Process Safety Beacon
Menssagens para o Pessoal de Operação
www.aiche.org/ccps/process-safety-beacon

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

Este número é patrocinado 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

A 5 de Fevereiro de 2021, um funcionário de uma estação de tratamento de água em Oldsmar, Flórida, verificou que o cursor se estava a mover de uma forma estranha no écran no computador de controlo do processo. Inicialmente, não se preocupou, pois a instalação usava software de acesso remoto para permitir aos técnicos partilharem écrans e resolução de problemas de TI. O seu supervisor também se ligava frequentemente ao computador do operador para monitorar os sistemas da instalação. Algumas horas mais tarde, o operador verificou que o cursor se mexia e clicava nos controlos da estação de tratamento de água. Em segundos, o intruso estava a tentar alterar o setpoint do sistema de regulação do hidróxido de sódio de 100 partes por milhão (ppm) para 11,100 ppm. O operador apercebeu-se rapidamente da intrusão e repôs o hidróxido de sódio em níveis normais. Felizmente, não existiu impacto na qualidade da água.

Um ataque recente de ransomware ao Colonial Pipeline interrompeu o fornecimento de gasolina à Costa Este dos EUA durante vários dias.

Os sistemas da sua empresa estão provavelmente ligados à internet e necessitam de proteção às ciberameaças. Existem muitas estratégias usadas pelas empresas para parar as ciberameaças tais como: firewalls, software anti-virus e políticas para proteger contra malware e vírus informáticos.

Muitas pessoas estão a trabalhar remotamente; este facto aumentou as oportunidades para ciberataques.

Você sabia?

- Os cibercriminosos usam malware sofisticado para tirar vantagem de múltiplas vulnerabilidades e atingir os seus objetivos.
- Os ataques de ransomware estão a aumentar com organizações criminosas a usá-los como forma de obtenção de dinheiro.
- De acordo com um estudo recente ocorre um ciberataque a cada 39 segundos. (Ref. https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- O phishing é o envio de emails, supostamente de empresas credíveis, para induzir os indíviduos a revelar informação pessoal. Estes ataques são um método primário de introdução de malware.
- As ciberameaças podem entrar nos sistemas das empresas através de emails, anexos e a partir de unidades de armazenamento portáteis, tais como pens 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 pode fazer?

- Verifique sempre os pedidos de atualização de software com o seu departamento de TI antes de prosseguir e instale as atualizações aprovadas atempadamente.
- Assegure-se que os seus firewalls e outro software de rede estão atualizados e activos.
- Assegure-se de que efetua periodicamente backups do sistema e dos dados.
- Use passwords fortes para todos os acessos. Não partilhe passwords ou contas e altere as passwords regularmente.
- Não guarde as passwords nos browsers.
- Não clique em links ou anexos de emails de desconhecidos
- Nunca instale software não aprovado em nenhum computador da empresa, assegure-se que as chaves de acesso e outros dispositivos físicos de segurança estão devidamente guardados.
- Se usar um acesso remoto, siga os requisitos da sua empresa. Seja especialmente vigilante se usar pontos públicos de acesso à internet.
- Se algo no seu computador parecer estranho ou diferente, peça ajuda! Pode ser um hacker a tentar aceder..

Os ciberataques são reais. Você é uma parte vital da defesa.