La cybersécurité des systèmes industriels, enjeu critique pour l'adoption du modèle « Industrie du Futur – Industrie 4.0 »

Philippe GENOUX

Délégué Général
EXERA

La prise de conscience du monde industriel sur la réalité de la cybermenace remonte à 2010 et a été brutale avec la révélation de l'attaque informatique Stuxnet sur le site d'enrichissement d'uranium iranien, les industriels ayant longtemps cru être à l'abri de ce risque en raison du réputé cloisonnement des réseaux informatiques industriels.

Depuis, on apprend régulièrement que de nouvelles attaques cyber ont affecté les systèmes industriels les plus divers. À titre d'exemples marquants…

- Attaque Sandworm sur le réseau de distribution d'électricité en Ukraine pendant l'hiver 2015-2016,
- Attaque Wannacry, virus de type ransomware (cryptage des données, en mai 2017, première opération d'envergure mondiale puisque près de 150 pays ont été touchés,
- Attaque Notpetya, virus de type wiper (destruction de données), démarrée en juin 2017, deuxième opération d'envergure mondiale tout juste un mois après Wannacry.

Les impacts financiers des cyberattaques ont fortement augmenté avec le temps, et sont devenus un véritable sujet d'inquiétude pour les acteurs de la vie économique et pour les États. Ainsi, pour la seule cyber-attaque Notpetya, première attaque bien documentée, les montants communiqués par les entreprises victimes de cette attaque sont éloquents :

- Pertes estimée à 300 millions par Maersk, groupe danois de transport et de logistique, et fermeture temporaire de plusieurs sites ;
- Pertes estimées à 870 millions de dollars par Merck, laboratoire pharmaceutique américain ;
- Pertes estimées à 188 millions de dollars par Mondelēz International, groupe agro-alimentaire américain, propriétaire de la marque française « Biscuits LU » ;
- Pertes estimées à 400 millions de dollars par TNT Express, filiale européenne de FedEx groupe américain de transport international de fret ;
- Pertes estimées à 384 millions de dollars par Saint-Gobain, groupe français de production de matériaux.

Par ailleurs, les nouveaux concepts « Usine du Futur » ou « Industrie 4.0 » ont fait leur apparition, et progressent à grands pas avec de sites-pilotes qui constituent des démonstrateurs de faisabilité. Derrière ces concepts, la digitalisation de l'entreprise, le décloisonnement

des services centraux et des sites de production - voire de partenaires externes - que facilite l'intégration toujours plus poussée de l'ensemble des fonctions de l'entreprise dans des systèmes d'information de type ERP/PGI puissants, l'émergence de technologies prometteuses telles que le big data et le recours à l'intelligence artificielle ouvrent de nouvelles opportunités. Les enjeux économiques liés à l'adoption de ces concepts sont considérables, puisque les retombées attendues de la numérisation de l'industrie sont estimées à 6% du chiffre d'affaires résultant des gains globaux de productivité. Parmi les facteurs contribuant à ces gains, on mentionnera notamment la réduction des coûts de maintenance de 12% liée au passage à la maintenance prédictive, la réduction du poste « Energie » liée à l'optimisation de la production, ces ratios étant observés dans les retours d'expérience issus des sites pilotes. En contrepoint, les investissements anticipés en lien avec la digitalisation des entreprises industrielles sont massifs, les estimations (avant Covid…) étant de 400 milliards de USD sur la période [2020-2024], dont 140 milliards de USD pour les pays de l'Union européenne.

Conséquences de ces évolutions, se généralisent les passerelles entre réseaux IT et réseaux OT et l'adoption de standards communs pour les réseaux d'information générale (IT) et pour les réseaux d'information technique (OT), qui constituent autant de vulnérabilités potentielles aux cyberattaques. Ainsi, la conjonction des premières cyberattaques ciblant les systèmes d'information industriels d'une part et d'autre part l'adoption croissante des concepts « Usine du Futur » ou « Industrie 4.0 » rendent encore plus critique le déploiement de solutions de cybersécurité des systèmes industriels indispensables à, sinon garantir, assurer la sécurité des réseaux vis-à-vis des cyber-agressions, tout en maintenant des flux d'échanges de données tant entre entités internes qu'avec des partenaires externes.

C'est dans ce contexte que les États ont pris conscience de la cybermenace sur les acteurs du secteur industriel, et qu'ils ont graduellement mis en place des dispositifs législatifs et réglementaires depuis le début des années 2010. C'est ainsi qu'en France, la Loi de programmation militaire du 18 décembre 2013 a élargi et renforcé le périmètre des attributions de l'ANSSI, agence dépendant du premier ministre, de manière à sensibiliser plus fortement les acteurs économiques à la cybermenace et à réduire leur niveau de vulnérabilité aux cybermenaces. Ont ainsi été recensés les systèmes d'information d'importance vitale (SIIV) déployés par les opérateurs d'importance vitale (OIV), SSIV desquels des discontinuités de service résultant de cyberattaques seraient particulièrement préjudiciables pour la vie économique et sociale du pays et de ses habitants. Ont également été définies des obligations à respecter par les OIV, destinées à prévenir les attaques et leur propagation, comme par exemple les déclarations d'incidents. L'ensemble de ces dispositions a été largement repris par le parlement européen pour l'établissement de la directive européenne « Network and Information System Security » (NIS) adoptée le 19 juillet 2016, transposée en droit national le 27 février 2018.

Répondant à la demande des entreprises, les acteurs du marché de la sécurité informatique se sont mobilisés pour proposer des solutions dans le domaine de la cybersécurité des systèmes industriels. Qu'il s'agisse d'entreprises établies ou de start-ups, les initiatives d'éditeurs de logiciels, de fabricants de matériels ou de sociétés de services informatiques sont nombreuses. Parmi les solutions émergentes, on retiendra les sondes

informatiques destinées à surveiller les réseaux d'information industriels (OT), les anti-virus, les pares-feux logiciels ou physiques (diodes), mais également les durcissements des plateformes, logiciels, OS et firmwares (stations SCADA, automates, capteurs de mesure, actionneurs intelligents, etc.), ou encore les solutions d'architectures de réseaux offrant une meilleure résilience. À côté de ces solutions d'ordre technique, apparaissent également les solutions d'ordre organisationnel et procédural (définition et déploiement de plans de réponse à cyberattaque) destinées à répondre aux obligations règlementaires ou aux recommandations émanant des agences gouvernementales en charge de la sécurité des systèmes d'information.

À la demande de ses adhérents, l'Exera a mis en place fin 2013 la commission technique « Cybersécurité des systèmes industriels ». Elle permet à ses membres de connaître l'offre du marché au travers de rencontres avec les industriels et start-ups porteurs de solutions en cybersécurité, au cours desquelles ceux-ci exposent le contenu technique de leurs produits et services. C'est ainsi que, de 2014 à 2019, ce sont quarante-trois acteurs qui ont été invités, et de nombreux autres acteurs restent à rencontrer, signe de la vitalité du secteur de la cybersécurité des systèmes industriels. La commission s'est aussi fixée pour objectif de mettre à la disposition de ses adhérents des guides à la rédaction de clauses des volets « cybersécurité » à inclure dans leurs dossiers de consultation couvrant les opérations externalisées en lien avec leurs activités (conception d'installations nouvelles, déploiement/mise en service, maintenance, exploitation externalisée, audits d'état des lieux initial, audit de réception, formation…). Ce travail est mené parallèlement au suivi des volets législatifs et règlementaires applicables à la cybersécurité des systèmes industriels, facilité par la présence d'un représentant de l'ANSSI au sein de la commission, et celui du volet de normalisation réalisé en liaison avec ISA - France.

Enfin, l'Exera organise depuis 2015 une fois par an une journée technique « Cybersécurité des systèmes industriels » ouverte aussi bien à ses adhérents qu'aux non-adhérents. Ces journées sont destinées à permettre de faire un point d'étape annuel sur les évolutions du marché de l'offre et à faciliter les échanges entre les participants et la dizaine d'exposants présents.

Pour plus d'informations, n'hésitez pas à vous rendre sur le site de l'association www.exera.com.