Comment l’industrie peut aussi anticiper les cyberattaques ?

Comment l’industrie peut aussi anticiper les cyberattaques ?

Les cyberattaques se multiplient ces derniers mois et ont augmenté de 51 % (*) cette année en France, en particulier à l'encontre des technologies de l'information (messageries hackées, serveurs victimes d'attaques #DDoS entre autres). Pourtant, un tout autre domaine suscite de nouvelles préoccupations : l'industrie.
Les systèmes industriels, ou Industrial Control System (ICS), désignant l'ensemble des moyens informatisés et automatisés assurant le contrôle et le pilotage de procédés industriels, subissent les mêmes menaces que dans le milieu IT.
Cependant, une attaque à l'encontre de l'ICS peut avoir des répercussions encore plus graves, non seulement sur l'industrie en elle-même, avec son corollaire de pertes financières, mais aussi, et surtout, sur l'homme et l'environnement.

Des réseaux vulnérables, car en flux tendus
Tandis que l'IT se soucie davantage de la confidentialité des données, les industriels se préoccupent essentiellement de la disponibilité et de la rentabilité de leur production. Il faut ainsi comprendre que pour des questions de coût, il est inconcevable pour un industriel de stopper sa production, nonobstant une menace imminente.

La dernière crise ukrainienne a illustré cette problématique. Malgré des bombardements massifs, le système de production n'a pas été arrêté. Les réseaux industriels sont d'autant plus vulnérables qu'il n'est pas possible d'effectuer de maintenance sur le système, puisqu'il est en cours de production.

Mais qui sont ces « pirates » qui tirent profit de ces vulnérabilités ?
Il s'agit de groupes bien organisés, de terroristes, qui s'attaquent directement à la vulnérabilité de l'État et des grandes entreprises. On parle d'une véritable cyberarmée qui s'attaque aux réseaux industriels de plusieurs manières : déni de services, prise de contrôle à distance des systèmes, vol de données, mise en faillite par détournement de fonds, pour n'en citer que quelques-uns. En 2003, la centrale nucléaire de Davis-Besse aux USA avait été la cible d'attaques DDoS.
Pour autant, la plupart des incidents de sécurité sont accidentels, liés par exemple à l'activation fortuite de malware se trouvant dans un mail, sur une clé USB ou encore des softwares mal sécurisés.
À l'échelle de l'industrie, les attaques peuvent entraîner des retards de production, un impact économique – consécutif au vol de secrets de fabrication – une perte d'image et de contrats. In fine, l'industriel se retrouve face à une véritable perte de compétitivité.
Les réseaux industriels étant en contact direct avec la vie humaine, celle-ci est également en danger. Ces attaques peuvent en effet entraîner des accidents physiques ; l'arrêt de la production d'énergie pouvant entraîner des coupures d'électricité dans les hôpitaux qui peuvent être critiques. À plus grande ampleur, la santé humaine et l'environnement sont également menacés dans le cas d'une attaque des systèmes nucléaires.
L'exemple le plus connu est celui de Stuxnet, un ver informatique découvert en 2010 et conçu pour attaquer une cible industrielle déterminée pour l'espionner. Le ver a affecté 45 000 systèmes informatiques, y compris des ordinateurs de la centrale nucléaire de Bouchehr ainsi que 15 000 ordinateurs et centrales situés en Allemagne, en France, en Inde et en Indonésie (**).

Les industriels ne sont pas suffisamment préparés à ces types d'attaques, car les moyens mis en œuvre sont limités et la sécurité est considérée comme annexe, dans la mesure où elle n'est pas fondamentale pour assurer les services. À cela s'ajoute qu'elle représente un coût additionnel pour la production, qui se répercute sur les consommateurs qui devront payer plus cher leurs eau, électricité et autres services.
Dès lors, quelles sont les mesures pour se prémunir de ces attaques ? Quels outils peuvent être mis en place ?
La loi est un instrument essentiel pour assurer la protection des ICS et aider à recréer de la confiance. La France a mis en place, en 2006, un décret qui définit 12 secteurs d'importance vitale comprenant notamment la gestion de l'eau, la santé, l'énergie, l'alimentation et les transports, des fondamentaux pour le fonctionnement d'un État.

« Le projet de loi de programmation militaire, prévu pour 2014-2019, précise qu'il est de la responsabilité de l'État d'assurer une sécurité suffisante des systèmes critiques des OIV (opérateurs d'importance vitale). À travers quatre mesures principales, il vise à établir un socle minimum de sécurité pour les organisations.
Il donne notamment au pouvoir exécutif la possibilité d'imposer aux OIV des obligations en matière de sécurisation de leur réseau, de qualification de leurs systèmes de détection, d'information sur les attaques qu'ils peuvent subir et de soumission à des contrôles.
Avec ce texte, qui sera examiné sous peu au Sénat, l'État fixera donc des règles en collaboration étroite avec l'ANSSI. Règles que les OIV seront tenus d'appliquer, à leur frais. Les sociétés mauvaises élèves seront susceptibles de se voir infligées une sanction pouvant aller jusqu'à 750 000 euros d'amende » (***).

Au-delà de cette législation, il est essentiel, pour retarder l'attaque, de mettre un point d'honneur à la sensibilisation de l'utilisateur dans la chaîne de production, mais aussi, et surtout, de la direction des industries, en l'incitant à appliquer de bonnes pratiques au quotidien et en investissant dans les hommes et les outils (firewall, anti-vers ou encore systèmes de détection d'intrus).
Cependant, même le plus puissant des firewalls n'est pas suffisant si l'on n'identifie et ne traite pas les menaces dans le détail, sur un service en particulier. Cela sous-entend qu'il y ait un opérateur qui assure la maintenance des systèmes d'informations, sans quoi les intrusions dans les réseaux industriels ne pourront être empêchées.

(*) Source : étude réalisée par le cabinet PwC
(**) Source : Wikipédia
(***) Source : Nextimpact.com

Réagissez à cet article

Source : *Les Echos.fr – Actualité à la Une – Les Echos*