Process Safety Beacon
Sikkerhedsmeddelser for fabrikspersonale
www.aiche.org/ccps/process-safety-beacon

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

Denne udgave sponsored af
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

Cybersikkerhed og kemiske operationer

Juli 2021

Figur 1. Oldmar, Florida USA vandbehandlingsanlæg

Den 5 februar 2021 bemærkede en ansat ved vandbehandlingsanlægget i Oldmar, Florida i USA, at cursoren bevægede sig mærkeligt rundt på kontrolcomputerens skærm. Til at begynde med havde han ingen bekymring da anlægget brugte remote-access software for at ansatte kan dele skærme og troubleshoot IT problemer. Ledere var ofte inde på operatøren's computer for at følge med i anlægges status. Et par timer senere bemærkede operatøren, at cursoren bevægede sig rundt og clickede sig igennem vandbehandlingsanlæggets kontrolsystem. Et par sekunder senere prøvede den ubudne gæst at ændre på systemets natriumhydroxid setpoint fra 100 ppm til 11,100 ppm. Operatoren opdagede hurtigt angrebet og returnerede natriumhydroxid doseringen til det normale niveau. Heldigvis var der ingen skade set på vandets kvalitet.

Et ransomware angreb Colonial Pipeline forsagede en nedlukning af benzinforsyningen til USA østkyst for flere dage fornylig.

Dit firmas computersystemer er formodentlig forbundet til internettet og behøver beskyttelse imod cyberangreb. Der er mange strategier firmaer kan benytte sig af til at beskytte sig imod cyberangreb såsom: firewalls, anti-virus software og politiker for at beskytte imod malware og computer viruser.

Flere og flere arbejder hjemmefra nuomdage; det øger risikoen for cyberangreb.

Vidste du at ?

- Cyberkriminelle benytter avanceret malware for at drage fordel af svagheder i IT systemerne for at nå deres mål.
- Ransom-ware angreb bliver mere og mere brugt af organisere-de kriminelle som en måde til at afpresse penge af firmaer.
- I henhold til en undersøgelse for nylig sker der et cyberangreb hvert 39 sekund. (Ref. https://www.securitymagazine.com/articles
- /87787-hackers-attack-every-39-seconds)
- Phishing er metoden med emails, tilsyneladende fra respekterede firmaer, for at få modtagerne til at give personlige oplysninger. Disse angreb er en ledende måde at få malware.
- Cyberangreb kan komme ind i et firmas IT systemer via e-mails, vedhæftede filer og fra bærbart udstyr, såsom thumb drives eller discs.
- 95 % af cybersikkerhedsbrud er forsaget af menneskelige fejl. (Ref. https://www.cybintsolutions.com/employee-education-reduces-risk/)

Hvad kan du gøre ?

- Check altid softwareopdateringer forespørgsler med jeres IT før du begynder, og installer godkendte opdateringer så snart det er praktisk.
- Vær sikker på dine firewalls og andet network software er det nyeste og er klar til brug.
- Backup dine computersystemer og data ofte.
- Brug stærke passwords for alle adgange. Lad være med at dele passwords eller accounts og ændre dine passwords ofte.
- Lad være med at gemme passwords på browsers.
- Lad være med at clicke på links eller vedhæftede filer i emails fra folks du ikke kender.
- Installer aldrig ikke-godkendt software på firmaets computere; vær sikker på, at adgangsnøgler og anden fysiske sikkerhedsudstyr er sikret forsvarligt.
- Hvis du bruger remote access, følg firmaets krav til sikre forbindelser. Vær specielt forsigtig med offentlige internet sites.
- Hvis noget på din computer virker mærkeligt eller anderledes, bed om hjælp !. Det kan være en hacker, som prøver at skaffe sig adgang.

Cyberangreb sker virkelig. Du er en vital del af forsvaret.