Process Safety Beacon
Missatges per al personal de producció
www.aiche.org/ccps/process-safety-beacon

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

Exemplar patrocinat per
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

Ciberseguretat i operacions químiques

Juliol 2021

Fig. 1. Planta de tractament d'aigua a Oldsmar, Florida

El 5 de febrer de 2021, un empleat de la planta de tractament d'aigua d'Oldsmar, Florida, va notar que el cursor es movia de manera estranya per la pantalla de l'ordinador de control; inicialment no es va amoïnar; la planta utilitzava programari d'accés remot per permetre al personal compartir pantalles i resoldre problemes. El supervisor sovint es connectava a l'ordinador de l'operador per controlar la instal·lació. Unes hores més tard, l'operador va notar que el cursor es movia i operava els controls de la depuradora. L'intrús intentava canviar el valor de consigna d'hidròxid de sodi del sistema de 100 ppm a 11.100 ppm. L'operador va detectar ràpidament la intrusió i va tornar l'hidròxid de sodi a nivells normals. Afortunadament, no hi va haver cap impacte en la qualitat de l'aigua.

Un recent atac de ransomware a Colonial Pipeline va aturar el subministrament de gasolina a la costa est dels EUA durant diversos dies.

Els sistemes de la vostra empresa probablement estan connectats a Internet i necessiten protecció contra les ciberamenaces. Hi ha moltes estratègies que utilitzen les empreses per aturar les ciberamenaces com: talla-focs, antivirus i polítiques per protegir-se contra el malware i els virus informàtics.

Amb més gent treballant a distància han augmentat les oportunitats d'atacs cibernètics.

Sabíeu que?

- Els ciberdelinqüents utilitzen programari maliciós sofisticat per aprofitar múltiples vulnerabilitats i assolir els seus objectius.
- Els atacs de ransomware estan augmentant amb delinqüents organitzats que l'utilitzen com a eina per guanyar diners.
- Segons un estudi recent, es produeix un ciberatac cada 39 segons (ref. https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds).
- El phishing és l'enviament de correus electrònics, suposadament d'empreses de bona reputació, per induir les persones a revelar informació personal. Aquests atacs són un mètode principal d'entrada de programari maliciós.
- Les ciberamenaces poden entrar als sistemes de l'empresa mitjançant correus electrònics, fitxers adjunts i des de dispositius d'emmagatzematge portàtils.
- El noranta-cinc per cent de les fallades de seguretat cibernètica són causades per errors humans. (Ref. https://www.cybintsolutions.com/employee-education-reduces-risk/)

I jo, què hi puc fer?

- Verifiqueu sempre les sol·licituds d'actualització de programari amb informàtica abans de continuar i instal·leu actualitzacions aprovades de manera oportuna.
- Assegureu-vos que els tallafocs i altres programes de xarxa estiguin actualitzats i estiguin activats.
- Feu còpies de seguretat de sistemes i dades amb regularitat.
- Utilitzeu sempre contrasenyes segures, i canvieu-les amb regularitat. No compartiu contrasenyes ni comptes.
- No deseu les contrasenyes als navegadors.
- No cliqueu als enllaços ni als fitxers adjunts dels correus electrònics enviats per algú que no coneixeu.
- Mai instal·leu programari no aprovat en cap equip de la companyia; assegureu-vos que les claus d'accés i altres dispositius de seguretat físics estiguin correctament protegits.
- Si utilitzeu accés remot, seguiu els requisits de la companyia; especialment si utilitzeu llocs d'internet públics.
- Si quelcom del vostre equip sembla estrany o diferent, demaneu ajuda. Pot ser un pirata informàtic que intenti accedir-hi.

Els ciberatacs són de debò. Tu ets una part vital de la defensa.