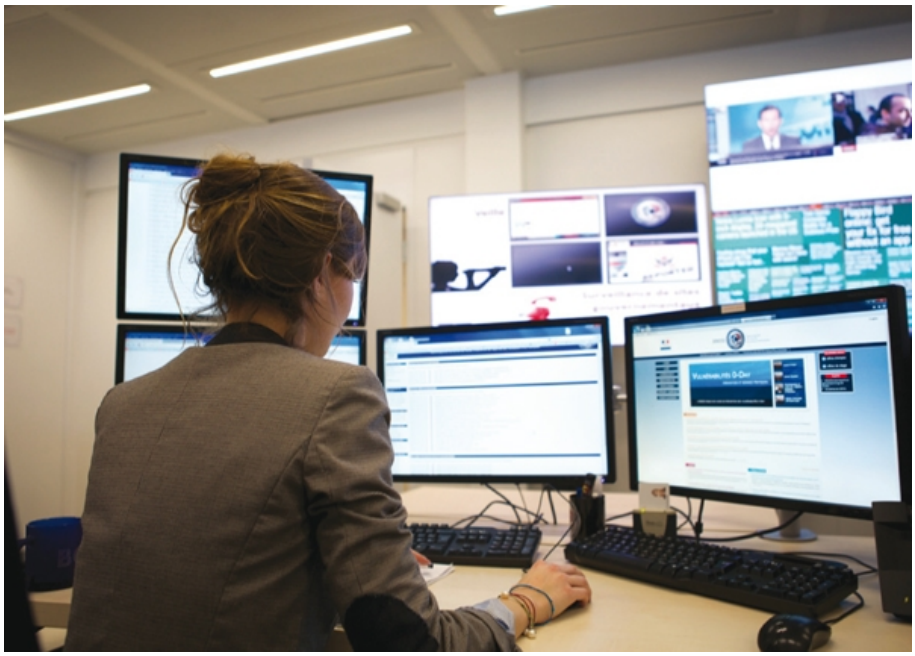
Les cyber attaques dans le transport maritime



Les cyber attaques dans le transport maritime

La cyber-défense est classée au rang des priorités par le gouvernement. Un plan d'investissement d'un milliard d'euros sur 5 ans a été dévoilé au début de l'année pour faire face à cette nouvelle menace.

Des cyber-attaques qui inquiètent aussi le monde maritime.
« Le transport et la logistique maritimes sont le prochain terrain de jeux des pirates informatiques » : c'est le BMI, le Bureau Maritime International qui le dit..
L'organisme est spécialisé dans la lutte contre la criminalité envers le commerce maritime, notamment la piraterie et les fraudes commerciales ainsi que dans la protection des équipages. Dans un communiqué publié le 20 août 2014, le BMI a tiré la sonnette d'alarme en appelant l'ensemble de secteur à se protéger contre les cyber-attaques..
Si ces cyber-menaces inquiètent c'est parce qu'aujourd'hui dans un bateau, presque tout est informatisé. Tout est connecté à Internet entre la terre et la mer.
Aujourd'hui il est possible pour un hacker (voire un État) de détourner des informations, de prendre le contrôle d'un navire ou même de son système d'armement..
Au début c'était un jeu, c'est devenu une véritable guerre. Vous avez des menaces de ce type-là qui sont organisées comme des réseaux terroristes.

Trafic de drogue, vol de données, kidnapping
Les spécialistes en cyber-défense ont identifié deux menaces principales, comme l'espionnage et le sabotage.
Un « espion » peut par exemple « voler les données techniques » pour connaître avec précisions le trajet emprunté par un bateau. Cela « permet à un concurrent de voler le marché et de pratiquer des prix plus bas », raconte Dominique Riban, de l'ANSSI (Agence nationale de sécurité des systèmes d'information).
C'est elle qui surveille les sites internet de l'État français. Elle a été créée après la publication du Livre blanc de la Défense en 2008.

Télécharger l'intégralité du Livre blanc de la Défense

« Tout est potentiellement attaquable »
L'angoisse des experts en cyber-défense c'est aussi l'attaque des géants des mers, ces containers géants qui débarquent dans les ports européens.
Le plus gros au monde doit transporter 20 000 containers pour une valeur de deux à quatre milliards de dollars. On y trouve tout un tas de systèmes de cartographie, d'informations. Tous ces systèmes là sont potentiellement attaquables.
Patrick Hebrard est titulaire de la chaire Cyber-défense des systèmes navals à l'Ecole navale. Il s'occupe aussi de cyber-défense chez DCNS. « La passerelle peut ne plus avoir la maitrise de sa propulsion et de sa gouverne », poursuit-il. « Un hacker pourrait complètement bloquer la barre d'un bateau. »
En 2011, l'Agence européenne de cyber-sécurité (ENISA) a publié un premier rapport européen sur la cyber-sécurité maritime. Elle évoquait déjà les menaces qui s'amplifiaient. Elles mettaient en garde sur les conséquences désastreuses de ces cyber-attaques.
La même année, le port d'Anvers (dans lequel des milliers de containers sont débarqués chaque semaine sur les quais) avait été piraté par un cartel de la drogue. Ils avaient réussi à récupérer la marchandise avant que les douanes n'inspectent les containers.

Un yacht (volontairement) piraté et détourné
En 2013, un groupe d'étudiants en école d'ingénieurs a fait une expérience en pleine mer : ils ont piraté un yacht de luxe pour le détourner de son trajet initial, en utilisant le système GPS..
C'était en fait un test organisé avec l'accord des propriétaires du bateau. Naviguant de Monaco à l'île de Rhodes, le yacht a été piraté en pleine mer Ionienne. Grâce à un faux boîtier simulateur GPS, ils ont envoyé des signaux de localisation avec de fausses données, des signaux plus forts que ceux transmis par les satellites. Les « faux signaux » se sont donc substitués aux vrais, en les brouillant. Le yacht a alors viré de bord, en modifiant le pilote automatique.
« Les armateurs prennent de plus en plus en compte ces menaces », explique Eric Banel, secrétaire général d'Armateurs de France. « Les politiques d'entreprises contiennent quasiment toutes un chapitre sur la cyber-criminalité. »
Quand aux constructeurs navals, comme DCNS qui construisent des bateaux pour la Marine nationale notamment, ils développent des moyens pour faire face à cette cyber-criminalité maritime, avec aussi des experts présents à terre pour surveiller les flux qui transitent entre la terre et le bateau.
L'école navale, Telecom Bretagne, DCNS et Thales se sont associés pour créer, avec le soutien de la région Bretagne, une chaire de cyber-défense des systèmes navals. Le but est de mettre en œuvre toutes les techniques pour lutter contre les menaces du cyberespace. Cette chaire universitaire mais aussi industrielle ambitionne de stimuler la cyber-innovation. Des chercheurs qui devront trouver des parades à la vulnérabilité des navires en mer, du porte-container au méthanier en passant par les navires de guerre.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.franceinter.fr/emission-le-zoom-de-la-redaction-les-cyber-attaques-dans-le-transport-maritime