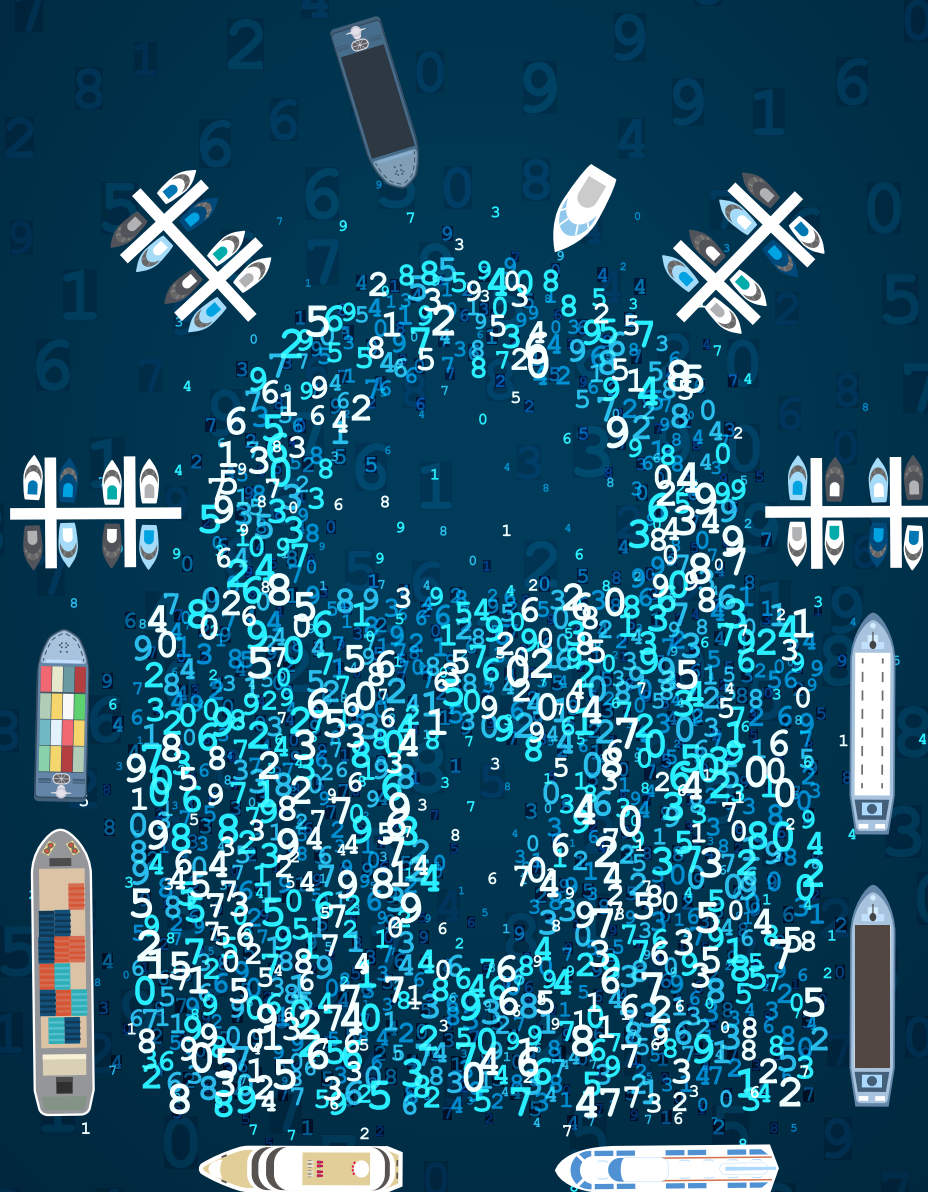


Guide des bonnes pratiques Cybersécurité en navigation intérieure En particulier pour les ports



Ce document ne crée aucune obligation légale pour le CESNI, ses États membres ou son Secrétariat et ne crée aucun droit pour les utilisateurs. Ni le CESNI et son Secrétariat, ni aucune personne agissant au nom du CESNI, ne peuvent être tenus responsables de l'utilisation qui serait faite des informations contenues dans ce document.

Table des matières



Introduction

Contexte

Champ d'application de ce guide et conseils pour sa lecture

4

6

7



Partie 1

Le paysage des menaces de cybersécurité dans les ports

Tendances générales en matière de cybersécurité et conséquences pour les ports

La sécurité informatique des ports, de leurs principaux actifs, et des bâtiments de navigation intérieure

Taxonomie des menaces pour les ports

Exemples de scénarios d'attaque contre des ports

Étude de cas : Campagnes d'ingénierie sociale

12

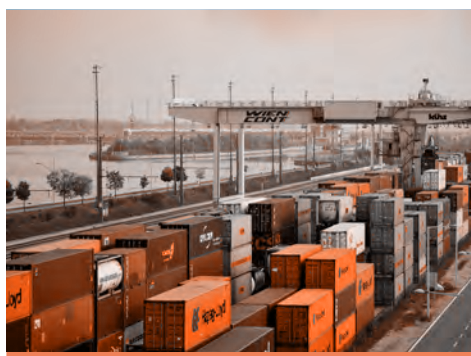
14

15

18

22

26



Partie 2

L'atténuation des risques liés à la cybersécurité

Aperçu de la réglementation et des politiques relatives à la situation des ports

Classification des mesures d'atténuation dans le présent guide

Politiques et procédures organisationnelles

Étude de cas : Programmes de sensibilisation pour le personnel

Étude de cas : élaboration d'une évaluation des risques liés à la cybersécurité

Politiques en matière de technologies de l'information (IT) et de technologies opérationnelles (OT) pour les ports

Étude de cas : protection des terminaux à conteneurs

Mesures techniques de cybersécurité pour les ports

28

30

30

31

36

39

41

47

48



Partie 3

Conseils pour la mise en œuvre des mesures d'atténuation des risques

52

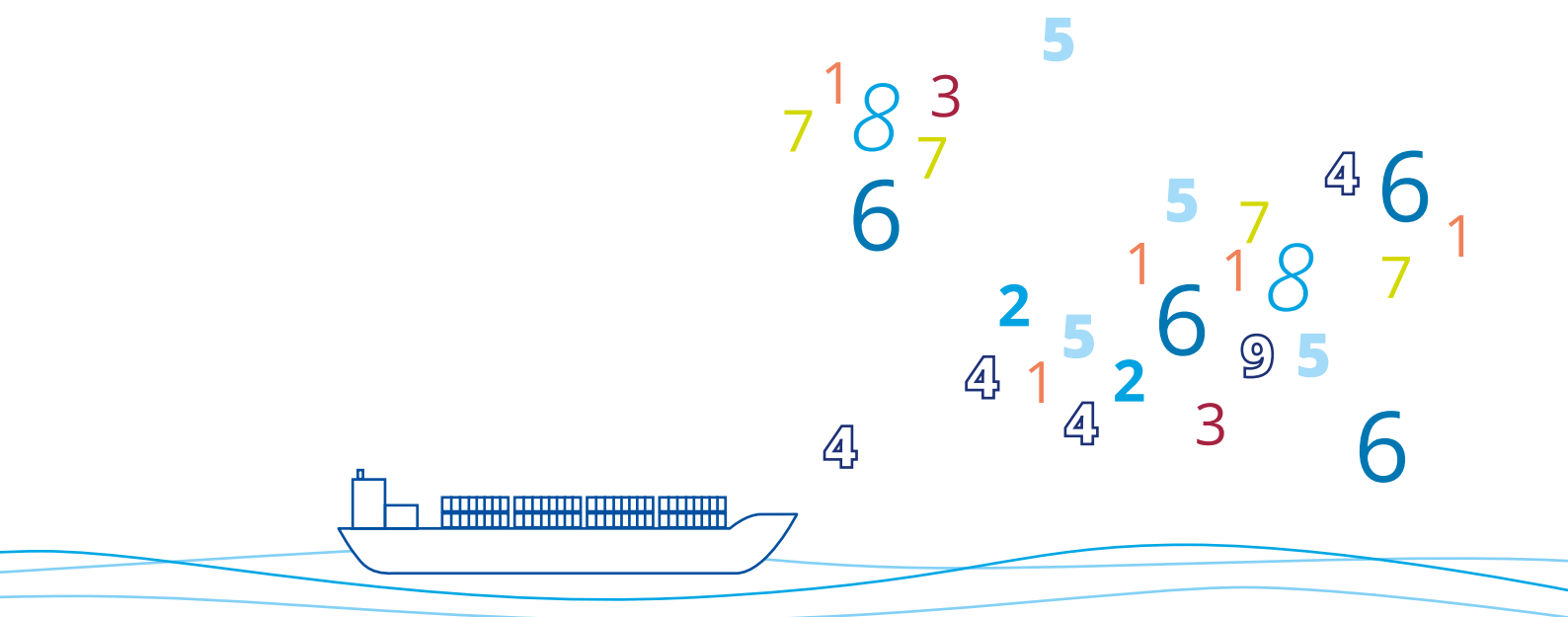
Cadre d'évaluation de la maturité

55



Glossaire

58



Introduction



Contexte	6
Guide élaboré à l'initiative du Comité européen pour l'élaboration de standards dans le domaine de la navigation intérieure (CESNI)	6
Pertinence pour les ports de navigation intérieure	6
Champ d'application de ce guide et conseils pour sa lecture	7
Public visé	8
Références à des normes et standards internationaux	8
Références à des réglementations nationales	9
Comment utiliser ce guide	9
Quelques éléments terminologiques utilisés dans ce guide	10

Contexte

Guide élaboré à l'initiative du Comité européen pour l'élaboration de standards dans le domaine de la navigation intérieure (CESNI)

Le Comité européen pour l'élaboration de standards dans le domaine de la navigation intérieure a pour mission notamment :

- d'adopter des standards techniques dans différents domaines, notamment en ce qui concerne les bâtiments, les technologies de l'information et les équipages, auxquels les réglementations respectives au niveau européen et international, comme celles de l'Union européenne et de la Commission Centrale pour la Navigation du Rhin peuvent se référer en vue de leur application ;
- de délibérer sur des thèmes prioritaires concernant la sécurité de la navigation, la protection de l'environnement et d'autres domaines de la navigation intérieure.

La déclaration de Mannheim¹ adoptée par les ministres en charge des transports des États membres de la Commission Centrale pour la Navigation du Rhin (CCNR) et le programme d'action NAIADES² de la Commission européenne identifient tous les deux la numérisation comme un sujet stratégique pour l'avenir de la navigation intérieure. Cette numérisation s'accompagne d'enjeux et de risques nouveaux comme la cybersécurité.

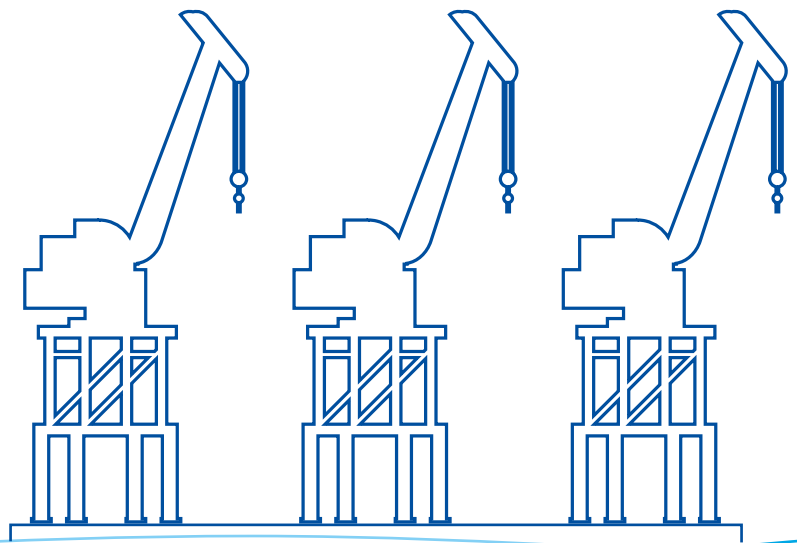
En partenariat avec la Fédération européenne des ports intérieurs (FEPI), le CESNI a donc décidé de rédiger un guide de bonnes pratiques en matière de cybersécurité et destiné aux ports de navigation intérieure.

Pertinence pour les ports de navigation intérieure

Dans un monde de plus en plus interconnecté et dépendant des services numériques, les attaques de cybersécurité augmentent continuellement. Plusieurs ports ont été victimes de cyberattaques au cours des dernières années, ce qui montre que ce secteur ne fait pas exception à la règle.

À titre d'exemple, en juin 2017, le terminal de l'entreprise APM, situé dans le bassin portuaire « Maasvlakte » à Rotterdam a été frappé par un rançongiciel (ransomware). Le port de Rotterdam a été fortement paralysé par le virus, subissant ainsi une indisponibilité au niveau de son exploitation chiffrée en jours. Les grues étaient hors service, et la gestion des conteneurs était à l'arrêt. Les répercussions de cette cyberattaque ont été ressenties dans l'ensemble de l'écosystème portuaire et maritime, confirmant un fait déjà largement connu, à savoir que les cybermenaces ne se limitent plus aux secteurs exclusivement tributaires de l'informatique.

En effet, à mesure que des ports tels que celui de Rotterdam s'avèrent de plus en plus connectés, numérisés et dépendants de systèmes informatiques avancés, ils deviennent également plus vulnérables à de telles cyberattaques³.



¹ https://www.ccr-zkr.org/files/documents/dmannheim/Mannheimer_Erklarung_fr.pdf

² https://transport.ec.europa.eu/transport-modes/inland-waterways/promotion-inland-waterway-transport/naiades-iii-action-plan_en

³ <https://www.dutchnews.nl/news/2017/06/smart-port-in-rotterdam-confounded-by-cyber-attack/>

Pour pouvoir lutter contre ces menaces, il est souhaitable de comprendre les risques liés à la cybersécurité dans le contexte des ports de navigation intérieure. Certains ports de navigation intérieure dépendent encore d'actifs matériels non connectés pour leurs opérations quotidiennes. Ils peuvent ne pas se sentir concernés par les questions de cybersécurité, mais il est indéniable que ces ports seront eux aussi de plus en plus interconnectés au fil du temps. Cela exigera toujours plus d'investissements pour sécuriser des actifs vulnérables aux cyberattaques, tels que des logiciels de logistique complexes, des systèmes de caméras et d'accès connectés, des programmes de navigation à distance, des applications en matière de gestion de conteneurs et d'autres technologies « intelligentes » destinées à accroître l'efficacité des opérations portuaires. À ce titre, le renforcement de la cybersécurité ne consiste pas seulement à renforcer la sécurité des ordinateurs et des systèmes informatiques des ports de navigation intérieure. Cela implique aussi une sensibilisation accrue à la cybersécurité des parties prenantes portuaires qui se dotent de toutes sortes de dispositifs connectés pour fournir divers services portuaires.

Dans ce contexte plus large, ce guide se veut un cadre accessible de bonnes pratiques de cybersécurité pour la manutention dans les ports de navigation intérieure⁴.

Champ d'application de ce guide et conseils pour sa lecture

De façon générale, face à un risque en matière de cybersécurité, il y a cinq façons de réagir :

1. accepter le risque, c'est-à-dire ne rien faire et assumer les conséquences ;
2. éviter le risque, c'est-à-dire l'éliminer par des mesures radicales, par exemple mettre hors-service une écluse, fermer le port à la navigation ou interdire certains bâtiments pouvant générer un risque donné ;
3. transférer le risque, par exemple en souscrivant une assurance ou en faisant appel à un tiers qui assumera les conséquences à sa place ;
4. partager le risque, c'est-à-dire passer un accord avec des tiers pour partager le coût ou les conséquences si le risque se concrétise ;
5. atténuer le risque, c'est-à-dire mettre en œuvre différentes mesures qui permettront de réduire la probabilité que le risque se concrétise ou bien de limiter ses conséquences.

Ce guide s'inscrit principalement dans une démarche d'atténuation du risque. Il comporte quelques éléments qui relèvent du transfert ou du partage, mais uniquement de façon marginale. Il doit être noté que ne rien faire en matière de cybersécurité revient de facto à accepter l'ensemble des risques, identifiés ou non.

Ce guide vise à donner une vision d'ensemble des risques, menaces et mesures d'atténuation en matière de cybersécurité, qui s'exercent principalement dans l'enceinte des ports de navigation intérieure. Il vise à permettre au public visé (voir ci-dessous) de comprendre les acteurs à l'origine des cyberattaques et leurs motivations, les actifs portuaires à prendre en compte lors de l'évaluation des menaces et des risques en matière de cybersécurité. Ce guide donne également un aperçu des bonnes pratiques pour la mise en œuvre des mesures d'atténuation contre les risques de cybersécurité.

⁴ <https://www.dutchnews.nl/news/2017/06/smart-port-in-rotterdam-confounded-by-cyber-attack/>

Pour mieux illustrer l'écosystème portuaire, y ont été inclus les actifs pertinents pour les bâtiments de navigation intérieure.

Le guide comprend trois parties :

1. le paysage des menaces de cybersécurité pour les ports de navigation intérieure : description du panorama des menaces portuaires, y compris des acteurs des menaces, des actifs portuaires, de la taxinomie des menaces et des scénarios d'attaque ;
2. l'atténuation des risques de cybersécurité pour les ports de navigation intérieure : présentation détaillée de l'éventail de mesures d'atténuation qui devraient être prises pour réduire les risques en matière de cybersécurité pour les ports ;
3. les conseils pour la mise en œuvre de mesures d'atténuation des risques : présentation des mesures d'hygiène réalisables en matière de sécurité, à prendre dans un premier temps par les parties prenantes du domaine de l'informatique et celles d'autres domaines.

Ce guide est destiné à servir de point de référence pour les parties prenantes portuaires et ne vient pas se substituer aux méthodes publiées en matière d'évaluation des risques de cybersécurité. Il doit en revanche permettre à chaque partie prenante d'identifier les mesures les plus adéquates permettant l'évaluation ainsi que le traitement des risques cyber.

Public visé

Ce guide vise en premier lieu les acteurs portuaires, à savoir :

- les autorités portuaires ou sous-traitants ;
- les opérateurs de terminaux ou sous-traitants ;
- les entreprises de logistique travaillant avec les autorités portuaires ou les opérateurs de terminaux.

Toutefois, un public plus large pourrait aussi être intéressé par la lecture de ce guide qui les concerne de façon indirecte :

- les autorités nationales de la navigation intérieure ;
- les entreprises de navigation ;
- les institutions publiques disposant d'un pouvoir de réglementation des voies d'eau intérieures ;
- les exploitants de bâtiments ;
- les conducteurs ;
- les équipages des bâtiments ;
- les fabricants de produits destinés au secteur de la navigation intérieure.

Au sein de ce public, ce guide distingue trois types de parties prenantes qui doivent être étroitement associées à la mise en œuvre des bonnes pratiques introduites dans ce guide :



**Équipes
informatiques**



**Responsables
opérationnels**



Direction

Références à des normes et standards internationaux

Ce guide ne se substitue pas aux normes et standards internationaux en matière de cybersécurité, ni même à la littérature existante sur ce sujet. Son objectif est de vulgariser les sujets de cybersécurité dans un contexte propre aux ports intérieurs.

Afin de rendre les choses plus concrètes, un ensemble de mesures sont proposées, sous forme de préconisations et de bonnes pratiques observées sur le marché et en cohérence avec les principes normatifs ISO/IEC 27001.

La mise en œuvre de ce guide ne constitue pas, en soi, une démarche de mise en conformité avec des standards pouvant conduire à une certification. Ce guide permet néanmoins d'entamer un cheminement et une sensibilisation aux questions de cybersécurité qui pourront ensuite faciliter grandement une démarche plus formelle de certification en matière de cybersécurité (par exemple ISO/IEC 27001).

La mise en place d'un système de gestion de la sécurité de l'information (SMSI) constitue par exemple un point important pour la mise en œuvre de la norme ISO/IEC 27001. Celle-ci inclut des exigences pour la définition, la documentation, la mise en œuvre, la surveillance, le maintien et l'amélioration continue d'un SMSI. Ce guide n'aborde pas ces points de façon aussi précise, mais il donne des mesures qui prépareront et faciliteront la mise en place d'un SMSI, si l'organisation décide de le faire.

Références à des réglementations nationales

De la même manière que ce guide ne se substitue pas aux normes et standards internationaux en matière de cybersécurité, il ne se substitue pas non plus aux réglementations en vigueur, notamment sur un plan national, qu'il convient d'appliquer, le cas échéant, prioritairement par rapport à ce guide.

Les réglementations locales existantes ou recommandations édictées par les agences nationales ou organismes internationaux peuvent (ou doivent) être utilisées dans le cadre du renforcement du niveau de sécurité informatique des ports.

Comment utiliser ce guide

Si vous lisez ce guide pour acquérir une **compréhension générale de l'environnement de menace qui entoure la cybersécurité dans les ports de navigation intérieure**, il est recommandé de commencer par lire la Partie 1 de ce guide.

La Partie 2 de ce guide correspond à l'ensemble des mesures proposées aux ports de navigation intérieure pour atténuer les risques liés à la cybersécurité. C'est le cœur de ce guide, avec environ 120 mesures adaptées au contexte des ports de navigation intérieure, regroupées en trois catégories :

1. les mesures relevant des politiques et procédures organisationnelles (OPP) ;
2. les mesures relevant de la politique en matière de technologies de l'information et technologies opérationnelles (ITOT) ;
3. et enfin les mesures techniques de cybersécurité (TSM).

Ces mesures sont expliquées et graduées selon **le niveau de maturité cible** en matière de cybersécurité au sein de chaque port.

Si vous souhaitez vous concentrer sur les **mesures de sécurité spécifiques à mettre en œuvre ou vous faire une idée de la maturité de votre organisation en cybersécurité**, il est recommandé de commencer par la Partie 3 de ce guide. Celle-ci vise à faciliter la mise en œuvre des mesures d'atténuation présentées dans la Partie 2. La Partie 3 de ce guide peut être lue indépendamment et utilisée comme une liste de contrôle vous permettant de voir rapidement si votre organisation a mis en œuvre les mesures correspondantes à ses objectifs en matière de cybersécurité. Ces conseils devraient être accessibles et utiles à tous types de lecteurs.

La Partie 3 propose un « tableau d'applicabilité », c'est-à-dire une grille de lecture des mesures d'atténuation présentées dans la Partie 2, en fonction des objectifs que le port se fixe en matière de cybersécurité et du type de partie prenante (équipes informatiques, responsables opérationnels et Direction).

Si vous envisagez de lire ce guide comme une introduction à la cybersécurité dans les ports de navigation intérieure, une lecture du début à la fin vous donnera une vision d'ensemble du sujet.



Izmail, Ukraine - Danube

Quelques éléments terminologiques utilisés dans ce guide

Afin de rendre la lecture de ce guide plus fluide, certains éléments terminologiques ont été simplifiés.



Ports

Par défaut et sauf mention explicite, le terme « port » désigne un port de navigation intérieure. Le terme peut aussi désigner un port mixte, c'est à dire un port qui est à la fois maritime et de navigation intérieure, sauf si le contexte appelle à faire la distinction entre un port strictement de navigation intérieure et un port mixte.



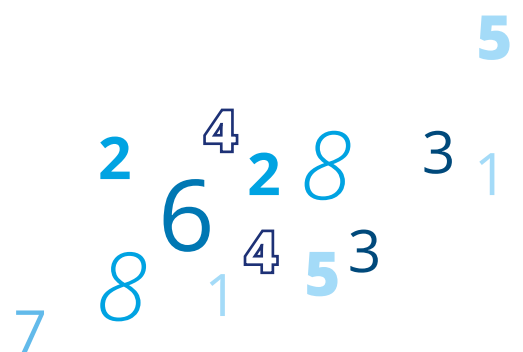
Actif

Dans le cadre de ce guide, un « actif » est toujours employé pour désigner un « actif numérique ». Un actif numérique se définit comme un ensemble de données numériques dont la propriété ou le droit d'usage est un élément du patrimoine d'un port de navigation intérieure. Les actifs (numériques) sont donc immatériels. Il peut s'agir par exemple de données ou de logiciels (le terme « donnée » est ici à considérer au sens large). Il est à noter que, parfois, un actif numérique peut être fortement couplé à un actif matériel « classique » dont il assure le bon fonctionnement. Par exemple, une écluse est un actif matériel, mais pour fonctionner elle a besoin d'un logiciel et de beaucoup de données spécifiques. Chaque élément matériel de l'écluse : les murs, les portes, mais aussi les capteurs, les ordinateurs, câbles informatiques, les caméras etc. ne sont pas des « actifs » au sens de ce guide. Cependant, tous les logiciels (et leur paramétrage) utilisés par n'importe lequel de ces éléments matériels est un actif numérique et sera donc un « actif » au sens de ce guide.



Systèmes IT/OT

Dans certaines sections de ce guide, il est fait référence à des systèmes IT/OT. Dans ce contexte, le terme IT (Information Technologies) désigne la partie du système dédiée au traitement de l'information (de la donnée), partie hautement programmable et modifiable. Le terme OT (Operational Technologies) désigne la partie du système dédiée au pilotage de machines ou de processus physiques. La partie OT est généralement très autonome et programmée pour accomplir une tâche précise (par exemple réguler la température ou la ventilation). Pour simplifier, l'IT traite des données tandis que l'OT manipule des objets physiques. Ces deux types de systèmes peuvent bien entendu être en interaction, et c'est en particulier le cas lorsqu'on parle de « systèmes IT/OT ».



Cybersécurité : Ce terme est très largement utilisé dans ce guide, à commencer dans son titre. Dans le cadre de ce guide, le terme « cybersécurité » est à prendre dans un sens très large. Il s'agit de la mise en œuvre d'un ensemble de techniques, de pratiques, de moyens et d'outils pour protéger les systèmes d'information et leurs données. Cette protection est également à prendre au sens large, de la prévention à la réparation en passant par la détection et la réaction aux événements. Cette protection s'exerce vis-à-vis de cybermenaces qui peuvent également revêtir plusieurs formes. Il peut s'agir d'attaques informatiques, mais aussi de négligences, d'accidents, de catastrophes naturelles ou d'erreurs humaines. La « cybersécurité » prend en compte les menaces informatiques, mais aussi les menaces liées à des aspects physiques et organisationnels. D'autres termes existent avec des significations variables selon les pays et les cultures, comme « sécurité des données » ou « sécurité des systèmes d'information » ou encore « sécurité informatique ».

Partie 1

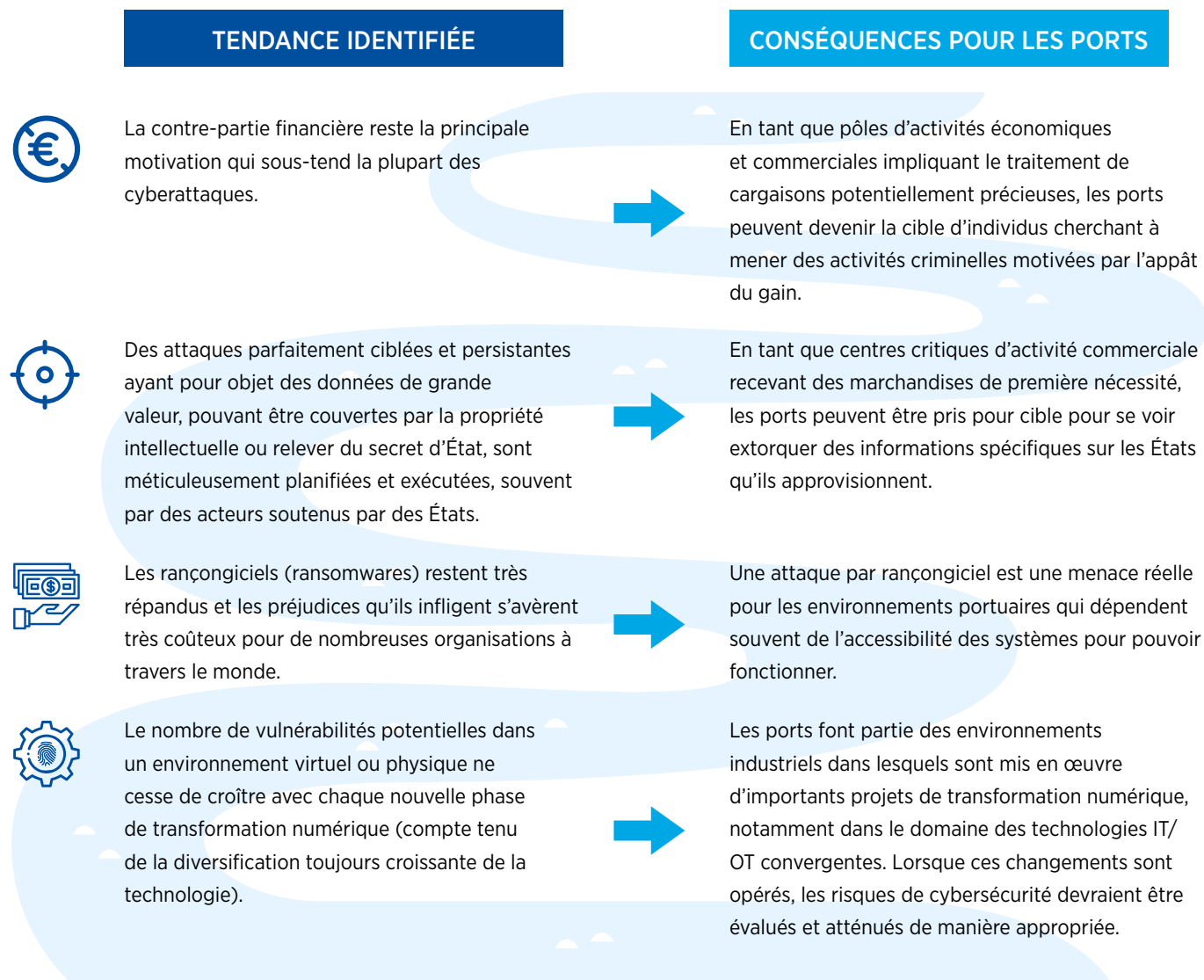
Le paysage des menaces de cybersécurité dans les ports



Tendances générales en matière de cybersécurité et conséquences pour les ports	14
La sécurité informatique des ports, de leurs principaux actifs, et des bâtiments de navigation intérieure	15
Principaux actifs des ports	16
Actifs des bâtiments	17
Taxonomie des menaces pour les ports	18
Attributs de la cybersécurité	18
Acteurs malveillants potentiels	19
Taxonomie des menaces	20
Impacts potentiels	21
Exemples de scénarios d'attaque contre des ports	22
Scénario 1	
Infiltration des systèmes contrôlant le fonctionnement des machines	22
Scénario 2	
Corruption de données pour faciliter le trafic de drogues illicites	24
Scénario 3	
Brouillage de l'équipement AIS	25
Étude de cas : Campagnes d'ingénierie sociale	26

Tendances générales en matière de cybersécurité et conséquences pour les ports

L'Agence de l'Union européenne pour la cybersécurité (ENISA) a publié, en 2020, un rapport sur le paysage des menaces applicables aux ports maritimes. Il contient les conclusions suivantes, qui méritent d'être soulignées dans le contexte du secteur des ports :



Ces conclusions s'appliquent au contexte des ports et indiquent qu'il faut considérer les questions ayant trait à la cybersécurité comme un risque réel pour les opérations portuaires critiques en matière de transport et d'économie. Il est donc souhaitable de prendre des mesures d'atténuation de ce risque.

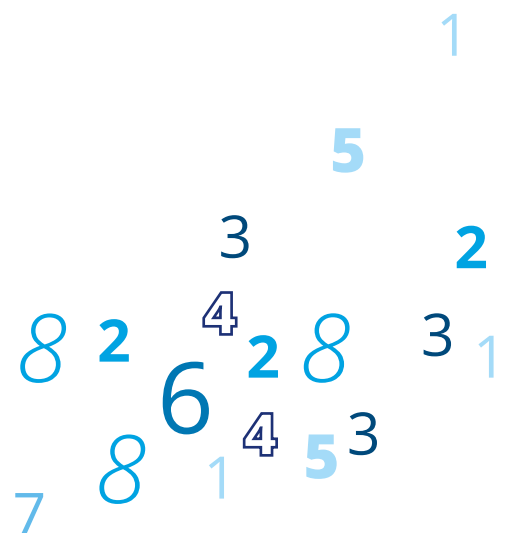
La sécurité informatique des ports, de leurs principaux actifs, et des bâtiments de navigation intérieure

Avant d'entamer l'examen des menaces qui pèsent sur la sécurité et les moyens de protéger une organisation contre ces menaces, celle-ci doit d'abord comprendre ce qu'elle essaie concrètement de protéger. À cet égard, la réalisation d'une cartographie des actifs s'avère un exercice utile, dont l'objectif est de recenser tous les actifs susceptibles d'être ciblés ou exploités dans le contexte d'une cyberattaque.

Pour faciliter cette tâche, ce guide propose un cadre d'évaluation des actifs des ports et des bâtiments. Bien que ces actifs puissent ne pas être présents ou pertinents pour tous les lecteurs, la liste ci-dessous est destinée à servir de référence aux fins de leur évaluation dans votre périmètre. Il importe également de noter que la criticité des actifs peut varier d'une organisation à l'autre. En effet, l'actif le plus critique d'un port spécialisé dans le transport pourrait regrouper les systèmes soutenant les opérations d'un terminal à conteneurs, tandis qu'un autre port pourrait accorder une importance particulière à un système central de gestion des écluses. Pour les ports assurant des prestations dans le domaine du transport de passagers, ces activités peuvent être considérées comme des missions critiques. Par conséquent, en tant qu'organisation, la première étape pour mieux comprendre et atténuer les risques de sécurité serait d'effectuer un examen complet des actifs. L'objectif est alors d'identifier les actifs critiques pour son périmètre et de définir la liste des « joyaux » (actifs à protéger au plus haut niveau).

Dans le cas des ports, il convient de noter qu'il y a, dans certains cas, une présence croissante de systèmes de commande industriel (ICS), y compris des systèmes de contrôle-commande et d'acquisition de données (SCADA) à travers lesquels les systèmes et machines industriels sont connectés à des réseaux afin d'être commandés à distance ou depuis la terre. Même lorsque ces actifs mécaniques ne sont pas, eux-mêmes, une cible directe sur le plan de la cybersécurité, ils sont toutefois accessibles par le réseau et fonctionnent avec des systèmes anciens (qui ne sont plus mis à jour par les fournisseurs). Aussi, les ICS peuvent être utilisés comme des points d'entrées en vue de cibler d'autres actifs. Pour cette raison, les ICS méritent d'être inclus dans les listes des actifs critiques.

La description ci-dessous détaille les principaux actifs des ports et certains actifs liés aux bâtiments, notamment ceux qui peuvent se trouver, à un instant donné, connectés aux systèmes portuaires.



Principaux actifs des ports



Réception et accostage du bâtiment

Concerne l'entrée et l'accostage du bâtiment dans le port. Comprend les systèmes d'infrastructure fluviale, tels que la gestion des ponts et des écluses (LBM), les capteurs et mécanismes de verrouillage connectés, les systèmes de gestion du trafic.



Sécurité et sûreté

Tout outil contribuant à la sécurité physique des sites portuaires, tels que les portiques connectés, les services de surveillance par caméras de vidéosurveillance, les portes et passages connectés, les systèmes de badgeage, les systèmes d'alarme connectés, les postes de garde.



Autorités et douanes

Outils permettant de procéder à la déclaration et à l'évaluation des marchandises pour le paiement des droits de port (d'assurer la coordination relative à l'agrément des douanes, de distribuer les formulaires pour les déclarations, de solliciter les autorités publiques et de traiter leur réponse).



Les systèmes dédiés aux bâtiments à passagers et de tourisme

Applications web pour la réservation et la billetterie des bâtiments à passagers, constituant un actif commercial majeur pour les ports touristiques et étant particulièrement vulnérables, s'agissant d'actifs accessibles au public. Faute d'accès à ces systèmes, les prestations touristiques pourraient être interrompues ou suspendues, ce qui aurait un impact commercial important sur les affilés ou associés des ports.



Les systèmes informatiques utilisés pour la gestion du trafic, tels que les services de gestion de la navigation (VTS)

Centres de contrôle VTS dans les ports se trouvant au cœur des opérations portuaires et pouvant s'appuyer sur des connexions Internet ou VHF, ce qui en fait des cibles potentielles de cyberattaques.



Service de soutien

Matériel, logiciels et applications informatiques portuaires, systèmes de communication du personnel portuaire, applications de gestion des biens immobiliers et des installations, applications de gestion des marchandises dangereuses et de gestion de la réfrigération. Les actifs des services de soutien comprennent également les « systèmes dédiés aux bâtiments à passagers et de tourisme » (voir définition spécifique).



Amarrage du bâtiment

Outils et processus permettant d'assurer les prestations nécessaires pour les bâtiments venus au port afin de faire le plein de carburant, reconstituer le stock de provisions alimentaires, se réapprovisionner en eau, faire procéder à des réparations etc.



Système d'identification automatique (AIS)

Système d'échanges automatisés de messages entre bâtiments par radio VHF qui permet aux bâtiments et aux systèmes de surveillance de trafic de connaître l'identité, le statut, la position et la route des bâtiments se situant dans la zone de navigation.



Service de répartition

Outils connectés permettant la répartition des conteneurs ou des marchandises en vrac à acheminer vers les gares de triage, les plateformes de transport – dont les systèmes assurent des prestations supplémentaires telles que le scannage de conteneurs – et les plateformes de communication pour la répartition. Sont également compris les outils connectés que l'on peut trouver dans les gares ferroviaires et alentours, ainsi que les wagons pour le transport de conteneurs.



Services énergétiques

Outils de gestion et applications informatiques permettant de superviser et de piloter les lignes, équipements, centrales et réseaux énergétiques requis pour approvisionner en énergie le port et son infrastructure.



Entreposage et haubannage des conteneurs

Gestion de chargement et de déchargement des bâtiments (CFM), outils de déchargement et d'entreposage des conteneurs tels que les logiciels de déplacement, de stockage et de manutention des conteneurs, les outils de manutention et de tri du vrac, les outils d'entreposage et de surveillance des conteneurs réfrigérés etc.

Actifs des bâtiments

Remarque

À l'exception des actifs assurant la communication entre le bâtiment et le port ou d'autres lieux à terre, les actifs du bâtiment eux-mêmes sont considérés comme exclus du champ d'application aux fins du présent guide.



Services d'Information Fluviale (SIF)

Suivi et repérage des bâtiments en navigation intérieure (AIS Intérieur), système de visualisation de cartes électroniques et d'informations pour la navigation intérieure (ECDIS), avis à la batellerie en navigation intérieure (NtS), système d'annonces électroniques en navigation intérieure (ERI).



Technologie de la communication et de l'équipage

Équipements de communication par radio, par satellite et autres dispositifs connectés à distance facilitant la connexion entre le bâtiment et la terre ; téléphones cellulaires, ordinateurs et tablettes de l'équipage utilisés à bord du bâtiment et ailleurs.



Machinerie

Dispositifs informatiques et électroniques contribuant au fonctionnement du bâtiment, y compris les appareils et installations de propulsion, les systèmes de contrôle de l'alimentation électrique, les systèmes de la timonerie, les systèmes de carburant, de batterie et de cargaison.



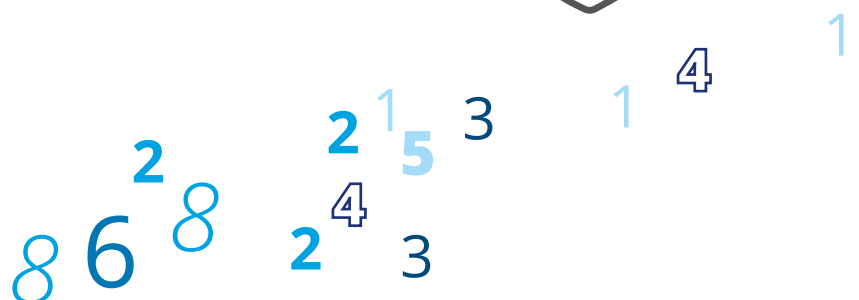
Cargaison

Outils utilisés pour communiquer des informations sur le statut de la cargaison, à la fois à bord et à terre, en ce qui concerne la livraison, le contenu et le type de cargaison.



Actifs opérationnels

Actifs permettant de faire fonctionner à bord et ailleurs les appareils liés à l'activité portuaire, notamment les ordinateurs personnels, les ordinateurs portables, les tablettes intelligentes et leurs applications professionnelles.



Taxinomie des menaces pour les ports

Lorsque nous aurons défini la liste des actifs critiques d'un port, ou des systèmes susceptibles d'être endommagés par une cyberattaque, nous pourrions identifier et analyser les types de menaces auxquelles ces actifs sont exposés.

On entend par « **menaces pesant sur la cybersécurité** » toute circonstance ou événement susceptible d'avoir une incidence négative sur les opérations organisationnelles, les actifs organisationnels, les individus, d'autres organisations, ou des intérêts publics. Cela pourrait se produire, par exemple, par l'accès non autorisé, la destruction, la divulgation, la modification des informations et/ou le déni de service. Une menace peut

être identifiée en corrélant la vulnérabilité d'un port avec les motivations des acteurs malveillants.

C'est pourquoi, afin de pouvoir évaluer les menaces, nous devons commencer par exposer en détail les attributs de cybersécurité que doit posséder un actif. Les attributs fondamentaux de la cybersécurité sont la confidentialité, l'intégrité et la disponibilité (communément appelées « triade CIA », l'abréviation anglaise « CIA » correspondant à « confidentiality », « integrity » et « availability »).

Dans le contexte des ports et des bâtiments, la notion de **possession**⁵ a été ajoutée.

Le tableau ci-dessous permet d'illustrer les quatre principaux attributs appliqués à l'écosystème portuaire.

Attributs de la cybersécurité

Confidentialité

Les données et les informations qui transitent par les actifs portuaires demeurent confidentielles, si nécessaire. Les utilisateurs non autorisés n'ont pas la possibilité d'accéder à des informations,, de les télécharger ou de les transmettre.

Possession

Le contrôle opérationnel des actifs du port et des bâtiments est limité au personnel autorisé. La capacité à conserver le contrôle des bâtiments des machines et d'autres équipements connectés est un attribut clé pour les ports et les bâtiments. La prise de contrôle non autorisée du système d'un bâtiment ou d'un outil opérationnel clé correspond à un scénario de menace tout aussi inquiétant que ceux décrits plus loin. La possession diffère de l'intégrité en ce qu'elle implique une possession et un contrôle physiques (plutôt que virtuels). En effet, par rapport à d'autres environnements ne disposant que d'actifs numériques, les ports associent l'informatique aux actifs de technologie opérationnelle (OT) pour pouvoir fournir une combinaison de services physiques et numériques. Ces services physiques, s'ils sont utilisés de manière abusive, peuvent entraîner d'importants préjudices sur le plan financier et de graves atteintes à la réputation, voire des lésions corporelles ou des décès.

Disponibilité

La disponibilité des informations, applications, outils ou dispositifs nécessaires au fonctionnement des activités portuaires et des bâtiments. Il s'agit de garantir leur fonctionnement aux moments (définis à l'avance) où on en a besoin. La disponibilité mesure aussi la capacité de résilience, c'est-à-dire le temps nécessaire à la remise en route d'un système ou d'un service après incident (en mode nominal ou dégradé).

Intégrité

Les informations, applications, outils ou dispositifs nécessaires au fonctionnement des activités portuaires et des bâtiments fournissent des données exactes et authentiques, qui n'ont pas été modifiées, entre l'expéditeur et le destinataire. L'intégrité inclut également la garantie de non-répudiation, c'est-à-dire la preuve (infalsifiable) qu'une information a bien été produite ou validée par une entité particulière.



⁵ La notion de possession a été ajoutée pour tenir compte du guide de bonnes pratiques publié par l'Institution of Engineering and Technology, intitulé « Cyber Security for Ports and Port Systems (2020) ».

Acteurs malveillants potentiels

Les acteurs de la menace de cybersécurité peuvent causer des dommages aux systèmes ou réseaux numériques de manière intentionnelle ou non. Ce guide se concentre sur les acteurs potentiels de la menace qui sont répartis en sept catégories :

Type d'acteur	Action	Exemple d'application dans le contexte de la navigation intérieure
Employé malveillant ou insuffisamment formé ou non sensibilisé	Ignorant (volontairement ou non) les bonnes mesures d'hygiène en matière de cybersécurité, cet acteur de la menace peut être animé de motivations malveillantes ou non. Mais, dans tous les cas, ses actions peuvent mettre son organisation en danger, que ce soit volontairement ou par simple négligence.	Le fait de cliquer sur un lien dangereux envoyé dans un courriel par un attaquant, entraînant le téléchargement de fichiers malveillants sur les systèmes informatiques du port.
Criminel	Motivé par l'appât du gain financier, cet acteur conduit des actions telles que le vol, la contrebande de marchandises, le passage clandestin de personnes, l'évasion fiscale, les déprédations.	Interception de communications dans le but de voler des conteneurs ou les faire passer en fraude sans payer de droits, voler des cargaisons sur un bâtiment, envoyer des rançongiciels pour geler les actifs informatiques du port et exiger un paiement.
Concurrents	Poussés par le désir d'obtenir des informations commerciales ou sur le marché, ces acteurs visent à intercepter des informations pour obtenir un avantage concurrentiel économique.	Obtenir des informations classifiées sur les processus de gestion portuaire afin de les utiliser pour le développement de leurs propres activités.
Militant ou « hacktiviste »	Motivé par la désobéissance civile, cet acteur utilise l'Internet pour diffuser son idéalisme ou créer une pression en faveur d'une cause spécifique.	Diriger un bâtiment de manière à ce qu'il bloque l'entrée d'un port en signe de protestation. Manipuler un ouvrage d'infrastructure fluviale (pont, écluse etc.) pour désorganiser le système.
État-nation	Agissant pour le compte d'un État-nation ou d'une autre structure gouvernementale souveraine, ces acteurs sont animés par le désir de se livrer à une forme de guerre (déclarée ou non) en provoquant des interruptions ou l'arrêt des activités.	Exécution d'une attaque par déni de service sur les actifs portuaires pour bloquer l'accès à une voie fluviale ou à un plan d'eau, en agissant par exemple sur un système d'écluses.
Terroriste	Utilisation de l'Internet pour inspirer la peur ou provoquer une sorte de chaos physique ou économique.	Prendre le contrôle d'un bâtiment pour endommager un port, faire des victimes. Intercepter des informations concernant l'arrivée de matières dangereuses dans le port et utiliser ces matières pour répandre une forme de chaos.
Individu se livrant à des activités d'espionnage	Exploitation des appareils connectés pour obtenir des données secrètes ou sensibles, à des fins de revente ou en tant qu'informateur. Les activités d'espionnage peuvent être menées par d'autres États ou par des concurrents.	L'obtention, par d'autres États-nations, d'informations sur les cargaisons sensibles transitant par un port (par exemple les vaccins et le matériel médical). Espionnage des opérations portuaires pour obtenir des informations sur la concurrence.

Certains exemples dans le tableau ci-dessus, comme la menace terroriste, relèvent de menaces externes qui sont en dehors du périmètre de ce guide dans la mesure où les ports ne peuvent pas prendre de mesures efficaces, à leur niveau, pour limiter ces risques. Ces menaces doivent toutefois être prises en compte dans le cadre de la coordination en matière de cybersécurité entre les ports et les autres acteurs en navigation intérieure.

Il est important de noter que les acteurs susmentionnés peuvent varier en fonction de leurs motivations, de leurs ressources et de

leur détermination. Les acteurs ayant des liens avec des États engagés dans des activités de guerre et d'espionnage peuvent disposer de ressources considérables dans lesquelles ils peuvent puiser. En effet, le piratage informatique parrainé par des États augmente, comme l'indique une étude récente de l'ENISA qui dresse un panorama des tendances en matière d'espionnage informatique⁶. Dans cette étude de 2020, il est noté qu'environ 38% des acteurs malveillants sont rattachés à des États-nations et que 11,2% des cyberincidents étaient motivés par le cyberespionnage.

⁶ <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage>

Cette étude met en avant les risques pesant sur les plateformes de transports de matières premières. Même si les ports ne sont pas cités de façon explicite, ils répondent à cette description et sont souvent vitaux pour les activités d'un État. Dans ce contexte, l'étude souligne que les attaques parrainées par des États se multiplient, notamment dans les services publics et dans les secteurs du gaz naturel, du pétrole et de l'industrie manufacturière. Ce type de menaces, parrainées par des États-nations, ne devraient pas être sous-estimées car il s'agit de campagnes confortablement financées, disposant de personnel hautement qualifié et dont les opérations sont implacables et les objectifs hautement préjudiciables.

Taxinomie des menaces

Les attributs et les acteurs de la menace exposés ci-dessus permettent d'envisager un certain nombre de scénarios. Sur la base de ces scénarios, il est possible d'établir une taxinomie des menaces pour les ports ou une liste des menaces face auxquelles un port peut se montrer vulnérable, et ce en fonction de ses caractéristiques propres.

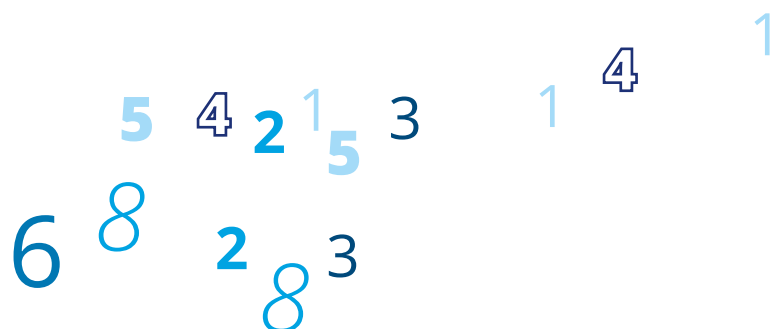
La taxinomie des menaces permet d'analyser les types d'événements de cybersécurité et leurs impacts potentiels. Les types de menaces décrits ci-dessous ont été identifiés à partir de l'analyse des publications existantes consacrées aux menaces pesant sur les navires et les ports maritimes. Les résultats obtenus ont été adaptés de manière à pouvoir s'appliquer à l'écosystème portuaire.

Description applicable aux ports	Exemple
 Défaillances, dysfonctionnements Les systèmes ou dispositifs nécessaires aux opérations portuaires sont compromis et ne peuvent pas fonctionner dans la mesure nécessaire.	 Le système d'exploitation du pont ou de l'écluse est compromis par une attaque en déni de service, ce qui gèle les opérations et entraîne l'interruption du fonctionnement du pont ou de l'écluse.
 Attaques physiques Une cyberattaque est combinée à un système de technologie opérationnelle (OT), conduisant à la prise de contrôle physique d'une machine à des fins de fraude, sabotage, vandalisme, vol, terrorisme, hacktivisme ou accès non autorisé.	 Prise de contrôle d'un système de machinerie de bâtiment par l'activation d'une menace persistante avancée. Le bâtiment est ensuite conduit dans un port à des fins terroristes.
 Écoute illicite, interception, détournement d'informations Des interventions malveillantes sur le réseau conduisent à l'interception de données sensibles ou du trafic réseau ou au détournement d'une session utilisateur.	 Les données stockées dans l'application de gestion des conteneurs, renfermant des informations sur les conteneurs de marchandises dangereuses, sont interceptées par des terroristes en vue de s'emparer de ces marchandises.
 Falsification (spoofing) ou brouillage (jamming) d'informations Falsification d'une communication ou d'une source de données (expéditeur d'un SMS, position GPS) visant à donner l'impression que les informations proviennent d'une source d'information connue et fiable alors qu'elles ont en fait été modifiées ou fabriquées par l'attaquant.	 Les informations GPS sont faussées pour donner une mauvaise localisation, ce qui entraîne un risque pour la navigation.
 Catastrophe Une catastrophe écologique ou naturelle est causée à l'écosystème portuaire par l'exploitation de failles sur des actifs portuaires connectés.	 Un pirate informatique falsifie les données de l'application dédiée à la gestion des conteneurs, ce qui entraîne une mauvaise manutention de conteneurs renfermant des matières dangereuses. Celle-ci peut, à son tour, provoquer un incendie dans le port, causant de graves dommages physiques aux actifs portuaires.
 Interruptions de fonctionnement L'approvisionnement des ports en ressources nécessaires à la conduite des opérations est interrompu. Les ressources concernées peuvent inclure le réseau, le personnel, le carburant, l'eau et l'électricité.	 Une attaque à grande échelle contre un réseau électrique connecté entraîne une panne de courant importante et le gel des opérations portuaires, retardant ainsi le transport des marchandises.
 Dommages non intentionnels Les dommages causés aux données, aux systèmes ou aux infrastructures physiques portuaires sont dus aux manipulations accidentelles par une personne interne.	 Un employé télécharge un fichier contenant un rançongiciel, gelant l'intégralité des systèmes informatiques du port. Une demande de rançon s'affiche sur l'écran verrouillé.

Impacts potentiels

Les menaces sont considérées comme « inquiétantes » car, si elles sont mises à exécution, elles peuvent infliger des dommages réels à une organisation. En cas de violation des attributs de cybersécurité décrits plus haut, le port ou les entreprises affiliées au port peuvent être impactés de manière très différente. La liste suivante contient des types d'impacts potentiels résultant de l'exploitation des failles par des menaces de cybersécurité.

Type d'impact	Description détaillée
Atteinte à la réputation	Une violation ou un incident cybernétique peut porter durablement atteinte à la réputation de l'organisation à son nom et à sa marque. Les atteintes à la réputation sont difficiles à évaluer, car elles ne sont souvent pas tangibles, mais elles ont de multiples effets secondaires, tels que les dépenses à engager pour regagner la confiance des clients, renforcer la surveillance réglementaire et combler le manque à gagner.
Perte financière	Les coûts encourus par l'organisation à la suite d'un cyberincident peuvent être multiples, comprenant notamment les coûts de la reprise après sinistre et de la gestion de crise, les honoraires d'avocats, l'augmentation des primes d'assurance, la perte de marchandises et les coûts liés au retard accumulé dans les prestations de services portuaires.
Sanctions prévues par la réglementation	Un cyberincident peut entraîner des sanctions réglementaires, telles que des amendes et des mesures de responsabilisation accrues pour l'organisation en cause.
Destruction de biens	Une attaque contre des systèmes informatiques portuaires peut entraîner la destruction de biens numériques, tels que des données et des informations, qui n'ont pas été correctement sauvegardés. Elle peut aussi conduire à la destruction de biens physiques, tels que le matériel informatique, les systèmes SCADA et – en conséquence d'une attaque – les bâtiments du service portuaire, les actifs d'exploitation, les conteneurs et leur contenu.
Pertes en vies humaines ou lésions corporelles	En cas de cyberévénement à visée terroriste, des personnes peuvent être blessées, voire tuées. Une inondation peut être causée par le dysfonctionnement d'une écluse. Des matières dangereuses peuvent créer une explosion.
Activités criminelles : fraude, commerce illicite	Les criminels peuvent utiliser des techniques de cyberattaque, telles que l'interception du trafic réseau, pour obtenir des informations et mener des activités illégales, telles que le trafic de substances non autorisées dans des conteneurs ou le passage clandestin d'êtres humains.
Vol de biens	Les criminels peuvent utiliser des techniques de cyberattaque dans le but de perpétrer des vols dans le port : dérober des conteneurs, leur contenu, de la marchandise ou bien du matériel (machines, véhicules, pièces détachées...).
Catastrophe écologique	Un cyberévénement pourrait avoir pour conséquence une mauvaise manutention des matières dangereuses ou du carburant, ce qui pourrait aboutir à une catastrophe écologique sur les voies navigables intérieures.





Exemples de scénarios d'attaque contre des ports

Ce guide examinera trois exemples de scénarios d'attaque, sélectionnés parmi les menaces exposées plus haut, présentant des différences en ce qui concerne les motivations et les acteurs de la menace. Cette analyse a pour but de fournir des exemples tangibles des types de menaces pesant sur les actifs décrits ci-dessus. Chaque scénario d'attaque a été sélectionné à partir d'un exemple réel d'attaque survenue ces dernières années, applicable à l'écosystème des ports.

Scénario 1

Infiltration des systèmes contrôlant le fonctionnement des machines

En 2013, deux pirates informatiques ont infiltré les systèmes de contrôle d'un petit barrage dans l'État de New York⁷. Le barrage, utilisé en prévention des effets d'une tempête, était piloté par un système SCADA connecté directement à l'Internet via un modem cellulaire. Le système utilisait cette connexion Internet pour fournir des données sur l'état et le fonctionnement de l'installation (niveaux d'eau, etc.). Cela permettait aux opérateurs d'assurer le contrôle à distance des systèmes de vannes, qui, à leur tour, permettaient de contrôler les niveaux d'eau et les débits. Les pirates n'ont pas réussi à actionner les portes, qui étaient alors heureusement déconnectées du système pour des raisons de maintenance. Ce type d'attaque, visant à perturber ou à réquisitionner des installations qui, comme les écluses, assurent des opérations critiques, constitue un scénario classique qui se révèle également pertinent pour les ports. Une telle attaque pourrait avoir des répercussions importantes en matière de sécurité de la navigation et avoir un important impact commercial.

Ce scénario d'attaque pourrait être reproduit en prenant pour cible des installations portuaires telles que les réseaux électriques des ports, les stations de traitement des eaux, les commandes des écluses, etc.



Lyon, France - Saône



Wijk bij Duurstede, Pays-Bas - Canal Amsterdam-Rhin

⁷ <https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged>

Les principales étapes d'une infection de systèmes industriels par un logiciel malveillant, telle que celle décrite ci-dessus, qui a failli aboutir, et d'autres scénarios d'attaque de systèmes de contrôle industriel (ICS), sont exposées en détail ci-dessous :



Étape 1 - Infiltration

Un acteur malveillant parvient à infecter les systèmes d'une installation connectée. Un dispositif externe tel qu'une clé USB, un lien actif, un fichier téléchargeable, ou simplement une page Internet externe, peut lui permettre d'arriver à ses fins. En ce qui concerne la clé USB, elle est insérée dans un ordinateur, et le code exécutable qu'elle renferme est susceptible de se propager à travers les réseaux informatiques.



Étape 2 - Espionnage

Le logiciel malveillant s'incruste dans les systèmes de l'entreprise, espionnant les communications du réseau pour identifier les possibilités de reproduction et d'expansion.



Étape 3 - Sabotage des processus de sécurité

Le logiciel malveillant identifie les logiciels présentant des vulnérabilités ou des portes dérobées à exploiter pour empêcher le déclenchement de mécanismes potentiels de détection des intrusions ou des menaces. Il reste intraçable, se livrant à des attaques qui vont progressivement atteindre les systèmes d'exploitation et, dans le cas d'un réseau électrique portuaire, les automates programmables industriels (PLC) présents dans les systèmes de technologie opérationnelle. La compromission des PLC permet potentiellement d'exécuter des fonctions industrielles, telles que la surveillance par capteurs de la pression de l'eau ou encore l'ouverture et la fermeture de vannes.



Étape 4 - Prise de contrôle

Le logiciel malveillant détourne les fonctions prévues du PLC en agissant par exemple sur les données en entrée ou sur sa programmation interne. Dans le cas d'une écluse entre deux bassins au sein d'un port, le PLC pourrait actionner la commande d'ouverture des portes sur la base de données erronées concernant le niveau de l'eau de part et d'autre, déclenchant ainsi leur ouverture dangereuse. Si le code malveillant inversait la fonction d'ouverture et de fermeture sur une des deux portes, le résultat pourrait être l'ouverture simultanée des deux portes de l'écluse.



Étape 5 - Action

Le pirate utilise frauduleusement le système pour effectuer une action donnée dans le but d'atteindre un objectif donné. Par exemple, dans le cas décrit ci-dessus, au lieu de fermer la porte amont de l'écluse, la porte aval est ouverte au moment où un gros convoi est dans le sas, l'entraînant ainsi violemment vers l'aval, provoquant des blessés ou des morts parmi l'équipage, des dégâts matériels sur les bâtiments du convoi, ainsi qu'en amont et en aval de l'écluse en raison de l'écoulement violent de l'eau.



Étape 6 - Réplication

Le logiciel malveillant se réplique pour cibler d'autres systèmes ou dispositifs. Dans l'exemple de l'écluse entre deux bassins, le logiciel malveillant tente de détecter la présence d'autres systèmes PLC à proximité qu'il pourrait prendre pour cible.



Scénario 2

Corruption de données pour faciliter le trafic de drogues illicites

En 2013, les autorités belges et néerlandaises ont arrêté une douzaine de suspects qui tentaient de faire passer plus de 1 000 kilos de cocaïne et plus de 1 000 kilos d'héroïne par des conteneurs après avoir pu accéder aux systèmes informatiques de l'entreprise portuaire⁸. Les criminels, de mèche avec des pirates informatiques, ont pris le contrôle des ordinateurs des terminaux à conteneurs pour pouvoir étiqueter et suivre les conteneurs renfermant leurs drogues illicites. Ils ont procédé de la manière suivante, qui s'appliquait très bien au contexte des ports :



Étape 1 - Intrusion

Le criminel envoie aux employés du terminal à conteneurs des courriels dont les pièces jointes malveillantes renferment des logiciels téléchargeables leur permettant d'installer des logiciels espions sur les ordinateurs des employés.

Étape 2 - Contrôle

Le criminel prend le contrôle des ordinateurs infectés et peut donc accéder aux systèmes de gestion et/ou aux bases de données des conteneurs.

Étape 3 - Surveillance

Les conteneurs renfermant les drogues illicites à passer en contrebande sont identifiés dans le système et étiquetés pour pouvoir les suivre. Les criminels prennent connaissance de la localisation de leur cargaison et des contrôles à venir (scans, rayons X, inspections, etc.).

Étape 4 - Récupération

Les criminels utilisent leur accès aux systèmes de gestion des conteneurs pour choisir un emplacement et une heure de dépôt. Ils accèdent au conteneur avant le personnel du port et peuvent ainsi récupérer leurs cargaisons de drogues illicites.

Le principal enseignement à tirer de cette manière de procéder, c'est que la prise de contrôle des applications du système de conteneurs a commencé par l'erreur inconsciente d'un employé. Toutes les études convergent pour dire que l'ingénierie sociale et plus généralement le « facteur humain » est le principal facteur de risque en matière de cybersécurité, et que ce facteur est généralement sous-estimé. Les chiffres varient, mais le facteur humain serait le facteur clé dans au moins un cas sur deux.

Cette étude de cas démontre comment, en téléchargeant un fichier malveillant, les employés mettent en danger leur organisation et leur employeur en permettant qu'une activité criminelle soit menée à bien. Seules des formations et une sensibilisation régulière du personnel peut aider à réduire progressivement cet effet du facteur humain dans une organisation.

⁸ https://www.europol.europa.eu/sites/default/files/documents/cyberbits_04_ocean13.pdf

Scénario 3

Brouillage de l'équipement AIS

Un appareil AIS Intérieur sert à transmettre la position d'un bâtiment aux autres bâtiments alentours en utilisant la VHF. Par ailleurs, des antennes fixes positionnées le long des voies d'eaux captent ces transmissions et les acheminent jusqu'aux centres de trafic à terre, qui les utilisent pour connaître l'état du trafic et la position de chaque bâtiment. Comme ces transmissions VHF ne sont pas cryptées et ne nécessitent aucune authentification, elles sont très vulnérables aux cybermenaces.

En 2017, au moins une vingtaine de navires naviguant en mer Noire ont signalé que leur appareil AIS indiquait qu'ils se trouvaient à un endroit situé à 30 kilomètres à l'intérieur des terres⁹. Étant donné que l'émetteur-récepteur AIS a un rôle important dans la sécurité de la navigation, ce cyberincident (qui repose sur une technique de « spoofing ») a eu un impact direct sur la sécurité du bâtiment et de son équipage. Les motivations peuvent être multiples, allant du terrorisme à l'hacktivisme ou à l'activité criminelle. Les étapes d'une attaque en spoofing de ce type seraient les suivantes :



Étape 1 - Reconnaissance

Les bâtiments dont l'appareil AIS est activé sont reliés à une entreprise par une antenne ou par une connexion à distance pour la transmission de leur géolocalisation. Il est possible d'accéder à ces éléments de localisation et de positionnement en interceptant les informations relatives à la connexion ou à la transmission.

Étape 2 - Interception

Un acteur malveillant pourrait capter les signaux AIS à terre, en suivant la position du bâtiment grâce aux informations disponibles sur l'internet. L'acteur malveillant pourrait alors transmettre des signaux radio indiquant un positionnement du bâtiment destiné à confondre les récepteurs ou simplement brouiller/bloquer le signal.

Étape 3 - Action

L'acteur peut brouiller les signaux radio avec plusieurs plans d'action consistant, notamment, à envoyer une mauvaise localisation à l'appareil AIS et engendrer ainsi une représentation erronée de la position du bâtiment ou empêcher le bâtiment d'envoyer un positionnement précis. Ceci représente un risque pour la navigation.

Ce scénario de menace est particulièrement pertinent pour les ports, car le personnel portuaire s'appuie sur le positionnement émis par l'appareil AIS pour faciliter et gérer la navigation dans la zone portuaire. Les autorités portuaires transmettent également des messages spécifiques grâce aux appareils AIS. La corruption de systèmes dont la fiabilité est essentielle pourrait avoir de graves répercussions, allant au-delà des préjudices financiers et des atteintes à la réputation, en compromettant la sécurité et générant un risque de pertes humaines.

⁹ <https://www.ship-technology.com/features/ship-navigation-risks/>



Étude de cas Campagnes d'ingénierie sociale

Comme nous l'avons vu dans les exemples ci-dessus, des scénarios d'attaque très différents peuvent exploiter à un moment donné le facteur humain. Les cybercriminels le savent et exploitent presque systématiquement cette vulnérabilité pour atteindre leurs objectifs.

Les cybercriminels et les acteurs malveillants qui cherchent à réaliser une cyberintrusion s'appuient souvent sur des techniques d'ingénierie sociale pour obtenir des informations et mettre à exécution les phases initiales de leurs attaques. De manière générale, l'ingénierie sociale consiste à tenter d'amener une personne à révéler des informations par le biais d'interactions artificielles. Dans ces interactions, les acteurs malveillants utilisent souvent des stratagèmes psychologiques pour mettre en place la supercherie. Parfois, **l'ingénierie sociale** peut être réelle et non pas uniquement virtuelle. Un individu peut par exemple chercher à pénétrer un site physique en utilisant des procédés de tromperie (falsification, malhonnêteté...). L'objectif d'une campagne d'ingénierie sociale peut être d'inciter une victime à cliquer sur un lien malveillant, à fournir des informations confidentielles telles que des codes, des mots de passe ou des données privilégiées.

L'un des principaux types d'attaques en matière d'ingénierie sociale est **l'hameçonnage (phishing)**, un procédé consistant à envoyer un message (e-mail, téléphone, SMS...) comportant un piège à un (très) grand nombre de personnes dans l'espoir qu'au moins quelques-uns se laisseront berner. Lorsque le piège fonctionne, l'attaquant s'attend à un gain financier ou bien à obtenir certaines informations personnelles ou confidentielles qu'il pourra utiliser par la suite à des fins malveillantes. On parle **d'harponnage (spear phishing)** lorsque la population ciblée est plus restreinte (parfois une seule personne), mais avec un piège généralement beaucoup plus travaillé, personnalisé et donc convainquant.

Dans cette étude de cas, nous allons approfondir cinq campagnes d'hameçonnage courantes reposant sur l'ingénierie sociale : la manipulation de liens (link manipulation), l'hameçonnage par sms (smishing), l'hameçonnage vocal (vishing), la contrefaçon de site Internet (website forgery) et les fenêtres contextuelles (pop-ups).

La manipulation de liens est un procédé par lequel un acteur malveillant incite un utilisateur à cliquer sur un lien vers un site web contrefait. Il peut s'opérer par le biais d'un courriel, d'un message texte, d'une publication sur les médias sociaux ou d'un autre type de plateforme de partage. Le site en question ressemblera à une source connue ou fiable, mais aura en fait été manipulé pour servir les besoins d'un acteur malveillant.

L'hameçonnage par sms est une forme d'hameçonnage par laquelle on essaie de tromper une victime en lui envoyant des informations privées par le biais d'un message texte. La forme la plus courante d'hameçonnage par sms est un texte contenant un lien qui télécharge automatiquement un logiciel malveillant. Un logiciel malveillant installé peut voler des données personnelles telles que des identifiants bancaires, des données de géolocalisation ou des numéros de téléphone provenant de listes de contacts, dans le but de voir le virus se multiplier de manière exponentielle. Une autre tactique d'hameçonnage par sms consiste à se faire passer pour une institution légitime et bien connue afin de soutirer des informations personnelles aux victimes.

L'hameçonnage vocal (vishing) est une escroquerie vocale, ou un type d'hameçonnage partant d'un appel téléphonique ou d'une interaction humaine afin d'inciter les victimes à partager des informations telles que des informations personnelles ou privées, des mots de passe ou d'autres données personnelles. Les personnes qui appellent peuvent se faire passer pour des employés d'un organisme officiel, tel qu'une banque ou une autorité gouvernementale, mais aussi pour le service informatique ou le service RH de l'entreprise (ou du siège) ou encore pour un responsable hiérarchique, afin de gagner la confiance de la victime et obtenir les informations désirées.

La contrefaçon de sites Internet consiste à faire passer un site Internet malveillant pour un site authentique, afin d'inciter les visiteurs à divulguer leurs informations sensibles, telles que leurs coordonnées bancaires, leurs mots de passe et leurs numéros de carte de crédit.

Les fenêtres contextuelles sont un moyen intrusif de rechercher des informations en envoyant directement une fenêtre contextuelle sur l'appareil de la victime, l'incitant à saisir des informations. Souvent, lorsque la fenêtre contextuelle apparaît sur leur appareil, la victime peut aisément être amenée à fournir des informations qui sont ensuite réceptionnées par des acteurs malveillants.

Les techniques d'ingénierie sociale telles que décrites ci-dessus présentent souvent les caractéristiques suivantes :

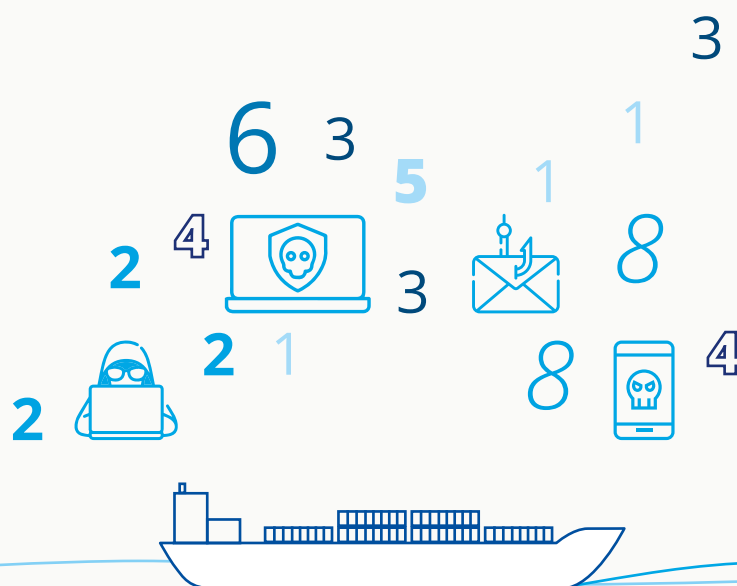
1. informations trompeuses : les URL ont souvent une apparence légèrement différente et les courriels et SMS peuvent contenir des fautes d'orthographe, étant généralement rédigés par des non-professionnels ou par des étrangers utilisant des services de traduction automatique ;
2. utilisation de formules insistant sur l'urgence : les acteurs misent sur la peur et la panique pour inciter les victimes à fournir des informations qu'elles ne divulgueraient normalement pas ;
3. promesses de récompenses attrayantes : des incitations telles que des promesses de gains ou de cadeaux sont utilisées pour susciter des interactions avec les victimes ;
4. demandes d'informations confidentielles : les informations personnelles, rarement requises par des organismes officiels, sont les objectifs de nombreuses demandes formulées dans le cadre de tentatives d'hameçonnage ;
5. pièces jointes suspectes : à travers des liens ou des fenêtres contextuelles qu'ils ont manipulés, les criminels peuvent inviter les victimes à télécharger des fichiers malveillants sur leurs appareils.

Si vous recevez un courriel d'hameçonnage ou un message qui semble suspect, les meilleures mesures à prendre sont les suivantes :

1. ne cliquez sur aucun lien et ne téléchargez aucun fichier joint au courriel ;
2. marquez le message en tant que spam ou courrier indésirable ;
3. le cas échéant, envoyez une copie du courriel ou une capture d'écran de l'adresse au responsable de la sécurité informatique de votre organisation pour l'informer de la situation et essayer d'empêcher toutes autres tentatives.

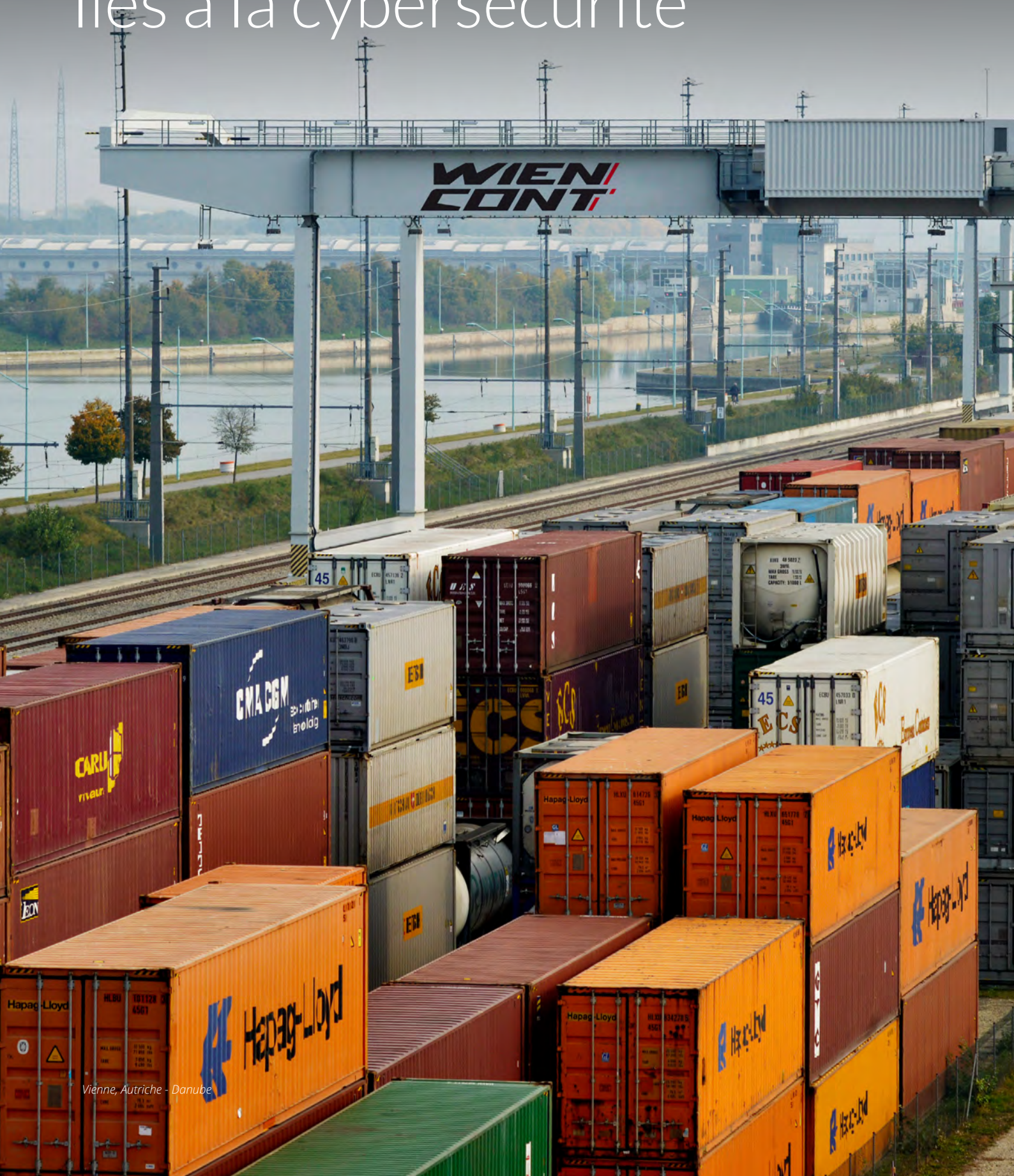
Dans le contexte des cybermenaces pour l'environnement portuaire, il est important de comprendre que la plupart des cyberattaques comptent sur le facteur humain à un moment ou à un autre de leur déroulement. C'est pourquoi les techniques d'ingénierie sociale, et en particulier les campagnes d'hameçonnage décrites ci-dessus sont très largement utilisées et doivent être prises très au sérieux. Et parfois, il suffit d'un seul employé pour compromettre l'ensemble de l'organisation.

La conclusion positive de cette étude de cas est qu'une bonne sensibilisation des employés du port, de la Direction, des fournisseurs et des autres parties prenantes « suffit » à se prémunir très efficacement de nombreuses cybermenaces. C'est une action simple, peu coûteuse et très efficace que d'informer régulièrement tous ces personnels de l'existence de stratagèmes d'ingénierie sociale et à les encourager à contribuer à préserver la sécurité en restant vigilants et mobilisés.



Partie 2

L'atténuation des risques liés à la cybersécurité



Aperçu de la réglementation et des politiques relatives à la situation des ports

À l'heure actuelle, il n'existe pas d'approche obligatoire commune visant à atténuer les risques de cybersécurité auxquels les ports sont exposés. Cela peut être attribué à la multitude des autorités réglementaires intervenant dans le secteur portuaire en navigation intérieure. Par ailleurs, l'essentiel de la réglementation existante s'applique aux ports maritimes mais n'aborde pas spécifiquement le cas des ports de navigation intérieure. C'est dans ce contexte que ce guide cherche à mettre en place un cadre pour les mesures d'atténuation des risques de cybersécurité, en comblant les lacunes que présentent les publications et l'environnement réglementaire fragmentés actuels.

Cela étant dit, il convient de mentionner – en ce qui concerne les États membres de l'Union européenne – que l'UE fournit un cadre juridique également appelé « Directive NIS » visant à stimuler le niveau global de cybersécurité dans l'UE (Directive 2016/1148 du Parlement européen et du Conseil). Cette Directive, qui est entrée en vigueur en août 2016, prévoit des dispositions particulières pour des acteurs particuliers identifiés comme « opérateurs de services essentiels ». Les opérateurs des transports par voie d'eau sont mentionnés dans la Directive, même si c'est à chaque État d'identifier ses opérateurs de services essentiels. Il est recommandé aux lecteurs de ce guide qui relèvent d'un État membre de l'UE, et qui recherchent des informations supplémentaires sur les dispositions à respecter, de se familiariser avec les sections de la Directive NIS applicables aux opérateurs de services essentiels, en particulier si les ports de navigation intérieure examinés sont considérés comme un service essentiel par leur État.

En outre, il existe une série d'autorités nationales qui publient des méthodes visant à atténuer les risques de cybersécurité pour les acteurs de la navigation intérieure. Il est recommandé aux lecteurs de se familiariser, parallèlement à la lecture de ce guide, avec les réglementations techniques et les mesures de mise en conformité qui sont applicables dans leur État.

Classification des mesures d'atténuation dans le présent guide

Aux fins du présent guide, les mesures d'atténuation visant à endiguer les risques de cybersécurité éventuels, décrits ci-dessus ont été classées dans les trois sections suivantes :

1. **Politiques et procédures organisationnelles (OPP, Organisation Policies and Procedures)**
Cette section regroupe les recommandations relatives à la structure organisationnelle, aux rôles et responsabilités, aux mesures de gouvernance ainsi qu'aux politiques organisationnelles pouvant être mises en œuvre pour renforcer la maturité en matière de cybersécurité d'un port.
2. **Politiques en matière de technologies de l'information/ technologies opérationnelles pour les ports**
Cette section examine les politiques pouvant être mises en œuvre pour sécuriser les actifs identifiés dans la Partie 1.
3. **Mesures techniques de cybersécurité pour les ports (TSM, Technical Security Measures)**
Cette section vise à donner un aperçu général des mesures de sécurité de base pouvant être mises en œuvre par le personnel informatique des ports pour sécuriser l'infrastructure informatique.

Chacune de ces sections a pour but de donner un aperçu général des mesures d'atténuation à envisager par un port, mais elles ne sauraient remplacer les exigences requises en matière de cybersécurité dans le cadre d'un audit ou d'une réglementation publiée par des agences de certification, des États ou d'autres organismes de réglementation.

Les mesures d'atténuation proposées ont été classées dans l'ordre croissant du niveau de maturité en matière de cybersécurité. Les mesures figurant au début de chaque tableau ci-dessous devraient être les premières à être mises en place dans une démarche de prise en compte de la cybersécurité. Puis, au fur et à mesure que ces mesures sont mises en place et que la maturité en matière de cybersécurité augmente, les mesures suivantes peuvent être, à leur tour, mises en œuvre. Un code couleur a été utilisé pour identifier le niveau de maturité de chaque mesure :

-  Niveau de maturité : **faible**
-  Niveau de maturité : **moyen**
-  Niveau de maturité : **fort**

Pour de plus amples informations sur ces classements, veuillez vous référer au cadre d'évaluation de la maturité figurant à la Partie 3.



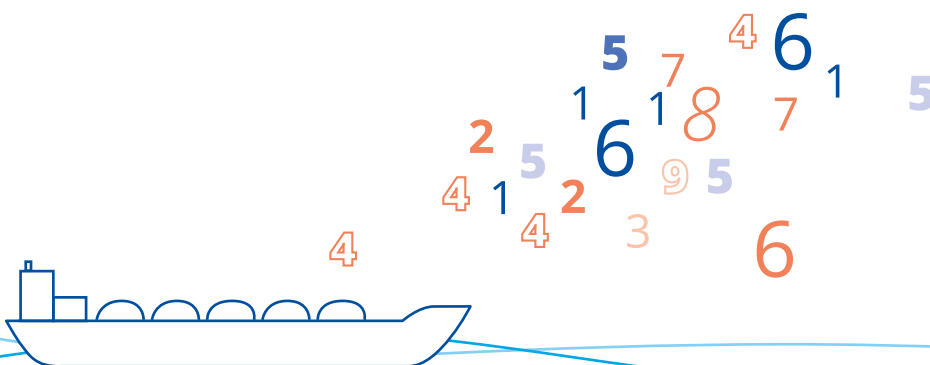
Politiques et procédures organisationnelles

Cette section donne un aperçu des politiques et procédures organisationnelles qui peuvent être mises en œuvre pour une organisation mature en termes de cybersécurité. Ces mesures peuvent être mises en œuvre par le responsable de la sécurité informatique du port ou, dans le cas d'un port de taille plus modeste, par un directeur ou un autre responsable. Ces mesures sont d'application générale, mais leur ampleur, leur profondeur et leur portée peuvent varier en fonction des différentes ressources dont disposent le port.

Rôles et responsabilités

L'attribution de rôles et de responsabilités clairs est la première étape de la responsabilisation visant à renforcer la maturité d'une organisation en termes de cybersécurité. Les ports devraient mettre en œuvre les mesures suivantes pour couvrir ce volet.

Numéro	Mesure
● [OPP] 1.1	La Direction doit intégrer les aspects de cybersécurité dans ses priorités et fournir les moyens et ressources adéquats pour mettre en œuvre les mesures appropriées, par exemple celles proposées dans ce guide. La Direction doit commencer par identifier un point de contact pour l'ensemble des mesures de cybersécurité ; les coordonnées et le rôle de cette personne devraient être largement diffusés à l'ensemble du personnel et des sous-traitants. La Direction doit garder en tête que si elle peut déléguer la mise en œuvre en matière de cybersécurité, elle ne peut toutefois pas déléguer sa responsabilité.
●● [OPP] 1.2	Une charte générale de la cybersécurité, énonçant clairement ce qui est attendu de l'ensemble du personnel, devrait être rédigée et signée par le personnel et les parties prenantes portuaires.
●●● [OPP] 1.3	Une stratégie générale de cybersécurité ou une politique de sécurité des systèmes informatiques devrait être définie et approuvée par la direction.
●●● [OPP] 1.4	La stratégie de cybersécurité devrait définir clairement les rôles de chaque partie prenante portuaire (autorité portuaire, opérateurs de terminaux, prestataires de services, fournisseurs, etc.)
●●● [OPP] 1.5	Tous les aspects de sécurité concernant des partenariats avec des tiers devraient être définis et documentés, en particulier pour les systèmes critiques fournis par des tiers.
●●● [OPP] 1.6	La stratégie en matière de cybersécurité devrait être régulièrement revue et mise à jour à la suite de chaque évaluation de risques, mise à jour organisationnelle ou incident de sécurité.



Processus organisationnels

Une fois les rôles et responsabilités clarifiés, la seconde étape est de disposer d'une documentation de référence étayant les processus et exigences visant à assurer la continuité du service, à se conformer à certaines réglementations en matière de sécurité et à garantir une bonne transmission des informations en cas de réorganisation des services au sein du port.

Numéro	Mesure
● [OPP] 2.1	Une évaluation complète du port devrait être réalisée afin d'identifier les principaux actifs, classés par ordre de criticité.
● [OPP] 2.2	Les exigences de base en matière de cybersécurité pour les fournisseurs concernés devraient être documentées et communiquées aux fournisseurs. Des clauses contractuelles standards relatives à la cybersécurité pourraient par exemple être rédigées puis utilisées dans tous les contrats avec des fournisseurs. La conformité vis-à-vis de ces exigences devrait être contrôlée par des employés compétents du port ou par une tierce partie de confiance dont c'est le rôle exclusif.
● [OPP] 2.3	Les antécédents des personnes devant occuper des postes de direction clés ou exercer des fonctions informatiques importantes (administrateurs système, opérateurs informatiques/techniques) devraient faire l'objet d'une vérification avant de procéder à leur recrutement. La preuve de ce contrôle devrait être conservée dans le dossier pour pouvoir, si nécessaire, la présenter aux autorités réglementaires.
●● [OPP] 2.4	Les dépendances et les flux d'information des actifs identifiés ci-dessus devraient également être documentés.
●● [OPP] 2.5	Une évaluation des risques correspondante devrait être réalisée pour identifier les risques de cybersécurité liés à chaque actif. La direction devrait veiller à ce qu'il soit procédé à une évaluation du risque en matière de cybersécurité pour chaque nouveau projet ou initiative, en particulier ceux qui font appel à de nouvelles technologies.
●●● [OPP] 2.6	Les actifs du port devraient régulièrement faire l'objet d'audits internes et externes de cybersécurité et d'évaluations de conformité. La fréquence et la nature (interne/externe) de ces audits et évaluations est à déterminer par la direction. Le port pourrait envisager d'automatiser certains audits techniques, lorsque c'est possible. Pour les ports qui ont développé des logiciels spécifiques, il est par exemple possible de prévoir une analyse régulière du code source avec des outils spécialisés pour chercher d'éventuelles vulnérabilités ou failles de sécurité connues.
●●● [OPP] 2.7	Les modalités de cybersécurité définies et appliquées devraient être documentées, validées et régulièrement révisées. Les sujets suivants sont susceptibles de faire l'objet de décisions écrites (la liste n'étant pas limitative) : • Mesures de cybersécurité en place pour sécuriser les portails et services web ; • Mesures de cybersécurité pour les liaisons de réseau ou de communication (y compris technologies de communication sans fil) ; • Mesures de cybersécurité pour la configuration logicielle ; • Exigences et les règles applicables à la connexion des appareils à l'environnement informatique (y compris la connexion d'appareil personnels) ; • Mesures relatives aux mises à jour logicielles et à la gestion des changements (lorsque ITIL est mis en œuvre) ; • Règles relatives à l'utilisation des radios mobiles personnelles ; • Règles concernant l'utilisation adéquate de l'infrastructure informatique par le personnel, en conformité avec la charte générale de cybersécurité ; • Configuration et gestion des privilèges des comptes utilisateurs et systèmes, y compris ceux du personnel tiers ayant accès aux systèmes portuaires (tels que l'alimentation, le chauffage, l'électricité, etc) ; • Processus de gestion de crise et d'incidents de cybersécurité.

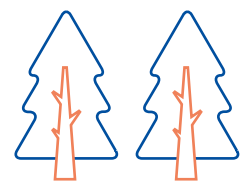
Sécurité physique

Dans le contexte de la cybersécurité, on parle de « sécurité physique » lorsqu'il est utile ou nécessaire de protéger physiquement des équipements informatiques. La « sécurité physique » est souvent opposée à la « sécurité logique » qui consiste à protéger les équipements informatiques du point de vue des accès au travers de logiciels ou du réseau. Toutefois, la sécurité physique est une dimension à part entière de la cybersécurité car elle peut entrer en jeu dans de très nombreux scénarios d'attaque. Le simple accès à un bouton marche/arrêt peut suffire à mettre hors service un serveur tout comme l'accès

à un port USB permet d'introduire des logiciels malveillants en ignorant les protections réseau. La sécurité physique prend en compte également la sécurité incendie ou la protection contre les surtensions ou les coupures de courant.

Des exigences en matière de sécurité physique devraient être prises en compte lors de la création d'un plan de cybersécurité. Les infrastructures informatiques critiques peuvent être vulnérables si elles restent accessibles à des personnes extérieures susceptibles d'être animées d'intentions malveillantes. Aussi les plans de cybersécurité devraient-ils prendre en compte les risques découlant des atteintes à la sécurité physique.

Numéro	Mesure
● [OPP] 3.1	La direction du port devrait définir des règles claires en matière de sécurité physique et mettre en œuvre des mesures de contrôle de l'accès physique afin d'éviter qu'il ne soit possible d'accéder aux systèmes sensibles du port et qu'ils soient exposés à des risques de vol et de dégradation. La liste de ces systèmes sensibles devrait être dressée et validée au préalable par la direction.
● [OPP] 3.2	Outre la protection des systèmes sensibles le port devrait protéger les équipements collectifs, (y compris les systèmes de chauffage, de ventilation et de refroidissement), contre les personnes non autorisées à l'aide de barrières de contrôle d'accès physique ou de portes verrouillées.
● [OPP] 3.3	Tous les accès physiques autorisés au port devraient être enregistrés et vérifiés au moins une fois par an.
●● [OPP] 3.4	Une procédure engagée en cas d'intrusion physique et l'intervention correspondante de membres du personnel du port et d'agences externes mis à disposition en conséquence, ainsi que la réponse apportée à l'événement, devraient être documentées et notifiées.
●● [OPP] 3.5	La question de savoir dans quelle mesure certaines zones portuaires sont accessibles à des tiers ou au public devrait être documentée et évaluée pour s'assurer que le risque pris est acceptable.
●● [OPP] 3.6	Une politique de contrôle d'accès physique devrait fournir des procédures étape par étape pour les opérations de sécurité critiques telles que la collecte des badges des membres du personnel qui partent, la mise à jour des codes d'alarme, la gestion des images de vidéosurveillance, etc.



Réponse apportée aux incidents et gestion de crise

Des politiques et procédures claires devraient être définies et mises en œuvre en cas d'incident ou de crise de cybersécurité.

Dans le cadre de ce guide, la distinction est faite entre les **incidents de cybersécurité** (situations pouvant être réglées

par le personnel informatique et/ou de la sécurité sans devoir remonter au niveau supérieur ni le consulter) et les **crises de cybersécurité** (situations de plus grande ampleur entravant le fonctionnement du port et nécessitant l'intervention de la direction).

Numéro	Mesure
 [OPP] 4.1	Le port devrait disposer d'un plan de gestion des incidents, validé par la direction, fondé sur la compréhension des causes à l'origine de perturbations de la cybersécurité applicables à son environnement, sur les systèmes essentiels recensés dans l'inventaire des actifs critiques et sur les ressources et capacités dont il dispose.
 [OPP] 4.2	Le port devrait disposer d'un plan de gestion de crise, validé par la direction, comprenant une présentation détaillée de la prise de décision et de la procédure à suivre en matière de communication lors d'incidents et dans le cas où un incident virerait à la crise.
 [OPP] 4.3	Le plan de gestion de crise devrait prévoir, le cas échéant, la communication et la concertation avec les autorités nationales.
 [OPP] 4.4	Le plan de gestion de crise devrait, si nécessaire, inclure une procédure de communication avec les parties concernées et les victimes de cyberincidents.
 [OPP] 4.5	Le personnel en charge de la gestion des incidents au sein du port devrait suivre l'actualité du secteur pour se tenir informés des incidents potentiels de cybersécurité subis par leurs pairs ; et il conviendrait de définir une procédure de collecte de renseignement sur les menaces afin de recueillir des informations pertinentes sur les menaces pour la sécurité auxquelles sont confrontés les ports.
 [OPP] 4.6	Le plan de gestion des incidents devrait donner une définition précise de ce qu'est un incident de cybersécurité, les rôles et responsabilités à assumer que recouvrent la gestion d'un incident, et le processus indiquant en détail quand un incident se transforme en crise.
 [OPP] 4.7	Il conviendrait de définir un plan de continuité des activités pour garantir la poursuite des opérations portuaires en cas de crise ou d'incident. Ce plan devrait comprendre des objectifs clairs. Il inclut des paramètres importants pour la continuité des activités portuaires, telles qu'un objectif de délai de reprise (RTO), un objectif de point de reprise (RPO), une durée maximale d'interruption tolérable (MTO) et un objectif de continuité minimale des activités (MBCO).
 [OPP] 4.8	Le plan de gestion de crise devrait inclure une phase d'analyse post-incident pour déterminer la cause de l'incident.
 [OPP] 4.9	Les processus définis pour faire face aux incidents ou aux crises devraient être régulièrement évalués et testés, éventuellement par des simulations de crise ou des exercices théoriques. Celles-ci devraient être étendues à autant de parties prenantes que possible afin de garantir la préparation tout au long de la chaîne d'approvisionnement.
 [OPP] 4.10	À la suite d'incidents de cybersécurité significatifs (sortant du commun ou ayant eu un impact opérationnel), la Direction devrait veiller à ce que les incidents soient signalés et les informations partagées afin que le secteur puisse en tirer des enseignements.
 [OPP] 4.11	Le port pourrait envisager la mise en place d'un centre chargé des opérations de cybersécurité (SOC) pour renforcer la sécurité et gérer les cyberincidents.

Plans cybersécurité : différents documents liés à la cybersécurité sont abordés dans les mesures ci-dessus, qui peuvent être considérés indépendamment, mais qui forment au final un ensemble cohérent :

- plan de gestion des incidents ;
- plan de gestion des crises ;
- plan de continuité des activités.

La « politique de sécurité » est un autre document (abordé dans les niveaux de maturité élevés des mesures « Rôles et responsabilités » développées plus haut), dont une partie est dédiée à expliquer comment ces différents plans doivent être mis en œuvre, révisés et testés.

Formation et sensibilisation

Les activités de formation et de sensibilisation s'adressant à toutes les parties prenantes sont cruciales pour la diffusion des bonnes pratiques en matière de cybersécurité. En effet, comme expliqué en première partie de ce guide, l'exploitation par le

cybercriminel du facteur humain est essentielle, en pratique, à la plupart des scénarios d'attaque de la vie réelle. Les mesures suivantes peuvent contribuer à réduire le risque lié au facteur humain en sensibilisant le personnel au rôle clé qu'il joue dans la cybersécurité.

Numéro	Mesure
 [OPP] 5.1	Le personnel devrait être sensibilisé à la prudence dont il faut faire preuve en ce qui concerne les courriels. Les points suivants devraient être soulignés : • Vérifier l'identité de l'expéditeur ; • Ne pas ouvrir les pièces jointes et ne pas cliquer sur les liens Internet provenant d'expéditeurs suspects ou inconnus.
 [OPP] 5.2	Le port devrait définir une politique de gestion des mots de passes. Cette politique doit comporter une dimension pédagogique pour sensibiliser le personnel à l'utilisation de mot de passe forts. Elle doit aussi préciser les règles applicables en matière de renouvellement des mots de passes. Cette politique doit être différenciée entre les mots de passe individuels des utilisateurs et les mots de passes liés à des comptes systèmes ou administrateurs qui peuvent être partagés pour raison de service, ou utilisés par des programmes.
 [OPP] 5.3	Le personnel devrait être sensibilisé à l'utilisation judicieuse des réseaux sociaux, des forums, des formulaires, etc., en particulier lorsqu'il s'agit d'informations relatives au port.
 [OPP] 5.4	Le personnel devrait être sensibilisé à l'installation de programmes et de logiciels. L'obligation de soumettre le téléchargement de logiciels à l'approbation des administrateurs du port devrait être communiquée expressément.
 [OPP] 5.5	Le personnel devrait être sensibilisé à l'utilisation du Wi-Fi, de la 4G/5G et des réseaux sécurisés : lors d'un déplacement professionnel, il devrait se montrer prudent vis-à-vis des réseaux Wi-Fi publics.
 [OPP] 5.6	Il convient d'instaurer, pour le personnel, une règle consistant à séparer les utilisations personnelle et professionnelle et à travailler sur ses propres appareils (« apportez votre équipement personnel de communication » - BYOD) et de bien communiquer à cet égard
 [OPP] 5.7	Le port devrait définir un programme périodique de sensibilisation à la cybersécurité pour tout le personnel, portant sur l'hygiène générale de base en matière de cybersécurité.
 [OPP] 5.8	Le port devrait définir un programme de formation à la cybersécurité afin de développer les compétences en matière de cybersécurité des membres du service informatique et du personnel chargé des actifs informatiques et/ou technologiques.
 [OPP] 5.9	Tous les membres du personnel utilisant des machines connectées devraient être formés aux pratiques de base en matière d'hygiène de cybersécurité informatique et/ou technologique.

Qu'est-ce qu'un « mot de passe fort » ?

Un mot de passe fort est un mot de passe difficile à deviner par un humain ou par un ordinateur. Mais attention : les humains programment des ordinateurs pour essayer des milliers de mots de passe chaque seconde. Alors comment faire ? La plupart des systèmes proposent des règles de « complexité » des mots de passe (nombre de caractère minimum, lettres, chiffres, caractères spéciaux, etc.). C'est un bon début, mais ce n'est pas suffisant car il est possible de créer un mot de passe faible qui respecte ces règles. Par exemple « P@sswOrd ». Parmi les bonnes pratiques, on peut noter qu'un mot de passe doit être suffisamment long (au moins 8, voire 10 caractères) et ne doit pas être basé sur un

mot du dictionnaire, même de façon lointaine. Il ne doit pas non plus être lié à la disposition du clavier (« qwerty », « azerty », « 123456 », etc.) ou lié directement à son utilisateur (date de naissance, prénom des enfants, etc.). Les bonnes pratiques actuelles tendent à développer l'utilisation d'une authentification « multi-facteurs », c'est-à-dire à compléter le mot de passe par un autre moyen d'authentification (par exemple un code à usage unique envoyé par SMS, email ou sur une application smartphone). La politique de gestion de mots de passe citée à la règle [OPP] 5.2 devrait détailler les règles et recommandations à suivre en la matière.



Étude de cas Programmes de sensibilisation pour le personnel

Ce guide souligne le rôle dévolu à l'ensemble du personnel, des fournisseurs et des autres parties prenantes pour assurer la cybersécurité des ports. Comme le montrent les scénarios d'attaques évoqués en Partie 1 de ce guide, de nombreux incidents de cybersécurité sont dus à des erreurs humaines. Dans ces conditions, la mise en œuvre d'un programme de sensibilisation du personnel est une mesure d'atténuation essentielle et « à effet rapide » (« quick-win »), qui peut être adoptée par les ports pour renforcer leur position en matière de cybersécurité. Pour faciliter cette tâche, cette étude de cas donne un aperçu des étapes que recouvre le lancement d'un programme de sensibilisation à la cybersécurité, détaille les types de modules qui peuvent être inclus dans ce programme et présente quelques facteurs clés de réussite pour son exécution.

Vue d'ensemble des étapes

Étape 1

Définir une référence de base pour le niveau actuel de sensibilisation à la cybersécurité au sein du port. L'évaluation du niveau de maturité actuel au sein du port permettra à ses dirigeants de comprendre où le programme de sensibilisation devrait commencer, d'identifier les points d'attention particuliers à traiter par le programme, et fournira un niveau de maturité bien défini à partir duquel il sera possible de suivre les progrès réalisés après les sessions de sensibilisation. Cela pourrait se faire à l'aide d'un questionnaire ou d'une autre méthode d'enquête informelle envoyée au personnel du port.

Étape 2

Rédiger une stratégie de sensibilisation à la cybersécurité pour le port. Cette stratégie devrait s'appuyer sur des objectifs tangibles, un calendrier réaliste, une répartition des rôles et des responsabilités, ainsi qu'un budget correspondant. Pour garantir le déploiement efficace d'un programme, il convient d'obtenir l'adhésion de la direction lors de la présentation de cette stratégie.

Étape 3

Sélectionner le format des modules de sensibilisation à mettre en œuvre. Une campagne de sensibilisation peut s'étendre d'un cours obligatoire à des webinaires, des exercices de formation, des exercices de phishing, etc. Le module de sensibilisation spécifique devrait être sélectionné pour répondre aux critères

définis dans la stratégie, notamment en ce qui concerne le budget et le calendrier dont dispose le port. Les programmes de sensibilisation peuvent également être conçus en collaboration avec des experts externes si l'organisation ne dispose pas des compétences nécessaires pour concrétiser une telle initiative. Ils peuvent aussi être adaptés à l'utilisation privée de l'informatique à domicile par les employés.

Étape 4

Déployer le programme de sensibilisation.

Étape 5

Documenter les résultats. Pour satisfaire à des exigences réglementaires ou pour les besoins du développement du port, il convient de recueillir des retours d'information auprès des participants au programme de sensibilisation. Un résumé des objectifs de sensibilisation abordés et atteints par ce programme devrait être documenté et sauvegardé. En outre, les organisations devraient veiller à s'améliorer en permanence en prenant note des bons résultats et des améliorations potentielles du programme de sensibilisation.

Étape 6

Planifier la prochaine itération. Pour être efficaces, les programmes de sensibilisation devraient être mis à jour et renouvelés à mesure que le port évolue. Une date cible devrait être visée pour cette deuxième phase, en accord avec la direction.

Types de modules pouvant être inclus dans les programmes de sensibilisation

Les programmes et initiatives de sensibilisation peuvent prendre de nombreuses formes et être adaptés en fonction des besoins du port. Les principaux types de modules correspondant au programme de sensibilisation sont détaillés ci-dessous.

Type de module de sensibilisation	Breve description	Avantage(s) majeur(s)	Inconvénient(s) majeur(s)
Cours en présentiel ou virtuels	Les cours de sensibilisation sont dispensés sous forme de session en temps réel avec un instructeur et un format de cours donné.	- Un instructeur dédié pour s'assurer de la compréhension et répondre aux questions. - La présence et l'attention portée au contenu peuvent être contrôlées.	- Exige beaucoup de temps et de ressources, impliquant une assiduité pendant les heures de travail. - Solution coûteuse.
Sessions d'apprentissage en ligne	Les cours sont dispensés automatiquement via une plateforme en ligne, généralement en format vidéo.	- Les cours de sensibilisation en ligne sont aujourd'hui largement disponibles, certains même gratuitement. - Les parties prenantes peuvent suivre des formations en ligne.	Il est difficile de vérifier l'assiduité et le degré d'attention des participants.
Jeux sérieux	Les parties prenantes « jouent » à un jeu en ligne ou mobile, conçu pour renforcer leur sensibilisation à la cybersécurité, et rendent ensuite compte des principaux éléments à retenir et des enseignements tirés.	- Les moyens ludiques et variés utilisés pour transmettre des informations permettent de capter l'attention et d'en faire une expérience marquante pour les parties prenantes. - La diffusion de cette formation exige moins d'implication de la part des personnes qui suivent la formation de sensibilisation.	- Une planification détaillée est nécessaire pour sélectionner un jeu sérieux, le configurer pour qu'il réponde aux besoins de l'organisation et mettre en œuvre le programme de sensibilisation. - Il est difficile de vérifier le degré d'attention et de s'assurer que le « jeu » a été mené à terme.
Exercices d'hameçonnage	Exercice de simulation au cours duquel un courriel d'hameçonnage est envoyé aux personnels du port ; les personnes qui se font piéger pendant l'exercice d'hameçonnage sont localisées et généralement redirigées vers un module de formation.	- Une expérience tangible qui reste gravée dans l'esprit de ceux qui ne réussissent pas le test. - Documentation et statistiques sur les types de parties prenantes qui se font piéger par les courriels d'hameçonnage.	- Ne couvre qu'un seul aspect de la cybersécurité : l'hameçonnage. - Ne garantit pas que ceux qui réussissent le test soient davantage sensibilisés, et ne permet pas non plus de savoir si un exercice « réussi » peut être considéré comme tel ou si le courriel a simplement échappé à leur attention.
Simulation de campagne de logiciels malveillants	Personnalisation des campagnes de sensibilisation aux logiciels malveillants afin d'évaluer le niveau de sensibilisation du personnel aux dispositifs et connexions externes. Ces campagnes présentent les mêmes caractéristiques que les campagnes d'hameçonnage, à la différence qu'elles diffusent des logiciels malveillants. Les scripts des logiciels malveillants ne sont pas persistants. Ils capturent uniquement les données en temps réel de la victime et du système.	- Une expérience concrète qui reste gravée dans l'esprit des participants. - L'effet « exercice d'incendie », qui permet de simuler une crise afin d'améliorer les performances de l'organisation en cas de crise réelle.	- La planification et l'exécution de cette simulation exigent beaucoup de temps et de travail. Peut nécessiter le concours d'une entreprise extérieure. - Des problèmes de confiance potentiels peuvent être engendrés chez les personnels qui ont été soumis à ce test et se sont laissés piéger.
Matériel pédagogique	Diffusion mensuelle de récits décrivant de réelles attaques contre des organisations, les problèmes de sécurité rencontrés, l'impact de ces attaques, les solutions appliquées et les enseignements tirés. Peut également inclure des sujets illustrant la tendance du secteur en matière de sécurité.	- Conception et distribution relativement simples : diffusion par courrier électronique. - Flashs d'information récurrents permettant aux parties prenantes de rester à jour.	Difficile de vérifier dans quelle mesure ces flashs d'information s'avèrent probants : certaines parties prenantes peuvent tout simplement ignorer ou contourner les communications.
Événements	Événement (petit-déjeuner, déjeuner et formation, etc.) organisé pour lancer une discussion ou une démonstration sur un sujet de sensibilisation à la cybersécurité.	- Regroupe les parties prenantes de l'organisation en une seule session et permet l'échange d'informations et la discussion. - Conception et exécution relativement simples.	- Interaction de courte durée. - Plus difficile de déterminer, à partir d'un événement, les enseignements qui ont été tirés et dans quelle mesure la sensibilisation a augmenté.

Facteurs clés de la réussite d'un programme de sensibilisation

1. Alignement du programme de sensibilisation sur des questions et défis opérationnels.

Un programme de sensibilisation adapté aux problèmes opérationnels rencontrés par le port aura un impact plus important et sera donc plus efficace. Un programme de sensibilisation devrait se concentrer spécifiquement sur les systèmes critiques du port et sur les impacts potentiels des événements de cybersécurité.

2. Faire participer autant de parties prenantes que possible

La participation du plus grand nombre possible de parties prenantes, y compris les tiers et les fournisseurs, garantira la diffusion des connaissances et de la sensibilisation tout au long de la chaîne d'approvisionnement. Cette notion revêt une importance particulière pour les ports, compte tenu du nombre important de tierces parties incluses dans les activités portuaires.

3. Mesure de l'impact et des progrès

La meilleure façon d'évaluer l'efficacité d'une campagne de sensibilisation est de proposer une sorte de contrôle des connaissances ou d'évaluation à la fin du module. Cela peut prendre la forme d'un bref sondage ou d'un questionnaire distribué aux participants.



Coblence, Allemagne - Rhin



Étude de cas

Élaboration d'une évaluation des risques liés à la cybersécurité

Pour pouvoir mettre en œuvre la plupart des mesures d'atténuation décrites ci-dessus, telles que la mise en œuvre d'une stratégie de cybersécurité, il est nécessaire d'identifier les actifs à protéger. Pour identifier ces actifs, les ports devront, à un moment ou à un autre, procéder à une évaluation des risques de cybersécurité. Cet exercice permettra de produire les éléments constitutifs d'une stratégie solide en matière de cybersécurité. En effet, les bonnes pratiques actuelles privilégient les approches axées sur les besoins, la compréhension des processus et l'identification des actifs critiques, plutôt que sur la conformité à des normes communes qui correspond aux approches antérieures. L'étude de cas suivante présente les étapes génériques d'une évaluation approfondie des risques de cybersécurité pour un port et met en évidence certains facteurs clés de réussite identifiés au cours de l'évaluation.

Vue d'ensemble des étapes

Étape 1

Identifier les actifs du port et les impacts potentiels des événements de cybersécurité sur ces actifs

- Identifier les principales opérations portuaires et les actifs nécessaires à la réalisation de ces opérations. Veiller à inclure une série d'actifs, tels que les systèmes de contrôle, les systèmes de gestion technique de bâtiment, les salles de contrôle, les outils de vidéosurveillance/alarme, les systèmes de navigation communiquant avec les bâtiments, les voies de câblage, les systèmes portuaires utilisés pour la planification et la réception des cargaisons, ainsi que les données collectées et stockées par les ports.
- Définir un critère de criticité pour les actifs : quelles sont les opérations les plus critiques ? De quels actifs la mise en œuvre de ces opérations dépend-elle ? Certains de ces actifs sont-ils communs à plusieurs processus opérationnels et donc essentiels aux opérations portuaires ?
- Pour les actifs des ports, documenter les systèmes qui les soutiennent. Noter si ces systèmes sont connectés à l'Internet ou s'ils dépendent d'une source d'énergie particulière.
- À partir d'un échantillon de ces actifs, définir les impacts potentiels sur l'activité au cas où l'intégrité ou la disponibilité de ces actifs seraient compromises.
- **Produit final clé** : une liste de tous les actifs des ports. Pour chacun d'entre eux, indiquer un impact majeur sur l'activité au cas où cet actif/ce dispositif était compromis. Bien sûr, ce produit final devrait être protégé et rester strictement confidentiel, compte tenu de sa sensibilité.

Étape 2

Exposer en détail les processus métiers portuaires

- Définir les processus métiers et les actifs sur lesquels ils s'appuient pour fonctionner.
- Documenter les flux d'informations et les échanges de données nécessaires au fonctionnement de ces processus. Cela permettra de déterminer les types d'interactions essentielles à la conduite des opérations qui pourraient avoir de graves répercussions sur l'activité si elles étaient interrompues.
- **Produit final clé** : un diagramme des flux de données et d'information pour les trois principales activités assurées par le port. Ce produit final devrait également être protégé et rester strictement confidentiel.

Étape 3

Identifier les menaces pour la sécurité

- Identifier les menaces possibles pour les actifs identifiés à l'étape 1. Les données relatives aux menaces peuvent être réunies sur la base des recherches existantes consacrées aux menaces de cybersécurité, qui sont pertinentes pour l'environnement portuaire (comme celles décrites ci-dessus), ou peuvent être établies en se livrant à des recherches plus exhaustives sur les menaces. Cette opération n'a pas besoin d'être très élaborée : une liste standard de menaces peut être définie, et ces menaces peuvent être associées aux actifs portuaires pour générer une liste complète des menaces pertinentes pesant sur un port.
- **Produit final clé** : un rapport contenant des renseignements sur les principales menaces auxquelles le port est confronté.

Étape 4**Évaluer la faisabilité et la probabilité de l'exploitation de ces menaces**

- Attribuer une estimation de faisabilité à chaque menace. Cette estimation peut être établie à partir de paramètres tels que la connaissance préalable requise des systèmes pour pouvoir générer la menace, la nécessité d'avoir un accès physique ou le niveau de privilège nécessaire pour exécuter des opérations spécifiques, le niveau d'interaction avec l'utilisateur nécessaire pour obtenir des privilèges, la complexité technique requise pour l'opération ainsi que la capacité du port à surmonter cette menace grâce à des modes de fonctionnement résilients (éventuellement en mode dégradé).
- Attribuer un profil d'attaquant à chaque menace afin de vérifier la réalité de son exécution. Les profils des attaquants peuvent être définis en évaluant le niveau de compétence que doit posséder l'attaquant pour pouvoir exploiter la menace, la motivation/récompense associée à son exploitation, la quantité de ressources requises et les connaissances/informations requises.
- Croiser le profil de l'attaquant avec les informations de faisabilité afin de générer, pour chaque menace, un score de probabilité d'exploitation.
- **Produit final clé** : une liste des principales menaces comprenant le score de faisabilité et de probabilité qui leur est associé.

Étape 5**Corréler la probabilité et l'impact des menaces sur les actifs vulnérables**

- À l'aide d'un tableau, mettre en corrélation l'impact sur l'activité que peut avoir une attaque contre un actif du port et la probabilité qu'une telle menace soit exploitée. Cela permet d'isoler les risques critiques (ceux dont les impacts et la probabilité sont élevés).
- L'évaluation des risques est à présent terminée, et la Direction devrait avoir une idée précise des principaux risques de cybersécurité auxquels le port est aujourd'hui confronté. Ces risques peuvent être utilisés pour hiérarchiser les mesures de sécurité à prendre ou pour élaborer une stratégie de cybersécurité organisationnelle à grande échelle.
- **Produit final clé** : tableau bidimensionnel (faisabilité/probabilité) incluant les menaces et permettant dans une étape suivante de prévoir les mesures nécessaires.

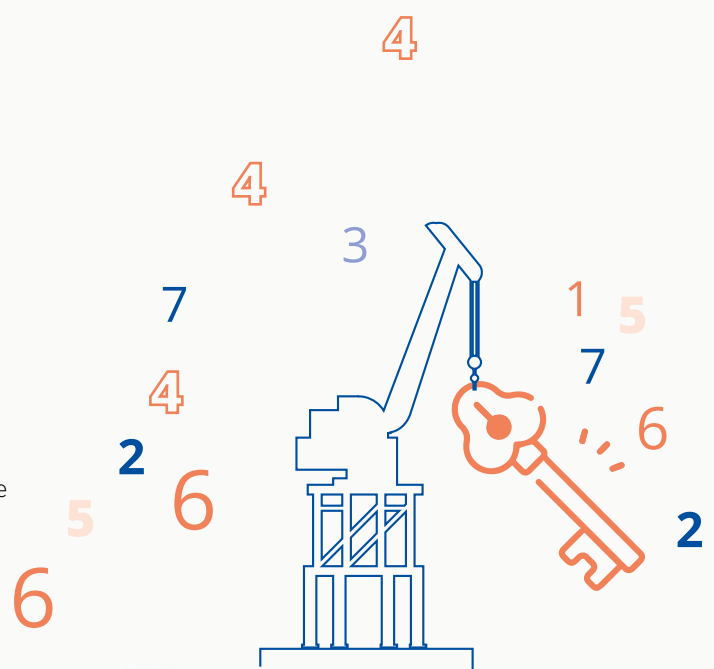
Facteurs clés de la réussite d'une évaluation des risques

- **Importance des menaces par rapport à l'activité**

Les menaces faisant l'objet de l'évaluation devraient s'inscrire dans le contexte de l'activité portuaire. Plus précisément, aux fins d'une évaluation pertinente des menaces, les ports devraient se concentrer sur celles auxquelles leur secteur est confronté aujourd'hui, peut-être en s'appuyant sur des rapports contenant des renseignements sur des menaces sectorielles spécifiques, en partageant des informations avec leurs pairs ou en participant à des groupes de travail sur la cybersécurité organisés par leur secteur.

- **Point de vue indépendant et objectif sur les impacts potentiels**

En procédant à une auto-évaluation, le défi consiste à mettre de côté ses convictions quant à ses capacités et à son organisation pour porter un jugement objectif sur les impacts potentiels d'une cyberattaque. Il est essentiel de rappeler que les analyses d'impact ont pour objectif de déduire de façon argumentée et factuelle l'impact potentiel qu'un cyberincident pourrait avoir sur un actif, et non pas à faire un sondage d'opinion sur son impact supposé. En effet, prendre des mesures pour limiter un impact supposé pourrait conduire à réaliser des travaux très lourds et très coûteux, et néanmoins inutiles car reposant sur des hypothèses infondées ou mal calibrées.



Politiques en matière de technologies de l'information (IT) et de technologies opérationnelles (OT) pour les ports

Cette section, applicable aux ports et à leurs fournisseurs, est consacrée aux bonnes pratiques de portée générale en matière de sécurité des systèmes IT/OT. Pour mémoire, le terme IT/OT est défini dans la Partie « Introduction » de ce guide. Pour simplifier, l'IT correspond à des systèmes qui s'intéressent au traitement des données tandis que l'OT correspond à des systèmes dont l'objectif est d'interagir avec des objets physiques. Ces deux types de systèmes peuvent bien entendu être en interaction, et c'est en particulier le cas lorsqu'on parle de « systèmes IT/OT ».

Cette section s'adresse donc aux parties prenantes des ports qui utilisent les systèmes opérationnels et les équipements que l'on peut y trouver. Les systèmes IT/OT peuvent varier d'un port à un autre, mais ces systèmes sont généralement considérés comme exécutant des tâches opérationnelles ou physiques, commandés par un ordinateur ou une passerelle connectée. Dans le contexte des ports, il peut s'agir, entre autres, et de manière non restrictive :



- systèmes de contrôle du trafic portuaire (suivi du trafic gestion des postes à quai, outils de surveillance météorologique) ;



- d'appareils de navigation communiquant avec les réseaux portuaires (AIS, GNSS) ;



- de systèmes de gestion des opérations du terminal (matériel d'exploitation, systèmes de transbordement et d'entreposage, systèmes d'exploitation de terminal) ;



- de systèmes de sécurité et de sûreté : contrôle d'accès, détecteurs d'intrusion, systèmes de surveillance et autres systèmes d'alerte.

Les systèmes IT/OT sont particulièrement pertinents pour la cybersécurité d'un port, étant donné qu'ils sont de plus en plus connectés, notamment par l'adoption de plus en plus généralisée de dispositifs reliés à l'Internet des objets (IoT)). Les systèmes IT/OT sont particulièrement vulnérables, ayant souvent été conçus sans intégrer les configurations de cybersécurité prises en compte dans les logiciels informatiques contemporains.

D'ailleurs, ils fonctionnent souvent sur des systèmes anciens, aux capacités de mise à jour réduites, voire inexistantes, et il arrive régulièrement qu'ils ne soient pas pris en compte dans les projets de cybersécurité et les plans de maintenance.

Responsabilités générales en matière de technologies de l'information (IT) / technologies opérationnelles (OT)

Outre la définition des rôles et responsabilités d'ordre général décrits plus haut, la Direction ou son représentant devrait attribuer des responsabilités, notamment en ce qui concerne les systèmes IT/OT. En effet, le groupe qui utilise ces systèmes peut être totalement différent de celui chargé de la gestion des opérations et des systèmes informatiques portuaires. Il est donc utile de rappeler que les personnes qui contrôlent les installations et les systèmes critiques pour les opérations portuaires ont un rôle important à jouer dans la cybersécurité. Ces systèmes opérationnels devraient être inclus dans les analyses des risques de cybersécurité des ports.

Numéro	Mesure
●● [ITOT] 1.1	Un inventaire de l'ensemble des actifs IT/OT utilisés dans les opérations portuaires devrait être réalisé. Les actifs inventoriés devraient ensuite être classés en fonction de la criticité du système.
●● [ITOT] 1.2	Les responsabilités en matière de cybersécurité devraient être clairement définies et documentées pour chacune des parties prenantes utilisant les actifs visés par l'inventaire susmentionné, quel que soit l'aspect concerné (par exemple, développement, intégration, exploitation, maintenance).
●●● [ITOT] 1.3	Des analyses de risques en matière de cybersécurité devraient être réalisées avant de mettre en œuvre un nouveau dispositif ou système relié à l'Internet des objets (IoT).
●●● [ITOT] 1.4	Les actifs IT/OT les plus critiques devraient faire l'objet d'une analyse de risques en matière de cybersécurité.



Gestion des identités et des accès (Identity and Access Management – IAM)

Les ports devraient suivre des politiques clairement définies en ce qui concerne l'accès et l'utilisation des systèmes industriels, des installations connectées et des autres systèmes opérationnels utilisés pour conduire les opérations portuaires. Les mesures suivantes peuvent être prises pour gérer les identités et les accès.

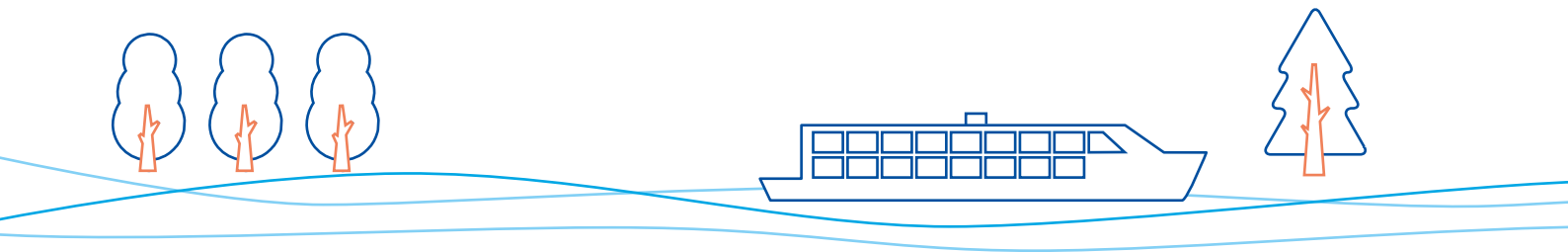
Numéro	Mesure
● [ITOT] 2.1	L'accès aux installations et aux systèmes devrait, si possible, se faire uniquement au moyen d'un nom d'utilisateur et d'un mot de passe. Les mots de passe devraient être robustes.
● [ITOT] 2.2	Les mots de passe par défaut des systèmes opérationnels devraient être modifiés et une procédure devrait être mise en place pour en changer régulièrement par la suite, selon une politique établie par l'organisation.
● [ITOT] 2.3	Lorsque l'authentification ne peut être appliquée (en raison notamment de contraintes opérationnelles), des mesures supplémentaires devraient être envisagées, y compris la mise en place d'un contrôle d'accès physique, la limitation des fonctionnalités offertes par le système, la mise en œuvre d'une authentification par badge, etc.
●● [ITOT] 2.4	Les ports devraient établir la liste des parties prenantes autorisées à accéder aux systèmes critiques, en précisant quels sont les systèmes critiques concernés. Cette liste devrait être mise à jour fréquemment.
●● [ITOT] 2.5	En cas d'échec de l'authentification, il conviendrait de mettre en place un délai d'attente et non un verrouillage.
●● [ITOT] 2.6	Les systèmes particulièrement sensibles devraient faire l'objet d'une authentification à facteurs multiple (par exemple avec code PIN et carte à puce).

Sécurité physique

Étant donné que les systèmes opérationnels, les systèmes industriels et les autres installations sont en général directement accessibles physiquement (contrairement à d'autres actifs tels que les données, les composants informatiques, les logiciels,

les applications informatiques, etc.), des mesures de sécurité physique adaptées et applicables à ces systèmes devraient être définies et mises en œuvre. En particulier, les mesures de sécurité physique décrites ci-dessous constituent quelques bonnes pratiques destinées à protéger physiquement les actifs contre les risques de cybersécurité.

Numéro	Mesure
● [ITOT] 3.1	Les points d'accès aux systèmes de contrôle industriels et autres dispositifs opérationnels ne devraient pas être accessibles aux personnes non autorisées. Cette restriction s'applique particulièrement aux ports avec une forte circulation piétonnière ou touristique.
● [ITOT] 3.2	Les unités centrales des stations de travail, les dispositifs réseau industriels et les automates programmables (PLC) devraient être placés dans des armoires fermées à clef ou dans des pièces fermées à clef.
● [ITOT] 3.3	Les systèmes IT et OT hébergés dans le port devraient être protégés conformément aux bonnes pratiques établies en matière de sécurité (détection d'incendie, climatisation, etc.) et de sûreté (contrôle d'accès, vidéosurveillance, etc.).

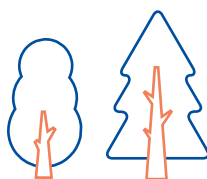


Maintenance et exploitation des systèmes IT/OT

Comme indiqué plus haut, les systèmes IT/OT sont souvent vulnérables aux cyberattaques étant donné qu'ils s'exécutent fréquemment sur d'anciens systèmes et sont exclus des efforts classiques en matière de cybersécurité, tels que les mises à jour et les correctifs. Les systèmes IT/OT font également l'objet d'une

maintenance de routine. Une bonne pratique en matière de cybersécurité consiste à intégrer certains principes de sécurité de base dans les processus de maintenance des systèmes IT/OT. La sécurité devrait également être prise en compte lors de la mise hors service et de l'élimination des systèmes IT/OT.

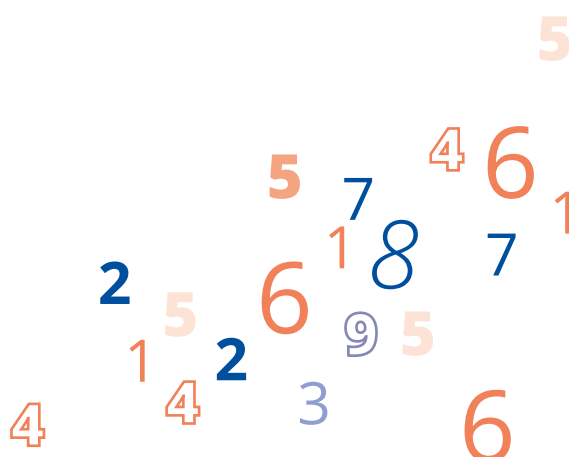
	Numéro	Mesure
●●	[ITOT] 4.1	Une procédure devrait être définie pour la mise à jour et la maintenance des systèmes opérationnels. Cette procédure devrait inclure la fréquence des mises à jour et les rôles et responsabilités des personnes chargées d'effectuer ces mises à jour. Les mises à jour du système devraient être décrites en détail dans les contrats de maintenance passés avec les fournisseurs.
●●	[ITOT] 4.2	Des outils ou des procédures devraient être mis en place pour vérifier les différences entre la version utilisée et la version à installer dans le cadre des opérations de mise à jour du système.
●●	[ITOT] 4.3	Toutes les opérations de maintenance devraient être validées. Une procédure de validation devrait être définie et communiquée aux personnels travaillant avec les systèmes opérationnels.
●●	[ITOT] 4.4	Une procédure de mise hors service des systèmes opérationnels devrait être suivie. Cette procédure devrait être étayée par des documents dans lesquels seraient consignés par écrit la date de mise hors service, les noms des parties concernées par cette mise hors service et les modalités relatives à l'élimination appropriée de l'équipement.
●●●	[ITOT] 4.5	Dans le cadre des interventions et des opérations de mise à jour, les éléments suivants devraient être consignés par écrit : • Le nom de la personne qui effectue les travaux et du donneur d'ordre, • La date et l'heure de l'intervention, • Le périmètre dans lequel les travaux sont effectués, • Les activités réalisées, • La liste des appareils retirés ou remplacés (y compris, le cas échéant, les numéros d'identification) ainsi que • Les modifications apportées et leur impact.
●●●	[ITOT] 4.6	Un plan d'audit régulier (dont la fréquence serait à déterminer par le port visant à évaluer si la procédure de mise à jour est bien respectée). Les recommandations émises à l'issue des audits devraient faire l'objet d'un suivi.



Mesures techniques de sécurité pour les systèmes IT/OT

Ces mesures techniques de sécurité devraient être prises en compte par les personnels des ports chargés de la configuration des réseaux, de la mise en place et de la configuration des systèmes opérationnels et de la maintenance technique générale de ces systèmes. En règle générale, il faudrait, si possible, veiller à isoler les systèmes critiques des réseaux généralement disponibles et du reste de l'infrastructure informatique.

Numéro	Mesure
● [ITOT] 5.1	L'accès à l'Internet à partir des systèmes industriels critiques (tels que les systèmes de gestion des ponts et/ou des écluses, les centrales électriques, les stations d'eau potable) devrait être limité au minimum.
● [ITOT] 5.2	Des outils de développement ne devraient pas être installés sur des machines actives et en fonctionnement. Seuls des systèmes d'exécution devraient être actifs sur des installations IT/OT.
● [ITOT] 5.3	En ce qui concerne les systèmes opérationnels, les protocoles non sécurisés (par exemple HTTP, Telnet, FTP) devraient être désactivés en faveur de protocoles sécurisés (par exemple HTTPS, SSH, SFTP).
●● [ITOT] 5.4	Des zones réseaux distinctes devraient être utilisées pour la connexion des systèmes opérationnels, pour tout dispositif relié à l'Internet des objets (IoT), pour le Wi-Fi à usage professionnel et pour le Wi-Fi public.
●● [ITOT] 5.5	Les systèmes de contrôle industriels (SCI) devraient être divisés en zones fonctionnelles ou techniques cohérentes. Ces zones devraient être séparées les unes des autres.
●● [ITOT] 5.6	Une politique de filtrage entre les zones et au niveau des passerelles administratives devrait être mise en œuvre selon un protocole strict défini (c'est-à-dire un protocole concernant les flux de données, la journalisation des activités, l'enregistrement des adresses IP, etc.)
●● [ITOT] 5.7	Dans la mesure du possible, un réseau privé virtuel (VPN) devrait être déployé et s'étendre aux passerelles, empêchant ainsi le trafic extérieur d'accéder aux zones opérationnelles des systèmes.
●● [ITOT] 5.8	Les stations de travail autorisées à se connecter sur des éléments du réseau avec des niveaux de privilèges élevés (administration) devraient, dans la mesure du possible, être séparées du réseau principal. Ces stations de travail devraient être contrôlées et ne devraient pas être utilisées à d'autres fins. Elles devraient être fréquemment mises à jour et renforcées par des politiques de durcissement.
●●● [ITOT] 5.9	Lorsque le contrôle à distance de systèmes opérationnels est nécessaire, les connexions à distance devraient être certifiées, les mots de passe de connexion devraient être gérés dans le cadre de la politique de mot de passe définie par l'organisation, la journalisation devrait être activée, des protocoles de communication sécurisés devraient être mis en place et les sessions de connexion à distance devraient cesser automatiquement après une période d'inactivité.
●●● [ITOT] 5.10	Des mécanismes tels que le cryptage, l'ICP ou les certificats numériques, les contrôles d'intégrité, la signature numérique, l'horodatage, en particulier lorsque les échanges sont effectués sur l'Internet, devraient être mis en place pour sécuriser les échanges de machine à machine (y compris les messages EDI et les interfaces de programmation d'application (API) utilisés principalement avec des parties prenantes externes) et assurer l'authentification mutuelle, l'intégrité et la confidentialité des données des systèmes portuaires.



Surveillance des systèmes IT/OT

Les activités de surveillance des systèmes opérationnels peuvent être hors de portée des ports disposant de peu de moyens opérationnels ou de ressources limitées. La Direction devrait envisager de telles mesures si leurs systèmes opérationnels revêtent une importance critique pour les opérations portuaires et qu'une priorité stratégique en matière de cybersécurité consiste à détecter et à anticiper les menaces de cybersécurité pesant sur leurs systèmes.

	Numéro	Mesure
●●	[ITOT] 6.1	Les modifications des paramètres des systèmes d'exploitation critiques devraient faire l'objet d'un suivi et être journalisées.
●●	[ITOT] 6.2	Les fonctions de traçabilité des activités et des événements relatifs aux systèmes opérationnels devraient être activées sur les systèmes critiques.
●●●	[ITOT] 6.3	Un processus de gestion des événements en matière de cybersécurité touchant les systèmes opérationnels devrait être mis en œuvre par les propriétaires des systèmes. Ce processus devrait définir le stockage des événements (à supposer que des journaux soient stockés, comment sont-ils stockés, sauvegardés et sécurisés), donner des indications de base sur ce qui définit une activité anormale du système et mettre en place les conditions permettant de déclarer si et quand un événement devient un incident de cybersécurité.
●●●	[ITOT] 6.4	L'installation d'outils de surveillance commerciaux devraient être envisagée par le port pour assurer la surveillance de la cybersécurité des systèmes opérationnels.

Réponse aux incidents et gestion de crise pour les systèmes IT/OT

Venant s'ajouter à la réponse apportée en cas d'incident et aux mesures de gestion de crise mentionnées dans les mesures consacrées aux politiques et procédures organisationnelles, ces mesures s'adressent particulièrement aux parties prenantes travaillant avec des systèmes IT/OT.

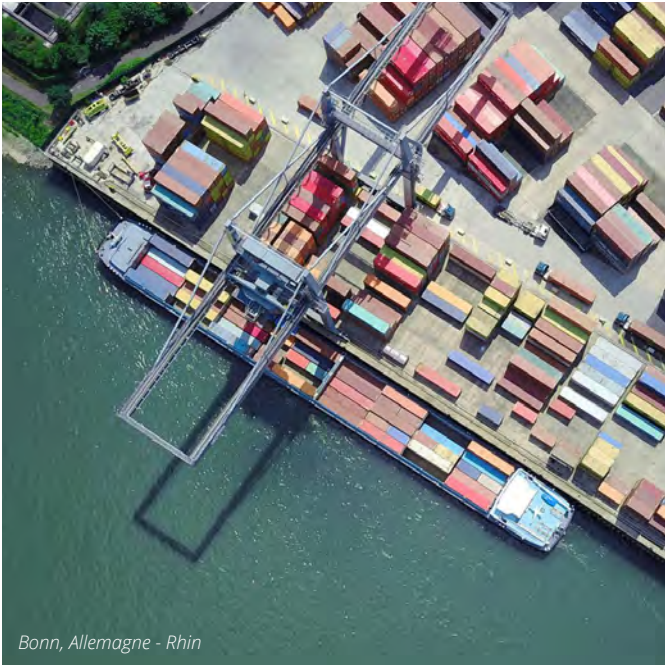
	Numéro	Mesure
●●	[ITOT] 7.1	Un plan de gestion des incidents, spécifiquement applicable aux systèmes IT/OT, devrait être défini. Ce plan devrait inclure des précisions sur la sauvegarde des données nécessaires au fonctionnement des systèmes IT/OT, sur les procédures d'intervention et l'activation du mode d'urgence des systèmes IT/OT, et prévoir la traçabilité des actions réalisées lors de la gestion d'un incident.
●●	[ITOT] 7.2	Des modes de fonctionnement dégradés devraient être disponibles pour les systèmes opérationnels, leur permettant de s'arrêter ou de fonctionner en mode manuel en cas d'incident.



Port of Switzerland, Suisse - Rhin

Sécurisation des systèmes de navigation

Cette section a été incluse pour fournir certaines mesures d'atténuation applicables aux systèmes de navigation IT/OT qui relient les ports aux bâtiments qui naviguent. Seuls les systèmes qui sont pertinents pour les ports ont été inclus aux fins de ce guide. Les systèmes ne concernant que l'équipage ou le bâtiment ne sont pas abordés dans le présent guide. Ces mesures d'atténuation pourraient permettre de faire face aux risques présentés dans les scénarios d'attaque spécifiques des ports décrits ci-dessus.



Numéro	Mesure
●● [ITOT] 8.1	Un manuel pour les situations d'urgence indiquant comment annuler toute programmation automatique des appareils de communication à distance devrait être mis à la disposition des utilisateurs. Il conviendrait en outre d'informer le personnel des ports du rôle crucial qu'il est en mesure de jouer dans la détection d'un comportement erratique ou anormal de ces systèmes.
●● [ITOT] 8.2	Les opérateurs portuaires devraient prendre des précautions particulières pour contrôler la sécurité des réseaux ayant accès aux systèmes de visualisation des cartes électroniques et d'informations (ECDIS) et s'assurer qu'ils sont protégés contre les accès extérieurs (depuis l'Internet). Les mises à jour et les correctifs des logiciels liés aux systèmes ECDIS devraient être systématiquement installés.
●●● [ITOT] 8.3	Les ports qui envoient et reçoivent des signaux GNSS et GPS devraient envisager d'adopter des mesures d'atténuation contre les risques d'usurpation de signaux. Ces mesures pourraient inclure la mise en œuvre d'outils et de techniques facilitant la détection d'anomalies dans les signaux reçus, comme le fanion RAIM (surveillance autonome de l'intégrité du récepteur) qui vérifie les incohérences dans les signaux satellites.
●●● [ITOT] 8.4	Les ports qui reçoivent des données AIS des bâtiments, devraient envisager d'adopter des mesures d'atténuation pour surveiller les comportements potentiellement anormaux. Les activités relatives à la surveillance des données peuvent être utilisées pour détecter des changements inattendus dans les itinéraires des bâtiments ou des informations statiques qui pourraient signaler une activité malveillante potentielle.





Étude de cas Protection des terminaux à conteneurs

Les terminaux à conteneurs, présents dans certains ports, nécessitent de nombreux équipements IT/OT pour pouvoir mener à bien les opérations, ce qui en fait un cas d'étude intéressant en ce qui concerne la mise en œuvre de mesures d'atténuation des risques de cybersécurité IT/OT. Ces terminaux ayant été identifiés comme critiques par de nombreux ports, ce guide propose une étude de cas présentant les principaux services et actifs d'un terminal à conteneurs et les risques éventuels correspondants en matière de cybersécurité.

Services et actifs des terminaux à conteneurs

Les terminaux à conteneurs assurent, pour les clients du port, le transit des conteneurs entre les bâtiments de navigation intérieure et les transporteurs routiers ou ferroviaires, ou vice versa. Les terminaux à conteneurs s'appuient généralement sur un **système d'exploitation de terminal** pour pouvoir interagir avec les clients – des transporteurs – et mener des activités internes. Ce système d'exploitation fournit les services suivants en se connectant à d'autres appareils :

Gestion des besoins des clients

Les clients ont accès à une **plateforme d'applications** en ligne pour transmettre des informations sur les conteneurs qu'ils souhaitent transporter et sur les caractéristiques propres à ces conteneurs (types de marchandise, poids, taille, exigences en matière de manutention, etc.). Cette plateforme s'appuie sur les informations stockées dans le système d'exploitation du terminal.

Entretien des conteneurs

Le système d'exploitation centralise les informations sur les dommages subis par les conteneurs, l'état des conteneurs reçus et expédiés, et en cas de dommages, **envoie des devis** aux clients aux fins de la réparation ou du nettoyage des conteneurs.

Manutention des conteneurs

Sur la base des informations stockées dans le système d'exploitation du terminal (taille, position, exigences en matière de manutention et type de conteneurs mais aussi les installations disponibles pour l'entreposage des conteneurs). Celui-ci peut envoyer des informations aux **portiques/grues de manutention** qui déplacent, soulèvent et empilent ensuite les conteneurs pour les entreposer ou les déplacer.

Gestion du service par le personnel

Les systèmes d'exploitation des terminaux envoient des informations sur les tâches, les exigences en matière d'entretien ou d'autres informations aux employés des ports via des **tablettes ou des appareils portatifs**.

Facturation client et gestion financière par le système

Les **factures sont envoyées** aux clients directement, en fonction des services fournis, de même que les accusés de réception de paiement.

Gestion des tierces parties/fournisseurs

Les tierces parties, telles que les chauffeurs routiers, intervenant dans le transport des conteneurs ont accès à une **application** permettant d'authentifier la collecte ou le dépôt de leurs conteneurs et de leur fournir des informations sur les heures et les lieux de collecte et de dépôt.

Risques liés à la cybersécurité pour les systèmes d'exploitation des terminaux à conteneurs

Sur la base des actifs et services exposés ci-dessus, deux principaux risques de cybersécurité ont été identifiés en croisant la probabilité d'occurrence avec l'impact opérationnel potentiel pour les systèmes d'exploitation des terminaux à conteneurs. Ces risques sont les suivants :

- **Une attaque par rançongiciel** contre les systèmes utilisés par des terminaux à conteneurs, notamment contre le système d'exploitation du terminal, gelant les opérations du terminal à conteneurs. Cette attaque empêcherait le système d'exploitation du terminal de fonctionner correctement et aurait donc un impact sur certains ou sur l'ensemble des services susmentionnés. Il est à noter que, si les grues procédant à la manutention des conteneurs n'ont pas la possibilité de fonctionner sans avoir communication des données détenues par le système d'exploitation du terminal, les activités opérationnelles seraient alors perturbées, voire paralysées.
- Un intrus malveillant **parvenu à intercepter des données critiques** sur les dates de chargement et de déchargement des conteneurs, leur localisation ou le détail de leur contenu, pourrait entreprendre des actions illégales (vol, trafic et récupération de marchandises illégales...). Bien qu'il puisse être plus difficile pour un intrus de parvenir effectivement à dérober un conteneur, en raison de la taille et de la logistique nécessaires pour déplacer l'objet, un intrus pourrait espionner les systèmes portuaires pour obtenir des informations sur la localisation et les mouvements d'un conteneur donné, un scénario qui a été décrit plus haut. Cela pourrait sérieusement entacher la réputation du port, affecter sa sécurité mais également engager sa responsabilité quant aux conséquences de l'interception de ces données.

Mesures techniques de cybersécurité pour les ports

Les mesures techniques de cybersécurité présentées en détail ci-dessous sont destinées au service informatique ou de la sécurité informatique d'un port ou d'un organisme travaillant avec des ports. Les mesures recommandées ci-dessous ont été adaptées au contexte d'un port, mais il s'agit de mesures générales de sécurité informatique que l'on retrouve dans toutes les organisations dotées de solides politiques de sécurité de l'information. En effet, il est à noter que toutes les mesures ne sont pas forcément pertinentes ou réalisables pour les ports dont les ressources et le personnel sont limités, comme par exemple un port ne disposant pas de service informatique dédié. Ces

mesures devraient néanmoins être consultées car elles peuvent constituer une bonne base de référence par rapport aux attentes fondamentales en matière de sécurité à prendre en compte à mesure qu'une organisation gagne en maturité informatique.

Gestion des identités et des accès (IAM)

Cette section est consacrée aux mesures de sécurité relatives à la gestion des utilisateurs des systèmes et dispositifs informatiques portuaires. Les mesures IAM applicables aux systèmes informatiques généraux et celles applicables aux technologies opérationnelles ont été présentées séparément pour les besoins du guide. Pour de plus amples informations sur les mesures IAM pour les systèmes IT/OT, il convient de se reporter à la section [ITOT] 4 présentant en détail un certain nombre de mesures. Dans la pratique, les deux sujets peuvent cependant être abordés ensemble.

Numéro	Mesure
 [TSM] 1.1	Le représentant de la sécurité informatique devrait s'assurer que les options d'authentification sont activées sur tous les PC, tablettes, logiciels, applications, et que les mots de passe par défaut ont été modifiés. Les mots de passe devraient, dans la mesure du possible, faire l'objet de stratégies et de règles tenant compte du degré de complexité nécessaire.
 [TSM] 1.2	Tous les utilisateurs du système informatique devraient être identifiés et devraient utiliser des comptes nominatifs individuels.
 [TSM] 1.3	L'accès aux systèmes informatiques ou aux bases de données des ports ne devrait être accordé à des tierces parties ou à des fournisseurs que pour une durée déterminée et dans un but spécifique.
 [TSM] 1.4	Il convient de faire la distinction entre les comptes « Utilisateur » et les comptes « Administrateur ». Des comptes « Administrateur » ne devraient être attribués qu'à ceux qui en ont besoin. Les privilèges des comptes « Utilisateur » devraient être limités au strict minimum. Les droits devraient être accordés selon le principe de la séparation des tâches, c'est-à-dire que chaque utilisateur ne devrait avoir accès qu'aux données nécessaires à l'exécution de ses tâches, et seulement celles-ci.
 [TSM] 1.5	Les comptes « Administrateur » ne devraient être utilisés que pour des opérations administratives telles que la gestion des comptes « Utilisateur », l'installation ou la mise à jour de logiciels et la maintenance. Il faudrait éviter d'utiliser les comptes « Administrateur » à d'autres fins, que ce soit pour naviguer sur l'Internet ou pour répondre à des courriels, par exemple.
 [TSM] 1.6	Les comptes anonymes ou génériques devraient être supprimés des systèmes informatiques
 [TSM] 1.7	Une procédure devrait être établie pour l'octroi et le retrait des privilèges du compte « Utilisateur ».
 [TSM] 1.8	Une procédure devrait être établie pour gérer le cycle de vie des comptes « Utilisateurs », y compris la création, la modification, les mises à jour, la sauvegarde des données et la suppression du compte. Cette procédure devrait également inclure les modalités relatives à l'ajout et au retrait des appareils de l'utilisateur.
 [TSM] 1.9	Des examens réguliers des droits d'accès aux comptes devraient être réalisés. À l'issue de ces examens, les droits considérés comme ayant été accordés sans nécessité devraient être révoqués. Les anciens comptes d'utilisateurs devraient, si possible, être supprimés ou, si ce n'est pas possible, désactivés/archivés.
 [TSM] 1.10	En fonction du nombre de parties prenantes intervenant dans les opérations portuaires, les parties prenantes concernées devraient envisager de mettre en place un outil de gestion des comptes et des autorisations d'accès aux actifs informatiques des ports. Les parties prenantes visées sont les autorités portuaires, les opérateurs de terminaux, les autorités locales, les tierces parties, etc.
 [TSM] 1.11	L'authentification à facteurs multiples (AMF) pour les applications et les bases de données les plus critiques, en particulier celles contenant des données personnelles, des données opérationnelles sensibles telles que des informations détaillées sur les bâtiments, et des informations sur les marchandises dangereuses et les cargaisons, devrait être mise en œuvre (voir mesure [ITOT] 2.6).
 [TSM] 1.12	Un processus de gestion des comptes à privilège (PAM) devrait être défini en intégrant les exigences de sécurité correspondantes relatives à ces comptes et règles pour en gérer le cycle de vie. Ce processus devrait être appliqué en particulier aux comptes privilégiés de tierces parties.

Sécurité des systèmes

Cette section présente en détail les opérations qui devraient être effectuées sur les systèmes et actifs informatiques pour renforcer leur sécurité globale. Ces tâches devront très probablement être accomplies par un expert en informatique ou en sécurité informatique, étant donné qu'elles nécessitent une configuration spécifique des actifs informatiques.

Numéro	Mesure
● [TSM] 2.1	Les équipes informatiques devraient s'assurer que des logiciels antimalware, antispam et antivirus sont installés et mis à jour sur tous les systèmes portuaires, y compris les ordinateurs de bureau et les serveurs. Lors des mises à jour, la priorité devrait être donnée aux équipements informatiques les plus sensibles et les plus vulnérables.
●● [TSM] 2.2	Un inventaire complet des actifs informatiques, y compris le matériel, les appareils, les logiciels, les systèmes, les serveurs, les réseaux et les composants de réseau, devrait être dressé et mis à jour régulièrement.
●● [TSM] 2.3	À partir de l'inventaire des actifs informatiques, il convient de définir la politique de mise à jour correspondante, indiquant la fréquence des mises à jour, les moyens à utiliser pour les mises à jour, les responsabilités et les éventuels processus de validation. Cette politique devrait préciser que seules devraient être utilisées les mises à jour obtenues auprès de sources de confiance, telles que les sites web officiels des éditeurs.
●● [TSM] 2.4	Les équipes informatiques devraient s'assurer que les connexions à distance sont correctement sécurisées, en utilisant des techniques telles que les VPN avec des niveaux de chiffrement élevés. Les mots de passe « Utilisateur » pour accéder aux ressources à distance doivent être renforcés ou couplés avec des dispositifs complémentaires (authentification à facteur multiple, certificat installé sur le PC, mot de passe à usage unique, etc.) afin de ne pas constituer une faille exploitable. La question de savoir si l'accès à distance devrait être limité à des utilisateurs ou à des systèmes spécifiques devrait être examinée.
●● [TSM] 2.5	Une politique devrait être établie en ce qui concerne l'utilisation des supports amovibles (qu'il serait préférable d'interdire), y compris clés USB, cédérom, disque dur externe, disquettes etc.
●●● [TSM] 2.6	Un processus de gestion des changements (au sens ITIL) devrait être défini afin d'introduire de nouveaux dispositifs dans les systèmes des ports.
●●● [TSM] 2.7	Une liste des matériels et des logiciels autorisés devrait être dressée et régulièrement mise à jour (y compris les versions précises autorisées pour chaque logiciel).
●●● [TSM] 2.8	Les équipes informatiques devraient définir une stratégie de protection des points de terminaison (PC, tablette, téléphone et tous les équipements connectés au réseau et directement accessible aux utilisateurs) visant à en assurer la surveillance et à en renforcer la sécurité en mettant en œuvre des outils et des mécanismes de sécurité tels que les antivirus, le chiffrement, la gestion des dispositifs mobiles et leur durcissement (renforcement de leur sécurité par la suppression de toutes les applications et logiciels installés par défaut mais non nécessaires pour l'usage visé).
●●● [TSM] 2.9	Les équipes informatiques devraient définir des politiques et des règles d'installation et de configuration et établir des principes de base en matière de sécurité afin d'installer uniquement les services et fonctionnalités nécessaires et d'autoriser les équipements essentiels à la sécurité et au fonctionnement des systèmes portuaires.
●●● [TSM] 2.10	Les équipes informatiques devraient effectuer des audits réguliers des mises à jour des logiciels et des serveurs.

Sécurité des réseaux

Cette section expose en détail les mesures pouvant être mises en place pour sécuriser les réseaux utilisés par les ports. Comme dans la section ci-dessus, la mise en œuvre de ces mesures

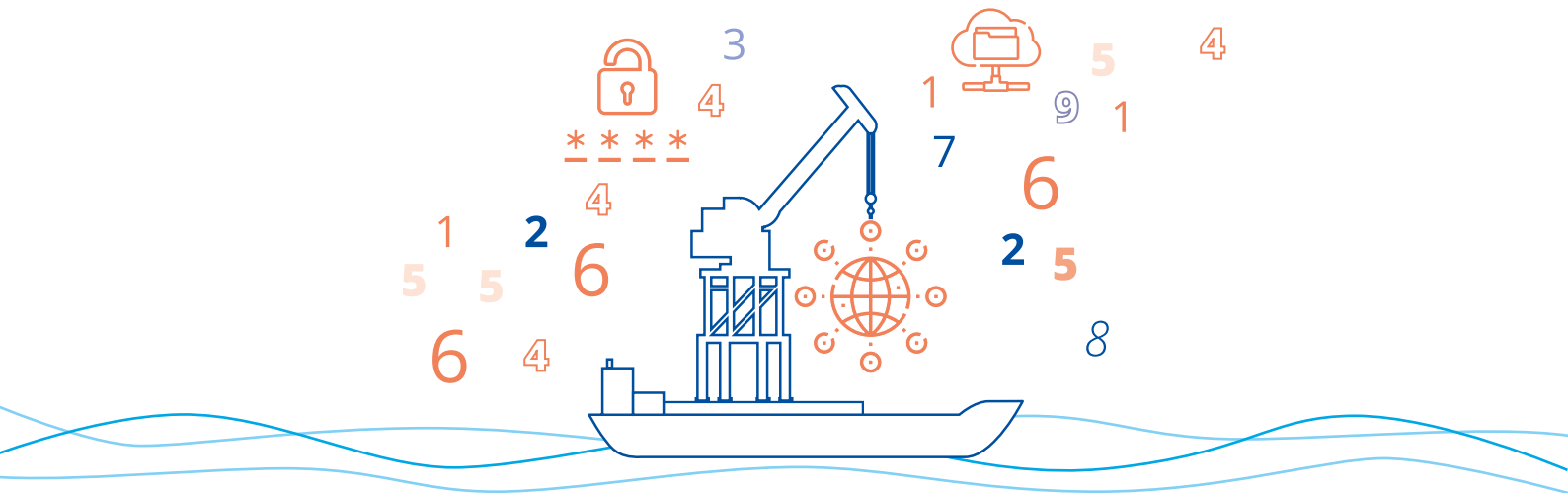
nécessitera très probablement l'intervention du personnel chargé de l'informatique (ou de la sécurité informatique). En ce qui concerne les ports ne disposant pas de personnel dédié à la sécurité informatique, il pourrait être envisagé de recourir aux services d'un spécialiste externe en sécurité informatique.

Numéro	Mesure
● [TSM] 3.1	Les équipes informatiques devraient veiller à la complexité du mot de passe Wi-Fi et faire en sorte qu'il soit modifié régulièrement.
● [TSM] 3.2	Les réseaux Wi-Fi utilisés par les équipes informatiques des ports devraient être configurés pour offrir le protocole de chiffrement « WPA2 Entreprise » ou « WPA3 Enterprise ». Si cela n'est pas possible, c'est le protocole WPA2-(PSK-)AES ou WPA3 (Personnel ou Transitionnel) qui devrait être utilisé.
●● [TSM] 3.3	Des règles appropriées de filtrage du réseau (concernant, par exemple, les adresses IP ou le trafic autorisé) devraient être mises en œuvre.
●● [TSM] 3.4	La distinction devrait être faite entre un réseau Wi-Fi professionnel (typiquement pour un usage professionnel par les employés, dûment authentifiés) et un réseau Wi-Fi public (typiquement pour des invités/visiteurs ou pour un usage personnel par les employés), qui devraient être séparés. Une politique de séparation des réseaux devrait être mise en œuvre pour empêcher la propagation des attaques au sein des systèmes portuaires et pour atténuer les risques d'accès depuis l'Internet.
●● [TSM] 3.5	Les points d'accès au réseau devraient être clairement identifiés et documentés par les équipes informatiques. Cette liste devrait être mise à jour régulièrement. Les points d'accès inutilisés devraient être désactivés.
●● [TSM] 3.6	Les équipes informatiques devraient définir et mettre en œuvre une politique concernant les appareils et logiciels autorisés afin de garantir que seuls des composants de confiance soient introduits sur le réseau.
●●● [TSM] 3.7	Les règles d'accès au réseau devraient subir des examens réguliers et, le cas échéant, les ajustements nécessaires. Des analyses régulières des réseaux devraient être effectuées pour détecter toute activité non autorisée sur le réseau.
●●● [TSM] 3.8	Une politique de déclaration et de traitement des activités anormales sur le réseau devrait être établie en coordination avec les processus de gestion des incidents décrits dans la mesure [OPP] 4.3.
●●● [TSM] 3.9	Une stratégie de surveillance de l'activité du réseau devrait être définie. Cette stratégie peut inclure une variété d'outils et de technologies de surveillance du réseau. Toutefois, cette stratégie devrait aussi prévoir que ces outils soient exploités, paramétrés et régulièrement vérifiés par du personnel formé et compétent.

Protection des données

Cette section concerne la gestion des données collectées, traitées et utilisées par les parties prenantes des ports. Il est noté que les ports situés dans l'Union européenne sont soumis au règlement

général sur la protection des données (RGPD) publié en 2016. Si la législation RGPD est applicable, elle doit être consultée en priorité en ce qui concerne le traitement approprié des données et des informations.



Numéro	Mesure
 [TSM] 4.1	Les personnels concernés des ports devraient connaître les dispositions réglementaires (telles que le RGPD) qui leur sont applicables et relatives à la collecte et la conservation des données. Une politique de gestion des données devrait être mise en œuvre, qui soit conforme à ces dispositions réglementaires, avec éventuellement des précisions ou des dispositions supplémentaires.
 [TSM] 4.2	Une politique de conservation des données avec des indications claires sur les règles de classification des données et les règles d'élimination des données devrait être définie. Les données personnelles identifiables et les autres données particulièrement sensibles devraient être chiffrées ou sécurisées à l'endroit où elles sont stockées, mais aussi lorsqu'elles circulent sur le réseau interne.
 [TSM] 4.3	Une politique concernant les sauvegardes de données devrait être définie et mise en œuvre. Ces sauvegardes de données devraient être régulièrement testées pour s'assurer de leur fonctionnalité, en donnant la priorité aux sauvegardes des systèmes et des données critiques.
 [TSM] 4.4	Un plan de récupération des données (DRP) devrait être établi, précisant le protocole à suivre en cas d'incident de cybersécurité ou de tout autre événement pouvant entraîner une perte de données.
 [TSM] 4.5	Une analyse des actifs de données devrait être détaillée et contenir des informations concernant : • Le type de données auxquelles le port devrait avoir accès afin d'effectuer les opérations minimales requises ; • Les sources de données et les flux de données traités par le port ; • Les modalités de stockage des données collectées et traitées ; • Les accès actuels aux bases de données par les parties prenantes internes et les tierces parties ; • Le cycle de vie des données et les besoins de conservation des données.
 [TSM] 4.6	Des disques de réserve et de l'espace de stockage en ligne devraient être disponibles en cas d'incident de cybersécurité.
 [TSM] 4.7	Des inspections des serveurs de stockage sur le réseau devraient être effectuées régulièrement afin de détecter le plus tôt possible d'éventuels dysfonctionnements concernant l'espace de stockage, les données ou les disques.

Gestion des vulnérabilités et surveillance des systèmes

Les mesures de gestion des vulnérabilités ont pour but de réunir des informations permettant de mieux remédier aux vulnérabilités existantes. Les activités de surveillance peuvent aider à détecter les comportements malveillants dans les systèmes portuaires.

Numéro	Mesure
 [TSM] 5.1	Les ports devraient définir une procédure de surveillance de la cybersécurité afin d'être informés des vulnérabilités nouvellement détectées et publiées (par les employés, les fournisseurs, les tierces parties, les pairs du secteur) et de prendre rapidement les mesures d'atténuation correspondantes. Cette démarche devrait être coordonnée avec celles préconisées pour les systèmes IT/OT et leurs propriétaires (voir [ITOT] 6.1).
 [TSM] 5.2	Les équipes informatiques devraient définir une procédure de gestion des vulnérabilités permettant d'identifier celles touchant les actifs (à l'aide d'analyses de vulnérabilité, par exemple) et une procédure permettant d'y remédier.
 [TSM] 5.3	Un système de journalisation devrait être mis en place pour enregistrer les activités et les événements, en particulier les événements concernant l'authentification des utilisateurs, la gestion des comptes et les droits d'accès, les modifications des règles de sécurité, ainsi que toutes modifications ou altérations du fonctionnement des systèmes.
 [TSM] 5.4	Pour chaque vulnérabilité identifiée, des mesures d'atténuation correspondantes devraient être définies et mises en œuvre. Si aucune de ces possibilités ne peut être exploitée ou si aucune mesure d'atténuation n'est définie, une explication documentée devrait être insérée dans le dossier.
 [TSM] 5.5	Les équipes informatiques devraient mettre en place des outils ou des procédures pour surveiller la disponibilité des systèmes et des équipements portuaires en temps réel. Les systèmes critiques (stations de travail dédiées à l'administration, dispositifs de communication, appareils de navigation) devraient être prioritaires dans ces activités.
 [TSM] 5.6	Les ports devraient mettre en place des systèmes de corrélation et d'analyse des journaux pour détecter les événements et contribuer ainsi à la détection des incidents de cybersécurité.

Partie 3

Conseils pour la mise en œuvre des mesures d'atténuation des risques



Cadre d'évaluation de la maturité	55
Tableau d'applicabilité des mesures	56

Cette Partie a pour objet de faciliter la mise en œuvre des mesures d'atténuation présentées plus haut. Compte tenu du large éventail de mesures proposées et des différents niveaux de complexité afférents, les ports devraient définir des priorités pour leur mise en œuvre en fonction des ressources dont ils disposent, du niveau de maturité visé et de leurs besoins en matière de cybersécurité.

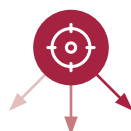
Le tableau ci-après propose des mesures à mettre en œuvre en priorité sur la base de deux critères : le niveau de maturité en matière de cybersécurité du port et les parties prenantes concernées.

Ce niveau de maturité peut se mesurer à un instant donné, par exemple à l'aide du cadre d'évaluation proposé ci-dessous. Une fois ce niveau connu, il est possible de le conserver, de

le renforcer ou bien de l'augmenter. Chacune de ces options correspond à un effort et donc à des coûts. Le choix du niveau de maturité cible doit être pris par la Direction en prenant en compte un grand nombre de critères comme la taille du port, son exposition, sa dépendance technologique, le nombre de fournisseurs et de sous-traitants, ses capacités techniques et financières, mais aussi son expérience et ses propres enjeux en matière de cybersécurité.

À titre d'exemple, voici quelques critères qui peuvent aider à fixer l'objectif de maturité en matière de cybersécurité. Ces critères sont fournis uniquement à titre indicatif ou comme source d'inspiration pour la Direction, qui doit en tout état de cause les fixer.

Niveau de maturité cible



Faible	Moyen	Élevé
Critères possibles - Le port n'est pas un centre d'expédition ou de commerce important pour la région. - Les équipes informatiques en place sont très petites ou les parties prenantes chargées de l'informatique sont des prestataires externes. - Les activités portuaires ne nécessitent presque pas d'infrastructure numérique pour fonctionner.	Critères possibles - Le port dispose de quelques infrastructures importantes mais ne constitue pas le centre de l'activité portuaire de la région. - Les fournisseurs de services informatiques sont présents et interviennent fréquemment ou l'organisation dispose d'une forme d'équipe informatique. - Certaines activités portuaires dépendent de l'infrastructure numérique.	Critères possibles - Le port est considéré comme un centre majeur de l'activité commerciale pour la région. Il abrite une importante plateforme d'expédition/de transport de conteneurs ou constitue une zone de transit majeure. - Une équipe informatique interne est en place, de même que les décideurs correspondants. - Les activités portuaires dépendent fortement des infrastructures numériques ; on relève la présence de certaines technologies portuaires intelligentes (« SmartPort »).

Les différentes parties prenantes considérées correspondent aux acteurs qui sont amenés à mettre en œuvre chaque mesure. Un certain nombre des mesures proposées ci-dessus ne peuvent être exécutées que par des spécialistes de l'informatique ou de la sécurité, tandis que d'autres nécessitent l'intervention de gestionnaires ou de dirigeants du port.

Par nature, le niveau de maturité ne peut pas évoluer trop rapidement. Un port qui évaluerait son niveau de maturité « faible » peut viser un niveau « moyen » après quelques années d'efforts soutenus, mais il ne peut pas viser directement le niveau « élevé » dans le même délai, quand bien même il y consacrerait des moyens financiers élevés. En effet, la maturité en matière de

cybersécurité est aussi une question d'expérience, de culture et de pratique qui nécessitent du temps.

Le niveau de maturité devrait par ailleurs être cohérent et aussi homogène que possible. Par exemple, un port ne devrait pas se contenter d'un niveau de maturité « faible » pour « politiques et procédures organisationnelles » et vouloir atteindre un niveau « moyen » ou « élevé » pour la « sécurité des réseaux ». De la même manière, il est inutile, voire contre-productif et certainement coûteux de vouloir mettre en œuvre une mesure située dans un niveau de maturité « élevé » si une grande majorité des mesures des niveaux « faible » et « moyen » ne sont pas déjà mises en place (voire la totalité). En effet, si la mise en œuvre de mesures

de cybersécurité est souvent comparée à la mise en place de fortifications, on comprend bien qu'il est inutile de fortifier un côté lorsqu'on laisse l'autre totalement exposé. Très souvent, les incidents de cybersécurité et les attaques se produisent là où la cybersécurité est la moins forte. Aussi une bonne stratégie consiste-t-elle à renforcer la cybersécurité là où elle est la plus faible. Mais il est toutefois possible, sans pour autant négliger le reste, d'aller un peu plus loin sur des domaines spécifiques lorsqu'ils ont été identifiés comme particulièrement critiques.

Cadre d'évaluation de la maturité

Ce guide propose ici un cadre d'évaluation pour déterminer le niveau de maturité actuelle d'un port.

Il s'agit d'une méthode d'auto-évaluation consistant à affecter une note de 1 à 5 pour chaque mesure définie dans la Partie 2. Idéalement, cette auto-évaluation devrait être réalisée par une petite équipe pluridisciplinaire avec au minimum un représentant de chaque partie prenante, c'est-à-dire :

- Un membre de la direction, idéalement responsable de la cybersécurité
- Un membre de l'équipe informatique ayant une bonne vue d'ensemble sur l'infrastructure et les applications
- Un responsable opérationnel ayant une bonne connaissance du fonctionnement des systèmes métiers (plusieurs responsables si un seul n'est pas suffisant pour couvrir l'ensemble des systèmes métiers)

Dans un second temps, les membres se réunissent et passent en revue leur notes. Lorsque des divergences sont constatées, les membres échangent et expliquent les motivations qui les ont conduits à donner leur note. Après cet échange, et en tenant compte des remarques des autres membres, le membre représentant la partie prenante à laquelle la mesure est rattachée décide de la note finale.

L'échelle de notation de 1 à 5 peut s'exprimer de la façon suivante :

Points	Description
1	La mesure n'est pas coordonnée et n'est mise en œuvre par personne ; il n'y a pas de programme officiel en place ou il n'existe pas de contrôles particuliers de ce genre.
2	Une communication informelle ou un processus informel s'articule autour de cette mesure, bien que la documentation et la procédure officielle fassent défaut.
3	Certains rôles et responsabilités liés à cette mesure ont été formalisés. Les processus correspondants existent, mais leur mise en œuvre n'est pas vérifiée systématiquement.
4	Les rôles et responsabilités sont clairement définis et des procédures de vérification formelles sont en place pour veiller à ce que cette mesure soit mise en œuvre.
5	Une culture d'amélioration continue s'articule autour de cette mesure, les processus qui la sous-tendent faisant l'objet d'un suivi quantitatif à des fins de compréhension et d'amélioration.

Une fois ce processus d'auto-évaluation terminé, la moyenne des notes des mesures figurant sur chacune des trois lignes du tableau d'applicabilité ci-dessous est calculée. Le résultat se résume donc à trois moyennes entre 1 et 5 pour chacun des niveaux de maturité (« faible », « moyen » et « élevé »).

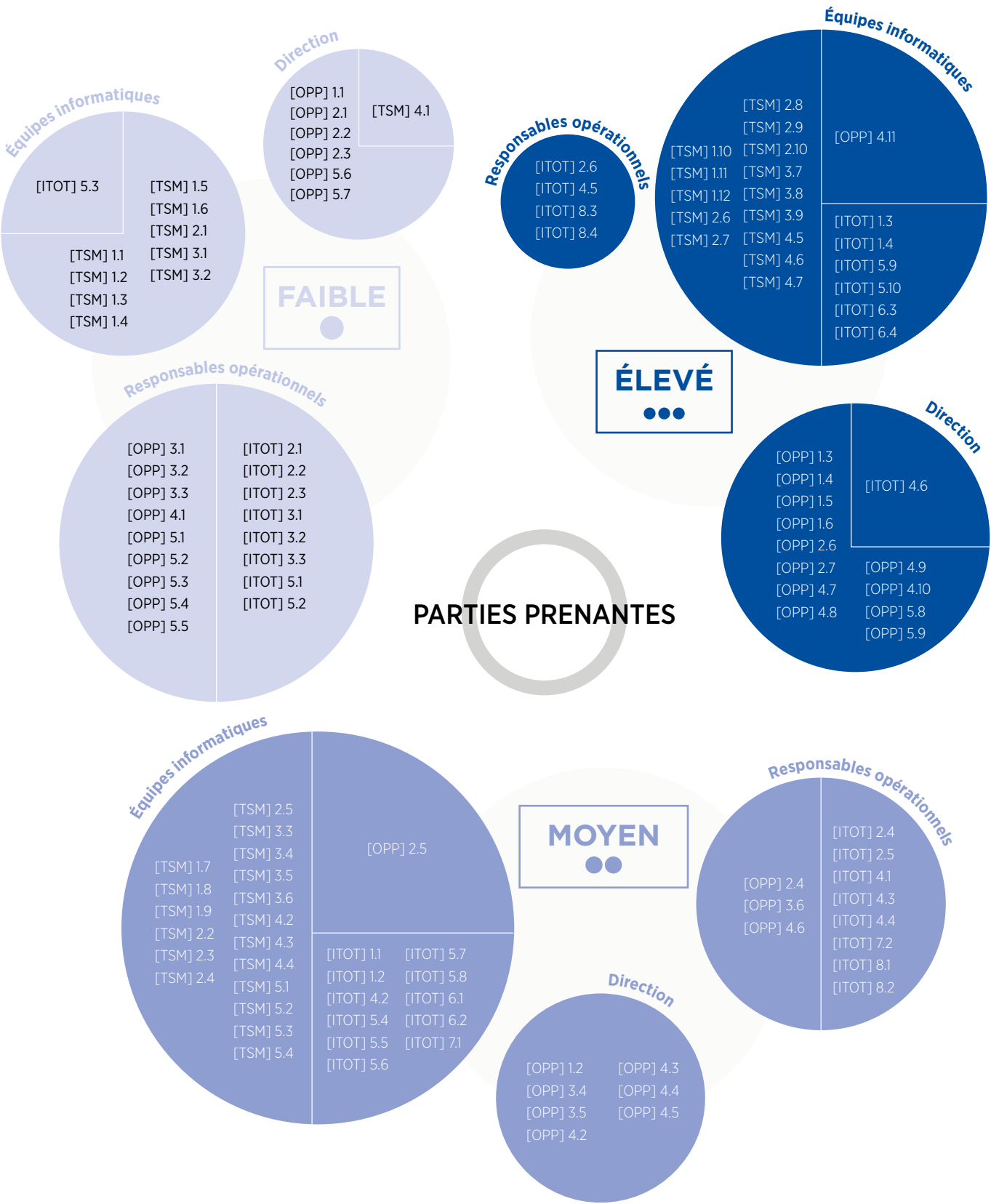
Le niveau de maturité est considéré comme atteint si :

1. la moyenne des mesures du niveau cible est au minimum de 2,5 ;
2. la moyenne des mesures du niveau immédiatement inférieur au niveau cible est 3,5 ;
3. la moyenne des mesures du niveau encore inférieur est de 4.

Par exemple, pour atteindre le niveau « moyen », il faut que la moyenne des notes des mesures moyennes soit de 2,5 ou mieux et que la moyenne des mesures de niveau faible soit 3,5 ou plus. Pour atteindre le niveau élevé, il faut une moyenne des mesures du niveau élevé de 2,5 ou plus, une moyenne des mesures du niveau moyen de 3,5 ou plus et une moyenne des niveaux faibles de 4 ou plus.

Tableau d'applicabilité des mesures

Le tableau ci-dessous propose les mesures à mettre en œuvre par les parties prenantes en fonction du niveau de maturité cible visé par la Direction.





Glossaire



Düsseldorf, Allemagne - Rhin

Automate programmable industriel (PLC « en anglais pour « programmable logic controller »)

Dispositif électronique numérique programmable destiné à la commande de processus industriels par un traitement séquentiel. Il envoie des ordres à des (pré)actionneurs à partir de données d'entrées (capteurs), de consignes et/ou d'un programme informatique. Les PLC sont largement utilisés dans presque tous les processus industriels. Pour les processus complexes, un SCADA est généralement présent pour assurer la coordination entre plusieurs PLC et leur mise en réseau à plus grande échelle¹⁰.

BYOD

Signifie "Bring Your Own Device" (apportez votre équipement personnel). Dans un contexte d'entreprise, le BYOD est une pratique des employés, parfois encouragée et parfois refrénée, d'utiliser certains équipements personnels pour travailler. Typiquement, il peut s'agir de leur smartphone et parfois aussi de leur ordinateur portable. Pour les employés, l'objectif est le confort d'utiliser des appareils que l'on connaît et que l'on apprécie. Pour l'entreprise, cette pratique peut permettre de faire des économies. Sur un plan de la cybersécurité, les équipements personnels peuvent représenter un défi car il est souvent impossible de les sécuriser convenablement et la multiplicité des marques et des modèles augmente les risques.

Centre des opérations de sécurité (SOC en anglais pour « Security Operation Center »)

Un centre des opérations de sécurité est un service au sein d'une organisation qui assure une fonction de centralisation des opérations de sécurité informatique. Ce service est capable d'intervenir auprès des employés de l'organisation, des processus et des technologies pour surveiller et améliorer en permanence la posture de sécurité de l'organisation tout en prévenant, détectant, analysant et gérant les incidents de cybersécurité¹¹.

CFM

Gestion de chargement et de déchargement des bâtiments.

Crown Jewel

Les « joyaux » sont les actifs les plus critiques pour l'accomplissement de la mission d'une organisation. Une analyse est nécessaire pour les identifier parmi l'ensemble des actifs.¹²

Durcissement (hardening)

Processus de sécurisation d'un système par suppression des composants inutiles au fonctionnement d'un système (par exemple un PC ou un serveur). Le durcissement consiste à réduire la « surface d'attaque » du système, c'est-à-dire à enlever toutes les choses inutiles installées par défaut et qui pourraient (potentiellement) contenir des vulnérabilités (applications, bibliothèques logicielles, modules optionnels, etc.). Il est communément admis que la quantité de failles exploitables dans un système est environ proportionnelle au nombre de lignes de codes qu'il contient. Donc, le fait de supprimer des composants non nécessaires a aussi pour effet de réduire le nombre de failles exploitables par un attaquant.

Hacktivisme

Piratage informatique (par l'infiltration et la perturbation d'un réseau ou d'un site web) visant à promouvoir les objectifs de l'activisme politique ou social¹³.

Hameçonnage (phishing)

Escroquerie par laquelle un utilisateur d'Internet est amené par la ruse (par exemple par un message électronique trompeur) à révéler des informations personnelles ou confidentielles que l'escroc peut utiliser de manière illicite¹⁴.

Impact

Ce terme désigne les conséquences d'un incident de cybersécurité, lorsque celui-ci survient (et indépendamment de sa probabilité de survenue). La question clé à se poser est donc : si tel incident de cybersécurité survient, alors – au pire – que se passe-t-il ensuite ? Dès le départ, l'impact peut être important ou non. Par exemple, la destruction d'un serveur (l'incident de cybersécurité) peut avoir un impact très différent selon qu'il s'agisse d'un serveur de développement ou d'un serveur critique opérationnel. Toutefois, l'impact peut être réduit en mettant au point des stratégies de contournement et en rendant le système plus résilient grâce à des procédures d'urgence par exemple. Dans le cas d'un serveur critique, on peut en prévoir un second prêt à prendre le relai si le premier est défaillant. En cas de perte de données, on peut avoir une sauvegarde, etc. L'impact est toujours évalué sans tenir compte de la menace (voir définition).

¹⁰ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>

¹¹ <https://www.trellix.com/en-us/security-awareness/operations/what-is-soc.html>

¹² <https://www.mitre.org/our-impact/intellectual-property/crown-jewels-analysis>

¹³ <https://www.merriam-webster.com/dictionary/hacktivism>

¹⁴ <https://www.merriam-webster.com/dictionary/phishing>

Incident (de cybersécurité)

Terme générique utilisé pour désigner un événement entraînant des conséquences négatives sur le plan de la cybersécurité. L'origine de cet incident peut être une panne matérielle (un disque dur défaillant), un plantage (un serveur qui redémarre), un sabotage (introduction volontaire d'un virus informatique), une erreur humaine (clic malheureux sur un email piégé) ou même une négligence (un employé inscrit son code PIN au dos de sa carte à puce). Lorsque les conséquences de cet incident sont traitées à temps, l'incident se termine. Lorsque ce n'est pas le cas, l'incident peut se transformer en crise avec un effet de propagation et des conséquences qui s'aggravent plus ou moins rapidement avec le temps.

Ingénierie sociale

L'ingénierie sociale désigne toutes les techniques visant à convaincre une cible de révéler des informations spécifiques ou d'effectuer une action spécifique pour des raisons illégitimes¹⁵.

ITIL

(Information Technology Infrastructure Library) est un ensemble de bonnes pratiques pour la fourniture de services numériques. La norme ISO-20000 est issue des bonnes pratiques décrites par ITIL.

LBM

Signifie "Lock and Bridge Management" (Gestion des ponts et des écluses) La gestion des ponts et des écluses est assurée par des ouvrages, tels que les ponts mobiles, et des installations permettant de modifier le niveau de l'eau, tels que les écluses et les sas, qui constituent des systèmes particulièrement critiques car présentant un risque d'inondation généralisée en cas de cyberattaque¹⁵.

Menace

Une menace est un acteur, une circonstance ou un événement susceptible d'avoir un impact négatif sur une organisation (ses opérations, ses actifs, son image ou des personnes qui y sont rattachées) ou, à travers elle, sur d'autres organisations en lien avec elle. Pour générer cet impact, la menace doit exploiter une ou plusieurs vulnérabilités selon un certain scénario. Plus le scénario est plausible, plus les vulnérabilités sont importantes et plus les menaces sont nombreuses, plus la probabilité de survenue d'un incident de cybersécurité est importante. On parle alors de menace élevée. Par exemple, le niveau de menace d'un serveur exposé sur l'Internet est plus élevé que celui d'un serveur exposé uniquement sur un réseau interne, car il y a potentiellement plus de personnes qui peuvent essayer de le pirater. Très souvent, pour réduire la menace, on agit au niveau

des vulnérabilités, soit en les supprimant (ou en réduisant leur nombre), soit en complexifiant leur exploitabilité (en ajoutant des protections par exemple). Parfois il est possible d'agir directement sur le nombre d'acteurs, de circonstances ou d'événement susceptibles d'avoir un impact négatif. La menace est toujours évaluée sans tenir compte de l'impact (voir définition).

Porte dérobée (backdoor)

Dans un logiciel, une porte dérobée est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel.

Risque

Ce terme est formellement utilisé en cybersécurité pour évaluer un ensemble de menaces pesant sur un système de façon plus ou moins probable avec des conséquences plus ou moins graves. On parle de risque élevé lorsque la probabilité et l'impact d'une menace sont élevés, et de risque faible lorsque ceux-ci sont limités. L'analyse de risque consiste à évaluer indépendamment les probabilités et les impacts des différentes menaces et à en tirer les conséquences globalement. À titre d'illustration, le « risque inondation » est évalué à la fois en fonction de la probabilité d'une inondation (zones inondables) mais aussi en fonction des caractéristiques de la zone concernée, par exemple si elle est fortement peuplée ou non. Aussi, le risque inondation est considéré à peu près identique dans une zone inondable mais très peu peuplée et dans une zone non inondable mais très fortement peuplée (par « zone non inondable », il faut comprendre avec une probabilité faible – mais non nulle – d'être inondée). La diminution du risque peut donc se faire en limitant l'impact ou en diminuant la probabilité. Dans le cas du risque inondation, on peut canaliser les cours d'eau, construire des barrages et des bassins de rétention (pour limiter la probabilité) ou bien créer des digues pour protéger les maisons, favoriser l'architecture sur pilotis et éviter l'accumulation de population en zone inondable (pour limiter l'impact)¹⁶.

SCADA

"Supervisory Control And Data Acquisition" (Système de contrôle et d'acquisition de données). Un système SCADA est un système de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémesures et de contrôler à distance des installations techniques. C'est une technologie industrielle dans le domaine de l'instrumentation. Sur un plan de la cybersécurité, les équipements SCADA constituent un enjeu fort car ce sont des équipements connectés à un réseau qui, si on en prend le contrôle, permettent de piloter les installations techniques sous-jacentes.

¹⁵ <https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering>

¹⁶ <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

Spoofing

Dans le contexte de la cybersécurité, le spoofing est un ensemble de techniques destinées à tromper une cible quant à l'origine réelle d'une information qu'elle reçoit. Selon les techniques mises en œuvre, on parle aussi d'usurpation, de masquage, de substitution, etc.

Vulnérabilité

Faiblesse d'un système informatique, des procédures de sécurité du système, des contrôles internes ou de la mise en œuvre qui pourrait être exploitée ou déclenchée par une source de menace.

WEP/WPA/WPA2/WPA3

Ces acronymes correspondent à des protocoles de sécurisation d'accès à un réseau sans fil (Wi-Fi). WEP (Wired Equivalent Privacy) est apparu en 1999. Le WEP était très peu sécurisé, c'est pourquoi le protocole WPA (Wi-Fi Protected Access) a été inventé pour le remplacer en 2003. Dès le départ, WPA a été conçu comme un protocole transitoire. De fait, il a été remplacé par WPA2 en 2004, qui est basé sur la norme 802.11i de l'Institute of Electrical and Electronics Engineers (IEEE). WPA3 a été publié en 2017, mais il ne constitue qu'une simple évolution de WPA2, qui n'est pas (encore) obsolète et reste très utilisé en 2023. WPA2 existe en deux versions. D'une part WPA2 version « personnelle » (aussi appelée WPA2-PSK pour « Pre-shared Key »), basée sur une clé partagée et destinée à un usage domestique, familiale ou dans une très petite structure. D'autre part WPA2 « Entreprise », basé sur une authentification RADIUS (plusieurs utilisateurs avec des comptes différents) et destiné à un usage en entreprise. À noter que WPA2-PSK permet l'utilisation de deux algorithmes de chiffrement : AES et TKIP. L'algorithme AES est plus sécurisé.

Crédits photos

Photos fournies par la Fédération européenne des ports intérieurs (FEPI)

P 28 : © Steve Haider

P 45 : © Patrik Walde, patrikwalde.com

P 46 : © AZS Group Bonn

P 58 : © Port de Düsseldorf

Shutterstock

Adobe stock

Direction artistique & Maquette : Agence dot. Deloitte France

