Questions à Thomas Houdy,

Expert en cybersécurité chez LEXSI

Comment faire lorsqu'il est trop tard ? Comment détecter une attaque dans son usine et réagir au mieux. Eléments de réponses avec ce spécialiste indépendant des éditeurs et des fournisseurs de matériels.

Quel est le premier réflexe à avoir lorsque l'on craint d'être attaqué ?

Etre attaqué est une chose, mais il faut se mettre en position de pouvoir le détecter. Cette anticipation de la cyber-attaque n'est souvent pas faite dans les entreprises. Afin de déceler une attaque, il est aussi important de maîtriser son environnement que d'avoir un inventaire à jour de ses équipements. Souvent, seules quelques personnes ont cette connaissance dans l'entreprise (ou chez des sous-traitants) et la crise arrive toujours au mauvais moment, quand la personne compétente n'est pas là. Et évidemment, l'anticipation passe par une analyse préalable des risques et le fait de jauger le risque de propagation d'une attaque dans son usine.

Les attaques actuelles sont de quels types ?

Chez Lexsi, nous bénéficions d'un CERT (Computer Emergency Response Team) qui recense les attaques partout dans le monde. En 2014, deux virus ont été virulents : Havex-Dragonfly et Sandworm. Ces deux virus s'épanouissent en milieu industriel. Les cybercriminels utilisent des techniques classiques pour cibler les industriels : phishing, ingénierie sociale. Dans le cas de Dragonfly, ils ont piraté les sites web de fournisseurs de composants industriels (eWON, MESA Imaging, MB Connect Line) pour y insérer leur virus, selon la technique du « *trou d'eau* », puis envoyé des emails invitant des profils industriels à se connecter sur le site web du fournisseur pour télécharger une mise à jour, renfermant le composant malveillant. Le virus utilisé scannait les machines OPC et cherchait à envoyer ses informations vers le serveur central des pirates, appelé « *serveur de contrôle commande* ». Evidemment, il y a aussi eu des attaques ciblées...

Les cybercriminels sont parfois des activistes, mais la finalité des pirates est quasi exclusivement monétaire. Soit le pirate veut détourner de l'argent ou en récupérer en volant des informations importantes, soit il a été payé pour faire un déni de service. Et ils sont souvent très bien informés de ce qui est important ou pas.

Comment détecter une offensive ?

Il n'y a souvent pas d'équipement de détection de cyberattaque dans les usines et en milieu industriel. Résultat, sept ans après son apparition, le virus Conficker continue de se propager régulièrement dans certaines usines. Heureusement, il n'est pas très dangereux… A la décharge des industriels, il y a peu de solutions disponibles. Par exemple, il n'existe pas d'antivirus industriel, pas de consoles de contrôle cybersécurité, de « *Scada de la cybersécurité* », sur le marché actuellement. Quand ce n'est pas tout simplement une clause contractuelle d'un fournisseur qui empêche l'industriel de sécuriser son système. Mais cela avance avec, par exemple un projet d'antivirus français dédié à l'industrie ou le développement de sondes de détection d'attaques cyber.

En attendant, pour se protéger, les industriels n'ont pas de choix : ils doivent mettre en œuvre une défense en profondeur, qui consiste à empiler des couches de sécurité. D'abord, ils doivent protéger les accès, en particulier les télé-

opérations - avec la mise en place progressive de l'industrie 4.0, de nouvelles solutions devraient apparaître dans ce domaine - et cloisonner les réseaux. Attention également aux points d'accès wifi, qui se multiplient dans les usines sans être bien maîtrisés.

La détection proprement dite de la menace peut passer par l'usage de sondes, des équipements qui « écoutent » ce qui passe dans les tuyaux. Le principe est simple : lorsqu'elle dit quelque chose, il faut réagir. Dans ce domaine, les industriels ont une chance : les réseaux y sont très statiques et il est ainsi relativement aisé de définir un fonctionnement nominal de l'usine puis ensuite de détecter toute déviation.

Bientôt, on devrait même pouvoir disposer dans les salles de supervision d'un écran supplémentaire dédié aux problèmes de cybersécurité. Mais attention : il faudra former les équipes. De plus, les industriels pourraient avoir un faux sentiment de sécurité, alors qu'ils ont des matériels et des firewalls mal configurés...

Quand je suis attaqué, quelle réaction adopter ?

Attention, débrancher tout pour couper les accès de l'extérieur peut être dangereux. Si l'on débranche le mauvais équipement, les conséquences peuvent être importantes, par exemple en termes de traçabilité. L'industriel doit, avant que le sinistre arrive, définir son plan de gestion de crise et un plan de reprise d'activité. Pas forcément complet et ultra-détaillé. Il s'agit surtout de savoir si l'on peut débrancher telle ou telle machine ou passer en mode dégradé sans mettre en danger tout le process. Quoi qu'il en soit, il est cependant fort peu probable que l'on puisse paralyser une usine entière avec un virus, même si certains sites européens, dont une aciérie allemande, ont subi des pertes importantes à la suite d'une cyber-attaque.

Le monde industriel est très en retard sur le monde de l'IT ?

Il est clair qu'il y a un problème de maturité des industriels dans ce domaine. D'ailleurs, malgré leurs efforts, il est encore très simple de modifier un programme automate, à commencer par tous ceux qui ne sont pas de dernière générations. Et les difficultés ne font que commencer, avec de nouvelles générations de salariés qui débutent leur journée de travail en mettant en charge leur smartphone, potentiellement truffé de virus, sur un port USB disponible... Dans le monde de l'IT, le directeur des systèmes informatiques peut verrouiller tout son système et instaurer de nouvelles règles de sécurité en quelques minutes sur l'ensemble de son réseau s'il le désire. Dans le monde industriel, il n'est pas envisageable de changer les règles de sécurité et les mots de passe comme cela, sans préavis. Il faut donc avant tout travailler sur des changements de comportement simples des employés. Le facteur humain est primordial : prise de conscience, formation et sensibilisation ; aussi bien pour le DG que pour le simple opérateur !

Les automates industriels sont si vulnérables que cela ?

Avec du matériel neuf, et en se posant dès le départ la question de la sécurité, un industriel peut atteindre aisément une note de 18/20 en termes de cybersécurité, même en employant des technologies

de communication transversales comme IO-Link ou OPC-UA. Les difficultés viennent plutôt du rattrapage de l'existant, car il y a encore énormément d'automates d'anciennes générations sur le marché qui sont truffés de failles de sécurité. De la même façon, certaines technologies de communication comme Modbus TCP sont considérées comme non sécurisés. Mais les solutions existent : si l'on utilise des réseaux de terrain qui ne sont pas sécurisés, il faut sécuriser autour.

Par contre, il est rare d'avoir des systèmes sécurisés par défaut. Afin d'en faciliter l'emploi, les fabricants des matériels d'automatismes préfèrent souvent neutraliser les protections d'emblée. Cela devrait être obligatoire ! De même, quand une machine ne fonctionne pas, on a souvent tendance à désactiver les différentes sécurités au fur et à mesure, jusqu'à ce que le problème soit réglé. Et on oublie alors de réactiver les protections après le retour en situation normale... Là encore, c'est un problème de comportement. ▮