

Primo Piano - *Cybersicurezza, attacchi ai sistemi di refrigerazione dei supermercati in Europa: sospetti su gruppi filorussi e piste statali*

Roma - 03 nov 2026 (Prima Notizia 24) **Gli esperti evidenziano l'elevata vulnerabilità delle infrastrutture collegate a Internet dopo l'ondata di sabotaggi che ha colpito la grande distribuzione.**

Non ci sono ancora rivendicazioni ufficiali o richieste di riscatto per la nuova e complessa ondata di cyberattacchi che sta interessando la catena della grande distribuzione in Europa, prendendo di mira i sistemi di gestione da remoto della refrigerazione di supermercati e magazzini agroalimentari. L'episodio, che nelle ultime ore ha registrato segnalazioni anche in Italia oltre che in Belgio, Svezia, Luxeburgo, Irlanda ed Estonia, ripropone la questione della vulnerabilità delle infrastrutture civili. Un'analisi condotta dalla società di cybersicurezza Forescout e dai ricercatori di Vedere Labs documenta come, dall'inizio dell'anno, siano stati censiti oltre venti attacchi diretti a strutture industriali e commerciali della filiera alimentare. Tra le sigle maggiormente attive sul campo figurano gruppi d'ispirazione filorussa come Z-Pentest Alliance e NoName057(16), già noti per azioni volte a creare disservizi nei Paesi occidentali. Le tecniche utilizzate prevedono l'accesso non autorizzato alle interfacce di controllo collegate in rete, permettendo agli aggressori di alterare temperature e cicli di sbrinamento da remoto e provocando il deterioramento dei prodotti senza la necessità di inoculare malware complessi. Sebbene gli analisti invitino alla cautela sull'attribuzione diretta degli ultimi eventi a una regia unica, la pista di un'operazione condotta da attori statali o da collettivi d'intelligence viene ritenuta plausibile dagli esperti internazionali interpellati dalle testate The Guardian e Computer Weekly. L'assenza di un ritorno economico diretto suggerisce finalità legate a dimostrazioni di forza o a sabotaggi a bassa tracciabilità, favoriti dalla scarsa traccia digitale che le intrusioni nei pannelli di controllo lasciano nei registri di sistema. A definire l'ampiezza del rischio è il dato globale rilevato da Forescout, che individua quasi 13.000 servizi di gestione della refrigerazione direttamente accessibili via Internet su scala mondiale, con un'elevata concentrazione di vulnerabilità in Paesi quali Italia, Francia e Grecia. La debolezza strutturale risiede nell'impiego di software obsoleti, credenziali di accesso fragili o pannelli di supervisione — come quelli già compromessi in precedenti attacchi sul territorio francese — capaci di governare interi impianti frigoriferi da un unico punto d'accesso.

(Prima Notizia 24) Martedì 03 Novembre 2026