Process Safety Beacon
Mensajes para el personal de Operaciones y Mantenimiento
www.aiche.org/ccps/process-safety-beacon

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

Ejemplar auspiciado por
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

Ciberseguridad y procesos químicos

Julio 2021

Fig.1. Oldmar, Florida – planta de tratamiento de agua

El 5 de febrero de 2021, un empleado de la planta de tratamiento de agua en Oldsmar, Florida, notó que el cursor se movía de manera extraña en la pantalla del PLC. Al principio no se preocupó, ya que en la planta se usaba un software de acceso remoto para permitir al personal compartir pantalla y solucionar problemas de TIC. El supervisor a menudo se conectaba al PLC para chequear también los sistemas de la instalación. Unas horas más tarde, el operador notó que el cursor se movía y hacía clic en los controles de la planta de tratamiento de agua. En segundos, el intruso estaba intentando cambiar el setpoint de hidróxido de sodio del sistema de 100 ppm a 11,100 ppm. El operador lo detectó rápidamente y devolvió al hidróxido de sodio a niveles normales. Afortunadamente, no hubo impacto en la calidad del agua.

Un reciente ataque de ransomware en Colonial Pipeline cortó varios días el suministro de gasolina en la costa este de los EE. UU.

Los sistemas de su empresa probablemente están conectados a Internet y necesitan protección contra ciberataques. Existen muchas estrategias para evitar estos ciberataques, tales como: firewalls, software antivirus y políticas para protegerse contra malware y virus informáticos.

El aumento de personas que trabajan de forma remota ha aumentado las oportunidades de ciberataques.

¿Sabía Ud?

- Los ciberdelincuentes utilizan malware sofisticado para aprovechar múltiples vulnerabilidades y lograr sus objetivos.
- Los ataques de ransomware están aumentando y los delincuentes organizados lo utilizan como herramienta para hacer dinero.
- Según un estudio reciente, se produce un ciberataque cada 39 segundos. (Ref. Https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- El phishing consiste en enviar correos electrónicos, supuestamente de empresas de renombre, para inducir a las personas a revelar información personal. Estos ataques son el método principal de entrada del malware.
- Los ciberataques pueden entrar en los sistemas de la empresa a través de correos electrónicos, archivos adjuntos y desde dispositivos de almacenamiento portátiles, como memorias USB u otros dispositivos de almacenamiento portátiles.
- El noventa y cinco por ciento de las infracciones de seguridad cibernética son causadas por errores humanos. (Ref. Https://www.cybintsolutions.com/employee-education-reduces-risk/)

¿Qué puede hacer Ud?

- Verifique siempre las solicitudes de actualización de software con TIC antes de continuar e instale las actualizaciones oportunamente aprobadas.
- Asegúrese de que sus firewalls y otro software de red estén actualizados y operativos.
- Realice regularmente copias de seguridad de sus sistemas y datos.
- Utilice contraseñas seguras para todos los accesos. No comparta contraseñas o cuentas y cambie las contraseñas con regularidad.
- No guarde las contraseñas en los navegadores.
- No haga clic en enlaces o archivos adjuntos en correos electrónicos enviados por alguien que no conoce.
- Nunca instale, en un ordenador de la empresa, software no aprobado; asegúrese que las claves de acceso y otros dispositivos de seguridad física estén debidamente protegidos.
- Si usa acceso remoto, siga los requisitos de la empresa. Esté especialmente atento si utiliza sitios públicos de Internet.
- Si algo en su ordenador le parece extraño o diferente, ¡pida ayuda! Podría ser un hacker intentando acceder.

Los ciberataques son reales. Tú eres una parte vital para prevenirlos.