ATELIER CYBER

PAR ARMATEURS DE FRANCE ET BESSÉ

29 NOVEMBRE 2021 - PARIS

RÉSUMÉ

Une soixantaine de participants étaient réunis à un atelier cybersécurité coorganisé par l'organisation professionnelle Armateurs de France et le courtier en assurances Bessé le 29 novembre 2021, à Paris et en visioconférence. Etaient portés à l'ordre du jour les enjeux stratégiques de la cybersécurité pour les compagnies maritimes, avec de nombreuses interventions et échanges consacrés notamment à l'analyse des risques, au cadre réglementaire, au M-CERT (Maritime - Computer Emergency Response Team), à la continuité et à la relance d'activité, ainsi qu'à la communication de crise.

Ouverture de l'atelier

Par Jean-Emmanuel Sauvée et Gildas Tual

En ouverture de l'atelier cybersécurité, **M. Sauvée** et **M. Tual** ont rappelé que toutes les compagnies maritimes risquent désormais d'être attaquées et qu'il est crucial pour l'industrie et ses partenaires sectoriels d'approfondir les échanges en la matière, partager une culture de la cybersécurité, et ainsi renforcer la capacité commune pour prévenir et se protéger des attaques. C'est tout l'objet d'un tel évènement, conçu pour faire progresser le partage d'informations, de bonnes pratiques et de retours d'expérience ainsi que sensibiliser plus largement à la problématique cyber.

Selon **M. Gérault,** ces enjeux doivent être adressés au plus haut niveau de chaque entreprise. Les risques cyber ont des impacts sur la sécurité des biens et des personnes à bord comme à terre. Ils ont aussi des impacts financiers, et sur l'image des compagnies maritimes. C'est un enjeu difficile à appréhender, notamment à cause de sa technicité.

Ouverture de l'atelier

M. Jean-Emmanuel Sauvée, Président d'Armateurs de France

M. Gildas Tual, Directeur logistique, maritime & défense chez Bessé

M. Jacques Gérault, Conseiller institutionnel du Groupe CMA CGM et Président du comité sécurité-sûreté d'Armateurs de France

Intervention du Grand Témoin

M. Emmanuel Naëgelen, Directeur Général adjoint de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)

Les enjeux de cybersécurité doivent être adressés avec pragmatisme et pédagogie. Selon **M. Naëgelen**, « l'idée n'est pas d'asséner une vérité ». Partant de ce constat il est opportun de proposer un état des lieux de la menace qui n'a fait qu'augmenter, surtout ces deux dernières années. Le secteur maritime est dans ce contexte une cible idéale pour les pirates informatiques :

- Les compagnies maritimes sont des sociétés qui peuvent réaliser d'importants chiffres d'affaires et sont donc en mesure de payer des rançons conséquentes ;

- Leurs activités sont au carrefour d'enjeux géopolitiques, géostratégiques majeurs et dont les armateurs sont des acteurs cruciaux. Selon le directeur général adjoint de l'ANSSI « vouloir s'attaquer à un armateur fait sens pour certains Etats, notamment dans le cadre d'actions d'espionnage ou de sabotage » ;

- Ces acteurs connaissent une importante transformation numérique de leurs métiers. Il y a 20 ans, un armateur pouvait exercer ses activités sans informatique, aujourd'hui c'est impossible. De plus en plus d'interconnexions entre l'informatique industrielle et l'informatique traditionnelle sont mises en œuvre.

> **VOULOIR S'ATTAQUER À UN ARMATEUR FAIT SENS POUR CERTAINS ETATS, NOTAMMENT DANS LE CADRE D'ACTIONS D'ESPIONNAGE OU DE SABOTAGE.**

Dans le contexte d'une menace cyber très prégnante pour le secteur maritime, quelles sont les pistes de travail à envisager ?

- **Se protéger** : en investissant dans l'équipement, les logiciels et les expertises. Malgré le marché tendu en France aujourd'hui par manque d'experts, il reste crucial d'investir en matière cyber.

- **Anticiper** : chaque opérateur doit se préparer à être attaqué. Avec pragmatisme, la question posée ne doit pas être « Vais-je être attaqué ? » ni « Quand vais-je être attaqué ? ». Elle doit être « Comment vais-je limiter l'impact de cette attaque ? ». La réponse suit deux axes simples : des actes réflexes qui doivent être largement connus (exemples : signaler les anomalies, débrancher les prises réseau en cas d'attaque, etc..) et une planification de la continuité et de la relance de l'activité. Cette planification permet de réduire par deux les dégâts et conditionne un retour normal de l'activité plus rapide.

- **Partager** : la meilleure méthode reste le partage et les échanges entre armateurs.

Quelles menaces et quels risques cyber pour le monde maritime ?

Mme Sylvie Andraud, Coordinatrice sectorielle de l'ANSSI
M. Didier Daoulas, Directeur du comité analyse des risques du Conseil Cyber pour le Monde Maritime (C2M2) - M. Xavier Rebour, Directeur de France Cyber Maritime

En introduction, **Mme Andraud** a évoqué la typologique de la cyber-criminalité en 2021 et rappelé quelques constats essentiels. L'écosystème de la cyberattaque fait appel à une multitude d'outils malveillants prêts à l'emploi (en particulier les rançongiciels dont l'usage a été augmenté de 255% en 2020) et proposés à l'achat dans de véritables supermarchés de la cybercriminalité. Il importe donc de s'informer sur les vulnérabilités des systèmes et de mettre en place les correctifs appropriés pour faire face à cette professionnalisation des attaquants. La sécurisation de l'ensemble de la chaîne logistique est également un enjeu de taille. La cybercriminalité devrait continuer de progresser avec l'exposition accrue des entreprises, la difficulté à identifier et punir les cybercriminels et la sophistication croissante des modes opératoires.
Dans ce contexte, l'ANSSI a un rôle de sensibilisation et d'accompagnement des compagnies maritimes et des ports, en particulier auprès des opérateurs d'importance vitale (OIV) et des opérateurs de services essentiels (OSE). C'est notamment l'objet d'une note d'alerte élaborée à l'intention des dirigeants des compagnies maritimes, avec la contribution d'Armateurs de France, qui a été partagée début décembre.

M. Daoulas a présenté l'analyse des risques Cyber des secteurs maritimes et portuaires, travail conduit pour l'ensemble du secteur maritime français sous l'égide du C2M2, d'avril à août 2021. Il s'agit d'une démarche méthodique en plusieurs ateliers destinés à :

- Définir le périmètre, les processus essentiels ainsi que les principaux évènements redoutés en fonction de leur niveau de gravité ;
- Recenser les sources de risques et les attaquants potentiels à l'origine des menaces et les objectifs visés par ceux-ci ;
- Identifier les scénarios d'attaque stratégiques critiques ;
- Elaborer les scénarios opérationnels (pour les compagnies maritimes et les ports).

Cette cartographie a fait l'objet d'un rapport présenté fin novembre au Secrétaire Général de la Mer et devrait être diffusé (de manière restreinte) d'ici fin 2021.

Dans la continuité des travaux du C2M2, et de la décision du Comité interministériel de la mer de 2018 a été créée, fin 2020, une structure dédiée au cyber pour le monde maritime, sous statut associatif : France Cyber Maritime. **M. Rebour** a rappelé les missions de l'association, qui consistent à fédérer le secteur maritime sur les sujets cyber ainsi que créer et opérer un M-CERT indispensable à la veille, au recueil et à l'analyse des incidents de façon confidentielle. Un des objectifs visés est de partager des informations anonymisées et actualisées sur la menace à l'ensemble des opérateurs.

France Cyber Maritime se structure autour de trois collèges, pour les acteurs publics (agence de l'Etat, Ministère, collectivité territoriale), les utilisateurs (armateur, port, pêche) et les solutions (matériel, audit, assurance, ...). Elle compte actuellement 45 membres, dont Armateurs de France et Bessé. A terme elle devrait développer une offre de service et de solutions qui s'adresse à tous. Elle a récemment conclu un partenariat avec la Marine nationale et la Gendarmerie maritime. Cette démarche commune à l'origine de la création de France Cyber Maritime doit être consolidée et s'inscrire dans une démarche de solidarité au sein de l'industrie maritime.

Table ronde n°1

IDENTIFIER ET PRÉVENIR LES RISQUES

M. Laurent Banitz, Chargé de mission sûreté & cybersécurité des navires à la Direction des Affaires Maritimes
M. Pierre Westphal, Responsable Développement Offres SI chez SGS
M. Frédéric Benon, Directeur des équipements communs de Genavir
M. Olivier Jacq, Directeur technique et scientifique de France Cyber Maritime

L'identification des risques est fondamentale pour les prévenir et limiter les impacts d'une cyberattaque. Les intervenants de la première table ronde ont ainsi rappelé l'importance des enjeux de gouvernance pour le secteur, en particulier au niveau national, et échangé sur les questions de certification, de structuration de la gestion des risques au sein des entreprises ainsi que de l'importance d'un partage approfondi des informations relatives aux incidents et aux attaques.

M. Banitz a présenté un rappel du cadre réglementaire en vigueur et des travaux en cours pour réviser le dispositif européen de la Directive NIS (Network and Information Security) pour notamment l'élargir à l'ensemble de la chaîne logistique. Pour chaque sous-traitant, chaque maillon de la chaîne logistique, pouvant présenter une vulnérabilité, il importe d'étendre des exigences approfondies en matière de cybersécurité et ainsi éviter une « multiplication en série des vulnérabilités ». Il a également rappelé l'importance de structurer la démarche au niveau national au sein de la stratégie nationale de cybersécurité maritime et d'agir dans la prévention (réaliser des exercices, favoriser le recours à la certification et au security by design).

M. Westphal a souligné les similitudes des problématiques rencontrées en matière cyber entre le secteur maritime et les autres secteurs d'activités. Les offres des acteurs indépendants avec des solutions validées et certifiées ont une importance majeure. Ces acteurs ont pour objectif de présenter des démarches professionnelles de la sécurité des systèmes d'information et travaillent également sur des standards internationaux pour une reconnaissance élargie de leurs référentiels et leur prise en compte dans la négociation de contrats d'assurance.

M. Benon a présenté un focus spécifique sur la compagnie Genavir qui assure l'exploitation de la flotte océanographique de l'IFREMER. De par la spécificité de ses activités, la compagnie produit, exploite et stocke beaucoup d'informations, en particulier avec la captation des données de recherche en mer. Genavir a structuré sa sécurité informatique et l'a appuyé sur quatre piliers : gouvernance, formation, technologie et assurance. La méthode employée pour renforcer sa sécurité suit une logique d'inventaire, puis d'analyse et enfin de préconisations. Tout cahier des charges adopté par l'entreprise en matière d'acquisitions informatiques prend désormais en compte la gestion des risques cyber. Les efforts se portent désormais sur la formation. Genavir envisage une collaboration approfondie avec France Cyber Maritime dont elle est membre.

Table ronde n°1

M. Jacq a partagé la vision de France Cyber Maritime sur les enjeux d'identification des menaces et de prévention des risques, ainsi que sur le partage de l'information.
L'anticipation en matière cyber reste compliquée, et la prise en compte de ces risques dans l'ISM des compagnies depuis début 2021 n'est qu'un début. Parmi les ressources disponibles, le guide du BIMCO sur la cybersécurité maritime est utile à l'identification des menaces et à l'élaboration de plans d'urgence. Il faut également approfondir l'analyse, le partage d'informations, les entraînements (testing des opérateurs, exercices de défense, entraînement à la communication de crise) et la surveillance sectorielle. A ce titre, France Cyber Maritime a pour mission de vérifier les expositions des acteurs ciblés sur internet. L'association réfléchit à la mise en place d'un SOC maritime (Security Operation Center – département qui au sein d'une organisation assure la sécurité et la veille permanente en matière de sécurité de l'information).

- Questions des membres -

Va-t-on vers une organisation et une homogénéisation de l'offre de formation cyber en France pour le secteur maritime ?

Pour les compagnies maritimes il y a un enjeu à ne pas se limiter à la conformité avec les prescriptions réglementaires et à anticiper sur une sensibilisation et une formation adaptée des personnels. Les enjeux de formation ont été évoqués au sein du C2M2. Aujourd'hui France Cyber Maritime a identifié une vingtaine de formations généralistes ou très pointues. Il reste encore à trouver la bonne plateforme en France pour héberger les formations. L'association y travaillera en 2022.

À l'heure actuelle, les pouvoirs publics parviennent-ils à arrêter des cybercriminels, et les traduire en justice ?

Oui, des réseaux de cybercriminalité ont pu être démantelés ces dernières années, mais il reste encore beaucoup à faire alors que la menace se renforce et devient plus sophistiquée.

Table ronde n°2

ET EN CAS D'ATTAQUE CYBER ?

M. Olivier Jacq, Directeur technique et scientifique de France Cyber Maritime
M. Christopher Kirman, Directeur des Systèmes d'Information de Brittany Ferries
M. Laurent Porta, Associé du cabinet de conseil Vae Solis
M. Christophe Madec, Directeur de clientèle chez Bessé

M. Jacq a décrit le caractère déterminant des premiers réflexes à adopter lors d'une attaque et présenté le M-CERT développé par France Cyber Maritime. Lors de l'attaque qui a ciblé la compagnie Maersk en 2017, il a fallu 7 minutes à l'armateur pour stopper la propagation de l'agression. Cet exemple, et les dernières attaques en date, illustrent l'importance de conclure un contrat avec un prestataire pour l'assistance en cas d'attaque, la nécessité de débrancher les machines lors de l'attaque (sans les éteindre pour conserver des preuves) et de porter plainte à l'issue de l'attaque. Disposer de sauvegardes régulières, testées et protégées est crucial.

IL FAUT ENTRE 3 ET 25 JOURS À UN PIRATE INTRODUIT DANS LE SYSTÈME POUR LANCER L'ENVOI DE RANÇONGICIELS. 75% DES ATTAQUES SONT CONDUITES PAR RANÇONGICIELS.

M. Kirman a évoqué les risques liés aux tentatives de fraude, notamment dans le cadre de transactions bancaires. Dans ce type d'attaque la vigilance des opérateurs est essentielle. En matière de prévention, les entreprises ont une réelle volonté d'allouer des ressources techniques en matière de cybersécurité mais il est parfois très difficile pour les personnels de se les approprier. Il faut bien sûr procéder aux audits externes et internes mais également remplacer le matériel à bord avec des équipements récents (et en redondance) et assurer la mise à jour des patchs de sécurité des systèmes opérationnels.

Pour l'entreprise, la structuration interne passe non seulement par le recrutement de personnels compétents mais aussi par la contractualisation de certains besoins avec des partenaires cyber et la prise en compte au plus haut niveau de l'entreprise de ces enjeux, idéalement avec un comité dédié directement rattaché à l'organe de gouvernance de l'organisation. En définitive, l'aspect comportemental joue un rôle majeur dans les conséquences d'une attaque : avant, pendant et dans la continuité de celle-ci, l'implication de l'ensemble des collaborateurs et la diffusion d'une véritable culture de la cybersécurité à tous les niveaux est essentielle.

POURQUOI FAUT-IL UNE COMMUNICATION MAÎTRISÉE EN CAS DE CRISE CYBER ?

M. Porta a évoqué les enjeux relatifs à la communication de crise lors de l'attaque. Il a lui aussi rappelé que le risque cyber doit être pleinement intégré au plus haut niveau de direction de l'entreprise. Lors d'une attaque, l'impact des défaillances occasionnées sur l'image de l'organisation peut être conséquent. La part de prévention est certes importante, mais une information et une communication efficaces doivent également être livrées aux partenaires et clients pendant l'attaque. Il est communément admis aujourd'hui que tout le monde peut être attaqué ou a déjà été attaqué. Cette acceptation repose sur la transparence qui permet de montrer que l'entreprise ciblée est résiliente. Il peut s'agir d'expliquer comment le contact avec les clients va être maintenu, tout en veillant à vulgariser le langage technique. Ne pas communiquer c'est aussi laisser à d'autres le soin de le faire, avec le risque d'une perte de confiance de l'opinion publique. La communication interne présente également une dimension majeure, avec de la pédagogie sur les travaux de remise en fonctionnement des postes de travail. Parfois l'origine de la problématique peut aussi se révéler interne : une notation de la maturité des employés sur les risques cyber est une option intéressante si elle est accompagnée d'une démarche de sensibilisation et de formation.

Table ronde n°2

M. Madec a présenté le rôle de l'assurance dans la couverture des risques cyber et évoqué deux aspects essentiels. Tout d'abord un volet assistance (avec une capacité de mobilisation d'une expertise et de compétences très utiles dans les premières heures de la crise) et la possibilité d'une mise en connaissance avec un véritable écosystème de la cybersécurité (communication de crise, questions juridiques, aspects techniques). Deuxièmement, un volet qui recouvre les attributions traditionnelles de l'assurance, à savoir la couverture financière des dommages et pertes d'exploitation qui peuvent se révéler très conséquentes.

Le marché de l'assurance cybersécurité pour le secteur maritime est en expansion mais à perte pour les assureurs (avec 130 millions d'euros de primes et 250 millions de sinistres couverts pour l'année 2020). À l'inverse, la cybercriminalité est une activité très rentable. Les assureurs sont donc devenus très stricts dans la sélection de leurs risques et l'application de majorations tarifaires, avec des primes et franchises en augmentation. Avec des exercices 2020, 2021 et 2022 jugés ou anticipés très mauvais, le domaine cyber peut être considéré comme un investissement déceptif. Comme pour d'autres risques la logique prédominante est celle du renforcement de la cybersécurité avec des investissements sur les plans techniques et humains, et la couverture des risques subsistants par l'assurance. En 2020, pour 1€ de prime versé, ce sont 10€ de garantie qui sont couverts par l'assurance pour le cyber.

Conclusion

VAE(2s) Arnaud Coustillère, Président du Pôle d'Excellence Cyber

L'Amiral Coustillère, pour conclure la rencontre, a illustré les enjeux de cybersécurité pour le secteur maritime par les thématiques communes et distinctes aux domaines de l'information et du maritime. Tout comme la mer, le domaine cyber est imprévisible mais présente également des risques particuliers. Il s'agit de risques liés au caractère innovant des attaques qui requièrent une solidarité d'autant plus prégnante des cibles pour se protéger, avec un partage de l'information étendu.

Dans ce contexte de menace, les navires et les compagnies françaises sont des cibles de 1er choix pour les cybercriminels. Elles exercent des prestations à haute valeur ajoutée et transportent des cargaisons de valeurs conséquentes. La préparation du secteur maritime français doit donc se concevoir, avec l'action du C2M2 et la création de France Cyber Maritime, en écosystème, avec le soutien de l'Etat.

À propos d'Armateurs de France

Armateurs de France est l'organisation professionnelle représentative des entreprises françaises de transport et de services maritimes. Porte-parole d'une industrie de pointe et diversifiée, elle représente 26 000 emplois direct en France. Sa mission : construire un cadre propice au développement de l'économie et de l'emploi maritimes en France, dans un contexte de forte concurrence internationale, en défendant activement les intérêts de la profession auprès des instances nationales, communautaires et internationales concernées.

Armateurs de France

À propos de Bessé

BESSÉ
CONSEIL EN ASSURANCES

Les hommes et les femmes de BESSÉ sont des experts du conseil et du courtage en assurances pour les grandes entreprises et les ETI. Au quotidien, ce sont 460 collaborateurs qui s'appuient sur leur expertise et leur capacité d'innovation pour accompagner les clients du Groupe en France et dans le monde dans la protection de leurs activités et de leurs salariés. En 60 ans, avec les mêmes valeurs et la même indépendance, BESSÉ a développé sa stratégie d'hyperspécialisation pour s'imposer au fil du temps comme un acteur global et l'un des leaders français sur son marché. L'entreprise, qui fait partie des « 500 champions des territoires », a été primée, pour la deuxième édition consécutive, Courtier #1 du Baromètre de satisfaction 2020 des Risk Managers (Golden & Partners et OMC Luxembourg). BESSÉ a réalisé en 2020 un chiffre d'affaires de 118,5 M€.