Process Safety Beacon
Berichten voor productiepersoneel
www.aiche.org/ccps/process-safety-beacon

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

Dit nummer is gesponsord door
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

Cyberbeveiliging in de chemische industrie

Juli 2021

Figuur 1. Oldsmar, Florida waterzuiveringsinstallatie

Op 5 februari 2021 merkte een medewerker van een waterzuiveringsinstallatie in Oldsmar, Florida, dat de cursor vreemd bewoog op het scherm van de besturingscomputer. In eerte instantie werd dit niet gezien als een probleem; de fabriek gebruikte software voor externe toegang om het personeel in staat te stellen schermen te delen en IT-problemen op te lossen. De supervisor maakte vaak verbinding met de computer van de operator om ook de systemen van de faciliteit te bewaken. Een paar uur later zag de operator de cursor bewegen en klikken door de bedieningselementen van de waterzuiveringsinstallatie. Binnen enkele seconden probeerde de indringer het natriumhydroxide-instelpunt van het systeem te veranderen van 100 delen per miljoen (ppm) naar 11.100 ppm. De telefoniste merkte de inbraak snel op en bracht het natriumhydroxide terug naar normale niveaus. Gelukkig waren er geen gevolgen op de waterkwaliteit.

Een recente ransomware-aanval op de ‘Colonial Pipeline’ heeft de levering van benzine aan de Amerikaanse oostkust enkele dagen stilgelegd.

De systemen van uw bedrijf zijn waarschijnlijk verbonden met internet en hebben bescherming nodig tegen cyberdreigingen. Er zijn veel strategieën die worden gebruikt om cyberdreigingen af te schrikken, zoals: firewalls, antivirussoftware en beleid ter bescherming tegen malware en computervirussen.

Meer mensen werken op afstand; hierdoor is de kans op cyberaanvallen toegenomen.

Bent u hiervan op de hoogte?

- Cybercriminelen gebruiken geavanceerde malware om te profiteren van meerdere kwetsbaarheden en om hun doelen te bereiken.
- Ransomware-aanvallen nemen toe en georganiseerde criminelen gebruiken het als een middel om geld te verdienen.
- Volgens een recente studie vindt er elke 39 sec een cyberaanval plaats. (Zie https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- Phishing is het verzenden van e-mails, zogenaamd van betrouwbare bedrijven, om persoonlijke informatie van individuen te verkrijgen. Deze aanvallen zijn een primaire toegangsmethode voor malware.
- Cyberdreigingen kunnen de systemen van het bedrijf binnendringen via e-mails, bijlagen en vanaf draagbare opslagapparaten, zoals USB-sticks.
- 95% van de cyberbeveiligingsinbreuken wordt veroorzaakt door menselijke fouten. (Zie https://www.cybintsolutions.com/employee-education-reduces-risk/)

Wat kunt u er aan doen?

- Verifieer altijd software-updateverzoeken met IT voordat u doorgaat, en installeer tijdig (goedgekeurde) updates.
- Zorg ervoor dat uw firewalls en andere netwerksoftware up-to-date en ingeschakeld zijn.
- Zorg ervoor dat u regelmatig een back-up maakt van uw systemen en gegevens.
- Gebruik sterke wachtwoorden voor alle toegang. Deel geen wachtwoorden of accounts en wijzig wachtwoorden regelmatig.
- Sla geen wachtwoorden op in browsers.
- Klik niet op links of bijlagen in e-mails die zijn verzonden door iemand die u niet kent.
- Installeer nooit niet-goedgekeurde software op een bedrijfscomputer; zorg ervoor dat toegangssleutels en andere fysieke beveiligingsapparaten goed zijn beveiligd.
- Als u externe toegang gebruikt, volg dan de vereisten van het bedrijf. Wees vooral waakzaam bij het gebruik van openbare internetsites.
- Als iets op uw computer vreemd of anders lijkt, vraag dan om hulp! Het kan een hacker zijn die toegang probeert te krijgen.

Cyberaanvallen gebeuren echt. Uw inbreng is onmisbaar in de bestrijding.