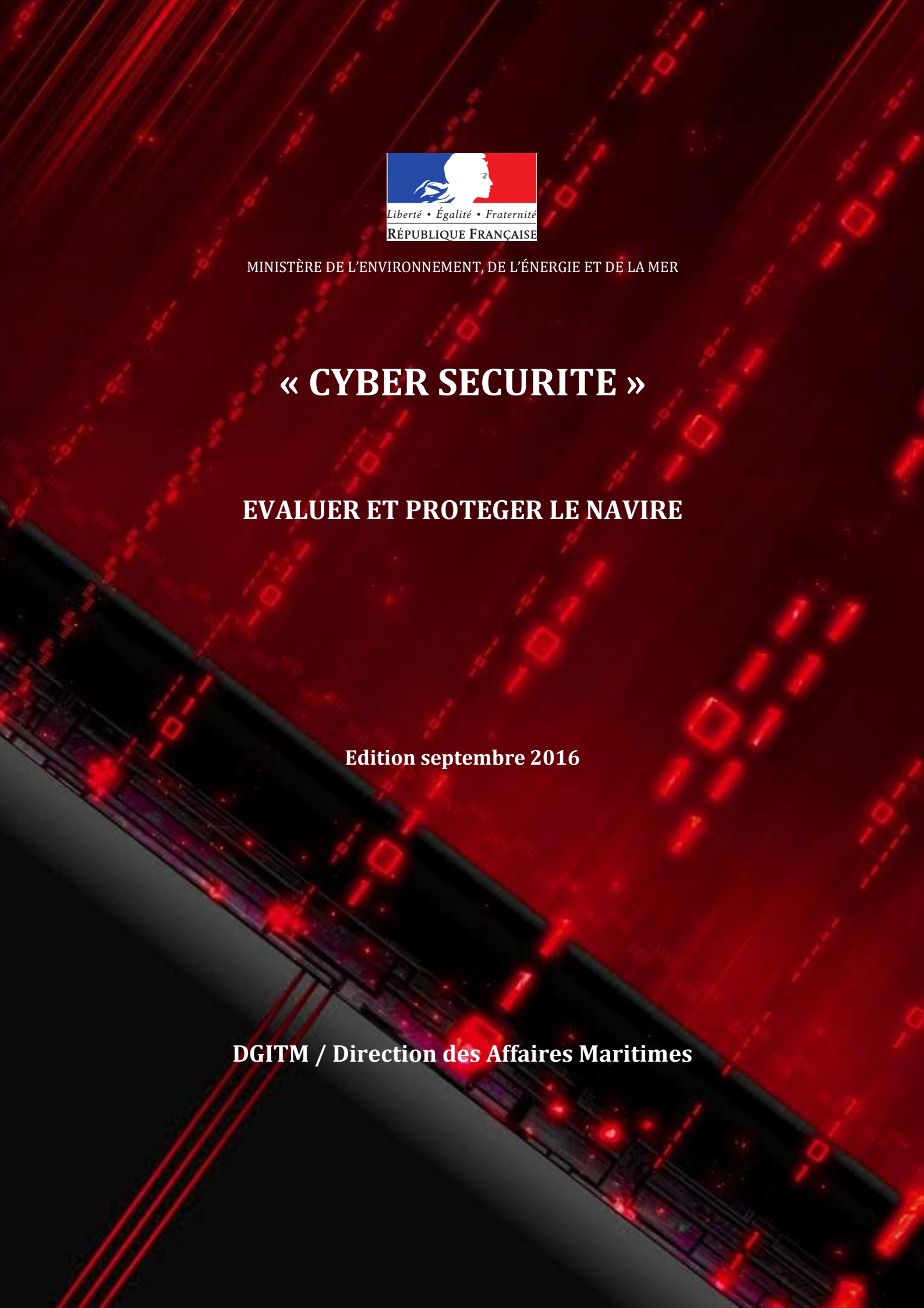


Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ENVIRONNEMENT, DE L'ÉNERGIE ET DE LA MER

« CYBER SECURITE »

EVALUER ET PROTEGER LE NAVIRE

Edition septembre 2016

DGITM / Direction des Affaires Maritimes

Contenu

STUXNET, SHAMOON, DUQU, DRAGONFLY (HAVEX), GAUSS, FLAME, SANDWORM, IRONGATE… cet inventaire à la Prévert correspond à un arsenal de cyber armes qui donne le frisson aux responsables en charge de la sécurité des systèmes de contrôle industriel (ICS). Bien connue désormais et découverte en juin 2010, la première cyber arme, STUXNET, a détruit partiellement le programme nucléaire Iranien. Par la suite, les dérivés de cette nouvelle arme technologique ont œuvré en détruisant 30.000 ordinateurs de la compagnie pétrolière SAUDI ARAMCO. Cette course à l'armement numérique a fait prendre conscience de la réalité des menaces de cyber sabotage, de cyber terrorisme et de cyber espionnage.

Dès lors, on peut raisonnablement se poser la question de la vulnérabilité numérique du navire. La prise de contrôle à distance d'un pétrolier est-elle envisageable ? Fiction ? Réalité ? Jusqu'à présent, seules les infrastructures terrestres, maritimes et portuaires semblaient concernées. En 2011, le port d'Anvers détecte une anomalie de son système de gestion des conteneurs. L'enquête conclura au « cyber-escamotage » de plusieurs conteneurs en provenance d'Amérique latine.

Le navire est un moyen de transport parmi tant d'autres, longtemps réputé à l'écart des connections de la toile. Est-il pour autant totalement étanche au « triangle de motivation » de la cyber menace : vol d'argent, vol de données sensible, activisme/acte de terrorisme ? La Direction des Affaires Maritimes (DAM) a souhaité, il y a un an, analyser la vulnérabilité du navire à la menace numérique.

Ce document issu de l'exploitation des données recueillies lors d'une enquête menée à bord de 68 navires, ne vous apportera pas l'outil ultime de haute technologie contre un acte de cybercriminalité. Néanmoins, cette étude indique les grands axes à suivre pour mettre en place une gestion de la sécurité des systèmes d'informations et de communications à bord du navire.

Reprenant les bonnes pratiques constatées, ces propositions permettront d'améliorer la gestion de la sécurité et de la sûreté à bord du navire, conformément aux directives de l'OMI, et en particulier la récente circulaire MSC.1/Circ.1526 du 01 juin 2016 – para 1.1.8.

Je vous invite à prendre en main ces recommandations afin de préserver votre navire et notre environnement contre un acte de malveillance numérique.

Thierry COQUIL
Directeur des Affaires Maritimes

A- LE NAVIRE DANS LE CYBER ESPACE

Début mars 2016, la société VERIZON spécialisée dans la conception, construction et analyse de réseaux fournit son bilan 2016 concernant l'analyse de 100 000 incidents, incluant l'analyse de 2260 compromissions de données dans 82 pays. Ce rapport illustre deux scénarios intéressants. L'un concerne la manipulation mystérieuse et inexpliquée d'automates contrôlant le processus de traitement d'une station d'eau. L'autre décrit un acte de malveillance contre une compagnie maritime. Les pirates se sont introduits par un « webshell » dans le réseau de la compagnie et établissent la liste des marchandises précieuses transportés à bord de navire. Dès lors, il ne restait plus qu'à envoyer une équipe à bord de navires pour récupérer les marchandises bien réelles. Le groupe criminel a commis plusieurs erreurs, ce qui a permis à la société VERIZON d'identifier la menace. La compagnie maritime a depuis renforcé ses mesures de sécurité, y compris l'exécution d'analyses de vulnérabilité de routine de ses applications, pour faire face à de futures attaques numériques. Cette dernière illustration démontre que le monde maritime n'est désormais plus totalement à l'abri d'un acte de malveillance via son système de gestion d'information. Cette menace s'amplifiera-t-elle avec la généralisation de mise en place de mouchard sur les conteneurs à forte valeur ajoutée (Société Traxens) ? Il est désormais important de prendre la mesure de cette menace et y faire face.

A1- LA NUMERISATION DU MONDE MARITIME

Avant toute chose, il apparait nécessaire de rappeler le contexte de ce type de transport. La mer est aujourd'hui un maillon essentiel et incontournable pour nos échanges économiques. Chaque pays est désormais interdépendant des échanges qui s'effectuent principalement par voie maritime. Près de 50 000 navires et un million de marins participent à cet échange mondial. Dans ce contexte d'échanges, le domaine du numérique n'a pas cessé de croitre depuis 25 ans à bord du navire de commerce. Le monde informatique est désormais omniprésent à bord. Cette technologie régule les moyens de communication, la conduite et les moyens de gestion de la cargaison du navire.

Cette transformation technologique du navire de commerce en a modifié sa gestion. Désormais les échanges sont quotidiens entre le navire, la compagnie, le port, l'agent maritime… Le navire ne bénéficie plus d'un niveau de sécurité informatique de type « air wall » consistant à l'isoler physiquement de tout réseau informatique. Le navire s'intègre naturellement dans cette toile planétaire du réseau des réseaux.

Notre navire est désormais devenu un ensemble complexe de systèmes industriels. La conduite de ces systèmes n'est malheureusement pas exempte de défauts numériques. Les systèmes embarqués peuvent ainsi être la clé d'entrée d'un acte de malveillance.

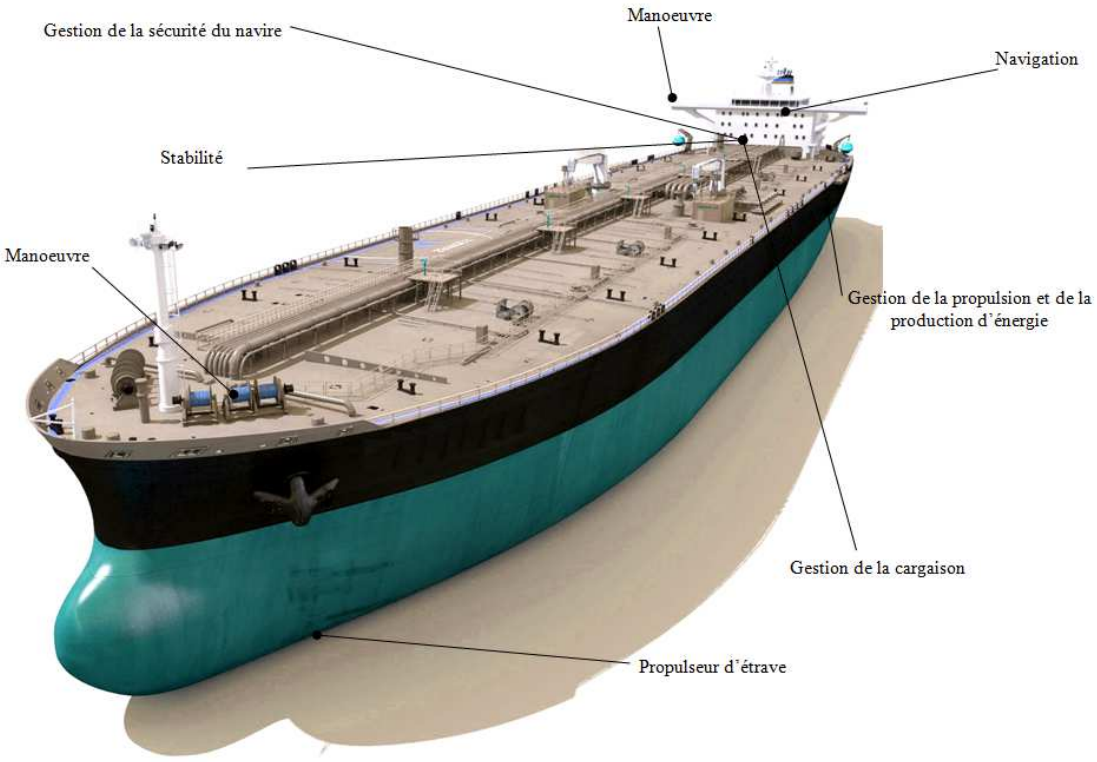
Ces simples constats démontrent que le navire peut être vulnérable à un acte de malveillance qui peut porter sur :

- **l'atteinte à l'image de la compagnie du navire** (acte d'intelligence économique offensive),
- **le cyber espionnage commercial du navire** (10% des attaques mondiales),
- **le cyber sabotage du navire,**
- **la cybercriminalité** (Deux tiers des attaques dans le monde).

Bien que les actes de malveillances restent à ce jour très limités contre un navire, il convient cependant de le protéger. Protéger le navire consiste à préserver les moyens opérationnels et organisationnels de ce type de transport. L'objectif final vise à garantir qu'aucun acte de malveillance ne puisse mettre en péril la conduite et l'exploitation du navire.

A2- VULNERABILITES SPECIFIQUES DU NAVIRE

Ces 3 dernières années, les systèmes de positionnement automatique et par satellite, le système de cartographie ECDIS (Electronic Charts Display Information System), le système d'enregistrement des données (Voyage Data Recorder) ont fait l'objet d'analyses. Ces dernières ont révélé plusieurs failles numériques à corriger. Plusieurs équipements apparaissent ainsi sensibles à une cyber attaque. La description des éléments de la vulnérabilité du navire est reprise au niveau de l'**annexe N°1** du document.



B- ENQUETE SUR LA CYBERSECURITE DU NAVIRE

Pour mettre en place une démarche de sécurité des systèmes d'information du navire, il est important de pouvoir identifier correctement les valeurs et les biens à protéger afin de lutter de manière efficace. Ceci implique une approche rigoureuse en fonction du type de navire et de son exploitation.

A ce jour, seul le code international pour la sûreté des navires et des installations portuaires (code ISPS) définit une recommandation en matière de gestion des procédés informatiques. Ce code précise que la vulnérabilité du système informatique devrait faire l'objet d'une évaluation dans le cadre de la sûreté du navire afin de disposer de mesures adaptées à une quelconque menace. Evaluer le niveau de menace, est par conséquent essentiel pour mettre en place des outils de lutte efficace.

C'est dans ce cadre que la DAM a mis en place une démarche d'évaluation du niveau de la cyber sécurité du navire. Cette dernière est déterminée au travers d'une enquête menée sur une année à bord des navires sous pavillon français et d'un audit navire réalisé par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

B1- NATURE DE L'ENQUETE

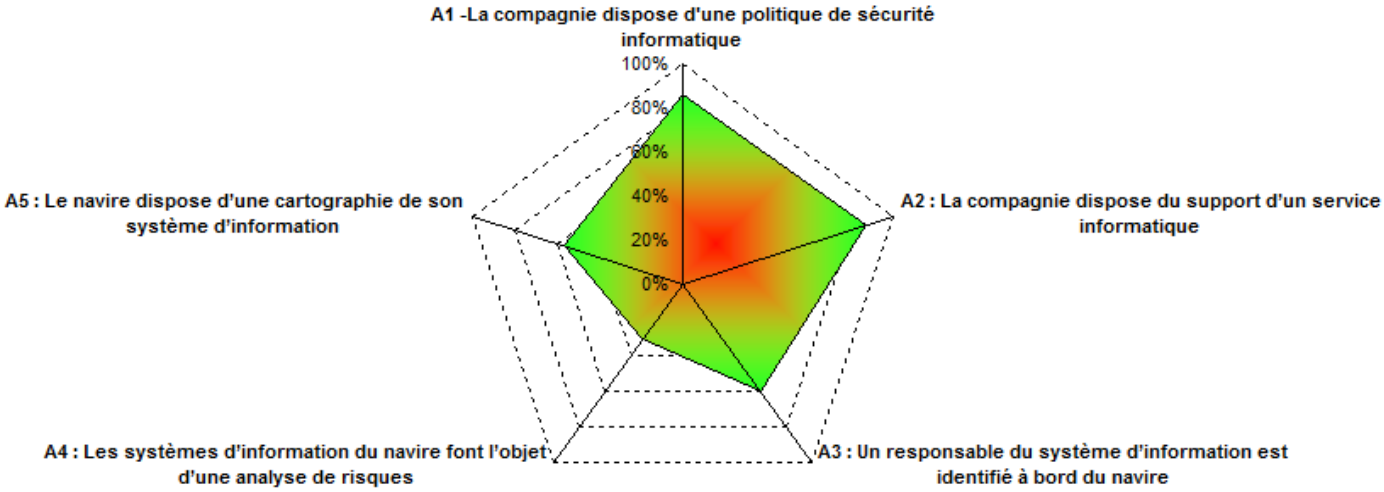
La prise en compte des secteurs vitaux du navire et des mesures d'hygiène de base de la sécurité des systèmes d'information du navire ont conduit à définir 9 rubriques (**Annexe N°2**) :

(1) Généralités sur la gestion SSI du navire,
(2) Localisation des systèmes d'information à bord du navire,
(3) Protections des échanges d'informations avec l'extérieur,
(4) Gestion des mots de passe,
(5) Mise à jour et changement de logiciels,
(6) Définitions des utilisateurs,
(7) Sauvegardes régulières des données,
(8) Incidents SSI,
(9) Contrôle des activités SSI du navire

Ces 9 rubriques proposent un ensemble de 34 questions fermées qui permettent un traitement direct et simple des réponses. **Cette enquête a été conduite à bord de 68 navires sous pavillon français disposant d'une certification en matière de sûreté. Ces navires représentent 26 compagnies françaises.**

B2- ANALYSE DE L'ENQUETE

GENERALITES SUR LA GESTION SSI DU NAVIRE :



Extrait de l'analyse :

D'une manière générale, cette enquête fait apparaitre que les compagnies françaises s'appuient d'une part sur un service interne pour gérer le système d'information du navire et d'autre part disposent d'une politique compagnie en matière de gestion du système d'information. Cependant, il convient de noter que cette politique est d'une manière générale très incomplète au regard des deux éléments suivants :

- le responsable à bord du navire n'est définit que dans 62% des cas (commandant, chef mécanicien, officier « électronicien », commissaire),
- la cartographie de la liste matérielle et logicielle du navire n'est répertoriée que dans 59% des cas,

Le point sensible de cette rubrique fait apparaitre que seulement 32% des navires sondés ont fait l'objet d'une évaluation des risques du système d'information du navire. La nature de cette évaluation n'a pas fait l'objet d'une analyse pour les 20 navires ayant répondu positivement à cette question.

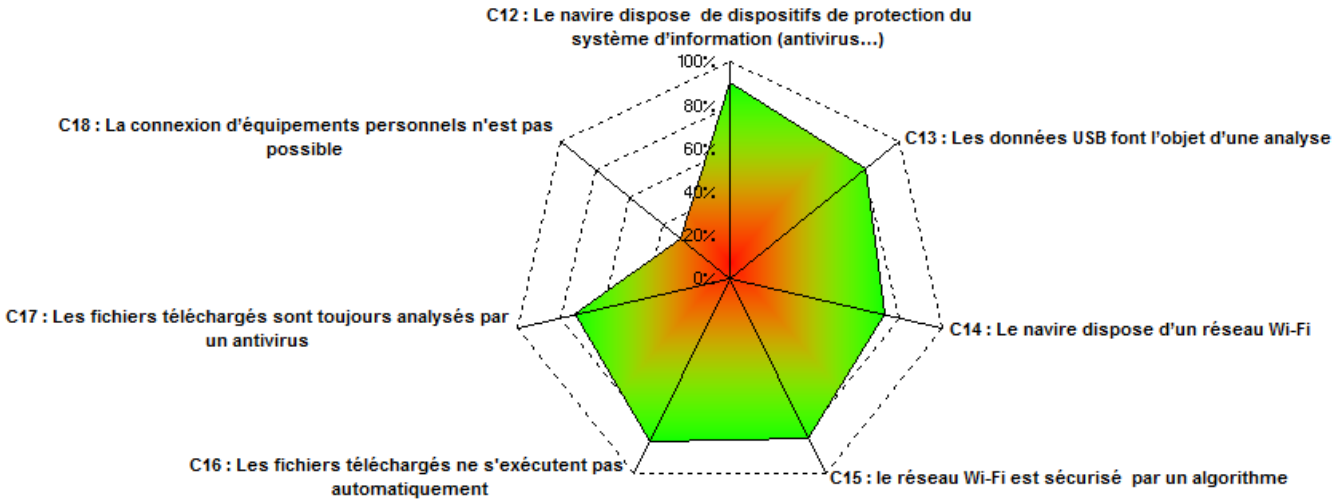
Enfin, en complément, il convient de préciser que près de 79% des navires sondés réalisent une télémaintenance entre la terre et le navire.

LOCALISATION DES SYSTEMES D'INFORMATION A BORD DU NAVIRE :

A de rares exceptions l'ensemble des systèmes d'information du navire sont localisés dans la zone d'accès restreinte du navire : zone définie au niveau du plan de sûreté du navire.

PROTECTION DES ECHANGES D'INFORMATIONS AVEC L'EXTERIEUR :

Extrait de l'analyse :

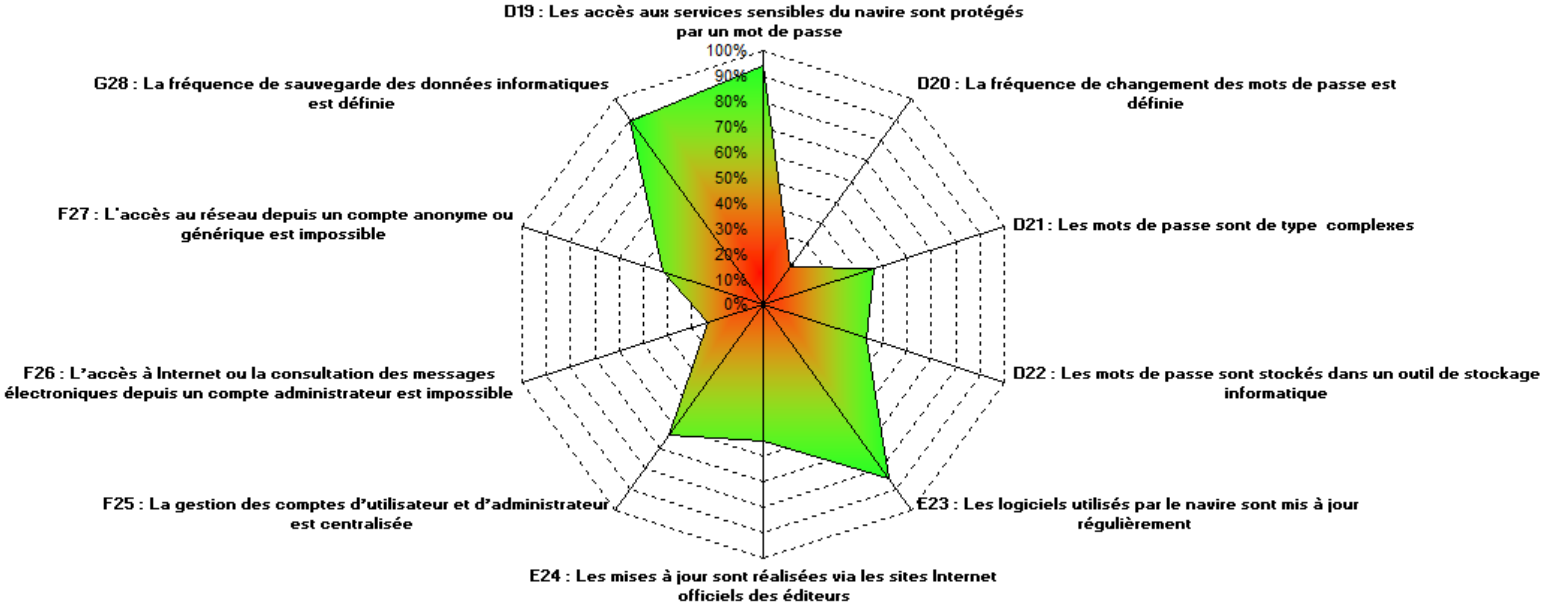


Cette rubrique permet de distinguer 4 éléments :

- Le premier fait apparaitre qu'un tiers des navires sondés disposent d'une connexion internet sur les systèmes d'information critiques (réseaux liées à la navigation, la propulsion, la gestion de l'énergie du navire, la gestion de la cargaison). Ces systèmes vitaux disposent dans les deux tiers des cas d'un moyen de connexion direct via un port USB (Questions C10/C11 n'apparaissant pas sur le graphique).
- Le second point porte sur la gestion des analyses de données. 91% des navires sondés disposent d'un logiciel antivirus permettant l'analyse de données réseaux et de données externes via un port USB. Les données téléchargées ne sont pas exécutées automatiquement dans 84% des cas.
- Le troisième point confirme la présence de système WIFI à bord des navires (75% des navires sondés). Ce système n'est malheureusement pas toujours sécurisé.
- Enfin le quatrième élément à retenir dans cette rubrique porte sur le fait que **dans 69% des cas, il est possible de relier un équipement personnel aux réseaux du navire.**

HYGIENE INFORMATIQUE (MOTS DE PASSE, ACCES, LOGICIEL, SAUVEGARDE) :

Extrait de l'analyse :

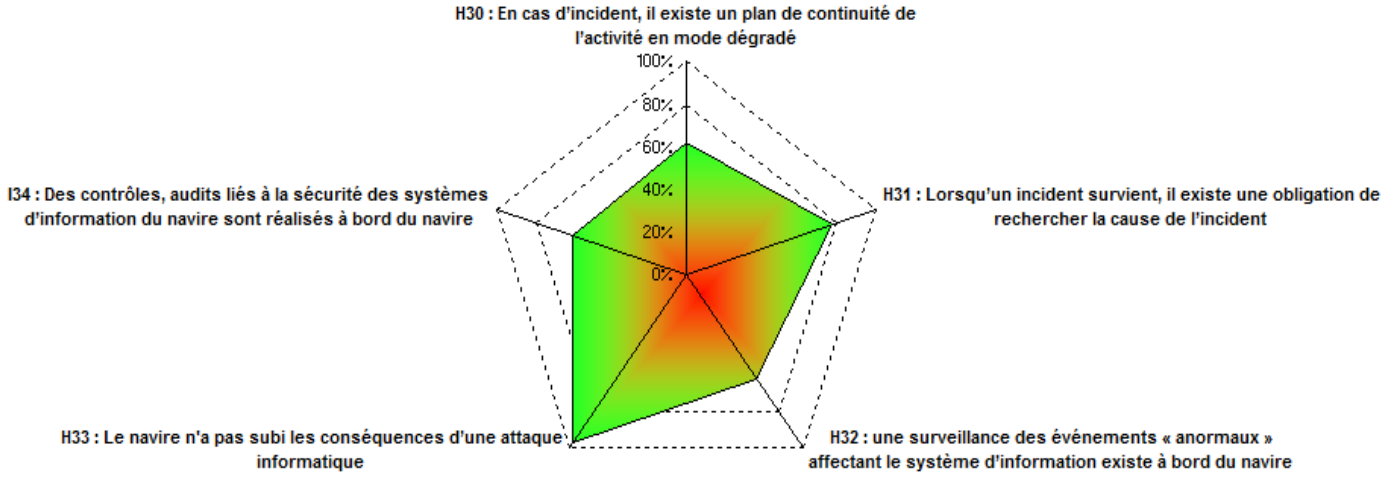


Les rubriques 4 à 7 de l'enquête permettent d'illustrer la gestion des systèmes d'information du navire par l'équipage. Les points positifs de cette rubrique portent sur l'utilisation quasiment systématique de mots de passe d'accès à un réseau, la mise à jour régulière des logiciels du navire et l'archivage de données. Cette gestion est très largement supportée par le service informatique de la compagnie. Cependant, en décryptant de plus près cette partie, il apparait les points sensibles suivants :

- Gestion des mots de passe : **la fréquence de son changement et son format ne sont pas adaptés**. Seulement dans 18% des cas, le mot de passe est changé avec une fréquence variant entre 6 mois et 3 ans. Ces mots de passe ne sont complexes dans 47% des cas.
- Les logiciels utilisés à bord des navires sondés sont mis à jour régulièrement. Les mises à jour sur le site officiel éditeur sont réalisées dans un cas sur deux.
- **La gestion des droits d'accès à bord du navire apparait plus préoccupante et faiblement maitrisée.** Seulement dans 22% des cas, l'accès à Internet ou la consultation des messages électroniques depuis un compte administrateur est impossible. De plus, près d'un navire sur deux dispose d'un compte anonyme ayant accès aux réseaux.
- Enfin, l'archivage de données est réalisé suivant une fréquence variable en fonction des compagnies : quotidienne à mensuelle. Il est à noter que l'utilisation d'une plateforme d'archivage de type « cloud » reste très rare à ce jour : 10% des navires sondés déclarent utiliser ce mode d'archivage de données navire.

INCIDENTS ET CONTROLE DES ACTIVITES SSI DU NAVIRE :

Extrait de l'analyse :



Cette dernière rubrique illustre le fait que très peu de navires témoignent d'avoir fait l'objet d'un acte de malveillance. Seulement deux navires ont déclaré avoir eu à traiter la gestion d'un virus sur le réseau de l'informatique de gestion. Néanmoins, cette information reste à titre d'information car un navire a pu faire l'objet d'une attaque sans en avoir eu connaissance.

L'enseignement principal de cette rubrique porte sur le fait que les compagnies françaises semblent sensibilisées à la gestion d'un acte de malveillance. Les mesures sont bien évidemment perfectibles. Néanmoins, l'idée de reprise en main du navire est prise en considération. Ainsi :

- 62 % des navires sondés disposent d'un plan de continuité en cas de dégradation du système d'information du navire.
- Dans 76 % des cas, il est nécessaire de rechercher la cause de l'incident.

Les axes d'amélioration sont à rechercher au niveau de la surveillance d'une activité anormale du système de gestion d'information du navire et de la mise en place d'un système d'autocontrôle de l'activité des systèmes d'informations à bord du navire. L'enquête fait apparaitre que ces contrôles sont réalisés dans 60 % des cas. Le service informatique de la compagnie est généralement en charge de ces contrôles ou audits de sécurité du système d'information du navire.

C- OUTILS DE PROTECTION DU NAVIRE

La sécurité du système d'information est fondée sur 3 principes : la confidentialité, l'intégrité et la disponibilité. Ces deux derniers points sont des éléments clés pour la gestion du navire. Ainsi, quel que soit l'acte de malveillance délibéré, il convient avant tout d'assurer la conduite du navire : assurer cette conduite par la définition des réseaux critiques à bord du navire. Ces réseaux correspondent aux définitions suivantes :

- **Réseaux critiques** : les réseaux liés à la navigation, la propulsion, la gestion de l'énergie du navire, la gestion des marchandises, la gestion des passagers et la gestion des alarmes devraient être classés « critique »,
- **Réseaux non contrôlés :** ces réseaux ne font pas l'objet d'une surveillance de sécurité de la part du navire ou de la compagnie (Réseau WIFI d'un navire à passagers). Il est néanmoins nécessaire de vérifier le cloisonnement des différents réseaux du navire.

Les outils à mettre en œuvre dans le cadre de la protection de la sécurité de l'information à bord du navire sont de trois ordres : les outils technologiques, les outils de gestion et la formation.

C1- OUTILS TECHNOLOGIQUES

Les outils technologiques doivent répondre à 4 engagements en matière d'hygiène de l'informatique :

- gérer l'architecture réseau,
- gérer les authentifications et autorisations d'accès,
- gérer le changement et la mise à jour de la sécurité des systèmes d'information,
- durcir les configurations,

La protection des données à bord d'un navire de la marine marchande ne réclame pas une approche du même niveau que celle requise par un navire de combat. La stratégie d'une cyber protection efficace du navire civil peut donc faire appel à des moyens simples et peu onéreux présents sur le marché. La combinaison des outils technologiques à mettre en place peut être la suivante :

- **Antivirus** : ce système ne correspond pas à la protection absolue. Néanmoins, ce système est un pré-requis qui doit être mis à jour afin de disposer de la signature des « malware » identifiés.

- **Pare-feu** : cet outil permet d'autoriser uniquement les flux légitimes à transiter sur le réseau. La première démarche d'un pirate numérique sera de détecter des cibles potentielles. Si toutes les portes sont fermées, l'adresse ne sera pas traitée : l'ordinateur est donc invisible aux pirates.

- **VPN (Virtual Private Network ou Réseau Privé Virtuel)** : une connexion VPN est aussi appelée connexion « tunnel ». Ce système crée une enveloppe de protection pour toutes les informations transitant par son intermédiaire. En complément, le VPN masque l'adresse des ordinateurs connectés et les remplacent par celles de serveurs intermédiaires.

- **Anti-spyware** : certains programmes espions ne sont pas considérés comme des virus. Ces derniers passent donc au travers de l'antivirus. Il convient d'associer ces 2 types de programmes pour protéger correctement le système. Un antivirus contient généralement un dispositif anti-spyware.

- **Logiciel de chiffrement de messagerie** : ce dispositif peu coûteux permet de rendre illisible le message même s'il est intercepté.

- **IDS (Intrusion Detection System)** : ces outils permettent de détecter les attaques/intrusions du réseau sur lequel il est placé. C'est un outil complémentaire aux firewall, scanneurs de failles et anti virus. Une alarme remonte dès lors qu'une activité liée à un comportement ou une signature anormale est détecté sur les réseaux et système.

- **NAS (Network Attached Storage)** : ce système permet d'archiver les données et de stocker sur un volume centralisé pour des clients du réseau. L'archive des données permet d'envisager la reprise en main du système en cas d'acte de malveillance.

C2- OUTILS DE GESTION

Les outils de gestion à mettre en place devraient utiliser les règles de certification internationale. Pour un navire, ces règles sont encadrées par les codes ISM (gestion de la sécurité) et ISPS (gestion de la sûreté). En référence à ces deux codes, le manuel de gestion de la sécurité inclut des références à la sécurité des systèmes d'information à bord du navire. Cependant, ces références sont généralement très basiques. Quant au plan de sûreté, il correspond à une approche purement physique de la sécurité des systèmes d'information du bord. Le plan de sûreté du navire et le manuel de la gestion de la sécurité sont les documents appropriés pour y inclure les références de gestion de la cyber sécurité :

- la politique de cyber sécurité de la compagnie,
- la gestion d'incident issue d'un acte de malveillance : reprise du navire,
- l'autocontrôle ou audit du système d'information du navire,
- la sauvegarde des données,
- la gestion des transactions (échanges) entre l'opérateur et la machine, entre les interconnections machine/machine et entre le navire et les intervenants extérieurs. Ce dernier aspect est essentiel car un cyber attaquant s'appuiera plus facilement sur un intervenant extérieur pour contourner les mesures mises en place par la compagnie.

D- LA NECESSITE D'ELEVER LE NIVEAU DE PROTECTION

Au fil des années, les navires sont devenus de plus en plus dépendants de leur système informatique embarqué. Le recueil des éléments de cette étude permet d'établir trois enseignements :

- Le premier porte sur la nécessite de « sacraliser » les systèmes industriels à bord du navire.
- Le second enseignement porte sur le besoin d'élever le niveau de protection du système d'information du navire en disposant d'outils systèmes adaptés à l'exploitation du navire et d'un système de gestion permettant de faire face à une cyber attaque.
- Enfin le troisième enseignement concerne le besoin de disposer de marins sensibilisés à cette menace. Ils pourront ainsi mieux détecter une incohérence système. Cette approche est désormais possible au travers d'un guide conjointement rédigé par l'ANSSI et la DAM (« *Guide des bonnes pratiques de sécurité informatique à bord des navires* » – Edition octobre 2016). **La cause première des attaques est liée à l'attaquant. Il est cependant à noter que le facteur humain joue la plupart du temps un rôle clé dans le fait qu'une attaque réussisse ou non.**

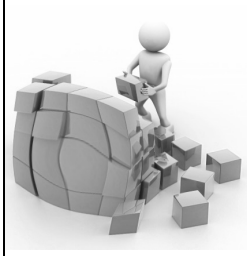
D1- SACRALISER LE SYSTEME INDUSTRIEL DU NAVIRE

Fonctionnant auparavant en architecture fermée, les systèmes de contrôle et d'acquisition de données (SCADA) utilisés à bord du navire sont désormais potentiellement connectés à internet. Ces systèmes industriels resteront par définition basés sur des technologies qui n'évolueront que très peu après leurs constructions. Ces systèmes sont par conséquent vulnérables. **Il est donc fondamental de cloisonner ces systèmes et d'éviter les interconnexions avec d'autres systèmes de gestion du navire**. Les interconnexions sont une source de vulnérabilités. Afin de réduire le risque d'un acte de malveillance sur le système industriel du navire, il convient d'intégrer les notions suivantes (Guide *« le risque industriel à bord du navire »* – Edition janvier 2017) :

- **Evaluer le risque :** cette analyse est le point de départ de toute démarche de cyber sécurité. Les systèmes doivent faire l'objet d'une analyse méthodique. Cette évaluation sera revue régulièrement,
- **Cartographier l'installation du navire :** cette illustration du système permet d'une part d'évaluer rapidement l'impact d'un acte de malveillance et d'autre part de contribuer à la résolution des incidents,
- **Contrôler :** Les autocontrôles ou audits internes permettent de vérifier régulièrement le système, le niveau effectif de cyber sécurité du navire. Ce contrôle doit statuer également sur la gestion des intervenants extérieurs,
- **Surveillance du système :** cette veille permet de prévenir la menace. Cette conduite doit s'assurer de la surveillance d'une intrusion au niveau du système,
- **Plan de continuité :** Le plan d'urgence du navire et de la compagnie doivent répondre à l'ensemble des scénarios d'incident entraînant un arrêt ou une dégradation d'une activité critique identifiée au niveau de l'évaluation des risques.
- **Télémaintenance :** Des procédures claires et des moyens de protection doivent être mis en place pour encadrer ce type d'opérations. La politique de la compagnie devrait définir le cadre de cette maintenance à distance.

D2- RECOMMANDATIONS AFIN D'ELEVER LE NIVEAU DE CYBERSECURITE DU NAVIRE

En février 2016, la Direction des Affaires Maritimes a transmis à l'Organisation Maritime Internationale (OMI) une soumission traitant des éléments sur la cyber sécurité appliqués au navire. Cette soumission a permis de participer activement aux travaux du comité MSC96**.** La circulaire MSC.1/Circ.1526 du 01 juin 2016 précise désormais le besoin de s'appuyer sur les codes déjà établies par l'OMI pour gérer la cyber sécurité du navire. Elever le niveau de cyber sécurité du navire consiste à appliquer un ensemble de règles qui conduise à intégrer la gestion des systèmes industriels du navire, la gestion des outils technologiques, la formation des marins et des procédures intégrées au niveau des codes déjà établis par l'OMI. **Les recommandations suivantes peuvent servir de fil conducteur aux compagnies pour élever ce niveau de protection**. Les lignes directrices à suivre devraient être les 7 suivantes :

R1 	**Réaliser une évaluation de la sécurité des systèmes d'information du navire.** Cette évaluation peut s'appuyer sur les directives sur la cyber sécurité à bord des navires de BIMCO, la norme ISO/CEI 27001 sur les technologies de l'information, le cadre NIST du National Institute of Standards and Technology des États-Unis, la norme NF EN 31010, le guide du DNVGL-RP-0496 ou autre. Cette évaluation devrait statuer au moins sur : ▪ la cartographie logicielle et matérielle du navire, ▪ la définition des éléments sensibles du navire, ▪ la gestion des vulnérabilités systèmes.
R2 	**Rédiger une politique compagnie des systèmes d'information du navire.** Cette politique devrait définir au moins : ▪ le responsable SSI du navire, ▪ le contrôle des accès, les mesures de sécurité SI (hygiène), ▪ le contrôle de la gestion des enregistrements, le contrôle « fort » de la télémaintenance et des échanges d'informations, ▪ les grandes lignes d'un plan garantissant la continuité opérationnelle du navire, ▪ préparation aux situations dangereuses : cellule de crise, utilisation d'un SOC (Security Operation Center), ▪ Faire référence au paragraphe 2.3 de la circulaire de l'OMI MSC.1/Circ.1526 du 01 juin 2016.
R 3 	**Appliquer des mesures d'hygiène en matière de gestion des systèmes d'information du navire.** Ces mesures doivent porter sur la gestion : ▪ des droits d'accès, gestion des privilèges, archivage des données, ▪ des mots de passe, sécurisation de la messagerie, ▪ de formation et de campagne de sensibilisation, ▪ du changement et mise à jour des logiciels du navire.

R 4 	**Appliquer un contrôle des échanges des systèmes d'information du navire.** Il convient de rédiger une procédure qui précise la définition d'accès aux équipements sensible du navire : ▪ Cette procédure définit le mode d'accès à ces systèmes (USB,CD, PC...), ▪ Les agents autorisés à accéder à ces systèmes, ▪ Les opérations qui nécessitent ces accès (maintenance, remplacement, intégration), ▪ La traçabilité de ces accès, ▪ Limiter les connections WIFI lors des opérations sensibles du navire (approches, gestion des opérations sensibles définis au niveau de la politique SSI de la compagnie), ▪ Proscrire les appareils sans fil ou utiliser un système de chiffrement (clavier, souris… systèmes vulnérables par ondes radio (*Keysniffer*)), ▪ Proscrire les outils informatiques non référencés et à plus forte raison connectés au réseau (Shadows IT).
R 5 	**Mettre en place un plan de continuité de fonctionnement après un incident**. Il convient de rédiger une procédure qui précise les éléments suivants : ▪ Définir les éléments sensibles (Résultat de l'évaluation SSI du navire), ▪ Système permettant de prendre le relais du système hors service, ▪ Description du mode opératoire de reprise du système hors service, ▪ Isoler le système défectueux. ▪ Définir une fréquence d'essais du plan de continuité, ▪ Définir une fréquence de restauration des données archivées,
R 6 	**Contrôler et gérer les incidents de systèmes d'information du navire :** ▪ Réaliser un contrôle de l'activité des systèmes d'information du navire, ▪ Assurer la surveillance, ▪ Analyser des activités anormales sur le système de gestion du navire.
R 7 	**Appliquer les mesures de protections physiques des systèmes d'information du navire.** Il convient de privilégier les Zones d'Accès Restreinte du navire pour installer les systèmes d'informations du navire.

D3- METTRE EN ŒUVRE LES RECOMMANDATIONS

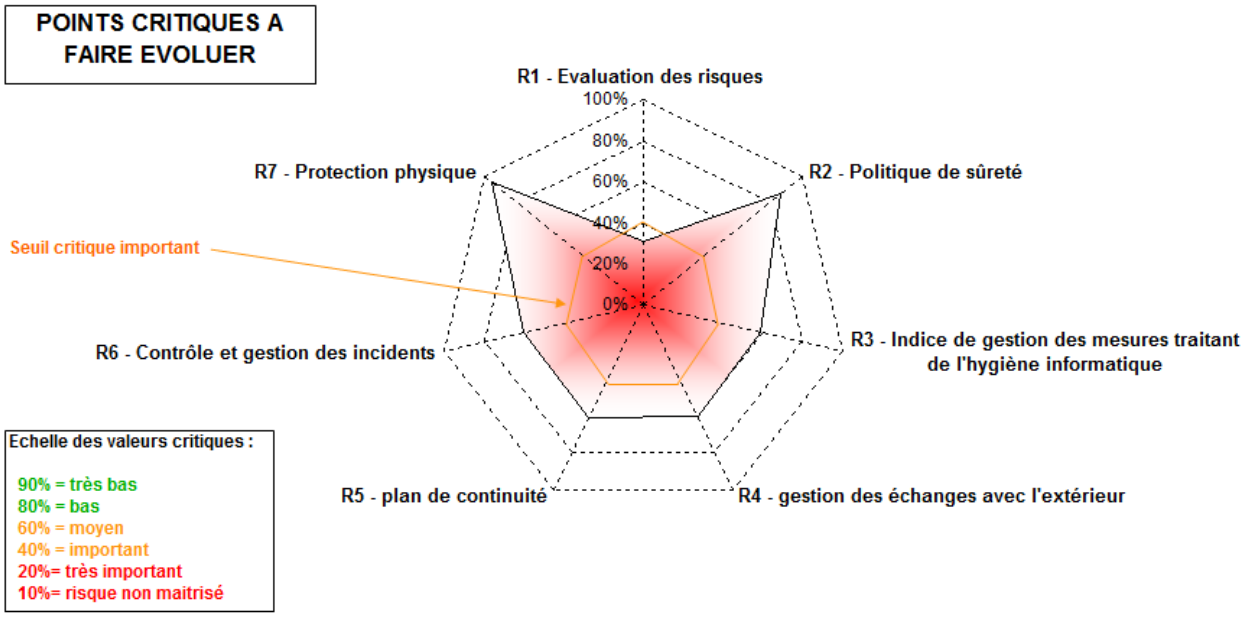
Les points critiques.

L'analyse des données de l'enquête fait apparaitre que les compagnies françaises ont pris en compte la gestion de la sécurité des systèmes d'informations au travers d'une politique et d'une protection physique de ces systèmes. En revanche, il apparait que l'évaluation des risques des systèmes d'informations reste marginale. Cette évaluation est pourtant la base de toute action à mener dans le cadre de la mise en place de la cyber sécurité à bord du navire. Cette action permet de réduire la criticité relative à la gestion des 4 domaines suivants :

- Mesures d'**hygiène** informatique à appliquer à bord du navire,
- **Echanges** avec les opérateurs extérieurs au navire,
- **Continuité** opérationnelle du navire,
- **Contrôle** des activités malveillantes vers le navire

Il convient d'alerter les compagnies sur la nécessité de réaliser une évaluation de ces risques afin de renforcer les contre-mesures pour faire face à un acte de malveillance numérique. Il est à noter que cette évaluation est obligatoire pour le pavillon français en référence au règlement européen CE725/2004 article 3.5. Cet article impose l'application de l'article B8.3 du code ISPS *: Une SSA (Ship Security Assessment) devrait porter sur les éléments ci-après à bord ou à l'intérieur du navire : .1-sûreté physique; .2-intégrité structurelle; .3-systèmes de protection individuelle; .4-procédures générales; .5-systèmes de radio et télécommunications, y compris* ***les systèmes et réseaux informatiques****, .6- autres zones qui, si elles subissent des dommages ou sont utilisées par un observateur illicite, présentent un risque pour les personnes, les biens ou les opérations à bord du navire ou à l'intérieur d'une installation portuaire.*

Cette évaluation est approuvée par l'autorité du pavillon dans le cadre de l'approbation du plan de sûreté du navire.

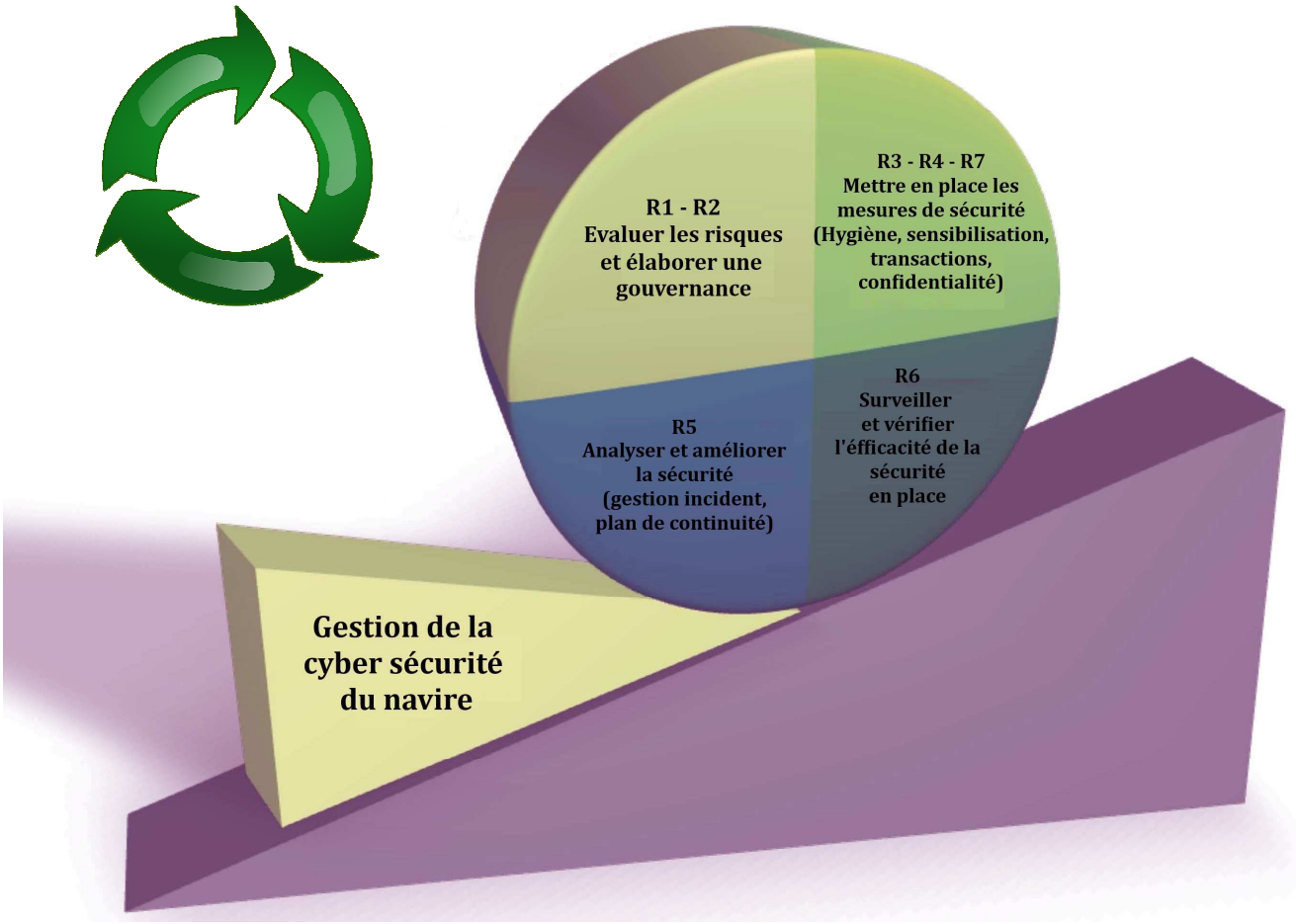


La mise en place de la cyber sécurité à bord du navire.

La mise en place de mesures de sécurité des systèmes d'informations à bord du navire devrait s'appuyer sur le principe de la roue de DEMING. La méthode comporte quatre étapes, chacune entraînant l'autre, et vise à établir un cercle vertueux au travers des 4 actions suivantes :

- Plan : **Préparer**, planifier,
- Do : Développer, **réaliser,** mettre en œuvre,
- Check : **Contrôler**, vérifier,
- Act : Agir, **ajuster**, réagir.

En application de cette méthode et en référence au paragraphe 2.5 de la circulaire de l'OMI MSC.1/Circ.1526 du 01 juin 2016, les 7 recommandations permettant de renforcer le niveau de cyber sécurité du navire s'intègrent naturellement dans la roue ci-dessous :



D4- QUEL AVENIR POUR LA CYBERSECURITE DU NAVIRE

La problématique de la cyber sécurité du navire est posée.

Le navire est relié à la toile. Les systèmes embarqués peuvent comporter des défauts. La menace est relativement faible à ce jour. Les systèmes technologiques et de gestion adaptés au navire existent. Le monde du « shipping » a posé un premier jalon de directives. Tout est donc en place pour protéger les 50 000 navires. Comme nous l'avons vu, l'acte de malveillance numérique à l'encontre du navire reste marginal à ce jour. Alors pourquoi protéger le navire ? La nécessité de mettre en place des mesures de sécurisation n'améliore pas la gestion de l'exploitation du navire et oblige cependant à investir dans un domaine qui ne rapporte pas ! Le résultat de l'équation parait simple, à quoi bon investir dans la cyber sécurité du navire.

Il faut cependant garder à l'esprit que la non prise en compte de cette menace à bord du navire pourrait être catastrophique et coûter bien plus chère qu'un investissement dans ce domaine. Imaginez les conséquences d'une cyber attaque sur un porte-conteneurs de 19 000 boîtes dont la valeur marchande peut atteindre 4 milliard de dollars !

Quel que soit le mode de pensée, ce type de menace est désormais incontournable pour le monde maritime : plus les navires se numérisent, plus ils sont exposés. Par conséquent, il est essentiel de sensibiliser les armateurs. Il est essentiel également d'accompagner les armateurs pour concrétiser la mise en place d'outils de gestion, d'outils technologiques et d'une formation adaptée. Cette enquête illustre les moyens disponibles pour répondre à ce risque qui n'a rien de marginal.

Maintenant, jusqu'où accompagner le pavillon français ?

Cette frontière est fonction de l'évaluation de la menace. Si cette dernière correspond à la gestion de virus paralysant temporairement la cartographie électronique du navire, l'équipage devrait pouvoir y faire face avec des procédures adaptées au navire. Si cette menace prend la forme d'une cyber arme sophistiquée dormante utilisant des failles système de type « ODay » ou d'un malware de type « air gap », il est évident que ni l'équipage, ni le support informatique de la compagnie pourra y faire face ! Ce genre d'arme fait pourtant partie de la panoplie des outils à disposition de groupes criminels, de groupes terroristes ou d'Etats. En complément, n'oublions pas que le navire représente une excellente vitrine médiatique. Dans ce contexte, on peut raisonnablement s'interroger sur le besoin de disposer d'une « cyber flotte maritime stratégique ». A l'image de nos approvisionnements stratégiques qui imposent un quota de navires, on peut s'interroger sur le besoin pour la France de disposer d'un ensemble de navires garantissant un niveau d'exigence en matière de cyber sécurité au travers d'une labellisation permettant d'assurer nos approvisionnements stratégiques. La France n'est pas à l'abri d'une cyber attaque en représailles à un choix fait par notre nation. : **« *Les hommes n'acceptent le changement que dans la nécessité et ils ne voient la nécessité que dans la crise* »** (Jean MONNET).

E- ANNEXE N°1 – VULNERABILITES SPECIFIQUES DU NAVIRE

1- AIS (*AUTOMATIC IDENTIFICATION SYSTEM*)

L'AIS est initialement destiné à aider les navires à éviter les collisions, les autorités portuaires et maritimes à surveiller la circulation et assurer un meilleur contrôle de la mer. Les récepteurs AIS ont fait leur apparition dans les passerelles depuis quelques années. Ils gèrent l'envoi et la réception des positions GPS, vitesse, cap, type, lieu et heure d'arrivée des navires, vers et depuis les navires environnants. L'AIS est un système d'échange de données entre navires rendu obligatoire par l'Organisation Maritime Internationale (OMI) depuis 2004. Cependant, la généralisation de l'AIS pose des problèmes de confidentialité liés à la sûreté : la sélection du navire par des pirates. Les données transmises par l'AIS sont à la portée de tous, y compris de la communauté scientifique. L'installation d'émission et de réception contient :

- un transpondeur (émission automatique déclenchée par une réception préalable) radio VHF avec 2 chaînes de réception et une d'émission ;
- une unité de contrôle et de visualisation (Minimum Keyboard Display MKD) incluant le processeur de communication et les interfaces de sorties vers les autres systèmes (ECDIS, ARPA).
- un récepteur GPS donnant la position du navire et le temps UTC nécessaire à la synchronisation des transmissions de données AIS ;
- un récepteur VHF ASN (Appel Sélectif Numérique) est parfois intégré au transpondeur et réglé sur le canal 70 pour un échange de messages type texto.

Basé sur l'échange automatisé de communications par radio VHF entre navires d'une part, entre navires et centres de surveillance maritime d'autre part, il permet une identification en temps réel des navires émetteurs. **le système est potentiellement vulnérable :**

- **Au brouillage,**
- **A l'envoi de fausses d'informations,**
- **A la transmission de virus informatiques** (l'AIS est géré par un mini-ordinateur).

Par ailleurs, le système AIS peut aussi être utilisé pour diffuser de fausses informations, qu'il est possible de « fabriquer » relativement facilement. L'objectif de ces faux messages (signal de détresse, fausse localisation de navire…) est avant tout d'attirer l'attention et de piéger les navires visés. En effet, l'AIS génère une alerte dans ce cas de figure.

2- ECDIS (ELECTRONIC CHART DISPLAY INFORMATION SYSTEM)

Un ECDIS est un « système de visualisation des cartes électroniques et d'information » qui permet de faire apparaître en temps réel la position du navire sur une carte présentée sur un écran.

Ce système permet de se passer de la carte papier.

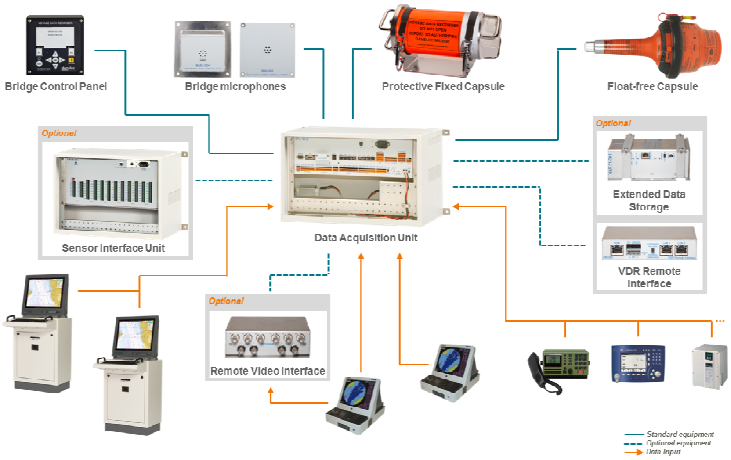
Il fournit au navigateur toutes les informations dont il peut avoir besoin pour faire route en sécurité : position instantanée du navire (fonction GPS), lignes de sonde et hauts fonds, éphémérides nautiques (pour le soleil et la lune notamment), feux côtiers et balises… Il est également couplé au système radar anticollision (ARPA). Le système est conforme aux normes édictées par l'OMI.

Le système ECDIS a quelques vulnérabilités sous-jacentes de la sécurité des logiciels qui pourraient conduire à des résultats désastreux pour les navires en mer. La base d'ECDIS est un système de cartographie de navigation qui utilise un système informatique pour afficher numériquement les cartes marines ainsi que l'emplacement exact et le suivi de son propre navire.

Les vulnérabilités de ce système peuvent porter :

- **sur le vecteur de mise à jour du système :** disques CD/DVD, par connexion internet/Inmarsat ou support USB,
- **la non mise à jour du système d'exploitation qui correspond à un poste de travail qui fonctionne généralement sur un support de type Windows non mis à jour.**
- **Ce système est interconnecté aux capteurs du navire : radar, NAVTEX, systèmes d'identification automatique (AIS), Vitesse Log, Sondeur, anémomètre.** Ces capteurs sont souvent connectés au réseau local à bord des navires (port série / NMEA aux adaptateurs LAN),

3- VDR / SVDR (VOYAGE DATA RECORDER)



Le système VDR ou SVDR correspond à la « boîte noire aéronautique » du navire. Il est obligatoire, depuis le 1er juillet 2002, sur tous les navires à passagers et tous les navires de charge d'une jauge supérieure à 3000. L'objectif de cet appareil embarqué est d'aider à analyser les circonstances qui ont mené à un accident par l'examen des données.

La configuration standard d'un VDR est constituée comme suit :

- Le DAU (Data Acquisition Unit) qui correspond au cœur de l'équipement marin : entrées VHF, entrée Radar, disque dur ou Flash disk extractible, batterie de secours autonome, micros, capsule haute résistance d'enregistrement des données, BAU (Bridge Alarm Unit), SIU (Sensor Interface Unit) qui collecte toutes les autres données, les codifie et les retransmet au DAU,
- L'enregistrement de données : date et heure, position du navire, vitesse surface (loch), cap gyro, compas magnétique, image radar, conversations passerelle, radio communications (émission/réception), hauteur d'eau sous la quille (sondeur), alarmes principales (incendie, machine, etc.), statut des ouvertures dans le bordé (ouvertes ou fermées), statut des portes étanches et des portes coupe-feu (ouvertes/fermées), angle de barre, ordres et réponses machine - (transmetteur d'ordre machine), propulseur, vitesse vraie ou relative du vent.

Tout comme le système ECDIS, les vulnérabilités de ce système peuvent porter :

- **sur le vecteur de mise à jour du système :** disques CD/DVD, par connexion internet/Inmarsat ou support USB,
- **la non mise à jour du système d'exploitation qui correspond à un poste de travail qui fonctionne généralement sur un support de type Windows non mis à jour.**
- **Ce système est interconnecté aux capteurs du navire.**

4- GNSS (GLOBAL NAVIGATION SATELLITE SYSTEM)

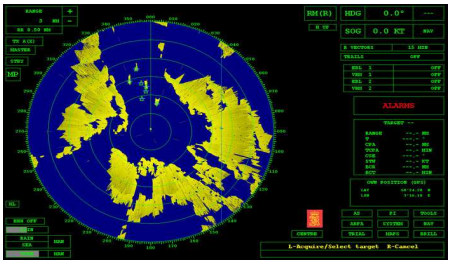
Le GPS est un système de géo-localisation de portée mondiale. Au travers d'un ensemble de satellites et un récepteur GPS, il est possible de connaitre sa position (2D ou 3D), sa vitesse, sa route, l'heure (UTC), etc. permettant ainsi de s'orienter sur mer, sur terre ou dans les airs. Plusieurs systèmes GPS existent aujourd'hui dans le monde. Le système offrant une couverture mondiale et le plus utilisé par le grand public est constitué de 24 satellites situés à une altitude d'environ 20000 km évoluant sur 6 plans orbitaux quasi circulaires inclinés à 55° sur l'équateur. Le principe du positionnement est basé sur des algorithmes de calcul de distance entre le récepteur GPS et plusieurs satellites. La précision du GPS peut atteindre 10 mètres. Cette précision peut être altérée par des perturbations atmosphériques.

Les signaux des satellites civils ne sont pas protégés par chiffrement. Il est donc possible de les intercepter et de les dupliquer.

Les vulnérabilités du système peuvent être les suivantes :

- **Faible puissance du signal - faiblesse inhérente,**
- **Possibilité d' interférence involontaire,**
- **Possibilité de brouillage intentionnel,**
- **Défaillance technique de la constellation de satellites.**

5- RADAR / ARPA



Le radar (RAdio Detection And Ranging) est un système utilisant les ondes électromagnétiques afin de détecter la présence et déterminer la position ainsi que la vitesse d'un objet, d'un obstacle. Les ondes envoyées par l'émetteur sont réfléchies par la cible et les signaux de retour (appelés *écho radar* ou *écho-radar*) sont captés et analysés par le récepteur. L'ARPA (*Automatic Radar Plotting Aid)* est l'équipement associé au radar de navigation permettant le suivi des échos afin d'aider l'officier de quart dans le choix d'une manœuvre pour éviter la collision.

Les vulnérabilités du système pourraient porter sur :

- **Possibilité d' interférence involontaire,**
- **Possibilité de brouillage intentionnel,**
- **Possibilité d'usurpation d'identité en transformant le signal retour,**

6- DP (POSITIONNEMENT DYNAMIQUE) DU NAVIRE

Le système de positionnement dynamique est un système contrôlé par ordinateur qui permet à un navire de maintenir sa position en utilisant ses propres moyens de propulsion.

Ce système est composé de trois parties. Les capteurs recueillent les informations, la console informatique effectue les calculs et sert d'interface pour l'opérateur et les actionneurs agissent sur la consigne. C'est un système automatique informatisé.

Les vulnérabilités du système correspondent aux faiblesses de sécurité des capteurs tel qu'un GPS et à l'interface homme/machine/machine qui utilise un système d'exploitation qui doit être mis à jour.

7- SYSTEME DE CONTROLE INDUSTRIEL (ICS , SCADA)

A bord du navire, le risque porte sur :

(1) l'ensemble des réseaux ICS (Industrial Control System) : gestion des capteurs et actionneurs,
(2) le SCADA (Supervisory Control and Data Acquisition) : l'ensemble des serveurs, poste de travail et applications de l'ICS pour superviser le procédé industriel.

A bord du navire, les ICS sont omniprésents. Ces systèmes gèrent :
(1)- la plateforme navire (propulsion, énergie, fluides…),
(2)- la conduite du navire,
(3)- les systèmes « métiers » du navire : sécurité et exploitation de la cargaison.

D'une manière très générale, la problématique de la gestion de la sécurité des systèmes d'informations industriels résident en deux points :

- La différence de durée de vie entre les outils du Scada (cycles de vie courts (3-5 ans)) et les réseaux industriels (cycle de vie longs de 15-20 ans : équipements figés et difficiles à faire évoluer).
- La culture de programmation qui ne va pas dans le sens d'une approche préventive de la sécurité.

La vulnérabilité des systèmes industriels n'est plus à démontrer. Les APT (Advanced Persistant Threat) de type STUXNET ont illustré leurs compétences en matière de sabotage**. Les failles du système pourraient porter sur 7 domaines :**

(1) **L'absence de développement sécurisé** : développements internes, absence d'intégration de la sécurité, session non verrouillée,

(2) **Un faible niveau de protection des accès** : contrôle d'accès très simple avec une gestion de l'utilisateur et du mot de passe trop faibles ou inexistant, absence d'antivirus sur les postes de travail et serveurs, des utilisateurs disposant de privilèges administrateur.

(3) **L'absence de cloisonnement entre les systèmes d'information de gestion et les systèmes industriels non sécurisé** : ce principe permet de s'introduire via le système de gestion informatique dans le réseau industriel. Cette faille est la cible de nombreuses attaques récentes. Ces ponts servent à remonter des informations issues de la production directement dans les systèmes de pilotage. Cette méthode d'accès permet à la fois le recueil d'information et le sabotage.

(4) **Absence de supervision anormale du système**,

(5) **La non mise à jour et la faiblesse des protocoles de gestion courants** (FTP, Telnet, VNC, SNMP…) utilisés sans chiffrement qui ouvre l'accès à la récupération de login/mot de passe, à des connexions illégitimes aux serveurs,

(6) **L'utilisation croissante de systèmes informatiques standards non durcis** : Ces produits sur étagères permettent une réduction des coûts et d'interopérabilité. Ces systèmes sont par conséquent la proie de logiciel malveillant.

(7) **L'absence de contrôle des intervenants sur les systèmes industriels :** la surveillance des sous-traitants reste bien souvent insuffisante. Les conséquences de cette non-gestion peuvent être la perte de données, la détérioration d'équipements, la mise en danger du navire de son équipage et de l'environnement.

Pour de plus amples informations, il convient de lire le guide « *Le risque industriel à bord du navire* » - Edition janvier 2017.

8- SYNTHESE SUR LA VULNERABILITE DES SYSTEMES PRESENTS A BORD DU NAVIRE :

Vulnérabilités	Mesures à adopter à bord du navire	Outils de mise en œuvre de la mesure à adopter par la compagnie
(1) Usurpation de signal (ECDIS, GPS, RADAR, DP, AIS)	Recouper les éléments de navigation au niveau de la conduite du navire notamment lors de l'approche de la côte.	**Système de gestion de la sécurité du navire (ISM) :** la procédure de conduite du navire doit intégrer la possibilité d'un acte de malveillance sur les outils de navigation.
(2) Absence de contrôle d'accès au système d'exploitation du système (ECDIS, DP, SCADA)	Contrôler les interventions sur les systèmes d'exploitation non verrouillés.	**Système de gestion de la sécurité du navire (ISM) : fiches R2, R4** La politique compagnie doit intégrer les relations avec les intervenants (interne/externe) sur les réseaux critiques de conduite du navire. Ces relations devraient être formalisées au niveau des contrats liant les différentes parties (Compagnie/Equipage/Prestataires de service). **Système de gestion de la sûreté du navire (ISPS) : fiche R7** Le contrôle d'accès au navire permet de gérer les accès aux réseaux critiques du navire.
(3) Absence de cloisonnements des systèmes d'entrées/sorties (DP, SCADA) **(4) Interférence volontaire du signal** (ECDIS, GPS, RADAR, AIS) **(5) Absence de supervision anormale du système** (VDR, ECDIS, DP, SCADA)	S'assurer de la possibilité d'isoler un système hors service et de reprendre la main en mode manuel.	**Système de gestion de la sécurité du navire (ISM) : fiche R5** La mise en place d'un plan de continuité de fonctionnement suite à un incident doit permettre la reprise de fonctionnement en mode dégradé du navire : système redondant ou reprise en mode manuel. **Système de gestion de la sécurité du navire (ISM) : fiche R6** La surveillance des événements anormaux doit permettre d'alerter le navire. Ce type d'évènement est un indice permettant d'illustrer la préparation d'une cyber attaque.
(6) Non mise à jour du système d'exploitation (ECDIS, VDR, DP, SCADA)	Suivi des recommandations constructeur et gestion de la configuration des systèmes d'exploitation et des logiciels à bord du navire.	**Système de gestion de la sécurité du navire (ISM) : fiches R2, R3** Le suivi de la mise à jour des systèmes d'exploitation via des « patch » systèmes doit permettre de disposer d'un système toujours à niveau.

E- ANNEXE N°2 – ENQUETE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'écologie, du développement durable et de l'énergie

DGITM / DAM / SM2 / Mission sûreté des navires

ENQUETE : Cybersécurité à bord d'un navire battant pavillon français

Pour exécution : bureau de la réglementation et du contrôle de la sécurité et de la sûreté des navires, Centre de Sécurité des Navires.

Résumé : Cette enquête a pour objectif de dresser un état des lieux du niveau de sécurité des systèmes d'information présents à bord du navire (cybersécurité du navire). A l'issue, les éléments de cette étude participeront à définir un standard sur la vulnérabilité du navire. Ces éléments pourraient être pris en compte dans le cadre de la refonte réglementaire du Décret 2007-937 et du Décret 84-810.

Mots clés :

- ✓ Cartographie du système d'information : ensemble d'éléments décrivant le système d'information et comprenant notamment la liste des ressources matérielles (modèles) et logicielles (versions) utilisées, l'architecture du réseau sur lequel sont identifiés les points névralgiques (serveurs sensibles, connexions externes).
- ✓ Zone d'Accès Restreinte : zone identifiée au titre du plan de sûreté du navire.
- ✓ Service sensible : conduite du navire, maintenance du navire, conduite des opérations en relation avec la gestion de la cargaison du navire (stabilité, transfert de cargaison, ventilation double coque, rejets…), messagerie électronique du navire.
- ✓ Mot de passe complexe : mot composé d'au moins 8 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux).
- ✓ Administrateur réseau : compte privilégié permettant la réalisation d'opérations de configuration et de gestion sur tout ou partie du système d'information : installation, gestion des configurations, maintenance, évolution du SI, supervision ou gestion de la sécurité.
- ✓ Réseau WIFI sécurisé : lors de la première configuration l'identifiant et les mots de passe ont été modifiées, protocole de chiffrement (WPA2 ou WPA-AES).
- ✓ Dispositif de protection du système d'information : dispositif technique mis en place en vue d'élever le niveau de sécurité du système d'information. Il peut s'agir par exemple de solutions de type antivirus (logiciel destiné à identifier, neutraliser et effacer des logiciels malveillants), de dispositifs de chiffrement des données (procédé cryptographique grâce auquel on rend la compréhension d'un document impossible à toute personne qui ne possède pas la clé de (dé)chiffrement), de pare-feu ou firewall (logiciel et/ou matériel permettant de protéger les données d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles pré définies).

Documents de référence :

- ✓ Code international pour la sûreté des navires et des installations portuaires (ISPS) : B8.3.5 sur l'évaluation des moyens de communication y compris les systèmes et réseaux informatiques.
- ✓ Instruction sûreté des navires en date du 26 janvier 2015 (Processus écoute client – système qualité DAM),
- ✓ Note technique sur la certification des navires en date du 25 février 2015,

Date de mise en application de l'enquête : 01 aout 2015
Durée de l'enquête : une année

Gestion du rapport d'enquête :
copie N°1 : Navire - document transmis au commandant du navire,
copie N°2 : Centre de Sécurité des Navires gestionnaire – dossier sûreté du navire,
copie N°3 : Mission sûreté des navires – dossier sûreté du navire,

REFERENTIEL ENQUETE « CYBER-SECURITE DU NAVIRE »

Identité du navire :	
N° OMI du navire :	
Lieu de l'enquête :	
Date de l'enquête :	
Membre(s) de l'équipe d'enquête :	
Enquête réalisée en présence de :	

Pratiques informatiques à bord du navire	oui	non	Commentaire
A- Généralités :			
A1 : La compagnie du navire dispose-t-elle d'une politique de sécurité informatique ?			
A2 : La compagnie du navire dispose-t-elle d'un service informatique ?			
A3 : Un responsable du système d'information est-il identifié à bord du navire ?			
A4 : Les systèmes d'information du navire ont-ils fait l'objet d'une analyse de risques ?			
A5 : Le navire dispose-t-il d'une cartographie de son système d'information ?			
A6 : Le système d'information du navire fait-il appel à une télémaintenance ?			
B- Localisation des réseaux informatiques :			
B7 : Les éléments informatiques de gestion de la navigation (pilotage du navire et moyens de communications) du navire sont-ils en Zone d'Accès Restreinte ?			
B8 : Les éléments informatiques de gestion de la plate-forme navire (propulsion, électricité, maintenance, vie du bord, formation) du navire sont-ils en ZAR ?			
B9 : Les éléments informatiques de gestion de la cargaison du navire (gestion stabilité du navire, transfert de la cargaison, protection environnement) du navire sont-ils en ZAR ?			
C- Protection des échanges informatiques avec l'extérieur :			
C10 : Les réseaux associés à la navigation, à la maintenance et à la propulsion du navire sont-ils connectés à Internet ?			
C11 : Est-il possible de se connecter à ces réseaux via un port USB ?			
C12 : Le navire dispose t'il de dispositifs de protection du système d'information ?			
C13 : Les données introduites dans le système d'information depuis les ports USB font-elles l'objet d'une analyse par un dispositif de type antivirus?			
C14 : Le navire dispose-t-il d'un réseau Wi-Fi ?			
C15 : Si oui, le réseau Wi-Fi est-il sécurisé et par quel algorithme ?			
C16 : Les fichiers téléchargés depuis Internet ou reçus par messagerie électronique sont-ils ouverts ou exécutés automatiquement ?			
C17 : Les fichiers téléchargés depuis Internet ou reçus par la messagerie électronique sont-ils toujours analysés par un antivirus ?			

C18 : La connexion d'équipements personnels au système d'information du navire est-elle physiquement possible ? Est-elle autorisée ?			
Pratiques informatiques à bord du navire	**oui**	**non**	**Commentaire**
D - Gestion des mots de passe :			
D19 : Les accès aux services sensibles du navire sont-ils protégés par un mot de passe ?			
D20 : La fréquence de changement des mots de passe est-elle définie ?			
D21 : Les mots de passe sont-ils complexes ?			
D22 : Les mots de passe sont-ils stockés dans un outil de stockage informatique ?			
E - Mise à jour régulière des logiciels :			
E23 : Les logiciels utilisés par le navire sont-ils mis à jour régulièrement ?			
E24 : Les mises à jour sont-elles réalisées via les sites Internet officiels des éditeurs ?			
F - Définition des utilisateurs des moyens informatiques :			
F25 : Existe-t-il une gestion centralisée des comptes d'utilisateur et d'administrateur réseau à bord du navire ?			
F26 : L'accès à Internet ou la consultation des messages électroniques depuis un compte administrateur est-il possible ?			
F27 : Existe-il des comptes anonymes ou génériques (stagiaire, contact) ayant accès au réseau informatique du navire ?			
G- Sauvegarde régulière des données informatiques :			
G28 : La fréquence de sauvegarde des données informatiques est-elle définie ?			
G29 : La sauvegarde des données du navire est-elle réalisée sur une plate-forme Internet « cloud » ?			
H- Incident :			
H30 : En cas d'incident, existe-t-il un plan de continuité de l'activité en mode dégradé ?			
H31 : Lorsqu'un incident survient, existe-t-il une obligation de rechercher la cause de l'incident ?			
H32 : Existe-t-il une surveillance des événements « anormaux » affectant le système d'information (transfert massif de données, tentative de connexion…) ?			
H33 : Le navire a-t-il déjà subi les conséquences d'une attaque informatique ?			
I- Autres :			
I34 : Est-ce que des contrôles ou vérifications liés à la sécurité des systèmes d'information du navire sont réalisés ?			

Avis complémentaire de l'équipe d'enquête sur la vulnérabilité de l'installation informatique du navire :
Pièce(s) jointe(s) :

E- ANNEXE N° 3 – GUIDES

Ces fiches comprennent les objectifs à mettre en place pour réduire le risque de cyber menace.

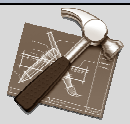
En complément, ces fiches font références aux outils sur lesquels la compagnie peut s'appuyer pour réduire ce risque :

- Outils technologique,
- Outils de gestion : code ISM et ISPS
- Outils de l'ANSSI : **http://www.ssi.gouv.fr/**

Ces 7 fiches font références aux recommandations de l'enquête menée par la DAM et se basent sur les directives de la circulaire de l'OMI MSC.1/Circ.1526 du 01 juin 2016 en matière de prolongement des pratiques utilisées à bord du navire.

- R1 / Evaluation de la sécurité du système d'information (SSI) du navire
- R2 / Politique de sécurité du système d'information du navire
- R3 / Mesures d'hygiène de la sécurité du système d'information du navire
- R4 / Mesures de protection des échanges d'information du navire avec l'extérieur
- R5 / Plan de continuité
- R6/ Gestions du contrôle et des incidents d'information du navire
- R7 / Protection physique des systèmes d'information du navire.

R1- EVALUATION (Confiance numérique du navire)



OBJECTIFS :

1. Déterminer le seuil acceptable de la menace du navire,
2. Définir le cadre de cette évaluation : prise en charge du navire à l'issue d'une construction, changement de pavillon, gestion de la maintenance du navire en matière de SSI, gestion du passage en cale sèche du navire, gestion d'une intervention à bord sur les réseaux du navire,
3. Définir les critères d'évaluation :

- Outils de base : cartographie (réseaux privés, réseaux non contrôlés) réseaux critiques, fournisseurs d'équipements, type de menace,
- Moyens de communication : satellite, TOIP, réseau sans fil, LAN,
- Propulsion/navigation : positionnement (AIS,GPS…), ECDIS, DP, Manœuvre, SMDSM, Radar, VDR,
- Contrôle accès du navire : CCTV, BNWAS, SSAS,
- Gestion cargaison : CCR, stabilité, pompes…
- Gestion passagers : contrôle, réseaux privés, divertissement…
- Eléments transversaux : routeur, commutateur, pare-feu, systèmes d'exploitation,

4. **Statuer sur la vulnérabilité du navire :** résultat, seuil de probabilité d'accident, système clé du navire, gestion des accès physique et informatique, faiblesse, identification des zones à risques en matérialisant l'impact d'une menace, système d'amélioration continue, conclusions d'ordres politiques et techniques SSI.

DOCUMENT DE REFERENCE : CODE ISPS

Cette évaluation du système de sécurité d'information du navire est un document sensible qui doit être intégré au niveau du plan de sûreté du navire et ceci en référence au code ISPS B 8.3. Ces données doivent être classées « confidentielle sûreté navire » : pas de diffusion.

CONTROLE DE L'APPLICATION :

Le contrôle de cette évaluation est approuvé par le pavillon dans le cadre de l'approbation du plan de sûreté du navire en référence au règlement CE 725/2004.

L'évaluation de la cyber sécurité du navire devra évoluer afin d'avoir toujours un seuil permettant de faire face efficacement à un acte de malveillance. Ce seuil doit répondre au besoin de continuité opérationnelle du navire. Le point clé reste la résilience du système au fil du temps.

SUPPORTS D'AIDE DOCUMENTAIRE OU TECHNIQUE :

1. Directives sur la cyber sécurité à bord des navires de BIMCO.
2. Norme ISO/CEI 27001 sur les Technologies de l'information.
3. NIST du National Institute of Standards and Technology des États Unis.
4. Norme NF EN 31010 (gestion des risques, techniques d'évaluation des risques),
5. Guide de société de classification : DNVGL – RP- 0496,
6. Méthode de travail : EBIOS, MEHARI , OCTAVE …

PRINCIPE :

Besoin d'une approche globale, afin que le dispositif ne présente pas de possibilités de contournement.

R2- POLITIQUE (Gouvernance)

OBJECTIFS :

1. Validation par le haut niveau de direction,
2. Définition de l'autorité SSI de la compagnie et à bord du navire,
3. Définition de la politique de formation SSI,
4. Définition de la notion de télémaintenance, du contrôle des accès, de la gestion des enregistrements à bord du navire,
5. Définition de la gestion de secours du SSI à bord du navire,
6. Imposer la réalisation d'une évaluation des risques SSI à bord du navire,
7. Imposer la mise en place d'une cartographie du système d'information à bord du navire,
8. Imposer des mesures minimales en matière d'hygiène informatique à bord du navire,

DOCUMENT DE REFERENCE : CODE ISM

Le système de gestion de la sécurité du navire permet d'intégrer la politique SSI de la compagnie : Code ISM chapitre 2 « *POLITIQUE EN MATIÈRE DE SÉCURITÉ ET DE PROTECTION DE L'ENVIRONNEMENT* ».

CONTROLE DE L'APPLICATION :

La vérification de l'application par la compagnie et le navire de cette politique s'effectue lors des audits interne et externe du siège de la compagnie.

SUPPORTS D'AIDE DOCUMENTAIRE OU TECHNIQUE :

1. ANSSI : Mémento sur l'élaboration de Politiques de Sécurité des Systèmes d'Information (PSSI -version 03 mars 2004),
2. ANSSI : Guide pour l'élaboration d'une politique de sécurité de système d'information (Section 1 à 4) (Version 03 mars 2004),
3. ANSSI : Élaboration de tableaux de bord SSI (Version 05 février 2004),

Le guide PSSI a pour objectif de fournir un support aux responsables SSI pour élaborer une politique de sécurité du ou des systèmes d'information (PSSI) au sein de leur organisme. Il est décomposé en quatre sections : (1) l'introduction, ce présent document, permet de situer la place de la PSSI dans le référentiel normatif de la SSI au sein de l'organisme et de préciser les bases de légitimité sur lesquelles elle s'appuie ; (2) la méthodologie présente, de façon détaillée, la conduite de projet d'élaboration d'une PSSI, ainsi que des recommandations pour la construction des règles de sécurité ; (3) le référentiel de principes de sécurité ; (4) une liste de documents de références de la SSI (critères d'évaluation, textes législatifs, normes, codes d'éthiques, notes complémentaires…).

PRINCIPES :

1. **La politique de sécurité doit être apparente :** l'existence de mesures de protection doit être perçue sans pour autant être connue de façon détaillée.
2. La politique compagnie doit permettre de répondre au principe d'un SOC (Security Operation Center). Ce format permet de répondre à la détection, à la prévention, à l'alerte et à l'aide à la décision pour faire face à un acte de malveillance.
3. Enfin, la cyber sécurité du navire sera assurée si l'action se réalise au niveau organisationnel en mettant en place des normes.

R3 - HYGIENE (Gestion des accès et des fuites de données)

OBJECTIFS :

1. Mot de passe :
- Définitions : structures, stockage, changement de fréquence,
- Protection des services sensibles du navire,
2. Logiciel : gestion de la mise à jour, autorité de mis à mise jour, maintient du niveau SSI suffisant,
3. Accès au moyens SSI du navire :
- Gestion des comptes SI du navire par la compagnie,
- Gestion des comptes SI du navire à bord du navire,
- Gestion des comptes anonymes ou génériques ayant accès au navire,
4. Sauvegardes des données : fréquence de sauvegarde des données du navire, dispositif de sauvegarde, support de secours,
5. Définir le rôle de chacun à bord en matière de SSI : administrateur navire, sensibilisation,

DOCUMENT DE REFERENCE : CODE ISM

Le système de gestion de la sécurité du navire permet d'intégrer la gestion d'une hygiène des systèmes d'information du navire au regard de deux chapitres du code ISM :

1. Code ISM chapitre 6 « *RESSOURCES ET PERSONNEL* » : dispositions en matière de formation SSI des marins (sensibilisation et administration),
2. Code ISM chapitre 7 *« ÉTABLISSEMENT DE PLANS POUR LES OPÉRATIONS A BORD*» : disposer d'une procédure traitant des moyens de gestions SSI du navire

CONTROLE DE L'APPLICATION :

La vérification de l'application par la compagnie et le navire de cette politique s'effectue lors des audits interne siège et navire dans le cadre du code ISM,

SUPPORTS D'AIDE DOCUMENTAIRE OU TECHNIQUE :

1. ANSSI : Guide des bonnes pratiques de l'informatique (12 règles) : sensibilisation des marins, (Version 1.1 mars 2015),
2. ANSSI : Guide d'hygiène de l'informatique : sensibilisation SSI compagnie (Version 1.0 janvier 2013),
3. ANSSI : Outils mis en ligne :
- Gestion du mot de passe : note technique du 05 juin 2012,
- Gestion du firewall : technique du 30 mars 2013,
- Mécanismes de cryptographie B1 et B2 du 21 février 2014,
- Durcissement des postes de travail : note technique du 16 septembre 2015,
- Profil de protection d'une passerelle VPN : 13 juillet 2015,
4. **Solutions techniques :** Système de sauvegarde NAS, activation et paramétrage pare-feu, technologie VPN, antispyware, technologie « sandbox », cryptographie messagerie,

PRINCIPE :

Principe de responsabilisation des utilisateurs ou gérer le « besoin d'en connaître » de chaque utilisateur, interne ou externe.

R4 - ECHANGES AVEC L'EXTERIEUR (Sécurisation des transactions)

OBJECTIFS :

1. Réseau WIFI :
- Mesures de protection des données WIFI : cloisonner les réseaux, système de cryptage„
- Limiter les échanges lors des opérations sensibles du navire (approches portuaires, gestion de la cargaison…),
2. Connections aux réseaux : cadrer les mesures de protections lors de la connections de dispositifs USB, PC…
3. Proscrire les systèmes sans fil (vulnérabilité radio de type « keySniffer),
4. Eviter les outils informatiques non référencés (Shadows IT) : gestion des accès,
5. Connections aux systèmes industriels du navire :
- Gestion des ports de connections,
- Traçabilité en matière de connections,
- Télémaintenance : activation des ports,

DOCUMENT DE REFERENCE : CODE ISM

Le système de gestion de la sécurité du navire permet d'intégrer la gestion des échanges avec l'extérieur au regard du Code ISM chapitre 7 *« ÉTABLISSEMENT DE PLANS POUR LES OPÉRATIONS A BORD»* : disposer d'une procédure traitant des échanges SSI du navire.

CONTROLE DE L'APPLICATION :

La vérification de l'application par la compagnie et le navire de cette politique s'effectue lors des audits internes siège et navire dans le cadre du code ISM,

SUPPORTS D'AIDE DOCUMENTAIRE OU TECHNIQUE :

1. ANSSI : Recommandations de sécurité relatives aux réseaux WIFI : note technique du 09 septembre 2013,
2. ANSSI : Recommandations de sécurité relatives à la téléassistance : note technique du 07 septembre 2012
3. ANSSI : La cyber sécurité des systèmes industriel : guide de janvier 2014,
4. **Solutions technique** : cryptage WIFI, séparation des réseaux, mécanismes basic d'authentification, désactivation port USB, gestion Business2Business, activation et paramétrage pare-feu poste industriel,
5. **Norme IEC 61162-460**
6. Mise en place d'une imprimante dédiée aux intervenants extérieurs (pavillon, RO, PSCO)

PRINCIPES :

1. **Principe d'autoprotection**, ou « tout ce qui est extérieur ne peut être considéré comme sûr ».
2. **Principe d'identification** : limiter, surveiller les connections vers l'extérieur, bloquer toutes les communications non nécessaires, authentifier les intervenants extérieurs.
3. Une attention particulière doit être portée aux systèmes sans fil et aux équipements mobiles.
4. Un navire utilisant la télémaintenance doit renforcer la surveillance de ses accès qui nécessitent des privilèges élevés. Les contrats avec les sociétés de services doivent contenir des engagements de responsabilité.

R5- PLAN D'URGENCE (Continuité de service)

OBJECTIF :

1. Mise en place d'un plan de continuité de fonctionnement suite à un incident (fonctionnement en mode dégradé du navire) :

- Procédure confidentielle uniquement sous format papier,
- **Procédure décrivant le mode de reprise de gestion manuel des éléments sensibles.**
- Procédure intégrant la perte des liaisons de communication,
- Procédure décrivant l'arrêt d'un appareil infecté : isoler la machine infectée (Eviter la prolifération du malware),
- Procédure précisant les coordonnées SI compagnie 24/24,
- Mise en œuvre de cette procédure annuellement au travers d'un exercice,
- Mise à jour du document,
- Réaliser une copie physique du disque, réinstaller le logiciel sein, changement des mots de passes.

DOCUMENT DE REFERENCE : CODE ISM

Le système de gestion de la sécurité du navire permet d'intégrer la gestion d'un incident SSI du navire au regard de deux chapitre du code ISM :

1. Code ISM chapitre 8 « *PRÉPARATION AUX SITUATIONS D'URGENCE*» : mise en place d'un plan de continuité de fonctionnement après un incident,
2. Code ISM chapitre 9 *« NOTIFICATION ET ANALYSE DES IRRÉGULARITES, DES ACCIDENTS ET DES INCIDENTS POTENTIELLEMENT DANGEREUX*» : report et surveillance du SSI du navire .

CONTROLE DE L'APPLICATION :

La vérification de l'application par la compagnie et le navire de cette politique s'effectue lors des audits interne siège et navire dans le cadre du code ISM,

SUPPORTS D'AIDE DOCUMENTAIRE OU TECHNIQUE :

1. **Solution documentaire** : plan d'urgence compagnie et navire ; gestion de la cellule de crise de la compagnie,
2. Application de guide de référence SOC (Security Operation Center),
3. Gestion des incidents de sécurité : norme ISO/CEI 27035,
4. Solution technique : sauvegarde des données afin d'éviter les « ransomwares » (fiche R3).

PRINCIPE :

Principe de confinement, ou « il faut toujours pouvoir isoler un membre infecté ». Ceci est particulièrement utile en cas d'attaque par de ver ou virus. A titre d'exemple, l' application de ce principe correspond à la mise en place de « sas de décontamination ». Ce sas peut lui-même constituer un sous-réseau, où une politique de sécurité particulière, moins stricte que celle du réseau interne, est mise en oeuvre, et sur lequel on peut placer des machines dédiées (serveurs Web, antivirus, de messagerie), mais aussi des outils de détection d'intrusion...

R6 – CONTROLE ET INCIDENT (Tracabilité et audit)

OBJECTIFS :

1. S'assurer de la bonne application de la politique SSI de la compagnie,
2. L'audit permettant de vérifier la conformité de la compagnie doit être réalisé par du personnel qualifié,
3. La fréquence de ces audits internes doit être formalisée,
4. La réalisation de cet audit SSI doit pouvoir être tracée par l'intermédiaire d'un rapport,
5. Détection d'un incident SSI,
6. Report de l'incident SSI : enregistrement, traçabilité de l'incident, recueil des preuves,
7. Correction de l'incident : identifier les causes, plan d'action,
8. Retour d'expérience du SSI : analyse, protection, revue de système, partage d'expérience.

DOCUMENT DE REFERENCE : CODE ISM

Le système de gestion de la sécurité du navire permet de cadrer la gestion d'un audit interne SI au regard du Code ISM chapitre 12 *« VÉRIFICATION, EXAMEN ET ÉVALUATION EFFECTUÉS PAR LA COMPAGNIE»* : la procédure audit devrait être complétée afin de disposer d'éléments complémentaires sur la gestion du système d'information de la sécurité du navire

CONTROLE DE L'APPLICATION :

La vérification de l'application par la compagnie et le navire de cette politique s'effectue lors des audits internes siège et navire dans le cadre du code ISM,

SUPPORTS D'AIDE DOCUMENTAIRE OU TECHNIQUE :

1. Solutions techniques : surveillance de port (Détection intrusion réseau IDS),
2. Solutions techniques : programmer correctement les pare-feux. Ils doivent filtrer tout le trafic non autorisé. Il devrait être doté d'un mécanisme de report d'information lors d'un constat anormal. Ces systèmes doivent être testés. Le trafic anormal doit être analysé par le responsable du navire.
3. Application de guide de référence SOC (Security Operation Center),

PRINCIPES :

1. **Vérification régulière de la mise en œuvre de la sécurité, ou « mieux vaut prévenir que guérir ».** L'application de ce principe et la mise en œuvre des mesures de protection qui en résultent seront vérifiées au départ, puis périodiquement, pour éviter des dérives, peut-être non-intentionnelles, mais bien réelles.
2. **Mise en place d'une défense en profondeur, ou « plusieurs lignes de défense valent mieux qu'une ».** Partant du constat que, dans les systèmes complexes, il faut toujours prévoir plusieurs lignes de défense, des mesures de protections bien distinctes, en particulier fonctionnellement, seront appliquées sur différentes composantes, de manière à ce qu'il n'y ait pas une ligne de défense unique.

R7- PROTECTION PHYSIQUE DES SI (Confidentialité)

OBJECTIFS :

1. Protéger en Zone d'Accès Restreinte les systèmes de gestion de navigation du navire,
2. Protéger en Zone d'Accès Restreinte les systèmes de gestion de la plateforme navire : propulsion, production d'énergie,
3. Protéger en Zone d'Accès Restreinte les systèmes de gestion de la cargaison ou de la gestion des passagers du navire,

DOCUMENT DE REFERENCE : CODE ISPS

La gestion de ces accès est précisée au niveau du plan de sûreté du navire et ceci en référence au code ISPS A 9.2 et 9.2.4. La description des mesures de protection de ces accès est confidentielle en référence à l'article A 9.8.1 du code ISPS.

CONTROLE DE L'APPLICATION :

La vérification de la gestion de cette évaluation s'effectue lors de l'approbation du plan de sûreté du navire et lors des audits de certification du navire,

SUPPORTS D'AIDE DOCUMENTAIRE OU TECHNIQUE :

1. **Plan de sûreté du navire** : description, localisation des systèmes d'information, cartographie SSI,
2. Redondance physique des équipements critiques définit au niveau de l'évaluation,

PRINCIPES :

1. **La sécurité physique est un aspect fondamental** de tout type de sécurité pour garantir l'intégrité, la confidentialité et la disponibilité des informations. Si quelqu'un réussit à accéder au système informatique du navire, il peut l'endommager ou même le détruire.
2. La sécurité physique consiste en l'usage de barrières, alarmes, serrures et autres contrôles physiques permettant de conditionner l'accès physique aux locaux, aux ordinateurs et aux équipements. Ces mesures sont nécessaires pour protéger les ordinateurs, leur contenu et les autres ressources matérielles contre l'espionnage, le vol et la destruction accidentelle ou intentionnelle.
3. **Nécessité d'une gestion dynamique du risque.** Le risque doit être géré de façon continue et dynamique dans un monde qui change très vite dans le domaine des technologies de l'information et de la communication. Pour une entité donnée, il faut, à tout moment, être informé des menaces les plus probables et des vulnérabilités publiées et préparer un certain nombre de plans : réactions, de continuité des opérations... applicables en cas d'incident, ou en cas d'attaque. Au-delà de ces plans, il peut s'avérer judicieux de faire appel, pour la gestion des incidents informatiques, à des spécialistes capables de caractériser l'attaque, d'évaluer les dégâts et de prendre des mesures de confinement et de réaction.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ENVIRONNEMENT, DE L'ÉNERGIE ET DE LA MER

Edition septembre 2016 – Révision n°1 de février 2017

DGITM / Direction des Affaires Maritimes