STORMSHIELD

Cybersécurité industrielle : un projet stratégique à ne pas sous-estimer

Par Robert Wakim, Offer Manager Industry - Stormshield

De nombreuses menaces sont susceptibles d'affecter les systèmes industriels et les infrastructures informatiques de l'industrie. Les exemples ne manquent pas et viennent chaque mois mettre en avant la grande vulnérabilité de nombreux acteurs : énergies, transports, etc. Dans ce contexte, le cyber terrorisme peut porter atteinte non seulement à la production, mais aussi à l'image des industriels. Mettre en place une politique de sécurité adaptée à cette industrie contribue largement à se prémunir contre les menaces informatiques et à préparer sereinement l'industrie du futur.

AVIS D'EXPERT

- Protéger l'ensemble de la chaîne industrielle
- Les postes opérationnels, des points sensibles à maîtriser
- Bien sécuriser les accès et les postes à distance
- Garantir la disponibilité du réseau

Protéger l'ensemble de la chaîne industrielle

Un réseau ouvert aux attaques entraîne un risque de dysfonctionnement du process industriel, des risques environnementaux, humains et financiers mais aussi des risques de perte d'informations confidentielles considérables. De nouvelles attaques montrent régulièrement la faiblesse des systèmes non protégés. De plus, les contraintes opérationnelles réduisent les possibilités de mise à jour des systèmes industriels. C'est pourquoi, il est indispensable pour les industries de s'appuyer sur des dispositifs centraux intégrant à la fois le domaine de l'OT (Operational Technology) et celui de l'IT (Information Technology), pour bénéficier d'une combinaison de protection des systèmes de production sans impact négatif sur l'activité.

Les postes opérationnels, des points sensibles à maîtriser

Dans un environnement Microsoft Windows, massivement utilisé dans le secteur industriel, les postes de travail constituent des points sensibles du système opérationnel. Une infrastructure adaptée doit permettre de faire face aux attaques informatiques les plus sophistiquées comme aux actes

À PROPOS

Stormshield, filiale à 100% d'Airbus CyberSecurity, propose des solutions de sécurité de bout-en-bout innovantes pour protéger les réseaux (Stormshield Network Security), les postes de travail (Stormshield Endpoint Security) et les données (Stormshield Data Security).

WWW.STORMSHIELD.COM

de négligence. Cela peut par exemple passer par l'utilisation de différents composants avancés, comme l'analyse comportementale, ou encore le contrôle des périphériques tels que les clés USB, qui sont un véritable danger et exposent le SI à différentes menaces.

Bien sécuriser les accès et les postes à distance

La plupart des infrastructures industrielles ont une connexion à Internet, à des fins de communication avec des tiers, notamment pour des opérations de maintenance et de supervision à distance ou d'optimisation des process (IOT et cloud computing). Or, cette connexion affaiblit le système et ouvre une porte aux cybercriminels. Il est donc primordial de prendre en compte ce risque, en assurant une protection de bout en bout : c'est-à-dire des connexions et de leurs extrémités.

Garantir la disponibilité du réseau

Les équipes de sûreté ont pour objectif de garantir à tout moment un fonctionnement sûr, ne mettant en risque ni la qualité du service ni la protection environnementale et humaine. Afin de conserver ce niveau de sûreté, il est indispensable que les équipements de sécurité soient compatibles avec les procédures en place. Les mécanismes de haute disponibilité ou de « fail open »* deviennent donc des fonctionnalités fondamentales.

Ces différents éléments mettent en évidence qu'une convergence IT / OT est obligatoire. La protection des systèmes d'information est aujourd'hui éprouvée alors que la protection des systèmes industriels est « naissante ». Or, les risques encourus par les systèmes industriels sont différents de ceux encourus par les systèmes d'informations. Ces deux mondes, qui aujourd'hui encore, cohabitent de façon indépendante, mais qui montrent des signes de rapprochement, doivent apprendre l'un de l'autre afin de réduire le risque de cyber sécurité.

** « Fail open » : Fonctionnalité garantissant la disponibilité en cas de défaillance électrique ou matériel. L'équipement reste en position « ouverte », laissant passer le flux comme si il n'était plus en place.*

Stormshield
22 rue du Gouverneur Général Eboué 92130 Issy-les-Moulineaux France