Process Safety Beacon
Messages for Manufacturing Personnel
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

Cybersäkerhet och kemiverksamhet

juli 2021

Bild 1. vattenreningsanläggning i Oldmar, Florida

Den 5 februari 2021 upptäckte en operatör vid vattenreningsverket i Oldsmar, Florida att markören på kontrolldataskärmen rörde sig på ett konstigt sätt. Initialt orsakade det ingen oro; anläggningen använde mjukvara som gör det möjligt för personalen att dela skärmar och felsöka när IT-problem uppstår. Även arbetsledaren kopplar ofta upp sig på operatörens dator för övervaka anläggningens system. Några timmar senare upptäcker operatören att markören rör sig och klickar runt på vattenreningsanläggningens funktioner. Inom några sekunder försöker inkräktaren att ändra systemets inställning för natriumhydroxid från 100 ppm till 11.100 ppm. Operatören reagerade direkt på intrånget och återställde tillsättningen av natriumhydroxid till normala nivåer. Som tur var påverkades inte vattenkvaliteten av händelsen.

Nyligen inträffade en utpressningsattack mot Colonial Pipeline, som stoppade bensinleveranserna till USA:s östkust under flera dagar.

Ert företagets datasystem är förmodligen uppkopplat till internet och behöver skydd från cyberhot. Det finns många sätt för företagen att upptäcka cyberhot, som t.ex brandväggar, antivirusprogram och riktlinjer för att skydda mot skadlig programvara och datavirus.

Fler och fler arbetar på distans; detta har ökat möjligheterna till cyberattacker.

Visste du?

- Cyberbrottslingar använder sofistikerad programvara för att dra fördel av många svagheter i systemen för att uppnå sina mål.
- Virusattacker ökar med organiserad brottslighet, som använder den som ett sätt att tjäna pengar.
- Enligt en nyligen gjord studie inträffar en cyberattack var 39 sekund. (Ref. https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- "Phishing" sker genom att epost skickas förment från trovärdiga företaget, för att förmå individer att avslöja personlig information. Dessa attacker är primärt en metod för att introducera ett virus.
- Cyberattacker kan komma in i företagets system genom epost, bilagor och från portabla lagringsenheter, som t.ex USB-minnen eller andra portabla lagringsenheter.
- 95% av brotten mot cybersäkerhet orsakas av mänsklig faktor. (Ref. https://www.cybintsolutions.com/employee-education-reduces-risk/)

Vad kan du göra?

- Verifiera alltid uppmaningar till mjukvaruuppdateringar med IT-avdelningen innan du går vidare och installera alltid godkända uppdateringar i rätt tid.
- Säkra era brandväggar och andra mjukvaror inom ert nätverk så att de är uppdaterade och aktiva.
- Se till att regelbundet göra backup av era system och data.
- Använd starka lösenord för all åtkomst. Dela inte lösenord eller konton och ändra lösenorden regelbundet.
- Spara inte lösenorden i webbläsarna.
- Klicka inte på länkar eller bilagor i epost, som kommer från någon du inte känner.
- Installera aldrig icke godkänd mjukvara på någon av företagets datorer; säkerställ att åtkomstnycklar och andra fysiska säkerhetsenheter är ordentligt säkrade.
- Om du arbetar på distans, följ företagets riktlinjer. Var speciellt försiktigt om du använder allmänna internetsiter.
- Om något på din dator verkar konstigt eller annorlunda, sök hjälp! Det kan vara en hacker som försöker få åtkomst till din dator.

Cyberattacker finns på riktigt. Du är en viktig del av försvaret.