Sécurité des infrastructures sensibles : de la protection physique à la cybersécurité

Les infrastructures font l'objet de nombreuses attaques, physiques et virtuelles. Seule une approche globale de la sécurité, capable de détecter le moindre dysfonctionnement et d'analyser le niveau de la menace, constitue une défense appropriée.

Michel Dran
Responsable Développement Activités Sécurité et Contrôle
Expert Sûreté/Sécurité, Michel a une longue expérience des systèmes de sûreté pour les infrastructures critiques notamment dans les domaines du Nucléaire et des OIV (Opérateur d'Importance Vitale).

Dans les infrastructures sensibles, la menace permanente, à but concurrentiel, terroriste ou criminel, peut prendre différentes formes : tentatives d'intrusion ou d'extorsion de fonds (ransomware), espionnage industriel, destruction ou dégradation de biens et même agressions physiques.

Le risque *« cyber »* est relativement nouveau, mais il s'est accru avec l'avènement des nouvelles technologies numériques. Certes, ces technologies apportent beaucoup plus de puissance de traitement, mais rendent aussi les architectures, ouvertes et communicantes, plus vulnérables. *« Les cyberattaques ciblent non seulement l'IT, mais aussi l'OT (Operational Technology), qui intègre les systèmes industriels et leurs environnements (sûreté, Gestion Technique Centralisée, sécurité industrielle...). »*

On ne peut pas parler de sécurité globale sans prendre également en compte la notion de sécurité fonctionnelle, liée à la sûreté de fonctionnement. Celle-ci a pour objectif de garantir qu'un système est sûr intrinsèquement, avec un niveau de sécurité déterminé par l'analyse de risques et selon la cible de sécurité définie.

Quand la propagation du ver Stuxnet, première cyberattaque d'envergure contre un système industriel, est arrivée en 2010, ce fût la preuve tangible que nos pires craintes d'attaques sur des installations sensibles pouvaient se réaliser. Via une simple clé USB infectée et non contrôlée, ce virus s'est introduit

“Les cyberattaques ciblent l'IT mais aussi l'OT”

dans tout le réseau opérationnel de l'usine d'enrichissement d'uranium de Natanz, en Iran. En France, à partir de cet événement et d'autres qui ont suivi, l'Agence Nationale de la Sécurité des Systèmes d'Information (Anssi) a pris un certain nombre de dispositions afin de sensibiliser les Opérateurs d'Importance Vitale (OIV) aux risques encourus par ce type de menaces.

Les faits démontrent le bien-fondé de cette démarche puisque les attaques sur des systèmes industriels se sont multipliées depuis, touchant entre autres des groupes pétroliers, des industries pharmaceutiques ou automobiles. Au printemps 2017, l'une d'entre elles - WannaCry - a notamment contraint Renault, et bien d'autres, à fermer certaines de ses usines quelques jours.

De nouvelles menaces utilisent l'attaque indirecte

Depuis, les cyberattaques ne cessent de se sophistiquer et de prendre des formes nouvelles en ne s'attaquant pas nécessairement au process lui-même, mais aux systèmes qui gèrent leurs environnements. *« Par exemple, un data center peut être mis hors d'état de fonctionner, non pas par le biais d'une attaque directe, mais en mettant hors service son système de climatisation. »* Privés de refroidissement, les calculateurs deviennent vite inopérants et les conséquences peuvent être aussi gravissimes qu'une attaque physique. Une telle situation est naturellement possible avec un virus (type Stuxnet) introduit lors d'une opération de maintenance sur le système de GTC.

Les attaques peuvent se combiner et affecter d'autres systèmes : *« Les*

“La seule réponse consiste à adopter une approche globale de la sécurité pour pouvoir détecter les signaux faibles”

intrusions sur site sont censées être repérées par le système de vidéosurveillance, mais si ce dernier est neutralisé ou piraté, par compromission des images, l'intrusion physique devient possible sans être détectée. » La sécurité d'une infrastructure se joue donc aujourd'hui à de multiples niveaux et tous les systèmes doivent être protégés selon le principe de défense en profondeur.

L'approche globale garantit **la sûreté des sites industriels**

Dès lors, comment assurer une protection maximale des biens essentiels, qu'il s'agisse des infrastructures, de l'outil de production, des systèmes d'informations ou encore des systèmes industriels ? La seule réponse consiste à adopter une approche globale de la sécurité, de manière à pouvoir détecter les signaux faibles, c'est-à-dire repérer tout événement potentiellement dangereux qui ne serait pas considéré comme tel s'il était isolé ou provenait d'un seul système. Mais, dès lors que les informations proviennent de sources multiples, qu'elles sont croisées, confirmées et corrélées, la cohérence globale peut être assurée et donner lieu à la génération d'une alarme avérée qui pourra alors être prise en compte et traitée.

Une supervision de sécurité (ou SIEM pour Security Information and Event Management), permet de gérer et corréler les *« logs »* : *« Ces solutions sont munies de moteurs de corrélation en vue de relier plusieurs événements à une même cause. Ainsi, tous les systèmes doivent être instrumentés, munis de sondes et autres capteurs pour permettre de remonter des événements vers le SIEM, en plus des événements et alarmes gérés par les systèmes eux-mêmes. »*

> **“Il y a de vrais enjeux à sécuriser la partie OT qui demandent des compétences métiers combinées à une expertise en cybersécurité”**

Ils comprennent le système industriel (de type Scada par exemple) et ses composantes de sécurité fonctionnelle (avec la notion de SIS / Systèmes Instrumentés), ainsi que les systèmes de protection de l'infrastructure comme la sûreté (vidéo, contrôle d'accès, dispositifs anti-intrusion) ou la GTC.

Le recours à un spécialiste de la sécurité physique et de l'informatique

Les entreprises ont aujourd'hui l'obligation de traiter la question de la sécurité au plus haut niveau et de mettre en place une gouvernance de la sécurité pour protéger leur outil industriel, IT et OT confondus. *« L'objectif est d'assurer la continuité des activités en cas d'attaque et donc d'avoir des systèmes résilients. Pour cela, il faut avoir recours à de véritables spécialistes qui maîtrisent les différentes composantes de la chaîne de sécurité couvrant à la fois la sécurité physique, la cybersécurité, la sécurité fonctionnelle et même tous les systèmes liés aux « utilities » comme la GTC notamment. »*

La sécurité globale se caractérise aussi par une vigilance de tous les instants, sur chacun des maillons de la chaîne. A cet effet, Assystem a co-développé avec le Cern, l'Organisation européenne pour la recherche nucléaire, la notion de *« Safety Status »* afin de garantir dans le temps qu'un système fonctionne dans ses conditions nominales de sécurité. ■

La Défense - Tour Egée
9/11 Allée de l'Arche
92400 Courbevoie - France

Tel: +33 (0)1 41 25 29 00
www.assystem.com