Process Safety Beacon
Mesaje pentru personalul din operaţiuni
www.aiche.org/ccps/process-safety-beacon

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

Publicaţie sponsorizată de:
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

# Securitatea cibernetică și operațiunile din industria chimică

Iulie 2021

*Figura 1. Oldmar, Florida instalaţie de tratare a apei*

În data de 5 Februarie 2021, un angajat al unei instalaţii de tratare a apei din Oldsmar, Florida, a observat pe ecranul calculatorului de control că, cursorul s-a deplasat în mod ciudat. Inițial, nu a existat nicio îngrijorare; în instalaţie se foloseau programe de acces de la distanță pentru a permite personalului să partajeze ecrane și să remedieze probleme IT. Supervizorul se conecta adesea la calculatorul operatorului pentru a monitoriza sistemele instalației. Câteva ore mai tarziu, operatorul a sesizat mişcarea cursorului şi accesarea unor controale ale instalaţiei de tratare. În câteva secunde, intrusul a încercat să modifice setarea sistemului de hidroxid de sodiu de la 100 părţi per million (ppm) la 11.100 ppm. Operatorul a sesizat rapid intervenţia şi a readus concentraţia hidroxidului de sodiu la nivele normale. Din fericire, nu s-a înregistrat niciun impact în ceea ce priveşte calitatea apei.

Un atac similar s-a produs recent asupra unei conducte interstatale de benzină şi a condus la oprirea aprovizionării cu benzină a Coastei de Est a SUA timp de câteva zile.

Sistemele companiei dvs. sunt probabil conectate la internet și au nevoie de protecție împotriva amenințărilor cibernetice. Există multe strategii utilizate de companii pentru a descuraja amenințările cibernetice, cum ar fi: programe de tip “firewall”, programe antivirus și politici de protecție împotriva programelor de access neautorizate și a virușilor informatici.

Mulți oameni lucrează de la distanță; acest lucru a sporit oportunitățile de atacuri cibernetice.

## Ce puteti face?

- Infractorii cibernetici folosesc programe sofisticate de acces neautorizat pentru a profita de vulnerabilități multiple și pentru a-și atinge obiectivele.
- Atacurile de tip “ransomware” (blocare conturi electronice până la platirea unei sume de bani) sunt în creștere, iar criminalii organizați îl folosesc ca instrument pentru a câștiga bani.
- Potrivit unui studiu recent, un atac cibernetic are loc la fiecare 39 de secunde. (Ref. Https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- Phishing-ul (trimitere de e-mail-luri frauduloase din surse de incredere) trimite e-mailuri, presupuse de la companii de renume, pentru a determina persoanele să dezvăluie informații personale. Aceste atacuri sunt o metodă principală de intrare pentru programele de access neautorizate.
- Amenințările cibernetice pot intra în sistemele companiei prin e-mailuri, atașamente și de pe dispozitive de stocare portabile, cum ar fi unități de stocare sau alte dispozitive de stocare portabile.
- Nouăzeci și cinci la sută din încălcările securității cibernetice sunt cauzate de erori umane. (Ref. Https://www.cybintsolutions.com/employee-education-reduces-risk/)

## Ce puteti face?

- Verificați întotdeauna solicitările de actualizare programe cu departamentul IT înainte de a continua și instalați actualizările aprobate în timp util.
- Asigurați-vă că firewall-urile și alte programe de rețea sunt actualizate și activate.
- Asigurați-vă că faceti în mod regulat o copie de rezervă a sistemelor și datelor.
- Folosiți parole puternice pentru acces. Nu partajați parole sau conturi și nu schimbați parolele în mod regulat.
- Nu salvați parolele în browsere.
- Nu faceți clic pe link-uri sau atașamente din e-mailuri trimise de o persoană pe care nu o cunoașteți.
- Nu instalați niciodată programe neaprobate pe niciun computer al companiei; asigurați-vă că cheile de acces și alte dispozitive de securitate fizică sunt securizate corespunzător.
- Dacă utilizați acces de la distanță, urmați cerințele companiei. Fiți deosebit de vigilenți dacă utilizați site-uri publice de internet.
- Dacă ceva de pe computerul dvs. pare ciudat sau diferit, cereți ajutor! Ar putea fi un hacker care încearcă să obțină acces.

**Atacurile cibernetice sunt reale. Sunteți o parte vitală a apărării împotriva acestora.**