Process Safety Beacon

Messages for Manufacturing Personnel

http://www.aiche.org/CCPS/Publications/Beacon/index.aspx

CCPS An AIChE Technology Alliance — Center for Chemical Process Safety

This Issue Sponsored by ioMosaic® Minimizing risk. Maximizing potential.® www.iomosaic.com

Cybersecurity and Plant Operations

July 2021

▲ Cyberattacks pose a major risk to facilities in the chemical process industries (CPI).

On Feb. 5, 2021, a water treatment plant employee in Oldsmar, FL, noticed that the cursor on the control computer screen was moving strangely. The employee was initially not concerned, because the plant used remote-access software to allow staff to share screens and troubleshoot information technology (IT) issues. The supervisor often connected to the operator's computer to monitor the facility's systems.

A few hours later, the operator noticed the cursor moving and clicking through the water treatment plant's controls. It became evident that an intruder was attempting to change the system's sodium hydroxide setpoint from 100 ppm to 11,100 ppm. The operator quickly noticed the intrusion and returned the sodium hydroxide setpoint to normal levels. The quick action prevented any impact on the water quality.

In another recent cyberattack, hackers targeted the Colonial Pipeline Co., disrupting the supply of gasoline to the U.S. East Coast for several days. The hackers were able to access the company systems through a dated virtual private network (VPN) that did not have multifactor authentication.

Today, most company systems are connected to the internet, necessitating protection from cyberthreats. Companies can use many strategies to deter cyberattacks, including firewalls, antivirus software, and policies that protect against malware and computer viruses.

Did You Know?

- Cybercriminals use sophisticated malware (*i.e.,* malicious software) to take advantage of system vulnerabilities.
- Cybercriminals are increasingly using ransomware attacks, in which they hack a system and block access to it unless a ransom is paid.
- More employees are working remotely, increasing opportunities for cybercriminals. According to a 2017 study, a cyberattack occurs every 39 sec. The frequency of cyberattacks is expected to increase to every 11 sec in 2021 (www.embroker.com/blog/cyber-attack-statistics).
- Phishing is when an attacker sends emails, supposedly from reputable sources, to dupe individuals into revealing personal information. These attacks are a primary entry method for malware.
- Cyberthreats can enter company systems through emails, links, attachments, and portable storage devices (*e.g.,* flash drives).
- 90% of cybersecurity breaches are caused by human error (www.cybintsolutions.com/employee-education-reduces-risk).

What Can You Do?

- Verify automated requests to update software with your IT department before completing any requests. Only install approved updates, and do so in a timely manner.
- Ensure firewalls and other network security software are up to date and turned on.
- Make sure to regularly back up your systems and data.
- Use strong passwords and change them often. Do not share passwords or accounts.
- Do not save passwords on browsers.
- Do not click on links or attachments in emails sent from an unknown address.
- Never install unapproved software on any company computer. Ensure access keys and other physical security devices are properly secured.
- If you use remote access software, follow company requirements. Be especially vigilant when using public internet sites.
- If something on your computer seems odd or different, ask for help. It could be a hacker trying to gain access.

Cyberattacks are real, and you are a vital part of the defense.