Process Safety Beacon
Messages au personnel de l'Exploitation
www.aiche.org/ccps/process-safety-beacon

An AIChE Technology Alliance
CCPS Center for Chemical Process Safety
aiche.org/ccps

Ce bulletin est commandité par
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

Cybersécurité et opérations chimiques

Juillet 2021

Figure 1. Usine de traitement de l'eau d'Oldsmar en Floride

Le 5 février 2021, un employé de l'usine de traitement de l'eau à Oldsmar, en Floride, a remarqué que le curseur sur l'écran de l'ordinateur de contrôle se déplaçait étrangement. Initialement, il n'y avait aucun souci; l'usine a utilisé un logiciel d'accès à distance pour permettre au personnel de partager des écrans et de résoudre les problèmes informatiques. Le superviseur se connectait souvent à l'ordinateur de l'opérateur pour surveiller également les systèmes de l'entreprise. Quelques heures plus tard, l'opérateur a remarqué que le curseur se déplaçait et cliquait à travers les commandes de l'usine de traitement de l'eau. En quelques secondes, l'intrus tentait de changer le point de consigne de l'hydroxyde de sodium du système de 100 parties par million (ppm) à 11,100 ppm. L'opérateur a rapidement repéré l'intrusion et a ramené l'hydroxyde de sodium à des niveaux normaux. Heureusement, il n'y a pas eu d'impact sur la qualité de l'eau.

Une récente attaque de type rançongiciel sur le *Colonial Pipeline* a arrêté l'approvisionnement en essence sur la côte Est des États-Unis pendant plusieurs jours.

Les systèmes de votre entreprise sont probablement connectés à Internet et ont besoin d'une protection contre les cybermenaces. Il existe de nombreuses stratégies utilisées par les entreprises pour dissuader les cybermenaces telles que: pare-feux, logiciels antivirus et politiques de protection contre les logiciels malveillants et les virus informatiques .

De plus en plus de gens travaillent à distance et de ce fait, cela a augmenté les possibilités de cyberattaques.

Le saviez-vous ?

- Les cybercriminels utilisent des logiciels malveillants sophistiqués pour tirer parti de multiples vulnérabilités et atteindre leurs objectifs.
- Les attaques de type rançongiciel augmentent de la part d'organisations criminelles les utilisant comme outil pour gagner de l'argent.
- Selon une étude récente, une cyberattaque se produit toutes les 39 secondes.
  (Réf.: https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- L'hameçonnage consiste à envoyer des courriels, soi-disant d'entreprises réputées, pour inciter les individus à révéler des informations personnelles. Ces attaques sont une méthode d'entrée principale pour les logiciels malveillants.
- Les cybermenaces peuvent pénétrer dans les systèmes des entreprises par le biais de courriels, de pièces jointes et de périphériques de stockage portables, tels que des clés USB ou d'autres périphériques de stockage portables.
- Quatre-vingt-quinze pour cent des intrusions envers la cybersécurité sont causées par une erreur humaine.
  (Réf.: https://www.cybintsolutions.com/employee-education-reduces-risk/)

Que pouvez-vous faire ?

- Vérifiez toujours les demandes de mises à jour logicielles auprès du service informatique avant d'y procéder et installez les mises à jour approuvées en temps opportun.
- Assurez-vous que vos pare-feux et autres logiciels réseau sont à jour et activés.
- Assurez-vous de sauvegarder régulièrement vos systèmes et vos données.
- Utilisez des mots de passe forts pour tous les accès. Ne partagez pas de mots de passe ou de comptes et changez régulièrement les mots de passe.
- N'enregistrez pas les mots de passe sur les navigateurs.
- Ne cliquez pas sur des liens ou des pièces jointes dans les courriels envoyés par quelqu'un que vous ne connaissez pas.
- N'installez jamais un logiciel non approuvé sur un ordinateur de l'entreprise; assurez-vous que les clés d'accès et les autres dispositifs de sécurité physique sont correctement sécurisés.
- Si vous utilisez l'accès à distance, suivez les exigences de l'entreprise. Soyez particulièrement vigilant si vous utilisez des sites Internet publics.
- Si quelque chose sur votre ordinateur semble étrange ou différent, demandez de l'aide! Il pourrait s'agir d'un pirate informatique essayant d'y accéder.

Les cyberattaques sont réelles. Vous êtes un élément essentiel de défense.