**Entre essor du cloud et ransomwares, quelles priorités pour la cybersécurité industrielle ?**

Le nombre de groupes industriels touchés par une cyberattaque a explosé en fin d’année 2020. Et l’année 2021 part sur des bases au moins aussi élevées. Alors que la 5G et l’IIoT sont régulièrement pointés comme de nouvelles portes d’entrée à cadenasser, les attaques observées récemment semblent finalement très classiques. De quoi réviser ses priorités pour 2021.

Les premières cyberattaques contre l’univers industriel concernaient principalement des entreprises de gaz, d’énergie, de nucléaire, d’eau… Et semblaient relever davantage de la géopolitique. Mais les cibles se diversifient et le nombre de cas médiatisés en France ces derniers mois révèlent des entreprises de toutes tailles et de tous secteurs.

La qualité de certaines attaques industrielles, très ciblées, interroge. Même les ransomwares sont de plus en plus sophistiqués. Jusque-là cantonnés aux réseaux IT, ils sont devenus une menace sérieuse pour les réseaux OT. Plus complexes, plus dévastateurs, ces malwares témoignent [de la complexification des techniques d’intrusion](https://www.industrie-techno.com/article/les-ransomwares-complexes-nouveau-standard-des-cyberattaques-contre-les-infrastructures-critiques.60916).

**Les fragilités des systèmes industriels**

En quelques années, [la cybersécurité des systèmes industriels](https://www.stormshield.com/fr/actus/it-ot-quelle-cybersecurite-des-systemes-industriels-industrie-40/) est devenue un enjeu de premier plan. Avec trois principales fragilités, qui restent encore à travailler en 2021 :

* **La gestion de parcs industriels étendus**, via une architecture distribuée, avec des usines de plus en plus connectées entre elles ;
* **La porosité croissante des systèmes industriels avec les systèmes d’information**, avecun va-et-vient permanent de communications en temps réel, des capteurs aux automates, des automates au SCADA et même des communications qui débordent du SCADA au MES et du MES à l’ERP – qui ouvrent de nouvelles fenêtres d’attaques ;
* **La gouvernance cyber**, avecdes équipes IT qui doivent monter en compétence sur les enjeux et particularités de l’OT et des équipes OT qui doivent quant à elles apprendre à travailler avec ces équipes IT, dans la démarche de sécurité globale.

Et avec l’industrie 4.0 et les promesses d’objets connectés boostés à la 5G, l’usine, historiquement conçue comme une citadelle isolée, devient un environnement interconnecté truffé de capteurs. Mais cette transformation numérique ne doit pas se faire au détriment de la cybersécurité car toute attaque côté IT impacte désormais l’OT. C’est justement ce qui est arrivé à plusieurs acteurs industriels.

**Segmenter, segmenter et encore segmenter**

Faire de la segmentation dans le monde industriel est le premier point de sécurité. Cela permet de s’assurer que le système de production, le système de qualité ou le système de sûreté ne soient pas tous interdépendants et de limiter les attaques par rebond. Cette hygiène numérique est essentielle et pose les bases d’une sécurité globale, avant même d’envisager le déploiement de la 5G ou de l’IIoT.

Elle consiste en trois grandes étapes de sécurisation :

* Maintenir la barrière entre l’IT et l’OT en segmentant les systèmes d’information pour faire en sorte qu’il y ait un premier niveau de sécurité qui soit apporté entre les usines et le reste.
* Segmenter le réseau industriel, afin de faire en sorte qu’un équipement touché par une attaque ne permette pas une propagation vers l’ensemble de l’usine.
* Être au plus proche des automates industriels et sécuriser les communications entre eux.

**Les nouveaux enjeux de sécurité du *cloud computing***

Il y a quelques années, les industriels ne juraient que par les environnements *on-premise* mais aujourd’hui, de plus en plus d’entreprises optent pour le cloud. Un cloud qui s’impose donc peu à peu comme un nouveau paramètre à prendre en compte dans la stratégie globale de sécurité. Et parce que le système industriel est connecté directement au cloud, utiliser celui-ci amène de nouveaux enjeux de sécurisation.

« Sortir » des données est une opération toujours risquée, face à des risques de fuites ou d’altération. L’industriel qui décide d’externaliser sa donnée doit s’assurer que l’applicatif et les outils mis dans le cloud soient sécurisés, [en mettant des firewalls dans le cloud](https://www.youtube.com/watch?v=FI_7IKO1iQE), pour sécuriser les accès et les données qui transitent entre le cloud et un site industriel. Par ailleurs, certains fournisseurs de cloud assurent aussi la sécurité, via des services managés ou décentralisés, opérés par un autre prestataire. Il est cependant important de s’assurer que les bonnes sécurités soient mises en place.

**L’erreur est (souvent) humaine**

Autre enjeu d’importance : la télémaintenance. Un réseau informatique basé sur le système d’exploitation obsolète Windows 7, l’absence de firewall entre Internet et le système d’information de la structure ou encore un même et unique mot de passe pour TeamViewer sur tous les ordinateurs de la station sont autant de trous dans la raquette et d’opportunités pour les cyber-criminels. Tous les mainteneurs, internes ou externes à l’entreprise, représentent une faille potentielle. Dès l’instant où une personne se connecte à distance sur le réseau de l’entreprise pour récupérer des données sur un serveur, elle ouvre une brèche entre le serveur et l’extérieur. Il est donc impératif que le tunnel de communication soit sécurisé afin d’authentifier la personne et que les échanges soient chiffrés.

**En 2021, priorité aux bases !**

Deux stratégies sont généralement mises en œuvre chez les industriels pour sécuriser leurs activités. D’un côté, la mise en œuvre d’une approche globale afin de tout sécuriser en même temps. De plus en plus d’industriels suivent cette démarche, en s’appuyant sur une société de conseils et un intégrateur pour assurer une sécurité complète de leurs usines. Mais cette approche suppose aussi de disposer d’un budget conséquent. De l’autre côté, certains industriels choisissent d’y aller par étape et de donner la priorité aux bases, d’abord en sécurisant la barrière OT-IT, puis en séquençant la sécurité des usines.

Segmenter ses réseaux, maintenir une bonne hygiène numérique et sécuriser son usage du cloud, telles sont les principales priorités pour le monde industriel cette année. De quoi bâtir des fondations solides avant d’envisager de déployer la 5G et l’IIoT.

Pour aborder l’ensemble de ses problématiques et construire l’industrie du futur en toute cyber-sérénité, [Stormshield propose une offre industrielle dédiée](https://www.stormshield.com/wp-content/uploads/SNS-FR-Security-Solutions-for-Industrial-Brochure-202009.pdf) – composée de firewalls industriels Stormshield Network Security et d’un agent de protection des postes et serveurs Stormshield Endpoint Security.