Process Safety Beacon
Mensagens para Pessoal Operacional
www.aiche.org/ccps/process-safety-beacon

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

Esta edição é patrocinada por
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

# Cibersegurança e Operações Químicas

Julho de 2021

*Figura 1. Estação de tratamento de água em Oldsmar, Flórida*

Em 5 de Fevereiro de 2001, um funcionário de uma estação de tratamento de água em Oldsmar, Flórida, observou que o cursor estava se movendo de uma forma estranha na tela do computador. Inicialmente, ele não se preocupou, pois a instalação utilizava *software* de acesso remoto para permitir aos técnicos compartilharem telas e resolução de problemas de TI. O supervisor também se conectava frequentemente ao computador do operador para monitorar os sistemas da instalação. Algumas horas mais tarde, o operador observou que o cursor se mexia e clicava nos controles da estação de tratamento de água. Em segundos, o intruso estava tentando alterar o *setpoint* do sistema de regulação do hidróxido de sódio de 100 partes por milhão (ppm) para 11.100 ppm. O operador rapidamente percebeu a intrusão e retornou o hidróxido de sódio a níveis normais. Felizmente, não houve impacto na qualidade da água.

Um ataque recente de *ransomware* ao Colonial Pipeline interrompeu o fornecimento de gasolina à Costa Leste dos EUA por vários dias.

Os sistemas da sua empresa provavelmente estão conectados à *internet* e necessitam de proteção às ciberameaças. Há muitas estratégias usadas pelas empresas para deter as ciberameaças, tais como: *firewalls*, *software* antivírus e políticas para proteger contra *malwares* e vírus.

Muitas pessoas estão trabalhando remotamente; este fato aumentou as oportunidades para ciberataques.

## Você sabia?

- Os cibercriminosos usam *malwares* sofisticados para tirar vantagem de múltiplas vulnerabilidades e atingir seus objetivos.
- Os ataques de *ransomware* estão aumentando com organizações criminosas usando-os como forma de obtenção de dinheiro.
- De acordo com um estudo recente, um ciberataque ocorre a cada 39 seg. (Ref.: https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds )
- O *phishing* é o envio de *emails*, supostamente de empresas críveis, para induzir as pessoas a revelar informações pessoais. Esses ataques são um método primário de introdução de *malwares*.
- As ciberameaças podem entrar nos sistemas das empresas atarvés de *emails*, anexos e a partir de unidades de armazenamento portáteis, tais como *pendrives* ou outros dispositivos de armazenamento portáteis.
- Noventa e cinco por cento das quebras de cibersegurança são causadas por erro humano. (Ref.: https://www.cybintsolutions.com/employee-education-reduces-risk/ )

## O que você pode fazer?

- Sempre verifique os pedidos de atualização de *software* com o seu departamento de TI antes de prosseguir e instale as atualizações aprovadas regularmente.
- Assegure-se de que seus *firewalls* e outro *software* de rede estejam atualizados e ativos.
- Assegure-se de efetuar periodicamente *backups* do sistema e dos dados.
- Use senhas fortes para todos os acessos. Não compartilhe senhas ou contas e altere as senhas regularmente.
- Não guarde as senhas nos *browsers*.
- Não clique em *links* ou anexos de *emails* de desconhecidos.
- Nunca instale *software* não aprovado em nenhum computador; assegure-se de que as chaves de acesso e outros dispositivos físicos de segurança estejam devidamente guardados.
- Se usar um acesso remoto, siga os requisitos da sua empresa. Seja especialmente vigilante se usar *sites* públicos de acesso à *internet*.
- Se algo no seu computador paracer estranho ou diferente, peça ajuda! Pode ser um *hacker* tentando obter acesso.

**Ciberataques são reais. Você é uma parte vital da defesa.**