Process Safety Beacon
Messages for Manufacturing Personnel
www.aiche.org/ccps/process-safety-beacon

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

N° sponsorisé par
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

Cybersécurité et industries de procédé

Juillet 2021

Figure 1. Station d'épuration d'Oldmar, Floride

Le 5 février 2021, un employé de la station de traitement des eaux d'Oldsmar, en Floride, a remarqué que le curseur se déplaçait bizarrement sur son écran d'ordinateur. Au départ, il n'y avait pas lieu de s'inquiéter ; la station utilisait un logiciel d'accès à distance pour permettre au personnel de partager les écrans et de résoudre les problèmes informatiques. Le superviseur se connectait souvent à son ordinateur pour surveiller également les systèmes de l'établissement. Quelques heures plus tard, l'opérateur a remarqué que le curseur se déplaçait et cliquait dans les commandes de la station d'épuration. En quelques secondes, l'intrus a tenté de modifier 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 un niveau normal. Heureusement, il n'y a eu aucun impact sur la qualité de l'eau.

Une récente attaque par *rançongiciel* contre le Colonial Pipeline a interrompu l'approvisionnement en essence de la côte Est des États-Unis pendant plusieurs jours. Les systèmes de votre entreprise sont probablement connectés à l'Internet et doivent être protégés contre les cybermenaces. Il existe de nombreuses stratégies utilisées par les entreprises pour prévenir ces cybermenaces, telles que les pare-feu, les logiciels antivirus et les politiques de protection contre les logiciels malveillants et les virus informatiques. De plus en plus de personnes travaillent à distance, ce qui augmente les possibilités de cyberattaques.

Le saviez-vous ?

- Les cybercriminels utilisent des logiciels malveillants sophistiqués pour tirer avantage des multiples vulnérabilités et atteindre leurs objectifs.
- Les attaques de *rançongiciels* se multiplient, les criminels organisés s'en servant comme d'un outil pour gagner de l'argent.
- Selon une étude récente, une cyberattaque se produit toutes les 39 secondes. (Voir : https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- L'hameçonnage (*phishing*) consiste à envoyer des courriels, provenant soi-disant d'entreprises réputées, pour inciter des personnes à révéler des informations personnelles. Ces attaques constituent une des principales méthodes d'entrée des logiciels malveillants.
- Les cybermenaces peuvent s'introduire dans les systèmes de l'entreprise par le biais de courriels, de pièces jointes et de dispositifs de stockage portables, tels que des clés USB.
- 95% des failles de sécurité sont dues à une erreur humaine. (Voir : https://www.cybintsolutions.com/employee-education-reduces-risk/)

Que pouvez vous faire?

- Vérifiez toujours les demandes de mise à jour de logiciels auprès du service informatique avant d'y donner suite, et installez les mises à jour approuvées en temps voulu.
- Assurez-vous que vos pare-feu et autres logiciels réseau sont à jour et activés.
- Veillez à sauvegarder régulièrement vos systèmes et vos données.
- Utilisez des mots de passe forts pour tous les accès. Ne partagez pas les mots de passe ou les comptes et changez les mots de passe régulièrement.
- N'enregistrez pas les mots de passe sur les navigateurs.
- Ne cliquez pas sur les liens ou les pièces jointes des e-mails envoyés par une personne que vous ne connaissez pas.
- N'installez jamais de logiciels non approuvés sur un ordinateur de l'entreprise ; assurez-vous que les clés d'accès et autres dispositifs de sécurité physique sont correctement sécurisés.
- Si vous utilisez un 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 vous semble bizarre ou différent, demandez de l'aide ! Il pourrait s'agir d'un pirate informatique qui essaie d'y accéder.

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