PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6187 di Mercoledì 04 novembre 2026

Cosa hanno in comune celle frigorifere e centrifughe per l'uranio?

Dai recenti attacchi ai sistemi di refrigerazione al caso Stuxnet: quando un comando remoto altera parametri critici, la sicurezza deve includere protezioni automatiche, locali e indipendenti dal software OT, con controlli separati.

Cosa hanno in comune le celle frigorifere dei supermercati e le centrifughe per l'arricchimento dell'uranio?

Può sembrare una domanda da 1 milione di dollari, ma in realtà l'esame di situazioni passate e recenti dimostra come tra queste due realtà vi siano numerosi punti di contatto.

I mezzi di comunicazione di massa hanno dato ampio risalto ai recenti attacchi condotti contro gli applicativi di gestione della temperatura delle celle frigorifere dei supermercati. Un primo attacco è stato effettuato a metà del mese di ottobre ed un secondo attacco all'inizio del mese di novembre. In entrambi i casi, i criminali informatici hanno alterato gli applicativi di controllo a distanza della temperatura delle celle frigorifere, facendo salire la temperatura fino a oltre 50° e obbligando quindi i titolari dei supermercati a gettare la merce avariata.

Penso che molti lettori ricorderanno cosa accadde qualche anno fa, quando gli israeliani riuscirono a inserire un applicativo fraudolento nel sistema di gestione delle dozzine di centrifughe, utilizzate per l'arricchimento dell'uranio. L'applicativo fraudolento prese sotto controllo il sistema centralizzato e inviò un comando di aumento del ritmo di rotazione delle centrifughe, superando i limiti meccanici delle stesse e portando alla distruzione di dozzine e dozzine di centrifughe, con evidenti riflessi sulle capacità di arricchimento dell'uranio, da parte degli iraniani.

In entrambi i casi, un comando proveniente dall'esterno altera i parametri di funzionamento del sistema attaccato, nel caso più recente aumentando la temperatura, nel caso meno recente aumentando la velocità di rotazione delle centrifughe.

Pubblicità

È evidente che il fatto che un attacco del genere possa essere stato perpetrato, dimostra che vi era una lacuna fondamentale nello sviluppo del software di gestione, sia delle celle frigorifere, sia delle centrifughe.

Davanti a situazioni estreme, deve essere inserito nell'applicativo un sistema automatico ed indipendente, che non può essere attaccato dall'esterno, in quanto residente presso il macchinario da proteggere.

Un esempio forse significativo riguarda il fatto che, ove nel nostro impianto elettrico domestico si abbia a superare il livello di corrente massimo ammesso, quale che sia il sistema di comando e controllo dell'impianto elettrico, l'interruttore automatico di sovracorrente scatta e la sua attivazione meccanica non è in alcun modo influenzabile da comandi a distanza.

Stupisce in particolare il fatto che, dopo l'attacco perpetrato a metà di ottobre 2026, i responsabili dell'altro sistema di gestione delle celle frigorifere non abbiano effettuato interventi correttivi tempestivi.

Ancora una volta, i buoni cercano di inseguire i cattivi, ma i cattivi sono sempre davanti!

Adalberto Biasiotti

Licenza Creative Commons
I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.

www.puntosicuro.it