GUIDE DES BONNES PRATIQUES DE SÉCURITÉ INFORMATIQUE À BORD DES NAVIRES

Systèmes d'information et réseaux informatiques ont progressivement envahi le monde du transport maritime et sont désormais omniprésents sur les navires : systèmes de navigation, postes bureautiques utilisés par l'équipage, systèmes « métier » tels que, par exemple, le poste de contrôle de la cargaison d'un super tanker, ou les systèmes de gestion de plate-forme (propulsion, électricité, fluides…).

Cette formidable évolution s'est accompagnée de l'émergence de nouveaux risques, encore trop souvent sous-estimés par les compagnies maritimes : intrusions au sein d'un réseau, vol de données, prise de contrôle à distance de systèmes informatiques, etc.

La protection face à ces menaces relève pourtant la plupart du temps de réflexes simples. Les mesures présentées dans ce guide, accessibles aux non-spécialistes, concourent à élever significativement le niveau de sécurité informatique à bord des navires. Issues du Guide des bonnes pratiques de l'informatique (CGPME – ANSSI, mars 2015), elles ont été adaptées aux spécificités du transport maritime.

Les premières de ces mesures s'adressent à l'équipage et, pour la plupart, devraient pouvoir être appliquées par tous ses membres. Les suivantes concernent davantage les responsables des systèmes d'information de la compagnie. Cette distinction dépend toutefois de la répartition des rôles et des responsabilités en matière informatique au sein de la compagnie, entre le bord et le siège.

Chaque compagnie est ainsi invitée à s'approprier ces différentes recommandations et à les adapter à son contexte et à son organisation spécifique.

Thierry COQUIL
Directeur des affaires maritimes

Guillaume POUPARD
Directeur général de l'agence nationale de la sécurité des systèmes d'information

En bref :

LES PRINCIPAUX CONSEILS À RETENIR PAR TOUT L'ÉQUIPAGE

Bien choisir ses mots de passe

Un mot de passe de qualité possède au moins 8 caractères de types différents, n'a pas de lien avec l'utilisateur et ne figure pas dans le dictionnaire. Définissez des mots de passe différents pour des systèmes ou des services sensibles distincts. N'enregistrez pas vos mots de passe dans un fichier ou dans un navigateur Internet, notamment en cas d'utilisation d'un équipement public ou partagé.

Utiliser sa messagerie avec vigilance

Vérifiez l'identité de l'expéditeur. N'ouvrez pas de pièce jointe et ne cliquez pas sur un lien Internet provenant d'un expéditeur suspect ou inconnu.

Séparer les usages personnels et professionnels

Ne transférez pas vos messages électroniques professionnels vers une messagerie personnelle. N'utilisez pas de moyens personnels de stockage (clé USB, disque dur externe, cloud…) pour enregistrer vos données professionnelles.

Être prudent sur Internet

Réseaux sociaux, forums, formulaires, … : veillez à limiter la diffusion de vos informations personnelles via Internet. Avant un paiement en ligne, vérifiez l'authenticité et le niveau de sécurité du site Internet.

Sauvegarder régulièrement ses données

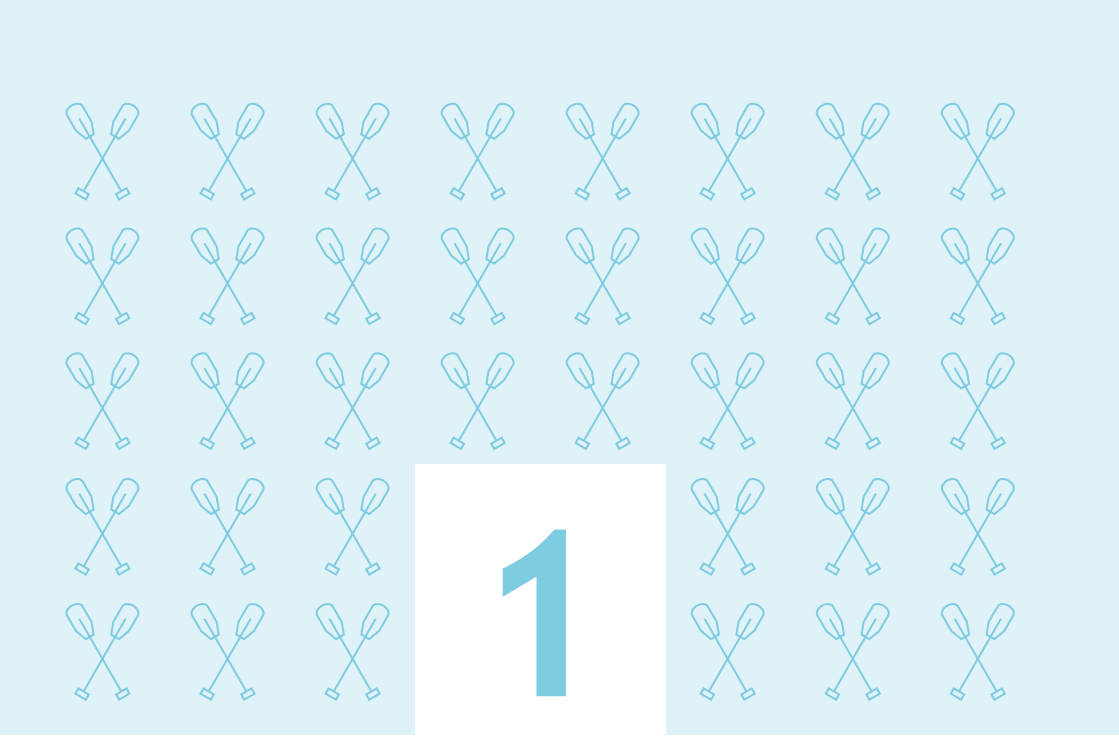
Anticipez une panne, une perte ou un vol, en sauvegardant régulièrement vos données, au moyen de supports externes dédiés, conservés en lieu sûr.

Maîtrisez les logiciels installés sur vos équipements informatiques

N'installez que les logiciels dont vous avez réellement besoin, et toujours avec l'aval préalable d'un référent informatique. Ne téléchargez vos logiciels que depuis des sites fiables et effectuez régulièrement les mises à jour.

I

RECOMMANDATIONS AUX MEMBRES D'ÉQUIPAGE



1

Choisir avec soin ses mots de passe

Le mot de passe est le moyen le plus fréquemment utilisé pour s'authentifier sur un équipement numérique et, ainsi, accéder à ses données ou commander des actions. Afin de bien protéger vos informations ou les équipements de bord, la qualité du mot de passe est essentielle.

Un mot de passe fort est un mot de passe difficile à retrouver avec des outils spécialisés mais facile à retenir. Un mot de passe fort doit avoir au moins 8 caractères (idéalement 12 caractères), dont au moins une majuscule, une minuscule, un chiffre et un caractère spécial. Choisissez des mots de passe n'ayant aucun lien avec vous (nom, date de naissance…) et ne figurant pas dans le dictionnaire [1].

Utilisez des mots de passe différents pour vous authentifier auprès de systèmes ou de services sensibles distincts. En particulier, les mots de passe protégeant des usages privés (messagerie personnelle, site Web marchand…) ne doivent jamais être réutilisés dans un contexte professionnel.

Lorsqu'un compte est partagé par plusieurs utilisateurs, son mot de passe doit être renouvelé à chaque départ ou réaffectation d'un utilisateur.

Ne stockez pas vos mots de passe dans des fichiers bureautiques. Si vous souhaitez sauvegarder vos mots de passe, utilisez une solution sécurisée dédiée.

À bord :

- déterminez des règles pour le format des mots de passe (longueur, complexité) et faites les respecter ;
- modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent ;
- ne conservez pas les mots de passe dans des fichiers ou sur des post-it ;
- lorsque vous naviguez sur Internet, ne préenregistrez pas vos mots de passe dans les navigateurs, notamment en cas d'utilisation d'un équipement public ou partagé.

Enfin, au-delà de l'utilisation d'un mot de passe fort, pensez toujours à verrouiller votre session, même lors d'une absence courte, afin d'empêcher tout accès non autorisé à votre poste.

---

1 : La méthode des premières lettres peut vous aider à définir simplement des mots de passe forts à partir des paroles d'une chanson, d'un proverbe… « Contre nous de la tyrannie, L'étendard sanglant est levé ! » permet par exemple de définir et de mémoriser le mot de passe « Cndlt,L'ésel! ».

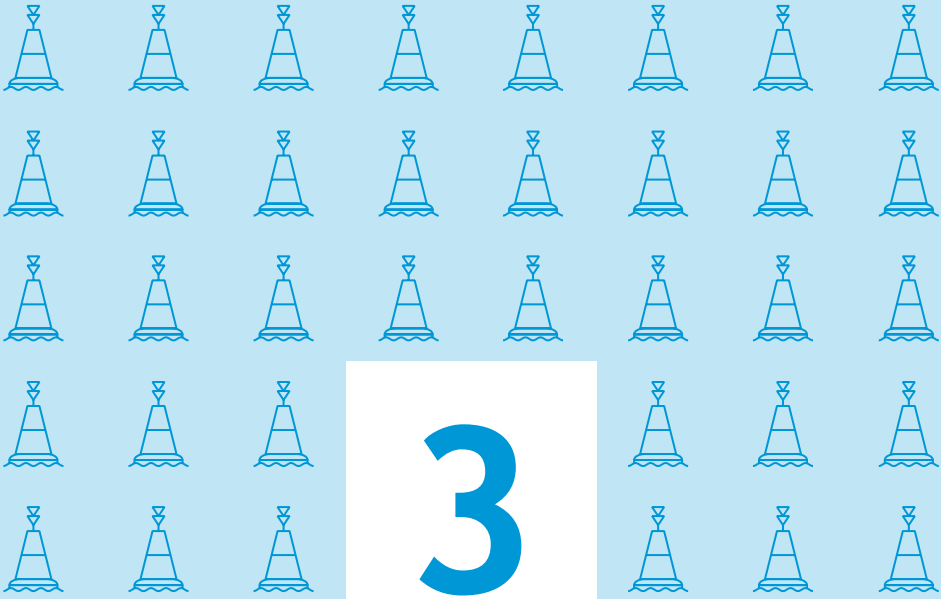
2

Être prudent lors de l'utilisation de sa messagerie

Les courriels et leurs pièces jointes jouent un rôle central dans la réalisation des attaques informatiques les plus courantes (courriels frauduleux, pièces jointes piégées, etc.). Un courriel malveillant peut porter atteinte au poste utilisé pour le consulter mais également à l'ensemble du système d'information auquel ce poste est connecté. C'est ainsi potentiellement toute l'informatique à bord qui peut être affectée.

Lorsque vous recevez des courriels, prenez les précautions suivantes :

- l'identité d'un expéditeur n'étant en rien garantie, vérifiez la cohérence entre l'expéditeur présumé et le contenu du message et vérifiez son identité. En cas de doute, n'hésitez pas à contacter directement l'émetteur du mail ;
- n'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts ;
- ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel, numéro de carte bancaire). En effet, des courriels usurpent les couleurs d'institutions dans le but de récupérer vos données. Il s'agit d'attaques par hameçonnage (ou « phishing ») ;
- n'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc. ;
- désactivez l'ouverture automatique des documents téléchargés.



3

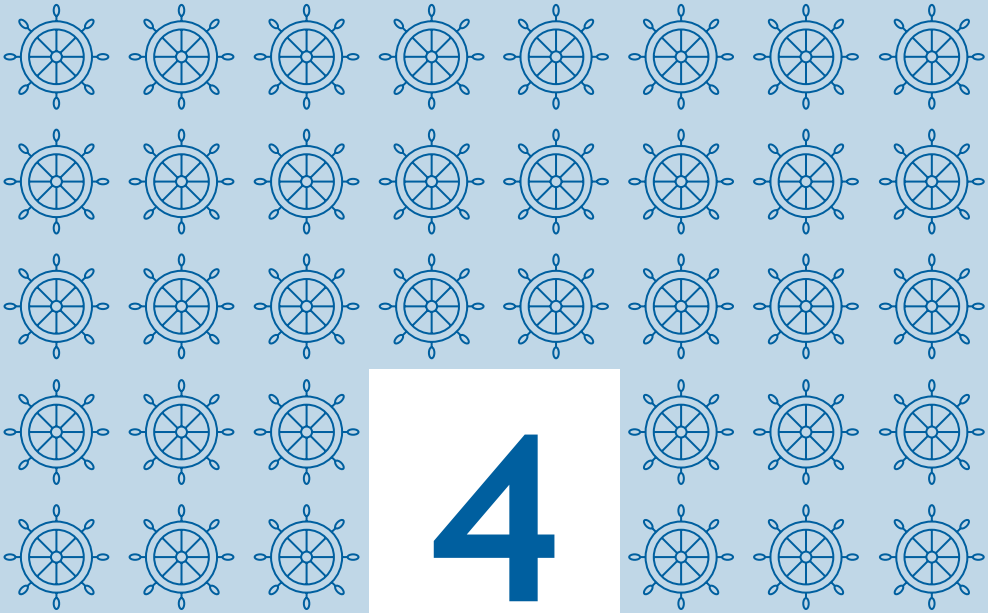
Séparer les usages personnels des usages professionnels

Les usages et les mesures de sécurité sont différents sur les équipements informatiques personnels et professionnels (ordinateurs, smartphones…).

L'utilisation d'équipements personnels dans un contexte professionnel peut porter atteinte à la sécurité des données du navire et de l'entreprise (vol ou perte des appareils, intrusion, manque de contrôle sur l'utilisation des appareils, fuite de données lors du départ d'un collaborateur).

Il est donc recommandé de séparer vos usages personnels et vos usages professionnels :

- ne faites pas suivre vos messages électroniques professionnels sur des services de messagerie utilisés à titre personnel ;
- n'hébergez pas de données professionnelles sur vos équipements personnels (clé USB, smartphone…) ou sur des moyens personnels de stockage en ligne ;
- ne connectez pas de supports amovibles personnels (clé USB, disques durs externes…) aux ordinateurs du navire ou de l'entreprise.



4

Être prudent sur Internet

Prenez soin de vos informations personnelles, professionnelles et de votre identité numérique.

Les données que vous laissez sur Internet vous échappent instantanément. Des personnes malveillantes peuvent récolter vos informations personnelles à votre insu, afin par exemple de deviner vos mots de passe, vous tendre des pièges à l'aide de courriers électroniques personnalisés, d'accéder à votre système informatique, etc.

C'est pourquoi la plus grande prudence est conseillée dans la diffusion de vos informations personnelles sur Internet :

- soyez vigilant vis-à-vis des formulaires que vous êtes amené à remplir, en ne transmettant que les informations strictement nécessaires et en pensant à décocher les cases qui autoriseraient le site à conserver ou à partager vos données ;
- ne donnez accès qu'à un minimum d'informations professionnelles sur les réseaux sociaux, et soyez vigilant lors de vos interactions avec les autres utilisateurs ;
- pensez à vérifier régulièrement vos paramètres de sécurité et de confidentialité (voir le Guide de la CNIL sur la sécurité des données personnelles) ;
- utilisez plusieurs adresses électroniques dédiées à vos différentes activités sur Internet.

Soyez vigilant lors d'un paiement sur Internet.

Lorsque vous réalisez vos achats sur Internet, vos coordonnées bancaires sont susceptibles d'être interceptées par des attaquants directement sur votre ordinateur. C'est pourquoi, avant d'effectuer un paiement en ligne, il est nécessaire de procéder à certaines vérifications relatives au site Internet :

- contrôlez la présence d'un cadenas dans la barre d'adresse (remarque : ce cadenas n'est pas visible sur tous les navigateurs) ;
- assurez-vous que l'adresse du site Internet commence par « https:// » ;
- vérifiez l'exactitude de l'adresse du site Internet en prenant garde notamment aux fautes d'orthographe.

De manière générale, ne transmettez **jamais** le code confidentiel à 4 chiffres de votre carte bancaire et n'hésitez pas à consulter votre banque pour connaître les moyens sécurisés qu'elle propose.

5

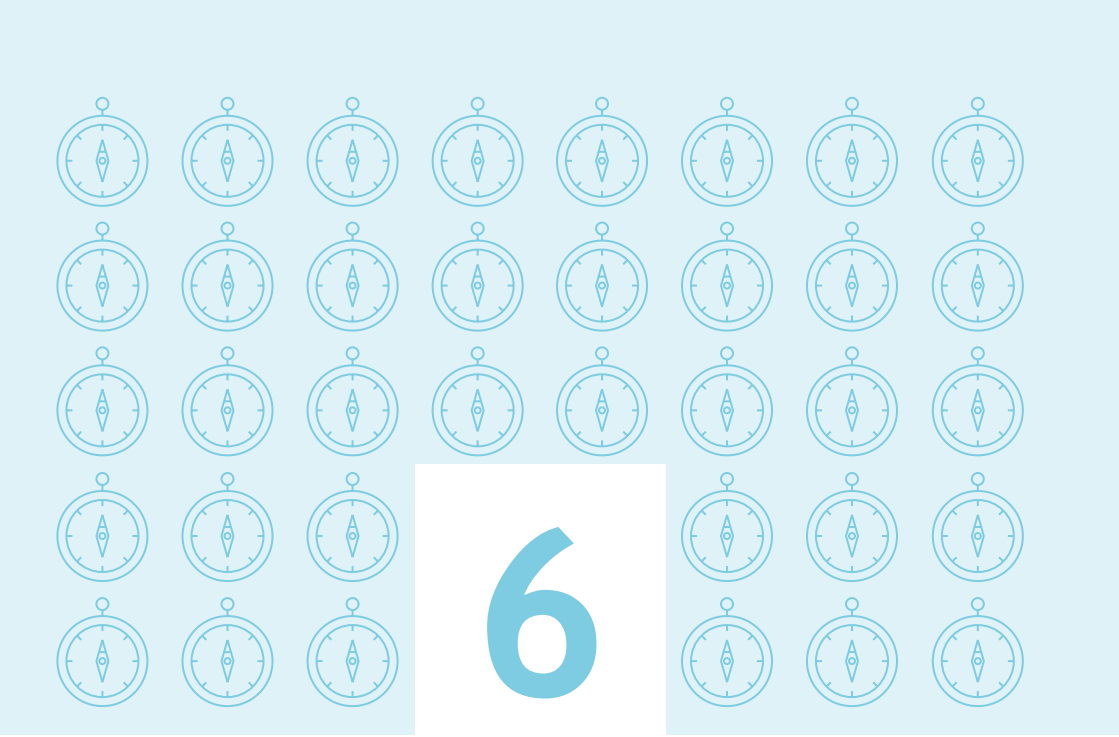
Télécharger ses logiciels sur les sites officiels des éditeurs

Si vous téléchargez du contenu sur des sites Internet dont la confiance n'est pas assurée, vous prenez le risque d'enregistrer sur votre ordinateur des programmes contenant des virus ou des chevaux de Troie . Cela peut permettre à des personnes malveillantes de prendre le contrôle à distance de votre machine et, potentiellement, des systèmes informatiques du bord, afin d'espionner, de voler vos données personnelles ou professionnelles, de lancer des attaques, etc.

Dans ce contexte, afin de veiller à la sécurité de votre ordinateur, de vos données et du navire :

- ne téléchargez pas vos logiciels sur des sites au contenu douteux. Privilégiez les sites des éditeurs reconnus ;
- lors de l'installation, pensez à décocher ou désactiver toutes les cases proposant d'installer des logiciels complémentaires ;
- restez vigilants concernant les liens sponsorisés ;
- désactivez l'ouverture automatique des documents téléchargés.

Plus généralement, n'installez jamais un logiciel ou une application sans l'accord ou l'avis préalable d'un référent informatique.



6

Quelques conseils supplémentaires

Soyez aussi prudent avec votre smartphone ou votre tablette qu'avec votre ordinateur.

Bien que proposant des services innovants, les smartphones sont aujourd'hui très peu sécurisés. Il est donc indispensable de leur appliquer certaines règles élémentaires de sécurité informatique :

- n'installez que les applications nécessaires et vérifiez à quelles données (informations géographiques, contacts, appels téléphoniques…) elles peuvent avoir accès avant de les télécharger. Il est recommandé d'éviter d'installer des applications qui demandent l'accès à des données qui ne sont pas nécessaires à leur fonctionnement ;
- en plus du code PIN qui protège votre carte téléphonique, utilisez un mot de passe pour sécuriser l'accès à votre terminal et le configurer pour qu'il se verrouille automatiquement ;
- effectuez des sauvegardes régulières de vos contenus sur un support externe pour pouvoir les conserver en cas de restauration de votre appareil dans son état initial ;
- ne préenregistrez pas vos mots de passe.

Protégez vos outils informatiques lors de vos déplacements.

À l'étranger, lors de vos déplacements à terre, soyez prudent si vous devez emporter des équipements informatiques (PC portable, smartphone…). Voyager avec des appareils nomades professionnels fait peser des menaces sur les informations qu'ils contiennent, dont la perte ou le vol peuvent avoir des conséquences importantes sur les activités de votre organisation. Il convient notamment de :

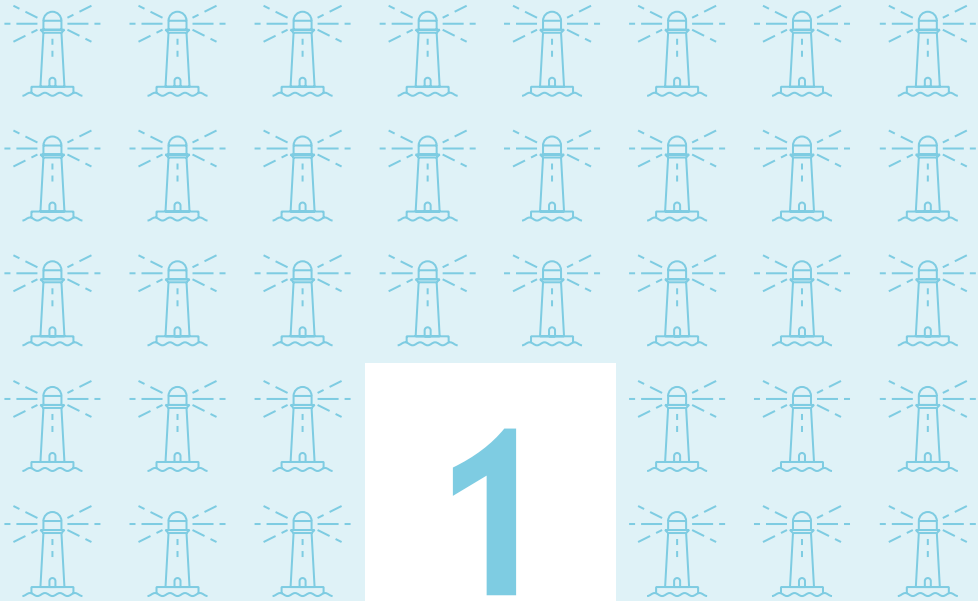
- vous assurer que vos données sont sauvegardées, afin de pouvoir les retrouver en cas de perte de vos équipements ;
- vérifier que vos mots de passe ne sont pas préenregistrés ;
- garder vos appareils et support avec vous (ne les laissez pas dans un bureau et, s'ils contiennent des informations sensibles, n'utilisez pas les coffres d'hôtel) ;
- désactiver les fonctions Wi-Fi et Bluetooth de vos appareils lorsque vous ne les utilisez pas ;
- éteindre votre téléphone et, lorsque cela est possible, en retirer la carte SIM et la batterie, si vous être contraint de vous en séparer ;

- informer votre hiérarchie en cas d'inspection ou de saisie de votre matériel par des autorités étrangères ;
- ne jamais connecter vos équipements à des postes qui ne sont pas de confiance ;
- refuser la connexion d'équipements appartenant à des tiers à vos propres équipements ;
- ne jamais utiliser les clés USB qui peuvent vous être offertes : très prisées des attaquants, elles sont susceptibles de contenir des programmes malveillants.

…Et pour compléter ces différentes recommandations, pensez à prendre connaissance de la Politique de sécurité informatique de votre compagnie.

II

RECOMMANDATIONS AUX COMPAGNIES



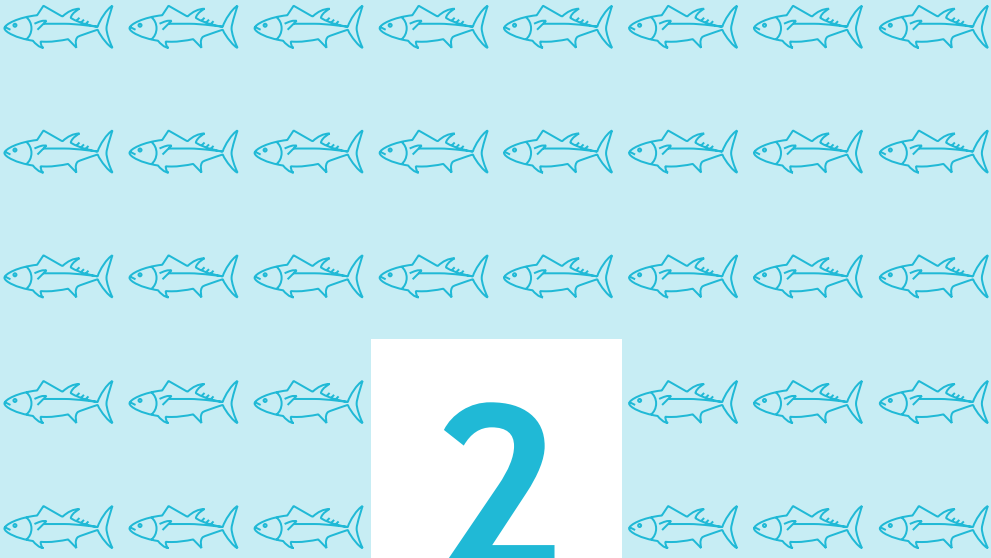
1

Sensibiliser les personnels

La sensibilisation de tous les membres de l'équipage et, plus largement, des personnels de la compagnie, aux bonnes pratiques élémentaires de sécurité informatique, est fondamentale pour réduire efficacement les risques liés à de mauvaises pratiques.

La prévention des incidents et attaques informatiques relève la plupart du temps de réflexes simples, tels que ceux présentés dans le présent guide. Il est donc primordial que chacun soit régulièrement impliqué et sensibilisé, au moyen de séances d'information, de guides et, idéalement, d'une charte d'usage des moyens informatiques.

Un référent informatique doit être identifié, notamment à bord, afin d'être l'interlocuteur du personnel pour toute question liée à la sécurité informatique.



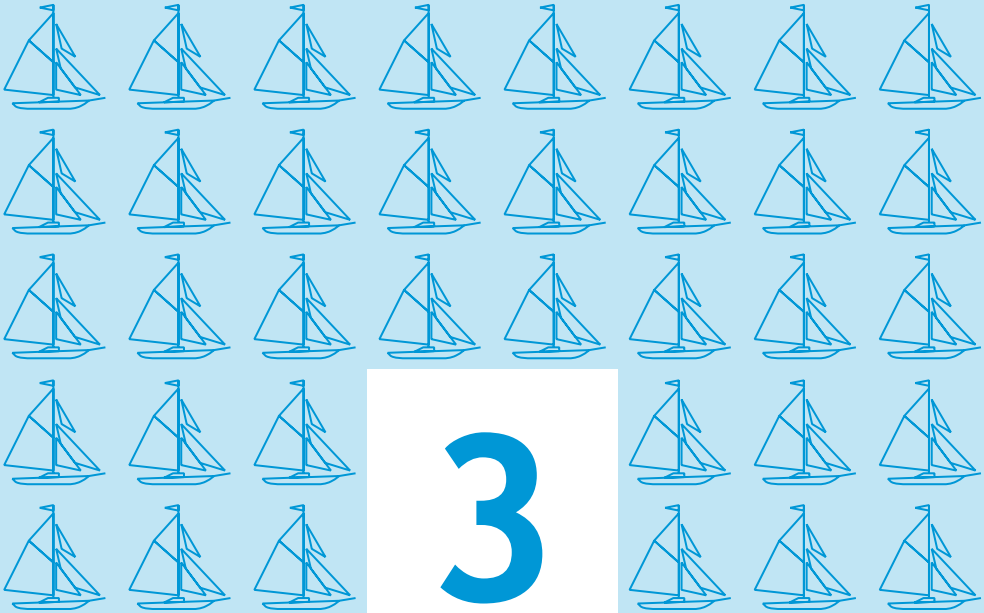
2

Prévoir des sauvegardes régulières

Pour veiller à la sécurité des données à bord, il est vivement conseillé d'effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires). Il sera ainsi possible d'en disposer suite à un dysfonctionnement du système d'exploitation, à une erreur de manipulation ou à une attaque informatique.

Pour sauvegarder les données, des supports externes tels que des disques durs externes réservés exclusivement à cet usage ou, à défaut, des CD ou DVD enregistrables devraient être mis à disposition de l'équipage. De tels supports doivent être rangés dans un lieu éloigné du système sauvegardé. Il convient en outre d'accorder une attention particulière à leur durée de vie.

Idéalement, un serveur de stockage sécurisé en réseau – ou NAS (Network Attached Storage) – pourrait être mis en place sur le réseau du bord. Un tel serveur comporte plusieurs disques de sauvegarde et, de ce fait, garantit un niveau élevé de disponibilité des données. Il convient de veiller à disposer de disques durs neufs de réserve en cas de panne et de procéder fréquemment à une inspection du NAS afin de détecter au plus tôt le dysfonctionnement d'un disque dur.



3

Bien connaître ses utilisateurs et ses prestataires

Lorsque l'on accède à un système informatique, que ce soit un PC bureautique ou un système « métier », on bénéficie de droits d'utilisation plus ou moins élevés sur celui-ci. On distingue généralement les droits dits « d'utilisateur » et les droits dits « d'administrateur ».

Les différents comptes sur les systèmes de bord doivent être créés et gérés avec la plus grande attention :

- N'attribuez de comptes administrateurs qu'aux personnes en ayant strictement besoin du fait de leur fonction à bord (exemple : officier électronicien en charge de l'informatique).
- Les comptes administrateurs doivent être utilisés uniquement pour certaines actions liées au fonctionnement du système informatique, telles que la gestion de comptes utilisateurs, l'installation ou la mise à jour de logiciels, la maintenance, etc.. Ils ne doivent jamais être utilisés pour des actions qui ne le nécessitent pas, en particulier pour naviguer sur Internet ou utiliser la messagerie.
- Dans l'utilisation au quotidien, on ne doit se servir que des comptes utilisateurs.
- Identifiez précisément les différents utilisateurs de chaque système informatique et les types de comptes qui leur sont attribués.
- Supprimez tous les comptes anonymes ou génériques. Chaque utilisateur doit pouvoir être identifié nommément afin de pouvoir relier chaque action à un utilisateur.
- Établissez et faites respecter des procédures encadrant les mouvements de personnels : il convient de s'assurer que les droits octroyés sur les systèmes d'information sont appliqués au plus juste et qu'ils sont révoqués dès le départ d'une personne.

4

Mettre régulièrement à jour ses logiciels

Dans chaque logiciel, application ou système d'exploitation, il existe des vulnérabilités potentielles. Une fois découvertes, celles-ci sont corrigées par les éditeurs, qui proposent alors aux utilisateurs des mises à jour de sécurité. Malheureusement, de nombreux utilisateurs ne procèdent pas à ces mises à jour et les attaquants peuvent alors exploiter ces vulnérabilités encore longtemps après leur découverte et leur correction.

Il convient par conséquent de définir et de faire appliquer, pour les systèmes à bord du navire, une politique de mises à jour régulières compatible avec les contraintes du bord. Cette politique identifiera les éléments à mettre à jour, les acteurs en charge de ces mises à jour, ainsi que les moyens de récupération de ces mises à jour.

Seules des sources fiables doivent être utilisées pour la récupération des mises à jour, telles que les sites Internet officiels des éditeurs.

Afin de procéder aux mises à jour en toute sécurité de certains systèmes « métier » indispensables à l'exploitation du navire, il peut être préconisé d'effectuer celles-ci lors des mises en cale sèche périodiques.

5

Sécuriser l'accès Wi-Fi du navire

Si l'utilisation du Wi-Fi présente certains bénéfices, il ne faut pas oublier qu'un réseau Wi-Fi insuffisamment ou mal sécurisé peut permettre à des tiers d'intercepter vos données et d'utiliser la connexion Wi-Fi à votre insu pour réaliser des opérations malveillantes. En escale, la portée du Wi-Fi (une centaine de mètres) peut permettre des connexions non légitimes au réseau du navire depuis la terre.

À bord des navires équipés d'un réseau Wi-Fi, celui-ci doit être configuré de manière à utiliser le protocole de chiffrement WPA2. À défaut, le protocole WPA-AES doit être utilisé (ne jamais activer le chiffrement WEP, cassable en quelques minutes).

La clé de connexion doit être un mot de passe de plus de 12 caractères de types différents. Elle n'est communiquée qu'à des personnes de confiance et doit être changée régulièrement.

Le réseau Wi-Fi du navire ne devrait permettre l'accès qu'au réseau réservé à l'utilisation des ordinateurs personnels de l'équipage (parfois appelé réseau « Welfare »).

Enfin, lors des escales, à terre, n'utilisez pas les Wi-Fi « publics » offerts dans les ports, les hôtels…, pour des raisons de sécurité.

6

Mettre en place un cloisonnement du réseau

Dans un réseau « à plat », c'est-à-dire ne disposant pas d'équipement de filtrage, chaque équipement a la possibilité d'accéder à n'importe quel autre. Ainsi, la compromission d'un seul équipement pourra facilement s'étendre à l'ensemble du réseau. Il est en particulier essentiel de séparer le réseau bureautique connecté à Internet, par nature plus exposé aux attaques informatiques, des réseaux comportant les systèmes « métiers »

Les postes et les serveurs importants, les systèmes de navigation et de commande du navire, etc., doivent être isolés physiquement ou logiquement vis-à-vis les autres systèmes du navire.

Il est également recommandé de séparer les équipements destinés à des usages professionnels et les postes de travail destinés à des usages personnels, en les plaçant au sein de deux réseaux distincts.

La plupart des équipements d'accès (ou « box ») proposés par les fournisseurs d'accès à Internet par satellite et équipant les navires permettent ainsi la configuration de deux réseaux virtuels distincts et étanches (« VLAN » – virtual local area network). L'un devrait être exclusivement dédié aux équipements et usages professionnels, l'autre (parfois nommé « VLAN Welfare ») aux équipements et usages personnels.

Glossaire

- **Antivirus :** logiciel informatique destiné à identifier, neutraliser et effacer des logiciels malveillants.
- **Cheval de Troie :** programme qui s'installe de façon frauduleuse pour remplir une tâche hostile à l'insu de l'utilisateur (espionnage, envoi massif de spams,…).
- **Chiffrement :** procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui ne possède pas la clé de (dé)chiffrement.
- **Compte d'administrateur :** compte permettant d'effectuer des modifications affectant les utilisateurs (modification des paramètres de sécurité, installation de logiciels…).
- **Mise à jour :** action qui consiste à mettre à niveau un outil ou un service informatique en téléchargeant un nouveau programme logiciel.
- **Phishing (hameçonnage) :** méthode d'attaque qui consiste à imiter les couleurs d'une institution ou d'une société (banque, services des impôts) pour inciter le destinataire à fournir des informations personnelles.
- **Système d'exploitation :** logiciel qui, dans un appareil électronique, pilote les dispositifs matériels et reçoit des instructions de l'utilisateur ou d'autres logiciels.
- **Wi-Fi :** connexion Internet sans fil.

Version 1.1 - Octobre 2016
20161010-1200

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
www.ssi.gouv.fr / communication@ssi.gouv.fr