Le point sur :

La sécurité des systèmes industriels

Les systèmes industriels se rapprochent de plus en plus des systèmes informatiques de gestion : mise en réseau, client-serveur, systèmes de stockage, échanges d'informations, TMA…

Mais leur sécurité tarde encore à être gérée de façon structurée.

Voici quelques recommandations simples pour démarrer.

Faire collaborer le monde de la sécurité et les automaticiens

Mettre en place un projet commun qui réunit deux mondes qui n'ont pas l'habitude de se parler : les responsables de la sécurité et les automaticiens. Etendre les responsabilités du RSSI aux systèmes industriels.

Cartographier ses systèmes industriels

Etablir la cartographie de ses systèmes industriels, pour en avoir une vision globale et visualiser où sont les entrées et les sorties du système d'information, quels sont les chemins que peut emprunter un pirate informatique. C'est un prérequis pour établir une gestion des risques efficace.

Gérer les faiblesses et les vulnérabilités

Les mises à jour sont souvent problématiques dans le monde industriel. Pour faciliter cette tâche, mieux vaut savoir quel automate nécessite une mise à jour afin de pouvoir hiérarchiser les actions, les planifier et ainsi réduire la surface d'attaque. Il faut identifier régulièrement chaque automate du réseau, réaliser en permanence une veille pour détecter les nouvelles mises à jour à effectuer.

Identifier les types de données qui peuvent entrer et sortir des systèmes industriels

Faire une liste blanche : dresser une liste de tous les formats de données qui ont l'autorisation de sortir ou d'entrer dans le système d'information, afin de lutter contre la fuite d'informations et les attaques.

Définir une politique de gestion des clés USB

De nombreux systèmes Scada ne peuvent être mis à jour qu'à l'aide de clés USB. L'objectif est de constituer une barrière contre les attaques de type « BadUSB » (usurpation de périphérique via un malware, par exemple). L'enjeu consiste donc à maîtriser les menaces liées à ces périphériques :

- connaître quels automates ont besoin d'une clé USB pour effectuer les mises à jour,
- définir des périmètres d'usage en isolant les clés USB spécifiquement dédiées à ces mises à jour
- sensibiliser les collaborateurs

Mettre en place des stations neutres

Déployer des stations dédiées à la neutralisation des menaces USB et en faire des points de passage obligatoires :

- toute clé USB venant de l'extérieur doit être branchée sur la station, pour vérifier les formats grâce à la liste blanche préalablement constituée, et détecter/ bloquer les contenus malveillants.
- une autre clé USB "maîtrisée" et branchée en sortie du dispositif permet, elle, de récupérer l'ensemble des fichiers sains.
