Cyberattacco ai supermercati francesi: sbrinamento forzato causa perdite milionarie

Data: 10 dicembre 2026 | Autore: Redazione



Nella notte, un **attacco informatico**ha preso di mira i sistemi di refrigerazione di numerosi supermercati francesi, tra cui le catene **Intermarché**, **Leclerc** e **Super U**. I malintenzionati hanno sfruttato versioni obsolete del software del produttore danese **Danfoss**per attivare lo sbrinamento continuo degli impianti, portando le temperature fino a 50 °C. Questo ha causato la perdita di prodotti freschi e surgelati, con danni stimati in diversi milioni di euro.

Modalità dell'attacco

Secondo le prime ricostruzioni, gli hacker hanno approfittato di vulnerabilità note nel software **Danfoss**non aggiornato. Una volta ottenuto l'accesso ai sistemi di controllo, hanno manipolato le impostazioni di temperatura, innescando cicli di sbrinamento prolungati che hanno compromesso irreversibilmente la catena del freddo. Le autorità francesi stanno indagando per identificare i responsabili e verificare se si tratti di un attacco mirato o di un'azione casuale.

L'indagine della procura di Parigi: nel mirino il gruppo iraniano Shahid Kaveh

La procura di Parigi ha aperto un'indagine sul gruppo di hacker iraniano **Shahid Kaveh**, affiliato ai

pasdaran e sospettato dalla Francia di essere responsabile degli attacchi informatici che a ottobre hanno compromesso i sistemi di refrigerazione di centinaia di supermercati. L'inchiesta punta quindi a fare chiarezza sulla matrice dell'operazione, che secondo gli inquirenti d'Oltralpe porterebbe il marchio di un'azione orchestrata e non di un attacco casuale.

Impatto economico e sulla sicurezza alimentare

Le perdite economiche potrebbero essere ingenti: interi stock di merce deperibile sono andati distrutti, costringendo i supermercati a smaltire prodotti per un valore di milioni di euro. Inoltre, l'episodio solleva serie preoccupazioni sulla **sicurezza alimentare**e sulla vulnerabilità delle infrastrutture critiche nel settore della distribuzione. Le catene coinvolte stanno collaborando con le autorità per ripristinare le normali condizioni operative e rafforzare le difese informatiche.

Reazioni e misure di prevenzione

Danfoss, dal canto suo, ha dichiarato di essere a disposizione delle autorità e dei clienti per fornire supporto tecnico, sottolineando l'importanza di mantenere aggiornati i sistemi. Esperti di cybersecurity evidenziano come molti dispositivi IoT industriali, come quelli per la refrigerazione, siano spesso trascurati in termini di patch di sicurezza, diventando bersagli facili per i cybercriminali. L'incidente potrebbe spingere il settore ad adottare misure più stringenti per proteggere le reti OT (Operational Technology).

L'allerta dell'ACN per l'Italia

L'ondata di attacchi ha fatto scattare i riflettori anche sull'Italia: l'**Agenzia per la Cybersicurezza Nazionale (ACN)**ha lanciato un'allerta per gli operatori della grande distribuzione e della logistica alimentare. L'Agenzia ha ricevuto la notifica di un incidente da un'azienda toscana della ristorazione collettiva e ha individuato un attacco, non ancora notificato, ai danni di un'impresa emiliano-romagnola produttrice di surgelati. L'ACN raccomanda di rafforzare le misure di sicurezza dei sistemi di controllo e accesso remoto e ha convocato per domani un incontro con le principali aziende e federazioni del settore. Le indicazioni tecniche e operative sono disponibili sul sito dell'Agenzia.

La nota di Palazzo Chigi: impatto limitato in Italia

Nel frattempo arriva la prima valutazione ufficiale del governo italiano. Palazzo Chigi ha fatto sapere in una nota che gli attacchi informatici ai sistemi di refrigerazione commerciale, registrati in diversi Paesi europei, hanno avuto finora un impatto limitato in Italia, interessando poche attività. Non sono stati rilevati rischi per la salute dei cittadini legati a eventuali scongelamenti: "Non sussiste alcun allarme, ma permane la massima attenzione da parte di tutti i soggetti istituzionali competenti", si legge nella nota. L'ACN continuerà a monitorare la minaccia, collaborando con le aziende del settore e rafforzando le misure di prevenzione e sicurezza.

Possibili sviluppi

Le indagini sono in corso per determinare la provenienza dell'attacco e se vi siano state violazioni dei dati. Nel frattempo, i supermercati stanno valutando come risarcire i clienti e prevenire futuri episodi. Questo caso rappresenta un monito per tutte le aziende che utilizzano sistemi di controllo industriali obsoleti, evidenziando la necessità di una maggiore consapevolezza dei rischi informatici anche in settori tradizionalmente lontani dall'high-tech.

L'ondata di attacchi non si è limitata alla Francia. Nella notte, anche in **Svezia**le catene di supermercati **ICA** e **Coop**hanno segnalato anomalie ai sistemi di refrigerazione di alcuni punti vendita, mentre in **Belgio** almeno 40 negozi **Delhaize**sono stati interessati da un incidente analogo. In entrambi i Paesi si sospetta un attacco informatico. Alcuni supermercati hanno trasferito i prodotti su camion refrigerati per limitare le perdite. Gli episodi ricordano il cyberattacco del 12 ottobre in Francia, che aveva coinvolto centinaia di supermercati.

Anche l'Italia è stata colpita: il gruppo **Radenza**, che gestisce supermercati a marchio **Coop**in Sicilia, ha riferito che un attacco hacker ha interessato i sistemi di refrigerazione di tre punti vendita a **Catania** e di uno a **Palermo**, alterando i parametri di temperatura dei banchi alimentari e causando il deterioramento di alcuni prodotti. La **polizia postale**sta indagando sulla provenienza dell'attacco e su eventuali collegamenti con episodi analoghi avvenuti in altri Paesi europei. L'azienda ha attivato i protocolli di sicurezza e avvisato l'**Agenzia per la cybersicurezza nazionale**.

Articolo scaricato da www.infooggi.it
https://www.infooggi.it/articolo/cyberattacco-ai-supermercati-francesi-sbrinamento-forzato-causa-perdite-milionarie/156534