Rencontres Sécurité Numérique – Sécurité Portuaire (#SNSP)

Première édition

5 avril 2018 – Le Havre

COMPTE RENDU

ORGANISÉ EN PARTENARIAT AVEC

AVEC LE SOUTIEN DE

PARTENAIRE MÉDIA




OPENING SESSION

- **Eric BANEL**, *Conseiller pour l'économie maritime et portuaire, Secrétariat général de la mer (SG Mer), Premier ministre*
- **Jean-Baptiste GASTINNE**, *Vice-Président, Communauté d'Agglomération havraise (CODAH) – Vice-Président en charge des Transports, Conseil Régional de Normandie*
- **Eric LEHERICY**, *Directeur Général, Chambre de Commerce et d'Industrie Seine-Estuaire*

Les ports français ont pris conscience des enjeux liés au développement du numérique. Le monde portuaire évolue et les acteurs maritimes et portuaires s'emparent du sujet de la cybersécurité. La digitalisation monte en puissance dans tous les domaines de l'économie et apporte son lot d'opportunités, mais aussi de risques, auxquels le milieu maritime et portuaire cherche à s'adapter. Les Rencontres Sécurité Numérique – Sécurité Portuaire cherchent à anticiper et inscrire l'ensemble des ports français dans une transformation numérique sécurisée.

HAROPA – Port du Havre et l'Union Maritime et Portuaire (UMEP) ont souhaité coorganiser cette 1ère édition nationale des "Rencontres Sécurité Numérique - Sécurité Portuaire" pour aider les professionnels à mettre en commun leurs bonnes pratiques face au risque cyber, et travailler à offrir une vision novatrice et constructive sur la sécurité portuaire et maritime. L'objectif de cet événement, l'un des premiers à être labellisé *SmartPortCity*, est de faire de l'agglomération havraise et de ses acteurs une référence mondiale dans le domaine de la *Trade Facilitation*, en assurant un haut niveau de sécurisation des données.

> « ***Le gouvernement prend en compte au plus haut de l'État la sécurité portuaire et maritime, en incluant les acteurs à la démarche. La cybersécurité était d'ailleurs un sujet très présent durant le CIMer [Comité interministériel de la mer] de novembre*** ».
> **Eric BANEL**, *Conseiller pour l'économie maritime et portuaire, Secrétariat général de la mer (SG Mer), Premier ministre*

Le gouvernement incite les acteurs à intégrer la sécurité numérique nativement dans le processus de numérisation de l'activité des acteurs de la chaîne portuaire. En effet, la mise en conformité d'un outil ou d'un processus n'ayant pas été conçu en intégrant la sécurité numérique dès l'origine (*Security By Design*) est extrêmement coûteuse et complexe. Le développement du numérique se fait et se fera notamment par l'interconnexion croissante de l'ensemble des équipements, la cybersécurité devenant ainsi un questionnement nécessaire dans tout projet numérique. Il est nécessaire de fédérer les initiatives et accompagner les acteurs dans leur prise en compte de la cybersécurité.

La France possède le deuxième domaine maritime au monde et les enjeux relatifs à la cybersécurité sont semblables pour l'ensemble des écosystèmes portuaires, malgré les spécificités propres à chaque port. C'est la raison pour laquelle le gouvernement français raisonne au niveau national comme un seul « territoire portuaire ». Les Rencontres Sécurité Numérique - Sécurité Portuaire s'inscrivent ainsi dans une démarche nationale à travers des dynamiques locales ancrées sur les territoires. La volonté est celle de travailler ensemble et de concert pour porter une voix particulière. C'est dans cette dynamique que l'Etat considère que la réglementation doit accompagner, catalyser et anticiper les risques, pour favoriser le développement d'une culture commune de cybersécurité et faisant de celle-ci un avantage compétitif non-négligeable pour les ports français : agir efficacement ensemble est pour l'Etat un impératif aux niveaux local et national.

> « ***Nous devons travailler à fédérer une filière industrielle en matière de cybersécurité en France*** ».
> **Eric BANEL**, *Conseiller pour l'économie maritime et portuaire, Secrétariat général de la mer (SG Mer), Premier ministre*

TABLE RONDE

L'impact du cadre réglementaire français et européen de la sécurité numérique sur les acteurs portuaires, de la LPM à la directive NIS et au Règlement Général sur la Protection des Données (RGPD)

- Animateur : **Bénédicte PILLIET**, *Directeur, CyberCercle*
- **Jérôme BESANCENOT**, *DSI, Grand Port Maritime du Havre*
- **Tanguy JACOB**, *Chef de service, Service Systèmes d'Information, Grand Port Maritime de Nantes St Nazaire*
- **ICA Thibaut MARREL**, *Coordinateur sectoriel, ANSSI*
- **Thomas de MENTHIERE**, *Maritime & Transportation Development Manager, AIRBUS CyberSecurity*



L'impact économique de la compromission des systèmes informatiques d'un port serait incroyablement lourd, comme l'a montré l'attaque en Petya ayant touchée l'armateur Maersk en 2017, lui coûtant près de 300 millions de dollars. L'information et la donnée font partie intégrante du patrimoine de l'entreprise, et doivent donc être protégées contre les risques cyber. La cybersécurité doit ainsi être un élément de la politique de sécurité globale d'un port, et devenant aujourd'hui un facteur d'attractivité. Ne pas intégrer la cybersécurité dans la politique de sécurité serait aujourd'hui catastrophique pour un acteur portuaire, au regard des risques et des menaces issus du cyberespace et de la numérisation croissante des opérations portuaires.

Les systèmes d'information de l'ensemble de l'écosystème portuaire et maritime étant interconnectés et ouverts sur le monde, les acteurs portuaires doivent développer une véritable politique de sûreté-sécurité intégrant la dimension cybersécurité en accord avec la réglementation française et européenne en matière de sécurité numérique, plus particulièrement la Loi de programmation militaire (LPM), la Directive NIS et le Règlement Général sur la Protection des Données (RGPD).

Certes ce dernier, adopté par l'Union européenne en 2016, est un enjeu de taille et aura un impact conséquent pour les entreprises sur le traitement et la sécurisation des données. Mais s'agissant des ports, dans les faits, le RGPD n'entrainera probablement pas de grands bouleversements, la démarche de protection des données étant déjà engagée par ces derniers. Les enjeux relevant de la responsabilité ou encore les obligations de protection des données et du patrimoine informationnel des ports sont aujourd'hui une nécessité absolue, bien comprise et déjà mise en œuvre par les acteurs portuaires dans leur grande majorité.

Au regard de la taille du domaine maritime français, il est important pour l'Etat de travailler, avec l'ensemble des acteurs portuaires, à l'élaboration et au développement d'une réelle gouvernance, pour être en mesure d'accompagner l'ensemble de la chaîne des acteurs portuaires dans ses démarches de mise en conformité réglementaire, qu'il s'agisse à la fois des ressources et des moyens à mettre en œuvre. L'ANSSI travaille en ce sens, notamment en incitant au partage d'expériences et d'expertises entre Opérateurs d'Importance Vitale (OIV) du secteur portuaire, mais aussi entre OIV et l'Agence. Les acteurs les plus modestes doivent aussi être intégrés dans cette stratégie globale de cybersécurité portuaire, en les accompagnant dans l'élaboration et la mise en œuvre d'une politique de cybersécurité, et créer ainsi une véritable dynamique sectorielle.

MASTER CLASS

SECURITY BY DESIGN ET MILIEU MARITIME

Patrick HOUDU, *DGA Maîtrise de l'Information, ministère des Armées*

La DGA mène des opérations d'armement pour le compte de l'Etat-Major des Armées (EMA). La cybersécurité dans ces opérations d'armement suit un cheminement en plusieurs étapes : des études amonts, l'orientation, l'élaboration, la réalisation et finalement l'utilisation.

En matière de cyberdéfense, le rôle de la DGA est multiple, couvrant la sécurité des systèmes fournis aux forces armées, fournir aux forces des produits et outils de cyberdéfense, être l'expert référent du ministère et soutenir les opérationnels. L'analyse de la menace cyber telle que réalisée par la DGA doit mener à mieux connaître la menace pour mieux protéger les systèmes (aspects techniques, analyses de vulnérabilités, réalisation de preuves de concept…). Le but de toute cette démarche est l'élaboration de spécifications de sécurisation en matière de protection mais aussi de détection.

C'est cette démarche que la DGA a appliqué pour les bâtiments maritimes. Les navires disposent de sous-systèmes informatiques : le système de communication, le système de navigation, le système de combat, le système bureautique, les systèmes plateformes… L'ensemble de ces sous-systèmes comporte des vulnérabilités propres qui doivent être intégrée dans la vision d'ensemble de la sécurisation du navire.

La DGA classe le risque cyber en suivant un processus en trois étapes.
Etablir le niveau de criticité des systèmes porteurs des fonctions du navire.
-Identifier les systèmes en interfaces.
-Identifier des blocs de systèmes et allouer à chaque bloc une classe de cybersécurité.

La DGA utilise une classification élaborée par l'ANSSI pour les évènements redoutés dans le domaine maritime, regroupant les risques en trois classes, risque et impact faible, significatif et critique. 160 évènements redoutés ont été identifiés et analysés.

La Direction a mis en lumière le besoin de capteurs adéquats servant à surveiller l'ensemble des points d'accès d'un navire et surveiller ainsi les flux de données qui entrent dans les systèmes.

MASTER CLASS

MENACES ET DEMARCHE DE SECURISATION DANS LE DOMAINE MARITIME ET PORTUAIRE

Thomas de MENTHIERE, *Maritime & Transportation Development Manager, AIRBUS CyberSecurity*
Vincent SERUCH, *Responsable métier Sécurité des ICS, AIRBUS CyberSecurity*

Les Systèmes industriels des navires sont vulnérables du fait de nombreuses menaces : des systèmes d'exploitation souvent obsolètes, de vieux processeurs industriels sans protection, le manque de sensibilisation et de formation à la cybersécurité, l'absence de politiques de sécurité et de cybersécurité, des réseaux non séparés ou isolés, l'absence de contrôle d'accès aux ordinateurs et aux réseaux, ou encore l'absence de mécanismes de détection d'intrusion.

La méthodologie proposée par Airbus CyberSecurity se décompose en 5 étapes.

Cartographie des solutions

Il s'agit là d'une phase d'étude par une analyse comparative basée sur les critères d'exigences spécifiques à l'environnement industriel de l'acteur. Cette première étape vise à fournir une étude de comparaison avec des solutions éligibles.

Tests de qualification

Dans un environnement industriel virtualisé basé sur le Cyber Range d'Airbus CyberSecurity, des tests de performance avancés de certains IDS/ICS sont effectués pour qualifier la meilleure sonde IDS pour l'entreprise. Ces tests sont exécutés sur les IDS/ICS en incorporant des scénarios malveillants.

Conception de la protection ICS

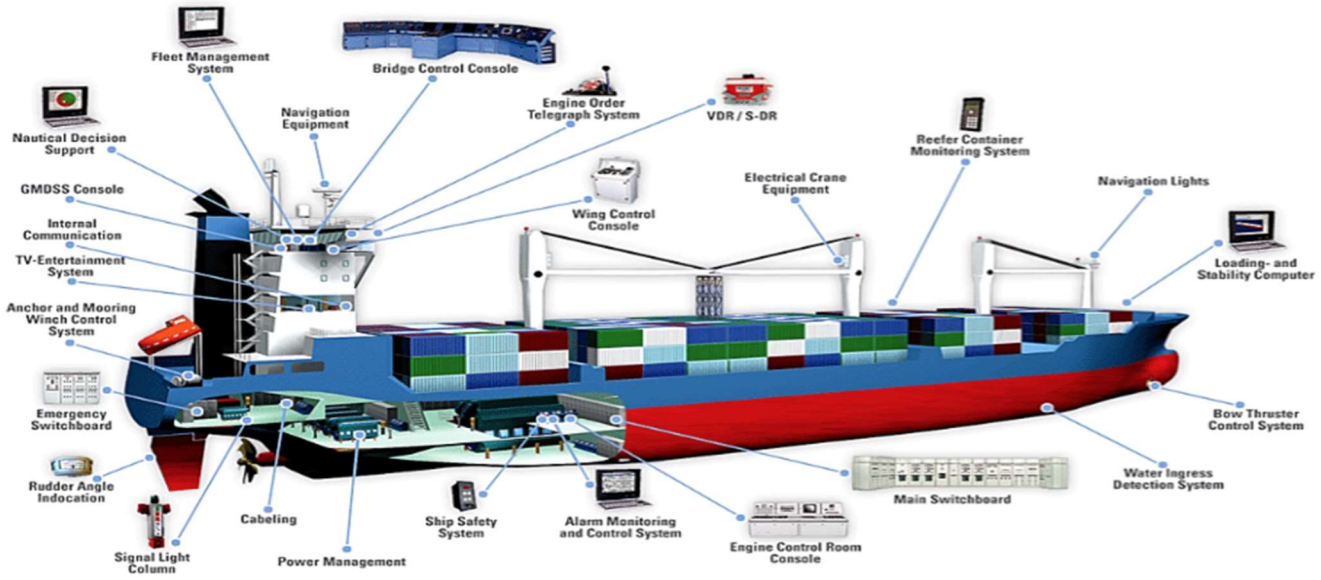
Avec le soutien des architectes ICS et du Cyber Range, une conception de l'architecture ICS de votre environnement industriel sera créée et réalisée à la fin de l'étude de conception. La Cyber Range permet de valider la pertinence et l'efficacité de cette architecture dans l'environnement virtuel, puis de passer à la phase de mise en œuvre.

Cybersécurité de l'ICS

Sur la base de l'étude de conception et des tests de qualification, nos architectes mettent en œuvre l'architecture spécifique pour les ICS de votre environnement. Ceux-ci fournissent également la configuration d'IDS à un journal central d'activité des logs pour préfigurer le logiciel SIEM qui sera une partie centrale du Security Operation Center (SOC) ICS.

SOC ICS – Monitoring IDS

L'étape finale est la construction du SOC ICS. Basé sur l'architecture ICS/IDS et couplé avec la centralisation des logs. Des cas d'utilisation spécifiques à votre entreprise permettront de détecter les menaces susceptibles de nuire à votre activité sur le terrain.



MASTER CLASS

LES SERIOUS GAMES COMME OUTIL DE SENSIBILISATION – FORMATION INTERNE

Thibault RENARD, *Responsable IE, CCI France*

Un Serious Game est un jeu, qui peut être soit vidéo soit de plateau. Mais il n'a pas uniquement une vocation ludique : il a pour objectifs la sensibilisation, la formation, la communication ou encore la découverte d'un produit.

Le monde des Serious Games est très varié. Ces derniers peuvent en effet être dédiés à une personne seule devant son écran pour une durée de quelques minutes, ou encore servir de support pour du Team Building ou du Business Game en simulant, pour une période plus longue, une situation de gestion de crise, ou encore des problématiques de management. Quant à la forme, un Serious Game peut aller d'une simple application a un réel événement.

Dans le domaine de l'Intelligence économique (IE), les Serious Games peuvent être généralistes et porter sur l'ensemble des thématiques propres à l'IE, ou au contraire se concentrer sur l'une des trois facettes de l'IE :

Sur les questions relatives à la sécurité, Info Sentinelle a été primé au niveau européen.

S'agissant de l'influence, France 5 a créé un Serious Game propre à ces questions.

Dans le domaine du traitement de l'information, des jeux plus informels que formels existent, comme Face Me.

Les Serious Games s'adressent à toutes les structures, quelle que soit leur taille. Mais en fonction de la nature et de la forme du jeu, le budget peut se situer entre 1000 et 500 000 euros.

Les grandes thématiques qui relient l'IE au jeu se rapportent à l'espionnage, ce qui justifie une forte présence naturelle des éditeurs de jeux d'espionnage et d'investigation. Nous disposons en France d'une véritable expertise dans le domaine des Serious Games, et nous devons en profiter. Il est stratégique que cette élite du jeu rencontre les praticiens de l'IE et que ces deux milieux travaillent de concert, s'hybrident car ils y gagneront mutuellement. Le marché des Serious Game est en pleine expansion et s'élève aujourd'hui entre 15 et 20 milliards d'euros.

TROIS MESSAGES PRINCIPAUX A RETENIR

- Il est nécessaire de fédérer les initiatives et accompagner les acteurs dans leur prise en compte de la cybersécurité
- La cybersécurité doit être un élément de la politique de sécurité globale d'un port, et un facteur d'attractivité
- Les acteurs les plus modestes doivent être intégrés dans une stratégie globale de cybersécurité portuaire, en les accompagnant dans l'élaboration et la mise en œuvre d'une politique de cybersécurité, et créer une véritable dynamique sectorielle

www.cybercercle.com

twitter @CyberCercle

LinkedIn CyberCercle

facebook CyberCercle

contact@cybercercle.com