Process Safety Beacon
Messaggi per il personale di produzione
www.aiche.org/ccps/process-safety-beacon

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

Questo articolo è sponsorizzato da
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

Sicurezza Informatica e attività Chimiche

Luglio 2021

Figure 1. Oldmar, Florida Impianto trattamento acque

Il 5 febbraio 2021, un dipendente dell'impianto di trattamento delle acque di Oldmar, in Florida, ha notato che il cursore si muoveva in modo strano sullo schermo del computer di controllo. Inizialmente, non c'era alcun problema; l'impianto utilizzava un software di accesso remoto per consentire al personale di condividere gli schermi e risolvere i problemi IT. Il supervisore si collegava spesso al computer dell'operatore anche per monitorare i sistemi dell'impianto. Poche ore dopo, l'operatore ha notato il cursore muoversi e cliccare sui comandi dell'impianto di trattamento delle acque. In pochi secondi, l'intruso stava tentando di cambiare il set point di dosaggio dell'idrossido di sodio da 100 parti per milione (ppm) a 11.100 ppm. L'operatore ha individuato rapidamente l'intrusione e ha riportato l'idrossido di sodio a livelli normali. Fortunatamente, non c'è stato alcun impatto sulla qualità dell'acqua.

Un recente attacco ransomware alla Colonial Pipeline ha interrotto la fornitura di benzina alla costa orientale degli Stati Uniti per diversi giorni.

I sistemi della tua azienda sono probabilmente connessi a Internet e necessitano di protezione dalle minacce informatiche. Molte sono le strategie utilizzate dalle aziende per scoraggiare le minacce informatiche come: firewall, software antivirus e policy per la protezione da malware e virus informatici.

Più persone stanno lavorando da remoto; questo ha aumentato le opportunità di attacchi informatici.

Lo sapevi?

- I criminali informatici utilizzano malware sofisticati per sfruttare molteplici vulnerabilità e raggiungere i loro obiettivi.
- Gli attacchi ransomware sono in aumento con i criminali organizzati che lo utilizzano come strumento per fare soldi.
- Secondo un recente studio, ogni 39 secondi si verifica un attacco informatico. (Rif. https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- Il phishing consiste nell'invio di e-mail, presumibilmente da aziende rispettabili, per indurre le persone a rivelare informazioni personali. Questi attacchi sono un metodo di ingresso principale per il malware.
- Le minacce informatiche possono entrare nei sistemi dell'azienda tramite e-mail, allegati e da dispositivi di archiviazione portatili, come chiavette USB o altri dispositivi di archiviazione portatili.
- Il novantacinque percento delle violazioni della sicurezza informatica è causato da errori umani. (Rif. https://www.cybintsolutions.com/employee-education-reduces-risk/)

Cosa puoi fare?

- Verificare sempre le richieste di aggiornamento del software con l'IT prima di procedere e installare gli aggiornamenti approvati in modo tempestivo.
- Assicurarti che i firewall e gli altri software di rete siano aggiornati e attivi.
- Assicurarti di eseguire regolarmente il backup dei tuoi sistemi e dei tuoi dati.
- Usare password complesse per tutti gli accessi. Non condividere password o account e modificare le password regolarmente.
- Non salvare le password sui browser.
- Non fare clic su collegamenti o allegati nelle e-mail inviate da qualcuno che non conosci.
- Non installare mai software non approvato su qualsiasi computer aziendale; assicurati che le chiavi di accesso e gli altri dispositivi di sicurezza fisica siano adeguatamente protetti.
- Se si utilizza l'accesso remoto, seguire i requisiti dell'azienda. Prestare particolare attenzione se si utilizzano siti Internet pubblici.
- Se qualcosa sul tuo computer sembra strano o diverso, chiedere aiuto! Potrebbe essere un hacker che cerca di ottenere l'accesso.

Gli attacchi informatici sono reali. Tu sei una parte vitale della difesa.