NEDIK

Ai membri dell'ATF
Associazione svizzera del freddo

Zurigo, 12 novembre 2026

Attacchi informatici contro impianti frigoriferi commerciali – informazioni importanti e misure immediate

Gentili signore e signori,

Da metà ottobre in diversi Paesi europei e ora anche in Svizzera gli impianti frigoriferi commerciali vengono attaccati in modo mirato tramite Internet. Gli aggressori assumono il controllo del sistema di comando, spengono il raffreddamento e fanno surriscaldare gli impianti, in parte ben oltre i 50 °C. Le conseguenze sono merci deteriorate e danni materiali. Sono colpite sempre più spesso anche piccole aziende.

Il presupposto per tali attacchi è che il sistema di comando dell'impianto frigorifero sia raggiungibile tramite un accesso di rete, ad esempio da Internet. Gli aggressori possono attaccare in modo mirato le impostazioni del sistema di comando e modificarle, in modo che l'impianto non raffreddi più, ma riscaldi.

Misure raccomandate

- Accesso a Internet e accesso remoto: Se l'impianto dispone di un accesso di rete o di un accesso a Internet, occorre verificare con il responsabile tecnico se il sistema di comando può essere scollegato dalla rete fino a ulteriori verifiche. Il sistema di comando non deve essere raggiungibile direttamente da Internet. L'accesso remoto agli impianti dovrebbe avvenire solo tramite un accesso di rete protetto. Se ciò non è possibile a breve termine, scollegate il sistema di comando dalla rete finché non avrete adottato misure adeguate. Il raffreddamento continua in genere a funzionare localmente.
- Dati di accesso all'impianto frigorifero: Assicuratevi che l'accesso al vostro sistema soddisfi gli standard di sicurezza attuali (p. es. sostituire le password predefinite, impostare password individuali e robuste, se possibile utilizzare l'autenticazione a due fattori e verificare gli accessi dei fornitori di servizi).
- Proteggere gli apparecchi: Assicuratevi, insieme al produttore o allo specialista competente, che il vostro impianto sia aggiornato. Ciò comprende l'installazione di un software aggiornato, la sostituzione degli apparecchi privi di supporto del produttore oppure il loro utilizzo in una rete propria e isolata, separata dall'informatica d'ufficio. L'installazione di aggiornamenti da sola non basta.
- Garantire un allarme di temperatura indipendente: Definire i valori limite e far passare l'allarme (p. es. via SMS) da un dispositivo indipendente dal sistema di comando. Una persona responsabile deve essere raggiungibile e conoscere il piano d'emergenza (raffreddamento sostitutivo o di emergenza).
- Elaborare un concetto di sicurezza: Poiché vengono scoperte continuamente nuove vulnerabilità, è importante elaborare un concetto di sicurezza insieme allo specialista informatico.

In caso di sospetto di attacco

Coinvolgete subito l'azienda del freddo e lo specialista informatico, se possibile fate funzionare l'impianto manualmente, conservate le tracce digitali (log, impostazioni) e non reimpostate l'apparecchio. Segnalate subito l'incidente alla polizia: in caso di danno in corso tramite il numero d'emergenza 117, altrimenti presso il vostro posto di polizia locale.

L'Ufficio federale della cibersicurezza (UFCS) ha pubblicato un avviso con ulteriori misure di protezione: www.bacs.admin.ch/it/warnung-kuehlanlagen-it.

Ulteriori informazioni sul tema della criminalità informatica sono disponibili su cybercrimepolice.ch/it.

Cordiali saluti
La vostra polizia / NEDIK (Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung)