Sécuriser les Scada : « ce sera cher et difficile », dit Kaspersky

Kasperky débarque sur le marché de la sécurisation des systèmes industriels, avec le lancement d'une solution dédiée (appelée Industrial CyberSecurity). « *Nous vivons une période de recrudescence des attaques contre les infrastructures critiques*, assure le fondateur et Pdg de l'éditeur, Eugène Kaspersky. *Les attaques criminelles contre ce type de cibles sont en croissance rapide, car les organisations criminelles traditionnelles migrent vers ces nouveaux environnements.* » Et de citer le cas découvert récemment d'une modification de température des cuves de stockage de pétrole afin de mettre sur pied une très discrète fraude aux volumes. « *Et encore ne voyons-nous probablement pas l'intégralité du tableau, car les entreprises sont aveugles, elles ne se rendent souvent pas compte qu'elles ont été piratées.* » Selon le dirigeant de l'entreprise russe, à cet inquiétant intérêt de la criminalité organisée pour les Scada, s'ajoutent des piratages qu'il qualifie de « *cyber-terrorisme* ». Une catégorie où il classe pêle-mêle le récent black-out sur le réseau électrique ukrainien, l'arrêt d'urgence d'un haut-fourneau en Allemagne ou les attaques contre les systèmes informatiques des hôpitaux (3 cas recensés au cours des derniers mois).

Pour Eugène Kaspersky, la prise de conscience du danger a toutefois eu lieu. « *Il y a quelques années, je devais expliquer l'importance de la question de la sécurité des systèmes industriels*, raconte-t-il. *Ce n'est plus le cas aujourd'hui. Ce sont même les ministres qui viennent m'expliquer qu'on est face à un problème !* » Pour l'éditeur, cette première étape de prise de conscience doit en précéder deux autres : la définition d'une stratégie et son implémentation. « *La plupart des gouvernements s'approche de la seconde marche* », résume Eugène Kaspersky.

Normes : le « *zéro absolu* » selon Kaspersky

Rappelons qu'en France, via l'Anssi (Agence nationale de la sécurité des systèmes d'information), le gouvernement entend encadrer la cybersécurité des OIV, ou opérateurs d'importance vitale : environ 200 organisations dont le bon fonctionnement est jugé critique pour le pays. Un renforcement de la régulation que le patron de Kaspersky appelle d'ailleurs de ses vœux : « *Quand vous construisez un immeuble, vous avez tout un corpus de règles à respecter, mais en matière de cybersécurité, c'est le zéro absolu. On pourrait prolonger la remarque aux opérations de maintenance dans l'industrie : si vous faites fonctionner une turbine, toute*

une série de contrôles et d'opérations physiques est programmée, par contre, tant que le système de contrôle fonctionne, la pratique majoritaire en matière de cybersécurité consiste à ne surtout pas y toucher. » Et de rappeler la paralysie de l'aéroport parisien d'Orly, causé par des systèmes de diffusion des prévisions de la météo fonctionnant… sous Windows 3.1.

« La complexité des systèmes en place »

Reste que la remarque d'Eugène Kaspersky montre aussi à quel point les priorités industrielles, tournées avant tout vers la sûreté de fonctionnement, sont éloignées des bonnes pratiques de la cybersécurité. « *Les industriels ont pris conscience du problème, mais la complexité des systèmes en place et la sophistication des attaques les placent devant un réel défi* », résume Cevn Vibert, un spécialiste de la sécurité des Scada travaillant pour l'intégrateur SolutionsPT. Reconnaissant, notamment en raison du caractère très spécifique de chaque environnement, que la tâche s'annonce plus ardue que celle consistant à sécuriser les SI des entreprises (c'est dire !), Eugène Kaspersky lance : « *Cela ne sera pas facile, cela coûtera beaucoup d'argent, nous manquons d'ingénieurs pour y parvenir, mais nous devons y arriver.* »

Pour apporter sa pierre à l'édifice – et ajouter une ligne à son compte de résultats -, l'éditeur explique vouloir monter des centres de formation sur le sujet un peu partout dans le monde. Le premier d'entre eux a vu le jour en Russie, et se concentre sur le secteur de l'énergie. La société a également mis au point des serious games permettant aux dirigeants d'une société de travailler sur des scénarios de crise. S'y ajoute évidemment le lancement de la solution dédiée à la sécurisation des Scada, censée protéger les terminaux et l'intégrité du réseau.

« *Elle offre aux entreprises du temps pour réagir et leur délivre des informations sur les attaques en cours*, assure le responsable de cette nouvelle offre. *Nous travaillons de façon passive.* » Aux technologies classiques de l'éditeur – comme la protection anti-malware -, Kaspersky Industrial CyberSecurity greffe des procédés spécifiques aux Scada, comme le contrôle d'intégrité des programmes des automates industriels, le monitoring sémantique des commandes de contrôle ou le suivi des données télémétriques. L'ambition affichée de l'éditeur est de dépasser la détection des menaces et la prévention sur les systèmes industriels, pour apporter aux entreprises une console de supervision leur permettant de développer des capacités de réponse aux incidents et des facultés de prédiction des incidents.

A lire aussi :

Scada : des hackers manipulent le retraitement des eaux

Les 10 principales défaillances des systèmes Scada selon Lexsi

Panne de courant via une cyberattaque : les spécialistes ne sont pas surpris