'incident.

Quelques minutes plus tard, c'est la messagerie électronique qui devient inaccessible. Rapidement, le service informatique constate qu'une grande partie des serveurs de l'entreprise est chiffrée et comprend alors qu'une cyberattaque est en cours. Elle décide d'isoler le réseau de l'entreprise en le coupant d'Internet afin d'empêcher la propagation de l'attaque. Sur certains postes de travail, un message de l'attaquant s'affiche et vous réclame une rançon de 50 bitcoins – soit plusieurs millions d'euros – contre une promesse de déchiffrement des données.

L'ensemble de votre compagnie fonctionnera en mode très dégradé pendant deux semaines, en dépit de la forte mobilisation de vos équipes informatiques. De nombreuses commandes seront perdues et certaines informations commerciales ne seront jamais récupérées. Votre compagnie ne retrouvera un fonctionnement nominal qu'au bout de 6 mois, au prix d'un lourd préjudice, tant en matière d'image que de chiffre d'affaires.
Les investigations techniques mettront à jour un scénario d'attaque tristement banal. Votre entreprise fournit à ses salariés une solution d'accès à distance, communément appelée « VPN[2] », pour se connecter en déplacement ou en télétravail. Lorsqu'elles sont mal configurées, non supervisées ou non mises à jour, ces solutions présentent des vulnérabilités communément exploitées par les attaquants. Elles offrent alors à l'attaquant une porte d'entrée dans le système d'information de l'entreprise. Ce dernier étant mal cloisonné, l'attaquant s'y déplace aisément et y déploie ses outils de chiffrement pour rendre indisponibles les applications critiques de la compagnie.

Si la grande majorité des attaques par rançongiciels est opportuniste et profite du faible niveau de maturité en sécurité numérique de leurs victimes, certains groupes d'attaquants, organisés comme une véritable industrie, peuvent cibler spécifiquement des organisations disposant de moyens financiers importants ou exerçant des activités stratégiques critiques.

Perte de vos contrats et atteinte à votre réputation suite à une opération de cyberespionnage

Au cours des derniers mois, plusieurs contrats importants, que vous considériez comme pratiquement acquis compte tenu de la relation de confiance construite de longue date avec les clients concernés, vous ont finalement échappé, au profit de l'un de vos principaux concurrents étrangers. La perte de ces contrats stratégiques menace désormais l'équilibre financier de votre compagnie.

Par ailleurs, depuis ce matin, plusieurs clients cherchent à vous contacter de toute urgence, afin de savoir si les informations publiées dans la nuit sur Internet, présentées comme des données commerciales issues de votre compagnie, sont authentiques.

Celles-ci, confidentielles pour la plupart, comprennent notamment des extraits d'accords commerciaux et de conditions contractuelles, ainsi que plusieurs grilles de prix et de taux de marge pratiqués pour chaque client. À la vue des informations exposées, vous commencez à comprendre le ton irrité de certains messages que des clients vous ont adressés depuis le début de la matinée…

Ces événements s'avéreront être les conséquences d'une opération d'espionnage informatique aux motivations économiques, menée depuis plusieurs mois, en toute discrétion. En effet, les investigations techniques mettront en évidence la réception, il y a quelques mois, de messages électroniques malveillants par des collaborateurs de votre compagnie.

Afin de rendre ces messages réalistes et convaincants, l'attaquant a utilisé les informations, personnelles et professionnelles, publiées sur les réseaux sociaux par des salariés peu sensibilisés à la menace informatique. Il a ainsi réussi à duper l'un des destinataires et à lui faire ouvrir une pièce jointe piégée. La contamination d'un seul poste de travail lui a suffi pour s'infiltrer dans le système d'information de la compagnie, le plaçant en capacité de récupérer de nombreuses données afin d'en tirer un avantage concurrentiel ou de les publier.

Soumises à une forte concurrence internationale, les compagnies maritimes sont particulièrement exposées à ce type d'attaques. Les impacts indirects, tels que la perte de marchés, ou l'atteinte à l'image en cas de divulgation publique de données exfiltrées par l'attaquant, peuvent s'avérer extrêmement préjudiciables.

2. Virtual Private Network, Réseau Privé Virtuel

VOTRE RÔLE ET VOS RESPONSABILITÉS EN TANT QUE DIRIGEANT/DÉCIDEUR

Considérant la nature stratégique des répercussions d'attaques informatiques à l'encontre des acteurs du secteur maritime, vous avez, en tant que décideur, un rôle primordial à jouer.

En tant que dirigeant d'entreprise vous êtes ainsi tenu :

- De veiller à la prise en compte de la gestion des risques cyber dans le système de gestion de la sécurité de la compagnie, conformément aux lignes directrices pour la gestion des cyber-risques maritimes adoptées par l'Organisation Maritime Internationale (OMI) en 2017[3] et entrées en vigueur en 2021. L'absence de prise en compte de la cybersécurité peut entraîner des non conformités lors des audits du siège et des navires.

- Suivre une formation et offrir régulièrement une formation similaire aux employés de l'entreprise afin que ceux-ci acquièrent des connaissances et des compétences suffisantes en matière de cybersécurité, et veiller le cas échéant au respect des exigences de la future Directive NIS 2[4] adoptée en 2022 par l'Union européenne. Cette directive sera transposée dans le droit français en 2025. Ces exigences concerneront notamment la gouvernance de la cybersécurité au sein de votre entreprise, des mesures de gestion des risques, des mesures techniques, et des obligations d'information aux autorités en cas d'incident. A noter que les sanctions en cas de non-respect de ces obligations peuvent aller jusqu'à 10 millions d'euros d'amende ou 2 % du chiffre d'affaires annuel mondial de la compagnie.

Votre responsabilité, en tant que décideur, pourrait donc être engagée en cas d'incident. Une absence de prise en compte de la cybersécurité peut également avoir des répercussions majeures du point de vue assurantiel. Vous seuls êtes à même de prendre *in fine* les décisions structurantes pour votre organisation, à la hauteur d'un risque bien réel dont les possibles conséquences sont encore parfois sous-estimées.

3. L'application des recommandations de la Résolution MSC.428 (98) est obligatoire en France.
4. Directive (UE) 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union Européenne.

Pour vous aider, voici quelques questions à vous poser en tant que décideur :

1. La cybersécurité est-elle un sujet régulièrement abordé lors de vos COMEX ?
2. Quelle part de votre budget informatique consacrez-vous à la cybersécurité à terre et à bord ?
3. À quand remonte votre dernier exercice de gestion de crise d'origine cyber à terre et à bord ? Savez-vous qui contacter en cas de cyberattaque ?
4. L'ensemble de votre personnel à terre et à bord est-il sensibilisé aux risques cyber spécifiques du secteur ?
5. Quelle est votre évaluation des principaux risques auxquels vous êtes confrontés à terre et à bord ? Les risques liés aux faux ordres de virement ont-ils fait l'objet d'un traitement particulier ?
6. Comment prenez-vous en compte la cybersécurité dans les contrats avec vos partenaires, prestataires, chantiers navals ? Par exemple :
   - Comment sont encadrées les interventions de prestataires à bord de vos navires ?
   - Avez-vous anticipé l'entrée en vigueur des Unified Requirements UR E26 et E27 de l'IACS pour les constructions neuves ?
   - L'hébergeur de votre site Internet est-il protégé contre les menaces de type déni de service ?
7. Avez-vous identifié les impacts opérationnels pour votre flotte d'un leurrage ou d'un brouillage GPS ?
8. Quelles sont les actions correctives que vous avez priorisées en termes de cybersécurité pour votre organisme, en application des lignes directrices de l'OMI ? Par exemple, conduisez-vous des audits cyber ou des tests d'intrusion informatique ?
9. Serez-vous soumis à la Directive NIS 2 ? Si oui avez-vous identifié les impacts de la Directive NIS 2 pour votre compagnie ?
10. Etes-vous en relation avec un CERT5 ?

Pour aller plus loin

- **Mon espace NIS2** : site, développé par l'ANSSI, qui permet, entre autre, de tester si votre entité sera soumise à la directive NIS2.
- **Guide d'hygiène de l'ANSSI** : ce guide permet de renforcer la sécurité de son système d'information en présentant 42 mesures non exhaustives.
- **France Cyber Maritime** : association loi 1901 spécialisée en cybersécurité maritime que vous pouvez contacter pour tout besoin : **projets@france-cyber-maritime.eu**
- **Documentation en cybersécurité maritime** : site du M-CERT qui recense des réglementations nationales et internationales, des bonnes pratiques, etc.
- **Armateurs de France** : organisation professionnelle des entreprises de transport et de services

5. Computer Emergency Response Team. France Cyber Maritime met en oeuvre un CERT sectoriel, pour le secteur maritime (M-CERT).

Armateurs de France

47, rue de Monceau
75008 PARIS - FRANCE
Tel. : +33(0)1 53 89 52 52

www.armateursdefrance.org
@ArmateursFR
Armateurs de France

Le Grand Large
Quai de la douane, 2ème éperon 29200 Brest
Tel. : +33 (0)2 57 52 09 87

www.france-cyber-maritime.eu/fr/
@FrCyberMaritime
France Cyber Maritime