Process Safety Beacon
Hinweise für das Betriebspersonal
www.aiche.org/ccps/process-safety-beacon

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

This issue sponsored by
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

Cybersicherheit und der Betrieb chemischer Anlagen Juli 2021

Abbildung 1: Wasseraufbereitungsanlage in Oldsmar, Florida, USA

Am 05.02.2021 bemerkte das Bedienpersonal einer Wasseraufbereitungsanlage in Oldsmar, Florida, USA, wie sich der Cursor auf dem Computerbildschirm der Anlagensteuerung ohne Eingriff bewegte. Dies war zunächst nicht beunruhigend, da die Steuerung der Anlage einen Zugriff von außen erlaubt (Fernzugriff), damit sowohl die Überwachung der Anlage durch das Betriebspersonal als auch Reparaturen/Wartungen an der Steuerung durch die IT-Abteilung möglich sind. Einige Stunden später bemerkte das Bedienpersonal, wie sich der Cursor durch die Bedienebenen der Steuerung der Wasseraufbereitungsanlage bewegte und Aktionen ausführte. Innerhalb von Sekunden versuchte ein Eindringling, den Sollwert der Natronlauge-Zugabe von 100 ppm auf 11.100 ppm anzuheben. Das Bedienpersonal bemerkte die Aktion des Eindringlings schnell und korrigierte die Natronlauge-Zugabe. Glücklicherweise hatte dieser unerlaubte Fernzugriff keine Auswirkungen auf die Wasserqualität.

Ebenfalls legte erst kürzlich ein Cyberangriff mit Erpressungssoftware (Ransomware) die Colonial Pipeline und somit die Benzinversorgung der US-Ostküste für mehrere Tage lahm.

Die IT/OT-Systeme der Unternehmen sind direkt/indirekt mit dem Internet verbunden und müssen vor Cyberbedrohungen geschützt werden. Es gibt in den Unternehmen viele Strategien, um Cyberbedrohungen abzuwehren, beispielweise Firewalls, Antiviren-Software und Richtlinien zum Schutz vor Malware und Computerviren.

Bei dem Thema Cybersicherheit kommt mittlerweile erschwerend hinzu, dass immer mehr Menschen aus der Ferne arbeiten (beispielsweise Home-Office); diese Arbeitsweise hat die Möglichkeiten für Cyberangriffe erhöht.

Wussten Sie schon?

- Cyber-Kriminelle nutzen ausgeklügelte Schadsoftware (Malware), um Schwachstellen in IT/OT-Systemen zu finden und für die Erreichung Ihrer Ziele auszunutzen.
- Angriffe mit Ransomware nehmen zu, da die organisierte Kriminalität sie als Werkzeug zum Geldverdienen verwenden.
- Laut einer aktuellen Studie kommt es durchschnittlich alle 39 Sekunden zu einem Cyberangriff (Quelle: Hackers Attack Every 39 Seconds | 2017-02-10 | Security Magazine).
- Phishing, also das Versenden von E-Mails von vermeintlich seriösen Absendern, um den Empfänger zur Preisgabe von persönlichen Informationen zu bringen, ist aktuell die bevorzugte Eintrittsmethode für Malware in IT/OT-Systeme.
- Cyber-Angriffe können über Internetseiten, E-Mails, Anhänge und/oder mobile Speichermedien (USB-Sticks, SD-Karten, SSDs, …) in die Systeme der Unternehmen erfolgen.
- 95 Prozent der Cyber-Sicherheitsverletzungen werden durch menschliches Verhalten ermöglicht. (Quelle: Why Educating Your Employees on Cyber Intelligence And Security Will Reduce Risk - 2018-06-15 - www.cybintsolutions.com)

Was können Sie machen?

- Wenn Sie zu Software-Updates aufgefordert werden, überprüfen Sie diese stehts mit Hilfe Ihrer IT-Abteilung. Installieren Sie genehmigte Updates rechtzeitig.
- Stellen Sie sicher, dass Firewalls und andere Netzwerksoftware auf dem neuesten Stand und aktiviert sind.
- Stellen Sie sicher, dass Sie regelmäßig Sicherungen (Backups) von Ihren Systemen und Ihren Daten anfertigen.
- Verwenden Sie grundsätzlich starke und unterschiedliche Passwörter und ändern diese regelmäßig. Geben Sie keine Passwörter oder Konten frei. Speichern Sie keine Passwörter in Browsern.
- Öffnen Sie keine Anhänge oder oder Klicken auf Links in E-Mails, die von Personen/Unternehmen/Institutionen geschickt wurden, die Sie nicht kennen.
- Installieren Sie niemals nicht genehmigte Software auf einen Firmencomputer. Stellen Sie sicher, dass Zugriffsschlüssel und andere physische Sicherheitsvorrichtungen ordnungsgemäß gesichert sind.
- Wenn Sie sich von außerhalb in das firmeninterne Netzwerk einwählen, folgen Sie den Vorgaben des Unternehmens. Seien Sie besonders aufmerksam, wenn Sie öffentliche Internetseiten aufrufen/besuchen.
- Wenn Ihnen etwas auf Ihrem Computer seltsam oder anders erscheint, melden Sie es unverzüglich der IT-Abteilung. Es könnten Hacker sein, die gerade versuchen, sich Zugang zu verschaffen.
- Weitere Informationen finden Sie bei dem Bundesministerium des Inneren, für Bau und Heimat unter: BMI - IT- und Cybersicherheit

Cyberangriffe sind Realität. Wir können mit unserem Verhalten den Erfolg dieser Angriffe beeinflussen!