FLASH ARIA
Février 2019

Cybersécurité industrielle : Périmètre et accidentologie

Aujourd'hui les usines sont de plus en plus automatisées. Les échanges d'information sur les réseaux de télécommunication sont en outre croissants. Tout le monde s'accorde ainsi à dire qu'il existe un « risque », peut-on en discerner toutefois les contours et en évaluer les conséquences notamment sur l'environnement à travers les événements recensés dans la base ARIA ?

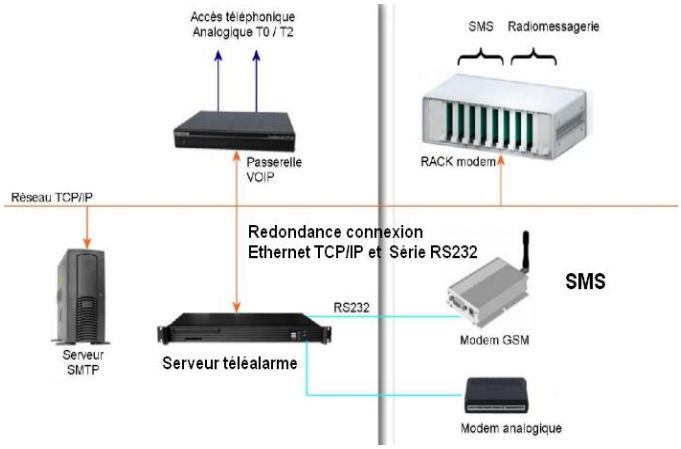
A l'origine, le mot cybersécurité est un néologisme. Il regroupe l'ensemble des outils, procédures, mécanismes de sécurité, formations, bonnes pratiques et technologies protégeant le « cyberenvironnement » d'une usine. Celui-ci est notamment constitué par les réseaux informatiques du site ou d'alerte qui y sont connectés. Sans oublier, le personnel, les sous-traitants, les applications et leurs mises à jour, les réseaux de télécommunication (GSM, RTC, fibre optique, Wifi,etc.), les chaînes d'automatismes (du serveur jusqu'à l'actionneur) et la totalité des informations qui sont transmises et/ou stockées via différents protocoles d'échange ou de chiffrement.

La base ARIA est une base événementielle sur les accidents technologiques. Elle ne permet pas de disposer de statistiques détaillées sur l'occurrence des attaques informatiques. Toutefois, les événements recensés dans cette dernière permettent de mettre en exergue quelques perturbations ou causes profondes dans le « cyberenvironnement » d'un site industriel.

ARIA 50755 - 15/09/2017 - Montoir-de-Bretagne
Défaillance d'un système de transmission d'alerte en cas d'accident

Lors du redémarrage d'un terminal méthanier classé Seveso, une fuite de gaz naturel se produit vers 6 h à la suite d'une mise en route d'une pompe haute-pression. Un opérateur donne l'alerte et la pompe est arrêtée manuellement. Vers 6h20, une nouvelle fuite de gaz avec formation d'un nuage de gaz inflammable se produit à la suite d'une nouvelle tentative de remise en route. L'exploitant déclenche son POI et alerte les entreprises voisines via sa **centrale d'alarme téléphonique**. Toutefois, une erreur dans la diffusion du message d'alerte se produit. **Un bug informatique ou une erreur de manipulation d'un opérateur en serait l'origine.** Par ailleurs, **les canaux de communication des talkies-walkies utilisés lors de la gestion de l'événement ont été surchargés.**

A la suite de l'événement, **des automatismes sont vérifiés** afin de s'assurer de l'absence de surpression en cas de fermeture / ouverture des différentes vannes (lignage). **Des lignes téléphoniques sont par ailleurs ajoutées** pour réduire le temps de diffusion des messages d'alerte via la centrale d'alarme. Enfin, l'opérateur au système de téléalarme est reformé à son utilisation.



Principe de fonctionnement d'une téléalarme, © DR

Vocabulaire des experts en cybersécurité : Menace, vulnérabilité et contre-mesure

Une **menace** représente une action susceptible de nuire.

Une **vulnérabilité**, parfois également appelée brèche ou faille représente le niveau d'exposition face à la menace dans un contexte particulier.

La **contre-mesure** ou parade, représente l'ensemble des actions mises en œuvre à titre préventif. Les **contre-mesures ne sont généralement pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisations des utilisateurs**, ou bien des règles clairement définies.

ARIA 51131 - 08/02/2018 - Europe
Attaque informatique d'une station d'épuration avec un logiciel de crypto-monnaie

Des logiciels malveillants d'extraction de crypto-monnaie sont détectés sur des serveurs connectés à un réseau d'une station d'épuration en Europe. C'est la première attaque de malware de cryptomonnaie documentée qui frappe un réseau d'un opérateur d'infrastructure critique. Les IHM (interface homme-machine) sont ainsi ralenties.

L'attaque a été découverte dans le cadre de la surveillance de routine du réseau puisqu'une attaque de ce type augmente la consommation en temps de calcul des machines et diminue la bande passante disponible sur le réseau, ce qui réduit les temps de réponse des outils (IHM/SCADA) utilisés pour superviser les installations. D'après la presse, le malware de cryptomonnaie est conçu pour fonctionner en mode furtif sur un ordinateur ou périphérique tout en désactivant ses outils servant à le protéger.

ARIA 42931 - 02/05/2012 - FOLKLING
Défaut de capteur à la suite de l'absence de mise à jour de carte électronique

Dans une usine de produits cosmétiques classée Seveso, un flexible de transfert gonfle au niveau du raccord vers l'installation fixe puis fuit lors d'une livraison de méthoxyméthane (DME). Une incompatibilité entre le matériau du flexible et le produit livré est à l'origine de l'évènement. L'opératrice constate la fuite et alerte le chauffeur qui ferme la vanne de fond de cuve et coupe le moteur du camion. Le bouton d'arrêt d'urgence est actionné pour déclencher la mise en sécurité du poste de dépotage et l'évacuation de l'usine par précaution pendant 20 min. Aucune conséquence humaine ou environnementale n'est à déplorer.

L'accident met en évidence **un défaut de capteur. La zone de dépotage est équipée d'une détection gaz qui s'est révélée inopérante à cause d'un défaut matériel des cartes électroniques de la centrale de traitement (cartes datant de 2001)**. Les capteurs, rapidement saturés, sont passés en signal « hors échelle ». Ce signal a été traité comme « défaut de capteur » sans action particulière (alors que le « hors échelle » doit normalement déclencher les procédures de sécurité).

Le fabricant de la carte aurait identifié le risque potentiel de dysfonctionnement depuis 2008 et remédié à la situation **(par changement des cartes et mise à jour du logiciel).** Toutefois, l'ensemble des cartes concernées n'avait pas été rappelées / mises à jour. L'exploitant de l'usine chimique remplace l'ensemble de ses cartes. Le coût de l'opération est évalué à 10 000 Euros. Il remplace également le capteur gaz de la zone de dépotage de technologie « semi-conducteur » par un capteur à technologie infra-rouge.

ARIA 5989 – 01/12/1994 - RIBECOURT-DRESLINSOURT
Mauvaise programmation d'automate

Dans une usine de fabrication d'engrais classée SEVESO, une fuite d'ammoniac blesse 3 ouvriers, provoquant le décès de l'un d'eux.
Mauvaise planification des travaux notamment lors de la consignation d'onduleurs et problème dans la programmation des automates pilotant une vanne sont mis en exergue dans le cadre de l'analyse des causes de l'accident.

Pour en savoir plus, découvrez la fiche détaillée de l'accident, en cliquant sur l'image :


Fuite d'ammoniac dans une usine de fabrication d'engrais
Le 1er décembre 1994
Ribecourt-Dreslincourt (60)
France

Les accidents analysés permettent d'identifier quelques points de vigilance sur le cyberenvironnement d'une usine :

- ✓ **Réseau de télécommunication / Système de téléalarme ou de diffusion de l'alerte aux populations voisines ou administrations concernées :**
  - Le système est-il correctement dimensionné : nombre de lignes téléphoniques ?
  - Les opérateurs (société de gardiennage) sont-ils suffisamment formés à son utilisation ? Est-il régulièrement testé ? La liste des personnes à prévenir est-elle régulièrement vérifiée (pertinence des numéros de télécopieur) ?...
- ✓ **Attaque virale :**
  - L'entreprise dispose-t-elle d'une politique de sensibilisation des utilisateurs ?
  - Une veille sur ces questions est-elle réalisée ? (site de l'Anssi, responsable cybersécurité dans l'entreprise).
- ✓ **Mises à jour du matériel informatique :**
  - Sont-elles régulièrement planifiées ? Font-elles l'objet d'une analyse de risque ? Comment s'assure-t-on que les mises à jour ne sont pas potentiellement dangereuses ?
- ✓ **Programmation des automates :**
  - Est-ce que le sous-traitant est audité et habilité pour les interventions qu'il a à réaliser (qualité de la programmation / connaissance du process industriel et des installations) ?

Pour aller plus loin dans la prévention de la cybersécurité industrielle, une étude est téléchargeable sur le site internet du BARPI à l'adresse suivante :

https://www.aria.developpement-durable.gouv.fr/wp-content/uploads/2017/08/2017-08-02_SY_cybers%C3%A9curit%C3%A9_JFM_finale.pdf