La cybersécurité dans les ports

7ème assises « Port du futur »

27 Septembre 2017

Jean-Marc Ayrault (21 février2014) : La cybersécurité « *est une question d'intérêt majeur et d'intérêt national qui concerne tous les citoyens, tous les Français, et c'est pourquoi il est important que le gouvernement s'engage totalement* »

Quelques notions générales en matière de cybersécurité

Sécurité et sureté

- **Sécurité / Safety** : actions préventives pour éviter de mettre en danger des biens matériels ou des vies humaines en organisant, souvent de manière planifiée, la détection ou le contrôle de défauts ou de défaillances prévisibles pouvant survenir dans la mise en œuvre de matériels ou d'actions dans le cadre d'une activité humaine sans intention maligne.
- **Sureté / Security :** actions préventives pour faire obstacle à une activité consciente et maligne menée par un ou plusieurs êtres doués d'intelligence, destinée à nuire à une population ciblée dans l'optique de la déstabiliser, de la frapper ou de l'éliminer

Définition et objectif de la cybersécurité

La cybersécurité est l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sureté, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques matériels et immatériels (connectés directement ou indirectement à un réseau) contre les attaques malignes de personnes ou d'organisations ayant l'intention de nuire.

L'objectif de la cybersécurité est de garantir la disponibilité, l'intégrité, l'authenticité et la confidentialité des informations circulant sous forme électronique via des réseaux câblés ou des ondes radio.

(Définition adaptée d'un texte de Wikipedia).

La cybersécurité dans les ports

Le Comité Interministériel de la Mer 15-10-22

- **Un constat**

« Points nodaux multimodaux, les ports constituent par ailleurs le maillon central du transport de marchandises. Une cyberattaque majeure sur un grand port serait susceptible de désorganiser massivement toute la chaîne d'approvisionnement et, par voie de conséquence, l'économie d'un pays. «

- **Chapitre 2** : Adapter les outils de sureté et de sécurité maritime aux nouveaux enjeux

Mesure 7 : améliorer la cybersécurité des navires et des ports afin de faire face avec les armateurs au développement des menaces.

Les systèmes informatiques portuaires

- Les systèmes exogènes indépendants … mais menaçants
- Les systèmes exogènes communicants
- Les systèmes endogènes fermés … qui deviennent communicants

Les systèmes exogènes indépendants … mais menaçants

- Presque toutes les entreprises et activités implantées sur le port ou susceptibles d'interagir avec le port sont pourvus de systèmes d'information permettant leur prise de contrôle à distance : centrales électriques, raffineries, usines, entrepôts, véhicules, etc.
- Si des failles existent dans leur processus de sécurité / sûreté, le port peut être impliqué, voire attaqué.
- Exemple :
  - prise de contrôle hostile d'un grand pétrolier,
  - explosion d'un point chaud dispersant radioactivité ou produits toxiques
  - Encombrement d'un chenal d'accès, d'une artère fluviale ou ferroviaire, d'un axe routier, etc…

Les systèmes exogènes communiquants

- **Les Cargo Community Systems (CCS)**
  - Locaux, de moins en moins nombreux
  - Nationaux : vers un système français unique. Il en reste essentiellement 2, tous deux « AP+ »
  - Internationaux – surtout européens : échanges d'informations douanières dans le cadre
    - des pré-déclarations vers certains pays comme les USA
    - des dédouanements centralisés prônés par le nouveau code des Douanes
- **Les réseaux d'information administratifs**, de service comme **Safeseanet** (outil européen de suivi de la circulation maritime) : avis d'entrée de marchandises dangereuses (agent maritimes ou organisateurs de transport), données de sûreté, déchets du navire, etc.

Les réseaux endogènes fermés… deviennent communicants !

- Réseaux propres au port sans vocation de communication extérieure : surveillance du port, manipulation des outils : caméras vidéo, portes et grilles d'entrée, écluses, pompes, grues, etc…
- En existe-t-il encore qui soient totalement fermés ?
- De plus en plus souvent il devient possible de prendre la main à distance pour les surveiller ou les actionner.

Les réponses des ports

Les GPM sont attaqués tous les jours (10 à 12 fois en moyenne) de manière plus ou moins experte. D'où la nécessité de réponses adaptées.

- Une bonne communication avec l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) et avec les associations spécialisées, en particulier PROTECT,
- Des échanges fréquents entre spécialistes portuaires sous l'égide de l'UPF,
- Une participation à la création ou la modification des logiciels existants pour réduire les sources d'intrusion,
- Un dialogue constant avec les armateurs pour éviter la transmission d'informations erronées concernant les navires et leurs marchandises suite, souvent, à des délocalisations du traitement de l'information loin des sites d'opérations.

Une normalisation adaptée

- **ISO 28000** (2007) : spécifications relatives aux systèmes de management de la sûreté de la chaine d'approvisionnement.
- **ISO 20858** (2007) : . Navires et technologie maritime – Évaluation de la sécurité des installations portuaires maritimes et réalisation de plans de sécurité. La norme a été publiée le jour de l'entrée en vigueur du Code ISPS (International Ship and Port Facility Security).
- **ISO 28001** : meilleures pratiques pour la préservation des marchandises dans la sûreté de la chaine d'approvisionnement.
  - Son but : le niveau de sûreté doit être homogène pour toute la chaîne logistique, notamment grâce au fait que cette norme soit multimodale et internationalement reconnue.
  - Elle s'applique au système de management de la sûreté pour la chaîne d'approvisionnement. C'est un système complet de certification des entreprises de transports de marchandises créé par le Comité Européen de Normalisation (CEN).
  - Elle propose des certifications de sûreté aux différentes étapes de la chaîne logistique du transport de marchandises.
  - L'ISO 28001 complète les mesures législatives portant sur la sûreté des ports de l'Union Européenne et les normes de l'Organisation Mondiale de la Douane. Elle ne remplace pas les mesures de sécurité et les exigences de certification des agences douanières pour les chaînes logistiques.

FIN … provisoire ☺

Annexe : la cybersécurité à Dunkerque

Le contexte de l'étude sur la cybersécurité au port de Dunkerque

Chef de projet : le commandant du port

- Suite à la loi de programmation militaire, l'ANSSI a mis en place un plan d'action basé sur les points suivants :
  - S'appuyer sur les OIV tous secteurs pour lutter contre la CYBER MENACE
  - Fixer des règles de sécurité sur les SSI
  - Fixer les modalités de notification des incidents (remontées d'informations suite attaque vers l'ANSSI et la MEEDE)
  - Organiser des contrôles et des Audits des SSI (en amont, après recette, après 5 ans….)
  - Prévoir les incidences sur les crises majeures
- Un arrêté daté du 27 mars 2015 décrit les mesures à mettre en place sur les sites concernés

Identifier les SIIV

(systèmes d'information d'importance vitale)

Les grands principes :

- Atteinte à la Disponibilité, l'intégrité et la confidentialité,
- Les mesures de sécurité mises en œuvre et le niveau d'exposition à la menace ne doivent pas être pris en compte dans la démarche d'identification des SIIV,
- Utiliser la typologie exposée par l'ANSSI et le Ministère et discuter ensemble lors du GT .

Typologie des SIIV

- **I - Les systèmes spécifiques aux secteurs du transport maritimes**
  - 1. Systèmes permettant d'assurer la gestion de l'escale et des navires (ex pour Dunkerque : SIRENE).
  - 2. Systèmes permettant d'assurer la gestion du fret (ex pour DK : MD : TIMAD , MD opérateur ferroviaire , déclaration douane, AP+, Droits de Port, etc.). Lister les applications dont le port est l'administrateurs aussi bien que celles dont il est utilisateur à travers des liens et/ou des Interfaces avec d'autres prestataires mais qui font partie du périmètre d'application).
  - 3. Systèmes permettant d'assurer l'inspection filtrage des passagers.
  - 4. Systèmes permettant la détection et la supervision du trafic (radar Signalis , AIS ...).
  - 5. Systèmes de contrôle de commande des ouvrages tels que ponts et écluses (Automates SCADA).

Typologie des SIIV

- **II - Autres systèmes** (à reconnaître …)
  - 1. Système assurant la gestion technique des bâtiments et ouvrages indispensables à l'activité (alimentation en énergie, serveurs, gestion de l'eau : évacuation, maintien niveau, climatisation …).
  - 2. Système assurant la sécurité physique des bâtiments et des ouvrages (contrôle d'accès, vidéosurveillance) en particulier des Processus d'Importance Vitale.
  - 3. Télécommunications indispensables à l'activité.
  - 4. Systèmes traitant des informations sensibles ou classifiées de défense.

Nota : Si un SI ne rentre pas dans la typologie proposée par l'ANSSI et le Ministère, il faudra le justifier par courrier.

La réponse par système devra fournir les renseignements suivants

- Nom du système ;
- Catégorie correspondante dans la typologie ;
- Brève description fonctionnelle ;
- Principaux types de matériels constituant le système (Description succincte du système, serveur, etc.) ;
- Impacts sur les activités vitales en cas d'atteinte au système.

Enquête de l'ANSSI

- 1 – Enquête sur la liste des systèmes d'information relatifs aux opérations d'importance vitale (SIIV). 7 inventaires ont été reçus jusqu'à maintenant par l'ANSSI .
  - Les réponses ont été très disparates, d'une dizaine de système à une centaine). Seuls les SI intervenant dans les fonctions OIV doivent être retenus. Par exemple, il est difficile de considérer une gestion du personnel comme SIIV, bien qu'elle puisse être un point d'entrée dans le SI de l'établissement.
  - Dans l'analyse proposée, tous ne précisent pas si le risque concerne la disponibilité, la confidentialité ou l'intégrité. L'ANSSI proposera un nouveau modèle de tableau plus précis et un commentaire personnalisé de chaque inventaire.

Enquête de l'ANSSI

- 2 – Remontée des alertes

La Loi de Programmation Militaire prévoit l'obligation pour les opérateurs de remonter toute attaque du SIIV vers l'ANSSI. Les modalités seront fixées par arrêté avec les objectifs suivants :

  - augmenter la visibilité de l'ANSSI sur les incidents critiques de SI affectant la mission des OIV
  - être en mesure de réagir au plus tôt à une attaque majeure
  - évaluer la menace au plus vite et de manière précise (action pompier de l' ANSSI)
  - obtenir et communiquer des signatures de compromission afin d'augmenter les capacités de détection des attaques sophistiquées.

- Le protocole n'est pas encore établi, mais nous aurons à définir en interne la procédure de gestion et de remontée des alertes.

Enquête de l'ANSSI

- L'ANSSI réfléchit encore au mécanisme technique pour la remontée des informations et à la structure des éléments qui seront à fournir.
- Les modalités de déclaration des incidents devraient tenir compte des principes suivants :
  - Déclaration à l'ANSSI au plus vite,
  - Communication à l'ANSSI des évolutions du traitement de l'incident,
  - Echange entre demandeur et l'ANSSI classifié Diffusion Restreinte,
  - Emploi des moyens mis à disposition par l'ANSSI,
  - Identification et communication à l'ANSSI des points de contacts chargés de la notification et de la mise à jour.

Règles de sécurité

Ces règles que la loi (et son décret d'application) imposera, sont au nombre de quinze, articulées autour de cinq thèmes qui constituent une base de travail :

- **1/** Gouvernance de la Cybersécurité : établir, communiquer et faire vivre la politique de sécurité des systèmes d'information (PSSI) locale en s'inspirant de la PSSI de l'Etat : travail demandé par le ministère de Tutelle,
- **2/** Maîtrise des risques : les actions de maîtrises aboutiront à une dossier d'homologation des systèmes d'information (SI),
- **3/** Maitrise des SI : connaissance technique, maintient à jour des systèmes et politique de maintien en sécurité,
- **4/** Gestion des incidents de sécurité : processus complet de gestion des alertes de sécurité passant par les phases de journalisation, détection, traitements, remontés des incidents et gestion de crise,
- **5/** Protection des systèmes : Aspect le plus technique qui impose la mise en œuvre de procédures et d'outils de sécurisation des SI.

Règles de sécurité

Plusieurs de ces points sont réalisés, en cours de réalisation ou en projet,

D'autres sont nouveaux et imposeront dans certains cas des investissements : par exemple des audits par des tiers labellisés par l'ANSSI). Il faudra évaluer les délais de mise en œuvre et leur coût.

Principales règles avec une incidence budgétaire :

- Les systèmes existants retenus comme Système d'Information d'Importance Vitale (SIIV) devront être homologués par un prestataire qualifié par l'ANSSI
- Les nouveaux systèmes devront suivre cette procédure d'homologation à la mise en service.
- Les anomalies devront être exploités journellement, mise en place de sonde

Le planning de mise en œuvre, sera proposé courant 2016.