In Francia gli hacker provano anche a scongelare le riserve di sangue: sventato attacco al Centro Trasfusionale di Roberto Cosentino

Un attacco anche in Norvegia. Il gruppo di hacker NoName rivendica la responsabilità della catena di malfunzionamenti in Europa (Fonte: https://www.corriere.it/ 4 novembre 2026)



Non solo cibo: anche il sangue dei donatori ha rischiato di essere un target per i criminali informatici che stanno sfruttando le vulnerabilità dei congelatori e frigoriferi. Fino a questo momento gli attacchi - prima negli Usa e poi anche in Europa - avevano preso di mira magazzini ed alimentari, ma ora l'allerta arriva anche le strutture sanitarie. Nella notte tra l'1 e il 2 novembre infatti, **l'ente pubblico francese responsabile della gestione del sistema trasfusionale** (Établissement français du sang, Efs) ha visto le apparecchiature fornite dal produttore **Coolworld rischiare di raggiungere la temperatura di 110°C**. Un provvidenziale intervento di un tecnico attento e i sistemi recenti e aggiornati hanno permesso di evitare il peggio.

L'incidente gestito senza conseguenze

Secondo Le Canard enchaîné nonostante il tentativo di attacco, **le celle sono state mantenute correttamente a -30°C**, anche se da remoto **è stato programmato, in modo fraudolento, il raggiungimento di una temperatura di 110°C**. L'incidente è stato dunque rilevato e gestito, tanto che ad Efs **non risultano perdite di materiale né conseguenze sanitarie**. «I sistemi di monitoraggio e allarme dell'Efs hanno consentito la rapida identificazione di queste anomalie e l'attuazione delle misure necessarie per garantire che nessun campione di sangue o prodotto ematico venisse compromesso. L'apparecchiatura interessata è stata riportata sotto controllo senza impattare i prodotti e i campioni, oppure neutralizzata; i prodotti conservati in queste celle

frigorifere sono stati preventivamente trasferiti in altre strutture», scrivono **in un comunicato ufficiale**. Il merito è stato riconosciuto anche a un attento tecnico di turno che ha rilevato l'allarme sull'aumento delle temperature e, come confermato dal ministro della Salute francese, **ha fatto sì che non vi fossero conseguenze operative**. Ad ogni modo i prodotti conservati all'interno delle celle sono stati trasferiti oppure messi in sicurezza, come affermato dall'ente d'Oltralpe al giornalista Raphaël Grably.
Nei casi precedenti, **rivendicati dai collettivi hacker filorussi NoName e Z-Pentest**, i sistemi colpiti (nei supermercati **statunitensi**, francesi e anche italiani), non erano aggiornati, oppure avevano raggiunto un'obsolescenza oltre la quale **non erano più soggetti a ricevere update, anche di sicurezza**. Ed è uno dei motivi per cui anche **l'attacco italiano**, nonostante le perdite subite dai punti vendita, è stato tutto sommato limitato. Come riportato dalla nota di Palazzo Chigi del 3 novembre, «La gran parte della catena di distribuzione risulta invece dotata di sistemi di protezione aggiornati, in grado di respingere intrusioni malevole».

Affrontare la crisi
Ma i sistemi aggiornati e rilevazioni tempestive non sono l'unico modo di affrontare la crisi. Come riporta **il bollettino di Acn**, l'agenzia per la cybersicurezza nazionale, **è necessario anche separare le reti**, implementare accessi remoti protetti, assicurarsi che vi sia **un'autenticazione robusta** e la **sostituzione dei dispositivi** che non ricevono più supporto. Inoltre, è necessario accertarsi che siano stati **effettuati gli aggiornamenti** previsti e che vi siano strumenti indipendenti per la verifica delle temperature.

Nel mirino la Norvegia: danni considerevoli
Intanto, anche altre nazioni europee sono finite nel mirino degli hacker. In un grande magazzino ad **Havarisent**, nell'area di **Oslo**, in Novergia, nella notte tra il 2 e il 3 novembre si è verificato un surriscaldamento dell'impianto frigorifero. Secondo il responsabile della società **Miko Trading**, Thomas Michelsen, **i danni sarebbero considerevoli**. Non vi sono allo stato attuale notizie aggiornate, benché **vi siano forti indizi** che riconducono ad un'intrusione informatica. L'apparecchiatura che ha subito il presunto attacco, anziché essere protetta da un firewall aziendale, **sfruttava un collegamento 4G esterno**. Lo stesso è accaduto ad un deposito di frutta; in questo caso un tecnico **ha però rilevato l'anomalia della temperatura** all'interno di una cella. Secondo la responsabile, Maria Strand, potrebbe essersi verificata una modifica dei parametri da parte di terzi. Un addetto del fornitore ha però scollegato il sistema dalla Rete, evitando così che, in piena stagione, le conseguenze potessero essere maggiori, benché non vi sia una quantità verificata di frutta distrutta.

La rivendicazione di NoName

Il gruppo di hacker filorussi **NoName057(16)** **ha rivendicato sul proprio canale Telegram l'attacco**. Secondo quanto affermato in un lungo messaggio condiviso **il 3 novembre, sarebbero stati attaccati 20 paesi** (maggior parte dei quali membri Nato). Ad essere colpiti perlopiù **sistemi di approvvigionamento idrico, centrali elettriche, impianti industriali, aziende vinicole e magazzini alimentari**.

Il gruppo cita **Danfoss**, gigante danese i cui prodotti sono finiti al centro degli attacchi segnalati in precedenza. L'attacco di NoName al produttore sarebbe senza esclusione di colpi. Il sito Web il 3 novembre è andato in down dopo un attacco **DDoS** (Distributed Denial of Service, attacco distribuito di negazione del servizio) ovvero una tecnica che prevede l'inoltro di numerose richieste ad un sito o un server che non è in grado di gestire e il conseguente disservizio.

Oltre a ciò, gli hacker rivendicano anche le modalità di attacco. Stando a quanto rivelato, **il primo attacco ai frigoriferi sarebbe stato sufficiente affinché Danfoss potesse analizzare gli errori e correggere le vulnerabilità** cosa che però non è avvenuta. Ancora, oltre all'attacco, anche un **data breach**. In mano ai criminali informatici vi sarebbe anche il database del produttore danese, con le credenziali di dipendenti e clienti **pubblicato sul Dark Web**. «Ma non siamo animali: abbiamo rimosso dal database i link e i moduli in cui questi dati venivano inseriti». Questo perché, affermano gli attaccanti «Crediamo che le persone comuni non debbano soffrire a causa della sicurezza fallace delle aziende». Persone comuni che non potranno acquistare chilogrammi di merce avariata per via delle loro azioni.