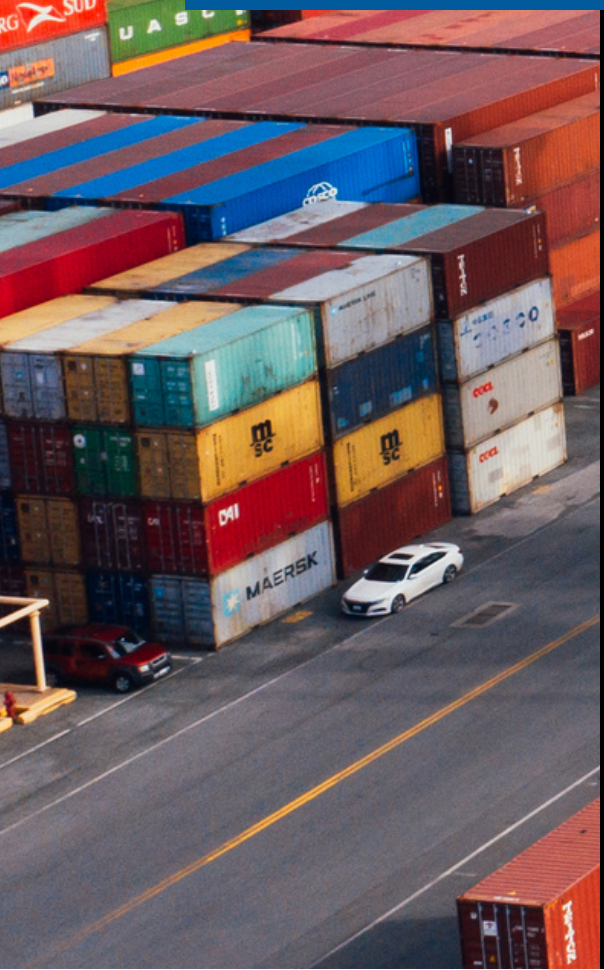
2023

CYBER GUIDE DES PLACES INDUSTRIALO-PORTUAIRES DE L'AXE SEINE

SEINEPORT UNION
PARIS – ROUEN – LE HAVRE

HAROPA PORT
Le Havre
Rouen
Paris



EN COLLABORATION AVEC :

SOGET
Fluidity for your business

easyport

VERSION 1.0 - JUILLET 2023

EDITO

Les récentes crises internationales ont illustré l'enjeu stratégique, pour la nation, d'assurer grâce à nos ports, la permanence de nos chaînes d'approvisionnement en marchandises, en matières premières et en énergie.

La cybersécurité portuaire est devenue au fil du temps une préoccupation majeure pour l'ensemble des organisations internationales, afin de préserver la continuité du commerce maritime. En particulier, il s'agit de garantir celle de la chaîne d'approvisionnement logistique, dans un contexte où les activités des ports dépendent toujours davantage du numérique et où les systèmes d'information des entreprises portuaires sont largement interconnectés pour échanger au quotidien d'importants volumes de données électroniques.

Les cyberattaques contre les ports se sont abondamment multipliées ces dernières années et ont entrainé des conséquences souvent très impactantes et coûteuses pour le secteur. Elles peuvent générer des dégâts immatériels en perturbant le fonctionnement des systèmes numériques comme l'informatique d'entreprise ou l'informatique industrielle, mais peuvent conduire à des dégâts matériels dans les entreprises voire potentiellement affecter l'intégrité physique des personnels qui y travaillent.

Face à la gravité de la menace, les acteurs portuaires s'accordent désormais pour intégrer le risque cyber avec une vision globale des processus d'activités ainsi que de leur criticité au sein de la communauté. Les dirigeants d'entreprises, d'opérateurs et d'autorités portuaires sont amenés à définir une stratégie de cybersécurité pour maintenir en condition opérationnelle leurs propres systèmes d'information en considérant également les sous-traitances potentielles.

En travaillant aussi collectivement au niveau de nos places portuaires, il devient possible de renforcer plus efficacement la cybersécurité de bout en bout, sur l'ensemble des échanges d'informations qui transitent dans nos différents systèmes d'information et procurer une défense harmonisée face aux cybermenaces, au bénéfice de la confiance que nous accordent nos clients et partenaires.

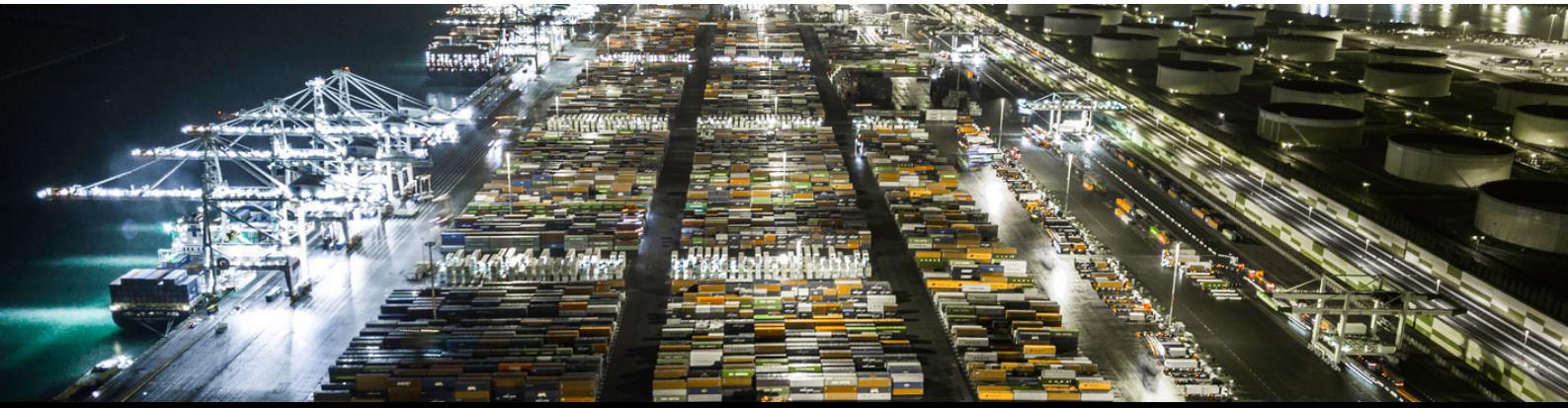
Une étape essentielle pour améliorer le renforcement de notre cybersécurité est la sensibilisation de l'ensemble des acteurs à la cybermenace et à l'importance d'adopter communément certaines bonnes pratiques élémentaires pour réduire considérablement le risque.

Préparé à l'initiative conjointe de HAROPA PORT et de Seine Port Union, ce présent guide sur la cybersécurité des places industrialo-portuaires de l'Axe Seine vise à accompagner cette démarche de sensibilisation collective auprès de l'ensemble des acteurs professionnels. Il est également une porte d'entrée pour appréhender d'autres manuels de référence plus détaillés et approfondis, utiles pour renforcer notre action en matière de cybersécurité portuaire.
Ce guide a vocation à constituer avant tout un outil simple et pratique commun pour lutter contre ce risque majeur et nous aider à le réduire efficacement, il sera amené à être régulièrement réactualisé en fonction de nos besoins et de l'évolution des cybermenaces.

Nous vous en souhaitons une bonne lecture et restons à l'écoute de vos suggestions pour en améliorer le contenu au fil du temps.

Stéphane RAISON
Président du Directoire
HAROPA PORT

Hervé BONIS
Président
SEINE PORT UNION



SOMMAIRE

INTRODUCTION

Le transport maritime est une activité essentielle pour l'économie de la France. La cybersécurité des ports est donc un enjeu crucial pour la sécurité nationale et la continuité des activités économiques.

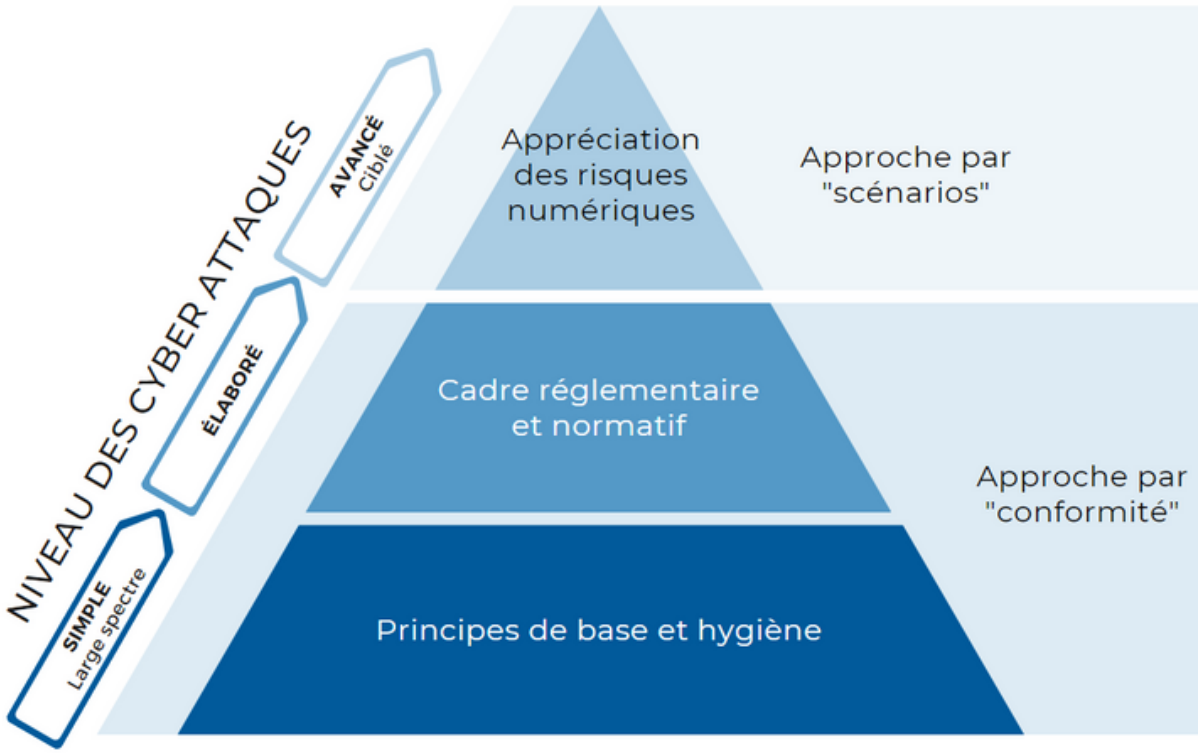
La tendance mondiale à la numérisation et les politiques et réglementations récentes obligent les ports maritimes à relever de nouveaux défis en matière de technologies de l'information et de la communication. Ils s’appuient en effet de plus en plus sur les technologies pour gagner en compétitivité, se conformer à certaines normes et politiques publiques et améliorer leur fonctionnement.

Les ports de l'axe Seine sont des points de passage obligatoires pour de nombreux navires, marchandises et personnes, et leur sécurité informatique est donc primordiale.

Ce guide cyber vise à aider les responsables de la sécurité des ports de l'axe Seine et de leurs partenaires à comprendre les menaces informatiques auxquelles ils sont exposés, ainsi qu'à adopter les mesures nécessaires pour protéger leurs systèmes et leurs données sensibles.

CONTEXTE ET ENJEUX CYBER

La cybersécurité des places portuaires est un enjeu crucial dans le monde maritime. Avec l'augmentation de la numérisation des opérations portuaires, de nouveaux risques ont émergé, tels que les cyberattaques, les fuites de données et les perturbations informatiques. Les places portuaires jouent un rôle vital dans le commerce international et toute perturbation de leurs activités peut avoir des conséquences importantes pour l'économie.



De plus, les places portuaires sont soumises à des réglementations strictes en matière de sécurité et de protection des données (exemple : la directive NIS), ce qui renforce l'importance de la cybersécurité. Elles doivent donc être en mesure de garantir la sécurité de leurs systèmes informatiques.

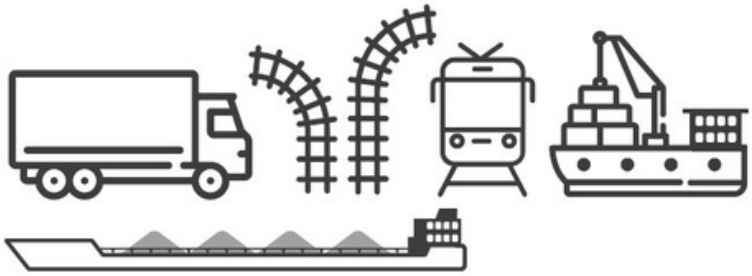
En outre, la complexité de l'écosystème portuaire, du fait du nombre et de la diversité des acteurs impliqués peut poser des défis supplémentaires en matière de cybersécurité ; cet écosystème étant composé d'entreprises de tailles différentes ayant ainsi une maturité et des capacités en cybersécurité variables. Il est donc crucial que les places portuaires soient en mesure de garantir la sécurité de leurs partenariats et de leurs opérations avec l'ensemble des acteurs.

LES PLACES INDUSTRIALO-PORTUAIRES

Comprendre et lutter contre les risques qui pèsent sur les activités maritimes et portuaires.

DE MULTIPLES SOURCES DE RISQUES

Lorsque la marchandise arrive à un port, elle traverse un certain nombre de points de contrôle et de systèmes informatiques, ce qui peut entraîner une série de risques pour la sécurité des données et des équipements. Tout au long de son parcours, la marchandise peut être vulnérable aux cyberattaques telles que les rançongiciels, les interceptions de données et les perturbations du système.



Erreurs humaines

Les ports sont confrontés à des risques liés aux erreurs humaines, telles que les erreurs dans les processus de traitement des données, les mauvaises configurations de sécurité et les faiblesses dans les protocoles de sécurité. Les ports doivent être en mesure de s'assurer que les employés disposent des connaissances et des compétences nécessaires pour garantir la sécurité des données et des équipements.

Partenaires

Les ports peuvent être vulnérables aux risques liés à leurs partenaires, tels que les transporteurs, les prestataires de services logistiques et les fournisseurs de services informatiques. Les ports doivent être en mesure de garantir que leurs partenaires disposent d'une sécurité adéquate pour protéger les données sensibles.

Données et équipements

Les infrastructures portuaires peuvent être une source de risques pour la sécurité des données et des équipements. Les ports doivent être en mesure de protéger leurs systèmes informatiques, tels que les systèmes de contrôle de la sécurité, les systèmes de communication et les systèmes de gestion de l'énergie, pour minimiser les perturbations et les interruptions de service.

En conclusion, lorsque la marchandise arrive à un port, elle peut être confrontée à une variété de risques pour la sécurité des données et des équipements, tels que les cyberattaques, les erreurs humaines et les vulnérabilités dans les systèmes informatiques. Les ports doivent adopter une approche proactive pour garantir la sécurité de leurs activités critiques et protéger les données sensibles.

LES 10 QUESTIONS À SE POSER

La cybersécurité est complexe et peut sembler difficile à appréhender. Voici dix questions indispensables pour nourrir votre réflexion.

01 Qui est mon RSSI ?

Le Responsable de la Sécurité des Systèmes d'Information doit être un intervenant régulier dans la vie de l'entreprise.

02 Quand ai-je entendu parler de cybersécurité pour la dernière fois ?

Se tenir informé régulièrement est essentiel pour avoir une approche pertinente et optimisée, ainsi que pour monter en compétences.

03 Quand faut-il parler de cybersécurité en interne ?

La sensibilisation des équipes est une étape essentielle pour gérer le risque humain. Les communications sur les bonnes pratiques adopter doivent être régulières.

04 Quelle est l'intensité de la menace qui pèse sur ma place portuaire ?

Les places portuaires sont des cibles attractives. À quel volume et fréquence d'attaque s'attendre ? Une attaque majeure a-t-elle déjà été repoussée ou déjouée ?

05 Quel est mon niveau de risque à titre personnel ?

Tout le monde est un facteur de risque potentiel, qui s'élève avec le niveau de responsabilité. Ai-je adopté les bonnes pratiques adéquates?

06 Quelles sont mes principales craintes ?

Se concentrer sur les cinq risques les plus importants aidera à établir et mener une stratégie cohérente.

07 Qui sont mes interlocuteurs ?

Est-ce que je sais à qui m'adresser selon les circonstances ? Est-il possible de contacter cette (ces) personne(s) aisément ? Peu(ven)t-elle(s) répondre suffisamment rapidement ?

08 De quand date le dernier audit ?

En réalisant des audits et des tests d'intrusion, on détecte les failles critiques et les vulnérabilités. Ils doivent être réguliers pour tenir compte de l'évolution des menaces.

09 Existe-t-il un plan en cas de crise ?

Les bonnes pratiques diminuent les risques, mais en cas de crise, de nouveaux comportements sont nécessaires. Toute l'entreprise doit être entraînée à réagir correctement.

10 Quels sont les risques juridiques ?

Jusqu'à quel point et comment les places portuaires sont-elles exposées ?

LES RISQUES HUMAINS

Les risques humains sont une source importante de vulnérabilité pour la sécurité des ports. Les menaces peuvent venir de l'intérieur, telles que les erreurs de personnel, la divulgation volontaire d'informations sensibles, la perte ou le vol d'équipement, ou encore les actions malveillantes telles que le piratage informatique. Il est possible de limiter les risques grâce à des solutions techniques, comme le blocage d'accès à certains sites web, l'utilisation de logiciels de gestion de flotte mobiles, le cloisonnement et la vérification des droits d'accès aux documents sensibles.

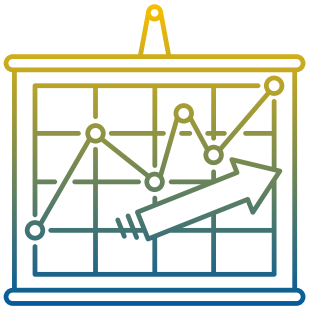
Il est également important de prendre en compte les menaces extérieures telles que les attaques de phishing, les actes de terrorisme, les actions de protestation, les actes de sabotage et les actions criminelles. Les employés doivent être formés à la sécurité des données et aux meilleures pratiques pour éviter les erreurs et les compromissions.

Il est donc crucial de mettre en place des stratégies de sensibilisation et de formation pour les employés afin de minimiser les risques liés aux actions humaines. De plus, il est important de développer des politiques de gestion des incidents pour gérer rapidement et efficacement toutes les situations potentiellement néfastes. La mise en place de systèmes de surveillance et de contrôle pour surveiller les activités suspectes peut également aider à protéger les systèmes et les informations critiques.

LES RISQUES LIÉS AUX INFRASTRUCTURES

Les risques liés aux infrastructures sont une préoccupation majeure pour la sécurité des ports. En effet, les ports présentent la complexité de devoir protéger à la fois leurs infrastructures informatiques (réseau, ordinateurs, serveurs, systèmes de surveillance, ...) et leurs infrastructures industrielles et maritimes (bâtiments, terminaux, zones de stockage, quais, écluses, grues, ...).

Les attaques telles que les défaillances matérielles, les pannes de courant, les incendies, les explosions et les inondations peuvent endommager ou détruire les infrastructures critiques. De plus, les systèmes de contrôle peuvent être compromis par les menaces telles que les virus informatiques, les logiciels malveillants et les attaques par déni de service.



Il est donc important de développer des stratégies et des barrières physiques et virtuelles pour gérer ces risques en minimisant les dommages potentiels. Cela peut inclure la mise en place de systèmes de sauvegarde de données pour protéger les informations critiques, la mise en place de systèmes de surveillance pour surveiller les activités potentiellement néfastes, et la mise en place de stratégies de continuité des activités pour garantir la continuité des opérations en cas de perturbation.

Il est également important de surveiller et de mettre à jour régulièrement les systèmes et les infrastructures pour éviter les vulnérabilités potentielles. Enfin, il est crucial de collaborer avec les fournisseurs et les partenaires pour garantir que les systèmes et les infrastructures utilisés sont sécurisés et conformes aux normes de sécurité en vigueur.

LES RISQUES LIÉS AUX PARTENAIRES

Le milieu portuaire est complexe avec une variabilité marquée en matière de maturité en cybersécurité parmi les nombreuses parties prenantes. Les interactions numériques et les dépendances mutuelles sont nombreuses, mais la réalisation de la mission du port dépend de la collaboration de toutes les parties prenantes (armateurs, compagnies de transport maritime, fournisseurs, ...).

Un consultant ayant accès aux SI devra connaître les pratiques internes de de l'entreprise, alors qu'un agent de sûreté pourra se contenter d'une formation plus générale

Autant d'acteurs qui, dans le cadre de leur relation avec la place portuaire, disposent d'un accès direct ou indirect à certains équipements ou données et peuvent donc être source de menaces. Il est donc essentiel de promouvoir une meilleure prise en compte des risques cyber dans les relations en intégrant de manière systématique des clauses cyber dans les contrats encadrant l'utilisation des systèmes et données. Ces clauses permettraient d'imposer le respect des bonnes pratiques définies par l'autorité portuaire et définiraient les responsabilités en cas de d'attaque.

La formation en matière de cybersécurité peut également être imposée contractuellement et adaptée en fonction du niveau de risque. En effet, demander une certification ou un label peut garantir que le partenaire dispose des compétences nécessaires pour respecter la politique de cybersécurité.

Il est important de porter une attention particulière aux fournisseurs de services Cloud, car ils peuvent être liés aux systèmes critiques de l'entreprise et présenter le même risque, sans que l'entreprise ait le contrôle sur les mesures de sécurité. L'utilisation de ces services doit donc être approuvée par les différentes parties concernées et encadrée par des contrats formels

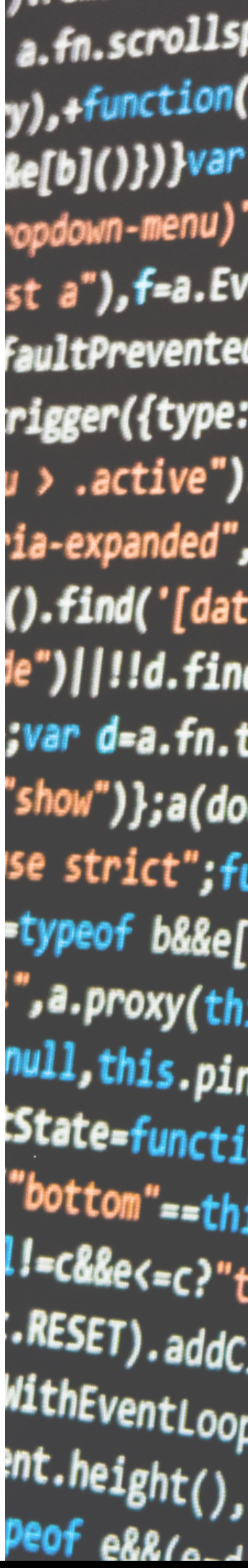
LES RISQUES LIÉS AUX DONNÉES

Pour protéger les informations sensibles qui circulent dans les ports, tels que les déclarations obligatoires, les autorisations accordées par les autorités, les données opérationnelles portuaires, les données financières ou les données de navigations, une politique de gestion doit être mise en place. Elle doit être supervisée par un ou plusieurs responsables qui classent et restreignent l'accès aux données. Les contrôles doivent être régulièrement mis à jour, et un plan d'action doit être établi pour faire face à des incidents tels que des attaques ou des fuites de données.

4 % OU 20 MILLIONS D'EUROS

Le RGPD impose de nouvelles règles pour le traitement des données personnelles, avec des sanctions financières sévères en cas de non-conformité (jusqu'à 4% du CA mondial ou 20 millions d'euros). Les clients et les employés disposent désormais de droits renforcés en matière d'accès, de modification, de portabilité et d'effacement de leurs données. La responsabilité de la conformité incombe au DPD, une nouvelle fonction dans l'entreprise.

La mise en conformité affecte principalement les processus, mais peut nécessiter une analyse pour les adapter. Parfois, cela peut être aussi simple que de mettre à jour les formulaires de contact sur le site web, ou nécessiter le changement de solution et la formation des utilisateurs.
Le RGPD établit également une répartition des responsabilités entre les différents acteurs d'une place portuaire ce qui impose une adaptation des contrats pour garantir leur conformité au règlement.



LES BONNES PRATIQUES

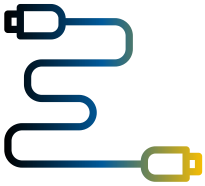
Tout le monde, dans l'entreprise, doit adopter les bonnes pratiques menant à une maîtrise des risques des places portuaires jusqu'à ce qu'elles deviennent instinctives.

Bien définir et utiliser ses mots de passe. Ne pas utiliser de compte partagé et privilégier un identifiant unique type adresse mail.

Effectuer des sauvegardes régulièrement

Faire les mises à jour de ses terminaux personnels

Protéger sa connexion lors de l'utilisation du WiFi public, et ne pas consulter de documents confidentiels



Eviter les transferts de données professionnelles vers les comptes personnels

Ne pas utiliser de support mémoire externe (CD, clé USB...) sans en connaître la provenance

Ne pas cliquer sur une pièce jointe ou un lien sans en connaître l'expéditeur

Éteindre ses équipements le soir

En cas d'attaque ou d'alerte, se déconnecter du réseau

Surveiller régulièrement ses comptes sociaux personnels pour réagir en cas de publication d'informations sensibles

ADAPTER SON ORGANISATION

Responsable de la Sécurité des Systèmes d'Information

Pour garantir la mise en œuvre d'une stratégie de cybersécurité, un responsable de la sécurité des systèmes d'information (RSSI) est nécessaire. Ce RSSI n'a pas de place prédéterminée dans l'organisation, mais sa position doit être optimisée pour son efficacité. En raison de la nature transversale des risques, le RSSI doit pouvoir agir dans tous les métiers du port et disposer de relais, le cas échéant. Pour accélérer les prises de décision, le niveau hiérarchique du RSSI doit rester proche de celui des instances dirigeantes.

Le mandat du RSSI doit être clairement défini, incluant les responsabilités juridiques et opérationnelles, les délégations de pouvoir, etc. Le RSSI peut arbitrer des choix stratégiques, techniques et organisationnels dans le cadre d'une gouvernance impliquant les directions métiers.

Directeur de la Protection des Données

Le directeur de la protection des données (DPD) doit disposer de moyens matériels et organisationnels, de ressources et d'un positionnement lui permettant d'exercer ses fonctions. Une bonne pratique consiste à séparer les fonctions de DPD et de RSSI, avec le DPD s'occupant de la conformité et le RSSI de la cybersécurité. Cependant, selon l'organisation de l'entreprise, les deux fonctions peuvent être gérées par la même personne.

QUEL BUDGET POUR SA CYBERSÉCURITÉ ?

3 À 10 %

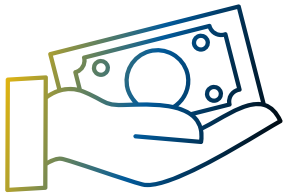
Selon l'ANSSI, entre 3% et 10% du budget informatique devraient être alloués à la cybersécurité selon la taille des entreprises - une entreprise de taille moyenne n'ayant pas les mêmes besoins qu'une multinationale.

3 DOMAINES

Ces fond doivent être répartis en trois domaines principaux :

- La cyberdéfense (protection, détection et réaction) ;
- La communication (formation et sensibilisation) ;
- Les processus de gouvernance.

2 À 5 %



En outre, d'autres dispositifs doivent être intégrés dans les autres budgets d'une entreprise, notamment le maintien en condition de sécurité des moyens techniques et l'évolution des moyens techniques et des processus. De plus, chaque projet devrait intégrer des actions en matière de cybersécurité, ce qui nécessite d'augmenter leur budget de 2 à 5%.

Il est important de rappeler que la cybersécurité est un investissement rentable, car elle permet d'éviter les pertes potentielles causées par une cyberattaque. De plus, elle contribue à la création de valeur de l'entreprise en instaurant la confiance auprès des clients et des partenaires.

EXEMPLES D'INDICATEURS

Domaine	Indicateurs clés	Objectifs
RH	• Nombre de formations en cybersécurité dispensées aux employés • Nombre d'opérations de sensibilisation menées	Mesurer le niveau de maturité des employés sur les sujets liés à la sécurité informatique et aux bonnes pratiques
Opérationnel	• Nombre de tentatives d'intrusion détectées et bloquées • Nombre de mises à jour de sécurité effectuées • Taux de détection de malware • Nombre de rapports d'incidents de sécurité	Mesurer la résilience face aux cybermenaces de l'organisation et évaluer ses capacités à résoudre les problèmes
Stratégie	• Temps de réponse en cas de crise de sécurité • Taux de conformité aux politiques de sécurité établies • Nombre de partenariats avec des fournisseurs de service de sécurité	Mesurer l'adéquation entre la stratégie mise en place par l'organisation en matière de sécurité informatique et le niveau de risque sectoriel

Il est important de noter que ces indicateurs peuvent varier en fonction de la taille et de la complexité de votre activité, et que certains peuvent être plus pertinents que d'autres pour votre organisation en particulier

En surveillant ces indicateurs, vous pouvez mesurer l'efficacité de vos efforts en matière de cybersécurité et prendre des mesures pour améliorer votre sécurité informatique. Cela peut également vous aider à évaluer les risques et à prendre des décisions éclairées pour protéger vos données et vos systèmes contre les menaces. Enfin, en surveillant ces indicateurs de manière régulière, vous pouvez établir une tendance sur votre sécurité informatique et prendre des mesures pour anticiper les futures menaces.

SE PROTÉGER SUR LE LONG TERME

La cybersécurité est un processus en constante évolution qui nécessite une attention constante. Il n'y a pas de fin à la tâche de sécurité des systèmes informatiques, il est donc important d'être toujours prêt à s'adapter aux nouvelles menaces et de sensibiliser les employés aux risques. La cybersécurité est une responsabilité partagée pour tous les utilisateurs et doit être abordée régulièrement à tous les niveaux d'une entreprise, du conseil d'administration aux employés.

Dans le cadre d'une stratégie de cybersécurité globale, il est crucial d'adopter une stratégie de sécurité informatique solide incluant des pare-feu, des systèmes de détection d'intrusion et du chiffrement des données sensibles. Des audits de sécurité réguliers peuvent identifier les faiblesses potentielles, et des protocoles clairs de réponse à une intrusion doivent être établis pour gérer les incidents de sécurité informatique. Par ailleurs, la création de tableaux de bord clairs et informatifs qui prennent en compte tous les facteurs est cruciale.

Les compétences de tous les employés de l'entreprise doivent également être évaluées et mises à jour fréquemment, tout comme les bonnes pratiques, grâce à un ensemble adéquat de formations et d'outils de communication.

En somme, protéger une place portuaire implique une approche combinant mesures techniques, formation et processus solides.

INFORMATIONS PRATIQUES

Bibliographie, lexique et contacts.

BIBLIOGRAPHIE

Cybersecurity Guidelines for Ports and Port Facilities
IAPH

Port Community Cyber Security
IAPH

Good Practices For The Maritime Security
ENISA

Cyber Risk Management For Ports
ENISA

Guide Ports Cybersécurisés
DGITM

EBIOS Risk Manager
ANSSI

Rapport d'analyse de risques cyber des secteurs maritimes et portuaires
Secrétariat général de la mer et Bessé

LEXIQUE

- DIRECTIVE NIS : adoptée le 6 juillet 2016, définissait un régime européen de cybersécurité en mettant l'accent sur la mise en place d'un niveau de sécurité élevé commun aux Etats Membres.

- FAILLE : vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.

- INCIDENT DE SECURITE : un incident de sécurité est un événement qui porte atteinte à la disponibilité, la confidentialité ou l'intégrité d'un bien. Exemples : utilisation illégale d'un mot de passe, vol d'équipements informatiques, intrusion dans un fichier ou une application, etc.

- PHISHING : vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime.

- RANÇONGICIEL (RANSOMWARE) : le terme « rançongiciel » est une contraction des mots « rançon » et « logiciel ». Il s'agit d'un programme malfaisant dont le but est d'obtenir de la victime le paiement d'une rançon.

- TEST D'INTRUSION : action qui consiste à essayer plusieurs codes d'exploitation sur un système d'information, afin de déterminer ceux qui donnent des résultats positifs.

- VULNÉRABILITÉ : faiblesse technique d'un système informatique présente dans la spécification, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser.

- VIRUS : programme ou morceau de programme malveillant dont le but est de survivre sur un système informatique (ordinateur, serveur, appareil mobile, etc.) et d'en atteindre ou d'en parasiter les ressources.

CONTACTS

HAROPA PORT

www.haropaport.com

SeinePort Union

Fédération des communautés portuaires de l'Axe Seine

www.seineport-union.fr

CPP

Communauté Portuaire de Paris

www.cpp.paris

CP-SA

Communauté Portuaire Seine Aval

www.cp-sa.fr

UMEP

Union Maritime Et Portuaire

www.umep.org

UPR

Union Portuaire Rouennaise

www.uprouen.org

Easyport

www.easyport.fr

SOGET

www.soget.fr