LesEchos.fr

Les pirates s'attaquent aux systèmes industriels

LES ECHOS | LE 09/10/2014 À 06:00

Les systèmes d'information industriels s'ouvrent de plus en plus et s'exposent ainsi à de nouvelles menaces ciblant les applications, les systèmes de contrôle-commande et les réseaux. - Shutterstock

Les usines et leur informatique en vase clos, c'est du passé.

Les responsables des systèmes d'information industriels sont des champions de la prudence. *« Rien ne sort jamais du périmètre de l'usine »,* assurent les uns. *« Seul ce qui est transmis par le calculateur industriel peut franchir le pare-feu »,* affirment les autres... Aujourd'hui, ils doivent cependant redoubler de vigilance. Car, après avoir longtemps fonctionné en vase clos, les systèmes d'information industriels s'ouvrent de plus en plus. Ils s'exposent ainsi à de nouvelles menaces ciblant les applications, les systèmes de contrôle-commande et les réseaux.

« Les menaces ciblant les systèmes industriels, rarissimes il y a seulement dix ans, deviennent bel et bien une réalité », observe Lionel Mourer, président du cabinet de conseil Atexio et administrateur du Clusif (Club de la sécurité de l'information français). Il y a d'abord eu le ver Stuxnet, qui a défrayé la chronique en 2010 en s'attaquant aux systèmes Scada (« supervisory control and data acquisition ») de contrôle-commande des centrifugeuses utilisées dans le cadre du programme nucléaire iranien. Puis, en juillet dernier, on a parlé d'un autre virus, baptisé « Dragonfly », qui serait, quant à lui, parvenu à corrompre certains systèmes de contrôle des opérateurs d'énergie. Dans le même temps, le Centre national d'études spatiales (Cnes) aurait été victime d'une série d'e-mails infectés qui ont ciblé ses ingénieurs.

De la sûreté à la sécurité

Comment les systèmes ont-ils pu être pris en défaut ? *« Les machines industrielles, à la durée de vie particulièrement longue, utilisaient jusqu'ici des systèmes d'exploitation propriétaires assez rares, en mode boîte noire,* relève Lionel Mourer. *Désormais, ces engins s'appuient de plus en plus souvent sur Unix, Linux et Windows. Ils sont aussi plus fréquemment reliés au réseau de l'entreprise, via des connexions Ethernet, GSM ou wi-fi, pas toujours suffisamment sécurisées. »* Dans certains cas, les machines font même automatiquement remonter certaines données vers un cloud, qui met à la disposition des décideurs des tableaux de bord permettant d'optimiser les processus.

Pour les industriels, habitués plutôt à travailler dans la durée, *« la première difficulté est sans doute de passer d'une logique de sûreté à une logique de sécurité »,* juge Dominique Meurisse, directeur des opérations de Wallix, spécialiste français des solutions de traçabilité et de sécurisation des accès. Ce qui implique qu'ils se préoccupent autant des questions de disponibilité et de remise en service de leurs machines que de la recherche d'éventuelles vulnérabilités.

D'où la nécessité de bien s'équiper. Lorsque Renaud Bidou, directeur technique de DenyAll, prêche pour des solutions capables de *« scanner les vulnérabilités et de filtrer tous les flux entrants »*, Cyrille Badeau, directeur Europe du Sud du pôle sécurité de Cisco, exhorte pour sa part les industriels à s'équiper d'une solution *« qui détecte les anomalies dans les données mesurées par leurs capteurs ».* C'est plus efficace que de s'appuyer sur des bases de connaissances forcément périmées.

Erick Hess, Les Échos

En savoir plus sur http://www.lesechos.fr/thema/cybersecurite-2014/0203829955422-les-pirates-sattaquent-aux-systemes-industriels-1051594.php?htPp81ZZgo3s7OzQ.99