Attacchi hacker ai frigoriferi dei supermercati, casi in Sicilia e vertice a Palazzo Chigi

Data: 11 febbraio 2026 | Autore: Redazione



Anomalie negli impianti di refrigerazione tra Catania e Palermo mentre altri Paesi europei segnalano episodi simili. Al centro delle verifiche la sicurezza dei sistemi e la conservazione degli alimenti

Gli **attacchi hacker ai sistemi di refrigerazione dei supermercati**arrivano all'attenzione del governo italiano. Dopo le segnalazioni provenienti dalla Sicilia e gli incidenti registrati in diversi Paesi europei, è stata annunciata per **martedì 3 novembre 2026 alle 11.30**una riunione a Palazzo Chigi, coordinata dal sottosegretario alla Presidenza del Consiglio **Alfredo Mantovano**, con i vertici dell'Agenzia per la cybersicurezza nazionale e delle agenzie di intelligence.

L'emergenza riguarda impianti che controllano frigoriferi, congelatori e banchi alimentari. La modifica delle impostazioni può interrompere la **catena del freddo**, compromettere la merce e costringere i negozi a sospendere la vendita dei prodotti coinvolti.

Supermercati in Sicilia, verifiche tra Catania e Palermo

Secondo quanto riferito da **Giuseppe Spadaro, direttore generale del gruppo Radenza**, gli episodi hanno interessato almeno tre punti vendita a Catania e uno a Palermo, gestiti dal gruppo con insegna Coop.

Le anomalie avrebbero comportato una modifica dei parametri di temperatura, con il conseguente riscaldamento dei banchi e il deterioramento degli alimenti. Gli interventi dei tecnici hanno consentito di risolvere alcune delle criticità, mentre resta in corso la quantificazione dei danni.

Il gruppo ha comunicato di aver contattato l'**Agenzia per la cybersicurezza nazionale**. Gli accertamenti della Polizia postale dovranno chiarire l'origine degli accessi e l'eventuale collegamento con gli incidenti avvenuti all'estero. La somiglianza degli episodi, da sola, non permette ancora di attribuirli agli stessi responsabili.

Refrigeratori manomessi anche in altri Paesi europei

Problemi agli impianti sono stati segnalati in **Belgio, Svezia, Lussemburgo, Irlanda ed Estonia**. Diversi operatori hanno riferito di modifiche non autorizzate ai sistemi di controllo, con ripercussioni sulla conservazione dei prodotti freschi e surgelati. reuters.com

In Belgio gli episodi hanno coinvolto punti vendita di più insegne, tra cui **Delhaize, Carrefour, Intermarché e Spar**. In alcuni casi sarebbe stata attivata a distanza la modalità di sbrinamento: una funzione prevista per il normale funzionamento degli impianti, ma che può provocare danni se utilizzata in modo improprio o prolungato.

Il bilancio complessivo delle perdite resta da definire. La necessità di svuotare frigoriferi e congelatori comporta conseguenze economiche per le aziende e un significativo **spreco alimentare**.

Il precedente francese e i sistemi esposti su Internet

La nuova ondata richiama gli attacchi emersi in Francia il **12 ottobre**, quando furono compromessi numerosi dispositivi per il controllo remoto della refrigerazione. L'allerta tecnica francese ha indicato apparecchiature di diverse famiglie e produttori, evidenziando soprattutto il rischio delle **interfacce di gestione accessibili direttamente da Internet**. CERT-FR

Questi dispositivi consentono ai manutentori di monitorare gli impianti e modificarne le impostazioni senza recarsi sul posto. Se l'accesso viene compromesso, le stesse funzioni possono essere utilizzate per alterare temperature e cicli operativi.

Tra i fattori da verificare figurano **software non aggiornati, credenziali insufficientemente protette e apparecchiature non più supportate**. Non è invece corretto individuare nella sola connessione 4G, rispetto al 5G, la causa della vulnerabilità: il punto centrale è come il sistema viene configurato, protetto e mantenuto. CERT-FR

Catena del freddo, perché ripristinare gli impianti non basta

Il ritorno alla temperatura corretta non risolve automaticamente le conseguenze dell'incidente. Per i prodotti coinvolti occorre valutare **quanto è durata l'interruzione della refrigerazione**, quali temperature sono state raggiunte e quali alimenti erano presenti nei banchi.

La gestione dell'emergenza comprende quindi sia il ripristino tecnico sia la verifica della merce, prima di un'eventuale rimessa in vendita. L'obiettivo è evitare che un problema informatico si trasformi in un rischio per la qualità e la sicurezza degli acquisti.

Sicurezza informatica e continuità dei supermercati

Gli episodi mostrano quanto la **cybersicurezza della grande distribuzione**riguardi anche gli impianti utilizzati nelle attività quotidiane, oltre ai computer e ai sistemi di pagamento.

Le indicazioni tecniche richiamano la necessità di proteggere gli accessi remoti, aggiornare i dispositivi supportati e ridurre l'esposizione dei pannelli di controllo su Internet. Per le apparecchiature obsolete occorre valutare interventi di sostituzione o adeguate misure di isolamento. CERT-FR

Restano da chiarire **responsabili, modalità di accesso ed eventuale coordinamento degli attacchi**. Le indagini dovranno distinguere gli elementi comuni ai diversi episodi dalle caratteristiche dei singoli impianti, mentre per i supermercati la priorità immediata è ripristinare il servizio e verificare gli alimenti coinvolti.

Articolo scaricato da www.infooggi.it
https://www.infooggi.it/articolo/attacchi-hacker-ai-frigoriferi-dei-supermercati-casi-in-sicilia-e-vertice-a-palazzo-chigi/157564