Crédit : Lenny Kuhne

Les usines soumises aux cyberattaques en raison des machines connectées

Les cyberattaques se sont accrues avec la pandémie, touchant tous les secteurs. De nombreuses entreprises sont concernées, tout comme les usines. Ces dernières ne sont pas encore suffisamment protégées contre le risque de cyberattaques paralysantes, liées à la connexion sans cesse plus importante des machines et systèmes de production, selon des experts rassemblés mardi au forum international de la cybersécurité (FIC) de Lille.

Pendant longtemps, les machines et automates installés dans les usines ont fonctionné coupés du réseau informatique de l'entreprise, et donc du monde extérieur. Mais, à l'ère de l'usine 4.0, les machines sont de plus en plus connectées, alors même que leurs systèmes internes n'ont jamais été conçus pour une telle ouverture au monde. Pourtant les attaques sur les machines industrielles sont bien réelles. « *Le nombre d'attaques que nous subissons augmente de façon très importante* » , en particulier via les fournisseurs, confirme Olivier Ligneul, en charge de la sécurité de l'informatique chez EDF. Le cabinet Wavestone, qui a mené une étude sur la cybersécurité de 40 sites industriels dans des domaines variés (pharmacie, énergie, industrie

manufacturière…) a constaté que 12% d'entre eux avaient subi une attaque cyber sur les 12 derniers mois, avec un impact direct sur la production, comme l'arrêt de machines.

Des attaques opportunistes

On est loin des spectaculaires attaques industrielles menées par de puissants Etats, comme l'attaque Stuxnet, attribuée aux Israéliens et aux Américains et qui avait visé les centrifugeuses du programme nucléaire iranien. « *Il y a beaucoup d'attaques non ciblées* » et relativement banales, *« qui visent par exemple à implanter un rançongiciel ou un mineur de cryptomonnaie* » , relève Arnaud Soullié, spécialiste de cybersécurité industrielle chez Wavestone. Les attaques industrielles sont souvent « *des attaques d'opportunistes* » habitués à cibler des réseaux d'entreprises classiques « *et qui en arrivent à contaminer des machines industrielles* » , décrit Loïs Samain, responsable de la sécurité informatique chez EDF Hydro. « *Il y a encore un parcours important à faire dans les entreprises industrielles sur la prise de conscience qu'à travers l'informatique, les automatismes, on peut leur faire beaucoup de mal* » , résume Hervé Constant, le directeur informatique du gestionnaire du réseau de transport de gaz GRTGaz, entreprise stratégique où la sécurité est une vertu cardinale.

Une prise de conscience

Sur le fond, Arnaud Soullié n'est pas pessimiste sur les capacités des techniciens, ingénieurs et autres responsables de production à mettre à niveau leurs systèmes. « *Nos interlocuteurs dans l'industrie sont sensibilisés aux questions de cybersécurité* » , souligne-t-il. « *Ils voient bien qu'il y a un problème lorsqu'ils se rendent compte qu'ils peuvent modifier des paramètres de machine sans code secret ou mot de passe par exemple, et ils agissent lorsqu'on leur propose les outils nécessaire*s », ajoute-t-il. En outre, « *c'est plus facile de faire de la cybersécurité dans des systèmes industriels qu'ailleurs, parce que ces systèmes évoluent moins vite: si je révise un système, ce sera valable 5 ans, 10 ans, cela va beaucoup moins vite que dans la bureautique par exemple* » , poursuit-il. Et il y a dans le monde industriel « *une culture de la qualité de la production, du respect des audits* » qui facilitent les choses, affirme t-il. « *Un jour, une attaque réussira, donc il faut s'entraîner à tous les niveaux de l'entreprise* » , prévient Thierry Trouvé, directeur général de GRTgaz, qui fait le point tous les deux mois en comité de direction sur les sujets de cybersécurité.

À lire aussi

11 manières de protéger son entreprise face aux cyberattaques

Article écrit par ANNE TAFFIN