Retour sur la matinée du 4 juillet consacrée à la « SÛRETE INDUSTRIELLE des sites et des systèmes d'information »

Cette réunion co-organisée par l'UIC Normandie & l'UIMM Rouen/Dieppe a rassemblé plus de **70 participants** autour de la thématique de la sûreté industrielle, reflétant l'intérêt manifeste des industriels pour ce sujet.

Pour cela, une **multiplicité d'acteurs** tous complémentaires les uns des autres se sont succédés (Siraced PC, DGSI, DREAL, Gendarmerie, Police, TGI, Entreprise), pour permettre aux participants de mieux appréhender la menace et leur fournir les clés pour **se préparer au mieux** tant sur le plan de la sûreté des installations que des systèmes informatiques.

A cet effet, une **clé USB** a été remise à tous les participants afin de leur permettre de disposer des présentations des intervenants et d'une **boîte à outils** (fiches réflexe, guides, coordonnées utiles, modèle de courrier…). Les personnes n'ayant pu assister à la réunion peuvent retrouver ces supports en cliquant sur ce lien*.

Voici une synthèse des principaux messages passés par les différents intervenants :

- La **menace a évolué**, nous sommes dans un état de menace permanente (même s'il n'y a pas de menace particulière sur la Normandie) qui nécessite d'adapter nos organisations.
- **Toutes les entreprises sont concernées**, qu'elles soient classées SEVESO ou non, petite ou grande, et quel que soit leur secteur d'activité.
- Il est important d'associer **différents acteurs de l'entreprise** pour mener une démarche efficace (Dirigeants, Responsables HSE, Responsables RH et Responsables informatique de nos entreprises).
- Le **processus de radicalisation** (au travers des 4 phases) et les signaux de basculement ont été présentés par le TGI afin de permettre à chacun d'être en mesure de détecter puis signaler tout comportement suspect.
- Le fait religieux en entreprise a suscité de nombreuses questions. Le représentant du TGI a insisté sur l'importance du **règlement intérieur** qui est un pilier pour permettre aux dirigeants de gérer efficacement ces situations.
- A ce sujet le Siraced PC et les différents services de l'Etat ont insisté sur **l'importance de signaler tout comportement suspect** (INCOHÉRENCE ⇨ ÉTONNEMENT ⇨ SIGNALEMENT)
    - via le Numéro Vert (**0 800 005 696, appel gratuit**) ou le formulaire en ligne de Stop-Djihadisme pour les potentiels cas de radicalisation
    - directement via les état-majors de sécurité des préfectures, gendarmerie et/ou police en utilisant la **fiche réflexe** remise sur la clé USB pour les situations jugées suspectes

*il peut être nécessaire de passer par le navigateur Mozilla ou Google chrome

- Chaque exploitant doit **identifier la vulnérabilité de son site industriel** (en quoi est-il une cible potentielle ?) Pour cela, il est possible de mener **une autoévaluation** (par exemple avec la fiche 8 de l'annexe 1 du guide de l'INERIS). Les **référents sûreté** des services de gendarmerie ou de police (selon la localisation de l'entreprise) peuvent également réaliser des **audits sûreté** (gratuits) pour les entreprises. Pour ce faire, l'industriel demandeur doit saisir le Préfet ou le directeur au commandant de groupement, suivant le modèle de courrier joint sur la clé USB.
- La DREAL, la Gendarmerie et la Police ont présenté les enseignements de la **campagne de visites sûreté menée sur les sites Seveso en 2015**, et les principaux écarts constatés qui portaient notamment sur les sujets suivants : insuffisance de clôture, d'éclairage, d'entretien des végétations… Le bilan de ces visites a néanmoins été qualifié de « rassurant » puisqu'aucune sanction n'a été émise.
- Il a été rappelé le **nécessaire équilibre à trouver entre transparence des informations et problématique de sûreté**. Dans ce cadre, l'Instruction du 19 mai 2016 relative à la mise à disposition et à la communication d'informations potentiellement sensibles pouvant faciliter la commission d'actes de malveillance dans les établissements Seveso, définit **3 catégories d'informations** : informations communicables, informations consultables sous conditions et informations non communicables. La DREAL a précisé que cette démarche se met en place progressivement, il est constaté que de nombreuses informations ont d'ores et déjà été retirées des sites internet et que de nouvelles pratiques se mettent en place (CODERST, SPPPI…). Il est néanmoins conseillé à chaque exploitant de consulter les différents sites internet, d'identifier les éventuelles informations sensibles et de **faire la demande au service concerné de les retirer.** Cette démarche peut également s'appliquer aux sites internet des collectivités et des associations.
- Les attaques informatiques n'ont de cesse de progresser en nombre, en efficacité et en complexité avec des conséquences parfois dramatiques : atteinte à l'image et à la réputation, indisponibilité des infrastructures ou encore impact financier (les alertes sont disponibles sur le site http://cert.ssi.gouv.fr/). La DGSI a rappelé les **piliers d'une démarche efficace : sensibilisation, chiffrement des données et audit de sécurité informatique**. Ces principes ont été confirmés par le témoignage de l'entreprise SERAPID, PME dieppoise dans le secteur de la métallurgie, sur la démarche menée après avoir été victime du virus Locky.

Cette matinée, riche en échanges, aura permis aux participants de comprendre le rôle de chacun des acteurs et de mesurer l'importance d'adapter son organisation et ses pratiques à la menace actuelle. A cet effet, la boîte à outils fournie sur clé USB donne des clés pour permettre aux entreprises de se préparer efficacement.