CYBERSÉCURITÉ

Protéger son informatique industrielle

De plus en plus connectées, les usines ne sont plus à l'abri des attaques informatiques. Pour se protéger, elles doivent adopter des mécanismes de cybersécurité.

HASSAN MEDDAH

En matière de sécurité industrielle, il y aura un avant et un après Stuxnet. En juin 2010, ce virus a pris le contrôle du système de commande des centrifugeuses chargé de l'enrichissement d'uranium du programme nucléaire iranien. En modifiant leur vitesse de rotation, il les a sévèrement endommagées. Selon les militaires, les dégâts pour l'usine ont été aussi efficaces qu'un bombardement! Désormais, les entreprises savent que leur parc industriel est une cible potentielle. «Depuis 2010, les attaques ayant pour finalité le sabotage d'installations industrielles se sont multipliées», souligne Stéphane Meynet, chef de projet sécurité des systèmes industriels à l'Agence nationale de la sécurité des systèmes d'information (Anssi). Or l'informatique industrielle est de plus en plus vulnérable. D'une part, les usines sont toujours plus connectées au monde extérieur. D'autre part, elles adoptent des technologies standardisées (réseaux IP, ethernet...) bien connues des hackers. Cybersécuriser son outil de production devient donc indispensable.

1 CARTOGRAPHIER SES INSTALLATIONS CRITIQUES

«Il faut d'abord procéder à un inventaire précis des installations matérielles, des systèmes et des applications critiques», explique Stéphane Meynet. Attention, cela exige des ressources techniques et du temps. À la différence de l'informatique de gestion où tous les serveurs et PC sont répertoriés dans un annuaire, l'informatique industrielle repose sur un parc de machines hétérogènes (automates et calculateurs de marques différentes, PC et serveurs avec des configurations spécifiques à chaque fois...) et nécessite souvent de descendre jusqu'aux ateliers de production et aux entrepôts afin de tout répertorier. Un grand industriel du domaine agroalimentaire, avec de nombreux sites répartis au niveau mondial, s'est lancé dans l'opération. «Nous avons réalisé une phase d'études pour établir un état des lieux de notre sécurité et faire une analyse des risques. Nous avons confié cette tâche à un binôme avec la double compétence, industrielle et informatique, pour se rendre sur site afin d'identifier les machines et les process à protéger. Cette étude s'est étalée sur un an et a permis de repérer plusieurs centaines d'actifs avec des risques de vulnérabilité divers», explique le responsable des systèmes d'information industriels. «Nous avons profité de nos déplacements pour sensibiliser les responsables locaux à la problématique de la cybersécurité», explique-t-il.

2 RÉDUIRE LE FOSSÉ ENTRE INFORMATICIENS ET AUTOMATICIENS

Très longtemps, les informaticiens et les automaticiens se sont ignorés. Les premiers, souvent proches de la direction générale au siège; les autres affairés sur les lignes de production, les mains dans le cambouis. Et la méfiance est plutôt de mise. «Quand j'ai débarqué dans les ateliers, on m'a tout de suite suspecté de me mêler de ce qui ne me regardait pas», souligne le directeur informatique d'un grand groupe industriel, évoquant ses premiers contacts avec ses collègues. Mais le risque informatique oblige ces deux univers à se rapprocher. Au sein du groupe agroalimentaire, c'est plutôt l'équipe chargée des systèmes industriels qui a pris l'initiative. «Nous avons organisé des réunions avec l'équipe informatique. C'était absolument nécessaire pour bien se comprendre et harmoniser les solutions», explique le responsable du système d'information industriel. «Le jargon et les normes sont différents», avertit Laurent Railler, le responsable marketing et sûreté de fonctionnement chez Schneider Electric. Quand on parle de la sécurité, les automaticiens pensent avant tout sécurité de fonctionnement de leur installation pour la protection des opérateurs et la disponibilité des machines, alors que les informaticiens sont obnubilés par les intrusions et les vols de données.

PASCAL GUITTET

Les installations industrielles sont de plus en plus souvent pilotées par l'informatique, comme ici chez Constellium.

3 DES ANTIVIRUS, OUI MAIS JUSQU'OÙ ?

Le déploiement à grande échelle des antivirus fait débat auprès des industriels, d'autant plus qu'ils peuvent dégrader les performances des machines temps réel. L'Anssi préconise un usage... à bon escient. « Il ne faut pas que le remède soit pire que le mal. Tous les automates ne sont pas forcément accessibles du monde extérieur. Il faut déployer les antivirus aux points de connexion avec les réseaux extérieurs », estime Stéphane Meynet. Pour ne rien laisser au hasard, l'industriel de l'agroalimentaire a généralisé leur déploiement sur tous les serveurs d'ingénierie qui donnent accès aux machines industrielles. Attention au faux sentiment de sécurité. Ce n'est pas parce que le réseau de production n'est pas connecté à l'extérieur qu'il est protégé. Les clés USB ou les PC portables qui se branchent aux automates pour réaliser les opérations de maintenance sont des vecteurs de propagation de virus. Comme pour les PC, il faut mettre à jour ses antivirus. Les sites web des fabricants d'automates sont une ressource utile. « L'utilisateur peut s'informer sur les découvertes de nouvelles menaces et télécharger les correctifs correspondants », explique Jérôme Poncharal chez Rockwell Automation.

4 RÉSISTER À LA SURENCHÈRE TECHNOLOGIQUE

Les fabricants proposent toujours plus d'options high-tech avec leurs automates : serveur web intégré, gestion à travers le cloud, pilotage par smartphone... « Gare à l'effet de mode. L'entreprise doit se demander si elle a besoin de toutes ces technologies. Le risque associé est souvent sous-estimé », prévient Stéphane Meynet. Par ailleurs, les règles de base de l'hygiène informatique doivent être respectées. « Dans certaines installations, on trouve les mots de passe usine non modifiés, ou les ports de communication des machines activés sans que cela soit nécessaire », précise Laurent Railler de Schneider Electric. Autre règle : le cloisonnement entre le réseau industriel et celui de gestion pour éviter la propagation du risque. Si une connexion est absolument nécessaire sur un automate critique, un mécanisme de diode réseau permet de remonter ses données en évitant toute infection. Enfin, les entreprises doivent muscler leur capacité à détecter les attaques. La nouvelle loi de programmation militaire va contraindre celles opérant dans des secteurs critiques (télécommunications, énergie...) à déployer des dispositifs capables de détecter des signaux faibles annonciateurs d'une attaque.