La cyberattaque contre le groupe Colonial Pipeline fait désormais office de référence mondiale - quels enseignements en tirer ?

Le 7 mai 2021, le groupe Colonial Pipeline révélait avoir été mis à l'arrêt par un ransomware et avoir placé ses systèmes hors ligne selon une stratégie proactive pour contenir au maximum la menace. Entre-temps, le FBI a confirmé que le groupe de hackeurs DarkSide était responsable de l'attaque. Par la suite, Colonial Pipeline a déclaré qu'il reprenait l'exploitation de ses oléoducs.

Même si nous n'avons toujours pas à ce jour le détail complet de la méthode utilisée, quelques éléments ont tout de même filtrés du moins sur l'accès initial au réseau informatique de Colonial Pipeline. Il semblerait en effet que les attaquants aient pu s'introduire au sein du réseau par le biais d'une connexion VPN d'un employé en récupérant un mot de passe ayant fuité. La défaillance porterait donc sur une mauvaise gestion des accès, alors même que la connexion n'était pas protégée par une authentification forte, et que le compte était actif alors que le compte n'était plus utilisé.

L'attaque a de plus mis en lumière plusieurs problèmes ayant un impact sur la sécurité des systèmes de contrôle industriels (ICS). Beaucoup l'ont comparée à l'attaque contre la station d'épuration d'Oldsmar, mais on constate tout de même des différences majeures : si les dégâts à Oldsmar ont été rapidement maîtrisés par les opérateurs et n'ont pas entraîné d'interruption des processus de traitement de l'eau, l'attaque sur Colonial Pipeline aura un impact économique réel sur les chaînes d'approvisionnement et les consommateurs.

Voici quelques-unes des principales leçons à tirer de cette cyberattaque :

L'émergence de ransomwares ciblés. DarkSide, le groupe à l'origine de l'attaque, cible des entreprises spécifiques à forte valeur ajoutée. Une fois l'infection survenue, une segmentation inadéquate entre les environnements IT et OT permet la propagation des ransomwares touchant les infrastructures OT. En isolant et en segmentant ces dernières, les entreprises peuvent donc empêcher la propagation latérale des ransomwares.

L'obsolescence technologique . Le nombre d'attaques contre les infrastructures critiques a augmenté en fréquence et en gravité. Alors que les cybercriminels cherchent à profiter d'opportunités d'extorsion, la dépendance à l'égard de technologies émergentes rend les infrastructures critiques particulièrement vulnérables, en raison de leur gigantesque surface d'attaque. De nombreux environnements ICS exploitent des technologies obsolètes, pour lesquelles le processus d'application de correctifs est rare, voire inexistant et, quand il existe, il est risqué voire inapplicable. Cela engendre une situation où les niveaux de risque en matière de cybersécurité sont supérieurs aux tolérances acceptables. La mise à jour des technologies et l'amélioration de la gouvernance sont donc des atouts majeurs dans notre quête d'atténuation des risques.

La nécessité de sécuriser les environnements distribués. Les pipelines sont des environnements hautement distribués et les outils utilisés pour permettre aux opérateurs de se connecter à distance favorisent davantage la facilité d'accès que la sécurité. Cela donne aux attaquants la possibilité de se faufiler à travers les cyberdéfenses, comme on a pu le voir dans l'attaque d'Oldsmar.

Les entreprises du secteur de l'énergie sont particulièrement exposées. Nos chercheurs de ont

constaté que les entreprises du secteur de l'énergie sont parmi les plus touchées par les vulnérabilités ciblant les environnements ICS. Ces vulnérabilités révélées par les acteurs de l'énergie au cours du second semestre 2020 connaissent une hausse d'une ampleur inédite : plus 74 % par rapport au second semestre 2018. Un chiffre qui montre que les cybercriminels disposent de nombreux moyens pour lancer des exploits sur les dispositifs de contrôle des réseaux industriels.

Comment les équipes de sécurité doivent-elles réagir ?

Il existe plusieurs façons d'atténuer un tel événement de cybersécurité et de s'y préparer

Appliquer une stratégie de gestion des correctifs sur l'ensemble des systèmes, ou à défaut établir des contrôles compensatoires. L'application de correctifs sur les systèmes des environnements OT nécessite certes de planifier des fenêtres de maintenance, mais elle est justifiée par le fait que les cibles préférées des cybercriminels sont plus souvent les vieux OS Windows, ou ceux dépourvus des indispensables correctifs. Si l'application de correctifs n'est pas possible, il faut s'assurer que des contrôles compensatoires sont en place (règles de pare-feu, listes de contrôle d'accès) afin d'atténuer le niveau de risque.

Instaurer une authentification forte pour tous les utilisateurs d'environnements OT. Malgré la sensibilité des environnements OT, de nombreuses organisations utilisent une combinaison à facteur unique (nom d'utilisateur et mot de passe) pour l'accès à leurs ressources. Certaines ont même recours à des mots de passe partagés, voire les mots de passe par défaut des équipements. Les entreprises doivent mettre en oeuvre une authentification forte, multifacteur, pour s'assurer que les utilisateurs sont bien ceux qu'ils prétendent être et définir leurs accès selon le principe de moindre privilège.

Segmenter le réseau. De nombreux environnements OT ont été conçus principalement pour les accès et non pour la sécurité. Ils sont donc « plats » et permettent potentiellement la propagation rapide d'une infection par ransomware. La mise en oeuvre d'une segmentation du réseau limiterait la portée et l'impact d'une attaque par ransomware.

Organiser des sessions de travail. Une session de travail de groupe peut aider les différentes parties prenantes à cerner le degré de préparation, aux niveaux organisationnel et technique, face à un événement de cette nature. Les capacités de sauvegarde et de restauration sont-elles effectives ? Les membres du conseil sont-ils prêts à agir ? L'entreprise a-t-elle souscrit une cyberassurance pour éviter de devoir verser elle-même une éventuelle rançon ?

Si l'on porte ces considérations à l'échelle des Etats-Unis, l'amélioration des infrastructures critiques de la nation va nécessiter des partenariats public/privé pour combler les lacunes actuelles, et atténuer le risque potentiel qu'encourent la sécurité nationale ainsi que la chaîne d'approvisionnement du pays. Ainsi, l'administration Biden a récemment annoncé un plan à boucler en 100 jours afin d'optimiser la cybersécurité du réseau national de distribution d'électricité. Étant donné que dans ce secteur de nombreux opérateurs d'infrastructures critiques sont des entreprises privées, des initiatives conjointes comme celle-ci sont impératives pour assurer la sécurité et la fiabilité des systèmes qui nous sont essentiels.