Le port du futur sera un port « smart » et cyber sécurisé !

Jérôme BESANCENOT
Chef du Service du développement des Systèmes d'Information
HAROPA Port du Havre

Le secteur portuaire : une dépendance au numérique, une interdépendance face au risque cyber

Face à la massification du transport maritime, un facteur clé de la compétitivité des ports repose désormais sur la capacité de leurs systèmes d'information à automatiser et traiter de volumineux flux d'information liés aux marchandises, aux passagers et aux navires.

Ces traitements sont opérés au travers du système d'information portuaire communautaire appelé communément « Port Community System » (PCS) et reposent sur des échanges dématérialisés de données en EDI de type BtoB interconnectant l'ensemble des parties prenantes de la communauté portuaire. Le volume échangé représente plusieurs centaines de millions de transactions par an pour le port du Havre.

La communauté du port rassemble de nombreux professionnels des secteurs portuaires, maritimes et aussi industriels ; de par sa nature, elle se caractérise par une grande disparité de sensibilisation et de culture face au risque cyber. Chaque acteur intervient de manière synchronisée dans la chaîne d'approvisionnement logistique : l'ensemble des opérations est coordonné par le biais du PCS. Ceci induit de fortes interdépendances entre les professionnels, en matière de règle d'hygiène cyber ; il s'avère fondamental de partager les bonnes pratiques numériques pour sécuriser l'ensemble de l'écosystème.

Cette dépendance de l'activité portuaire au monde numérique s'est considérablement accrue ces dernières années, du fait de l'automatisation qui est devenue une nécessité économique et un enjeu de performance. Le recours aux nouvelles technologies permettant de réduire les coûts, de fiabiliser le suivi des opérations portuaires et de mieux anticiper les interventions des acteurs de la logistique.

À ce titre, le concept du « SmartPort », présente un port « hyper-connecté » s'appuyant sur les technologies de l'internet des objets (IoT), sur le bigdata et sur l'intelligence artificielle (IA) qui laisse augurer une plus grande agilité due au pilotage de l'activité par la donnée numérique. Dans le même temps, l'augmentation de la surface d'exposition aux cybermenaces et du risque de leur propagation est le revers de la médaille.

Il devient donc nécessaire de s'extraire d'un fonctionnement qui reposerait uniquement sur une analyse en silo des risques de cybermalveillance, en combinant les analyses et en partageant davantage au niveau de la communauté portuaire une même stratégie globale de résilience de l'écosystème. Dans cet objectif, il convient de mettre en œuvre une véritable synergie de place afin d'amener l'ensemble

des acteurs à se pencher conjointement sur ce sujet sensible, trop souvent considéré comme une affaire de spécialistes en informatique et rarement appréhendé sous sa dimension organisationnelle.

Force est de constater que le secteur portuaire n'est plus épargné par les cyberattaques et certaines d'entre elles ont récemment eu de lourdes conséquences pour plusieurs ports mondiaux majeurs, notamment sur le plan financier et la continuité d'activité.

Le Programme « SmartPortCity » de HAROPA Port du Havre : un projet innovant en matière de cybersécurité portuaire

Pour faire évoluer les lignes favorablement et pour se mobiliser de manière proactive sur ce sujet complexe, HAROPA Port du Havre a initié, au sein du programme « SmartPortCity », lauréat du TIGA-PIA3 (Territoires d'Innovation Grande Ambition - Plan d'Investissement d'Avenir), un projet d'innovation en matière de cybersécurité portuaire, maritime et industrielle avec l'ensemble des parties prenantes du territoire havrais dont la communauté Urbaine Le Havre Seine Métropole, la communauté des professionnels portuaires de l'UMEP (Union Maritime et Portuaire), les industriels de l'association Synerzip et la SOGET leader mondial de solution PCS et éditeur de la plate-forme collaborative digitale S)One.

Le port du Havre est le premier port à conteneurs pour le commerce extérieur de la France et aussi le 1er port touché sur le range nord-européen. Il offre les meilleurs temps de transit entre l'Europe et le reste du monde et se positionne comme un corridor européen majeur. Localisé à l'embouchure de la Seine, il est relié directement aux ports de Rouen et Paris par route, fleuve et rail. Ces trois ports sont désormais regroupés sous HAROPA, portant une ambitieuse stratégie de développement et d'innovants services digitaux à l'échelle territoriale de l'axe seine. Dans ce contexte, la sûreté est une orientation clé pour HAROPA – Port du Havre qui est la première autorité portuaire européenne à avoir obtenu la certification ISO 28000 au titre de la sûreté de la chaine d'approvisionnement.

Le projet de plateforme de cybersécurité portuaire, maritime et industrielle vise à poursuivre cette stratégie de renforcement du port dans une dimension de compétitivité et d'attractivité, tout en assurant une amélioration du niveau général en matière de cybersécurité avec un enjeu double.

Le premier enjeu consiste à bâtir une démarche qui apportera de la visibilité aux clients du port sur le dispositif déployé de résilience de l'écosystème aux cybermenaces. Comme un service à valeur ajoutée au bénéfice de ses clients, le port améliorera sa compétitivité justement du fait de la prise en compte de la dimension cyber dans sa stratégie de développement. Cet enjeu est caractérisé par une image forte de construction « **du Havre : port Cyber-sûr** ». Il ne s'agit pas seulement d'identifier ce que le port pourrait « perdre » en cas de non-conformité cyber, mais plutôt de souligner ce qu'il gagne et la façon dont cet argumentaire devient un élément de décision susceptible d'apporter des trafics et de l'activité au port du Havre.

Le deuxième enjeu est d'aller au-delà de la stratégie de résilience en développant une culture d'innovation sur la cybersécurité portuaire, maritime et industrielle. Cela consiste à élargir les compétences des acteurs et à attirer de nouveaux talents sur le territoire dans cette discipline. Il s'agira essentiellement d'impliquer les acteurs pour créer une valeur ajoutée de type filière sur la promotion des métiers de la cybersécurité et favoriser ainsi la mise en œuvre de partenariats public-privé (PPP) dans ce domaine. L'idée est de susciter auprès de différents acteurs du monde numérique et de la recherche en cybersécurité, une meilleure prise en compte de la « Security by design » dans le développement informatique des solutions portuaires, dans la certification des installations technologiques, ou encore un meilleur niveau de formation initiale et continue. Cet enjeu vise à améliorer l'attractivité du territoire et à contribuer à fixer un savoir-faire local en

faisant « **du Havre le lieu d'amélioration de la cybersécurité** » de ses entreprises.

La cybersécurité, un facteur de compétitivité pour HAROPA Port du Havre et pour l'écosystème portuaire français

Le calendrier du projet a été défini pour établir en première priorité la gouvernance cyber de la plateforme en déclinant de manière opérationnelle des mesures pragmatiques, adaptées aux besoins du port et répondant à une gestion raisonnée des vulnérabilités : le piège d'une potentielle distorsion de concurrence avec d'autres ports devra être écarté, en s'assurant en permanence que les mesures adoptées ne soient pas disproportionnées ou trop difficiles à porter. Chaque entreprise, quelle que soit sa structure ou son organisation, deviendra alors un acteur essentiel de cette gouvernance et participera à son animation. Dans cette perspective, les évènements organisés depuis 2018 au Havre, en partenariat avec le CyberCercle, en faveur de la sûreté portuaire et la sécurité numérique, ont permis avec succès de sensibiliser l'ensemble des acteurs de la place portuaire sur des thématiques de réglementation, de sensibilisation, de gouvernance ainsi que d'innovation.

En parallèle, un échéancier pour les trois ans à venir, sur la base de cette gouvernance, va établir une feuille de route de création d'un portefeuille de services mutualisés d'assistance aux entreprises comprenant de la sensibilisation, de la formation, de l'analyse et des audits de risque, de la gestion de crise, de la recherche et innovation, un SOC portuaire (Security Operation Center) et une place de marché pour faciliter l'accès aux offres techniques de sociétés cyber-spécialisées reconnues.

La clé du succès du projet repose ainsi principalement sur la capacité collective à valoriser véritablement cette initiative sous l'angle du progrès, en dépassant le stade simpliste où elle ne serait perçue que selon son principe d'obligation réglementaire. La cybersécurité peut alors être appréhendée comme une opportunité permettant au port d'améliorer sa compétitivité en combinant l'accélération de la transformation digitale et sa sécurisation numérique. Elle devient alors un critère positif, et donc, un argument commercial garantissant la « compliance » de l'écosystème portuaire havrais. Cette « compliance » va pouvoir se valoriser auprès des entreprises de la place, en termes d'attractivité auprès des clients du port, permettre potentiellement de conquérir des parts de marché ou plus pragmatiquement par exemple, de réduire les primes d'assurances des entreprises du territoire.

Ce projet ambitieux revêt aussi une dimension d'intérêt général, car il est essentiel que le modèle défini et mis en place puisse être dupliqué sur d'autres territoires au niveau national comme à l'international. Il devra notamment pouvoir s'adapter aux différents contextes, en se déclinant aux besoins des ports plus petits où les moyens d'action font face à des contraintes fortes de moyens. Il s'inscrira aussi dans la politique nationale et européenne en matière de cybersécurité maritime en étroite collaboration avec le Secrétariat Général de la Mer (SGMer) où l'interopérabilité de la plateforme de cybersécurité portuaire, maritime et industrielle avec le futur M-CERT (Maritime - Computer Emergency Response Team) national est un enjeu clé du dispositif.

En résumé, HAROPA Port du Havre au travers d'une inédite démarche d'innovation s'engage sur un processus de progrès pour renforcer sa politique en matière de cybersécurité portuaire, maritime et industrielle, faisant de cette discipline un vecteur essentiel du développement de l'activité du port et de sa résilience. Cette initiative permettra aussi à l'État d'affermir sa souveraineté nationale en intégrant le « Port Cyber sécurisé » dans son dispositif global de cybersécurité maritime, contribuant ainsi à sécuriser le commerce international sur le moyen et long terme.