La cybersécurité des systèmes de commande devient incontournable

ARC Advisory Group estime les dépenses globales pour la cybersécurité des systèmes de contrôle industriel à 1,7 milliard de dollars en 2012. Ce marché qui couvre un large panel de produits a considérablement augmenté depuis la dernière étude et devrait connaître une hausse moyenne globale de 13,7 % d'ici à cinq ans.

La cybersécurité est devenue une préoccupation majeure des organisations de traitement de l'information (IT) aujourd'hui. Les cyber-attaques comme Stuxnet et les actions gouvernementales ont éveillé l'attention de toutes les entreprises. Les industriels partagent ce besoins de protéger leurs informations confidentielles et d'assurer la continuité de leurs activités, mais ils sont aussi inquiet au sujet de cyber attaques sur leurs systèmes, prenant le contrôle de leurs usines et de leurs équipements. Dans beaucoup de cas, c'est la préoccupation majeure car une intrusion dans ces systèmes peut impacter la santé et la sécurité des employés et de la population locale, de l'environnement, et paralyser l'entreprise.

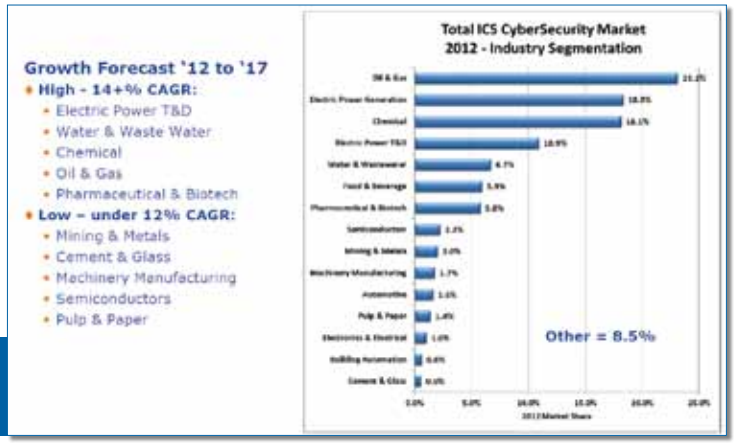
Un marché large

Cette étude concerne les produits et services de cybersécurité des systèmes de contrôle industriels (ICS). Elle couvre ainsi les matériels spécifiques à la sécurité tels que les firewalls, les composants de réseau et les serveurs qui apportent des fonctionnalités du type accès sécurisé à distance (VPN), la détection d'intrusion dans les réseaux, la gestion des menaces, la gestion des systèmes, etc. Elle concerne aussi les logiciels spécifiques de sécurité pour les ICS, les interfaces utilisateurs et les serveurs intégrés dans ces architectures, ainsi que les services associés : évaluation, conception, implémentation et gestion de la cybersécurité. A noter, les firewalls se taillent la part du lion sur ce marché. On retrouve dans cette catégorie les firewalls traditionnels et les firewalls spécifiques à certaines applications, utilisés pour protéger les appareils industriels en isolant certaines *« zones »* des systèmes. Viennent ensuite les antivirus et les logiciels de gestion d'habilitation (*Whitelisting*).

Trois types d'acteurs

Une solution de cyber sécurité des ICS n'est pas un produit unique. C'est la combinaison d'une architecture, de procédures, de comportements de composants de sécurité (matériels et logiciels) et de services tiers. Les fournisseurs de ces produits s'organisent en trois groupes : les généralistes, les fournisseurs de systèmes de contrôle (DCS, SCADA, HMI, PLC) et les spécialistes de la cybersécurité des ICS. Chaque catégorie suit une stratégie différente. Cependant, pour améliorer leurs parts de marché, les généralistes ont intérêt à s'allier à des spécialistes des ICS ou des intégrateurs pour mieux répondre aux besoins des industriels. Les spécialistes de la cybersécurité des ICS sont, quant à eux, peu nombreux et leurs offres se chevauchent peu. Ils doivent faire un effort important de marketing, devenir des partenaires de confiances pour leurs clients actuels et élargir leurs prestations auprès d'eux. ▮

L'intégralité de cette étude est disponible auprès de ARC Advisory Group.



Segmentation du marché global de la cybersécurité en 2012.