il Riformista

Mercoledì 4 novembre 2026 • Anno VIII numero 218 • Euro 2,00 • www.ilriformista.it • Quotidiano • ISSN 2704-6885

Direttore **Claudio Velardi**



GUERRA IBRIDA

Sabotaggio manda in tilt gli impianti della refrigerazione Allarme di Paganini: «Investire nella cybersicurezza» Lombardo: «Scudo democratico per la Guerra cognitiva»

Picasso, Paganini, Torchiaro e Lombardo a pag. 2

IL PARADOSSO DELLE *MIDTERM*

Andrea Molle

Donald Trump non compare sulla scheda elettorale, ma le elezioni del 3 novembre sono inevitabilmente un referendum sulla sua presidenza. Si vota per rinnovare la Camera e parte del Senato, ma soprattutto per decidere quanto potere politico resterà alla Casa Bianca. Il paradosso è che, mentre i repubblicani devono difendere il proprio operato, i democratici devono ancora chiarire quale alternativa intendano rappresentare.

Dopo le promesse arriva il momento del bilancio. Ma se i repubblicani devono rispondere dei risultati, i democratici devono rispondere della propria identità. Il problema è capire quanto questa capacità di mobilitazione sia traducibile in consenso nazionale. Emblematico, in questo senso, il caso del Michigan. Qui emerge il vero dilemma democratico. Il linguaggio che entusiasma gli attivisti non è necessariamente quello che convince gli elettori decisivi. Il radicalismo progressista può rappresentare una risorsa nelle primarie e nei collegi fortemente democratici, ma costruire una maggioranza nazionale richiede una coalizione sociale e politica assai più ampia. Ed è qui che le divisioni democratiche finiscono per intrecciarsi con il futuro di Trump.

Una maggioranza repubblicana consentirebbe al presidente di proseguire con maggiore continuità legislativa. Una Camera democratica aprirebbe invece una stagione di controlli parlamentari, conflitti sul bilancio e possibili inchieste. Un cambiamento anche al Senato inciderebbe sulle nomine e sui rapporti fra presidenza e Congresso. Ma un'opposizione capace di bloccare il presidente non è automaticamente un'alternativa capace di governare. Le conseguenze superano i confini americani. Il 3 novembre misura dunque due cose: quanto consenso conserva il progetto politico di Trump e quanto i democratici siano riusciti a costruire qualcosa che vada oltre la sua contestazione.



La guerra ibrida entra nei supermercati il nuovo fronte invisibile dell'Europa

Luca Longo

La sequenza comincia in Francia il 12 ottobre. Centinaia di supermercati subiscono un attacco ai sistemi digitali che controllano frigoriferi, congelatori e banchi refrigerati. Le stime arrivano fino a 700 esercizi coinvolti. Gli aggressori modificano da remoto i parametri degli impianti, in alcuni casi portando temperature (inizialmente intorno a -27 °C) oltre i 50 °C. Il danno è fisico prima che informatico: alimenti deteriorati, celle inutilizzabili e perdite economiche ingenti.

Tre settimane dopo, nella notte tra il 1° e il 2 novembre, lo stesso tipo di incidente si ripete in almeno sette Paesi: Belgio, Estonia, Finlandia, Irlanda, Lussemburgo, Paesi Bassi e Svezia. In Belgio vengono interessati circa 40 punti vendita Delhaize e 15 Carrefour, oltre ad altri esercizi, per un totale di circa 75 negozi. In Irlanda sono 13 i SuperValu coinvolti, mentre in Svezia vengono colpiti punti vendita ICA e Coop. Nei Paesi Bassi risultano interessate almeno 17 aziende. In alcuni casi i congelatori raggiungono i 50 °C. Un macellaio belga quantifica in circa 15.000 euro il valore della carne perduta.

Il bersaglio non è il frigorifero ma il sistema digitale che lo governa. I supermercati utilizzano piattaforme di supervisione collegate alla rete per controllare temperature, allarmi, cicli di sbrinamento e altri parametri. L'accesso remoto facilita manutenzione e gestione centralizzata, ma crea una superficie d'attacco che può essere sfruttata a distanza.

In Belgio, gli aggressori hanno portato gli evaporatori in modalità sbrinamento. In Estonia è stato compromesso un computer che controllava l'impianto e la temperatura è stata impostata a 50 °C. In altri casi sono stati modificati direttamente i parametri di funzionamento. Le autorità non hanno ancora stabilito quale sia stato il vettore iniziale dell'intrusione né se tutti gli episodi appartengano alla stessa operazione.

Tra le tecnologie finite sotto osservazione ci sono sistemi Danfoss. La loro sicurezza era già stata oggetto di segnalazioni nel 2025. La vulnerabilità CVE-2025-41450, con punteggio CVSS 8,2, riguarda un problema di autenticazione degli AK-SM 8xxA precedenti alla versione 4.2. Altre due vulnerabilità, CVE-2025-41451 e CVE-2025-41452, riguardano versioni precedenti alla 4.3.1 e possono consentire, in determinate condizioni, l'esecuzione remota di codice o compromettere la disponibilità del sistema. Non esiste tuttavia una prova pubblica che colleghi direttamente queste vulnerabilità agli attacchi di novembre.

È proprio l'assenza di una richiesta economica a rendere la vicenda particolarmente significativa. Nessun gruppo ha rivendicato gli attacchi e nessuno ha chiesto un riscatto. L'ipotesi del ransomware convenzionale perde così forza, mentre resta aperta quella del sabotaggio. Non è però possibile attribuire oggi l'operazione a un attore specifico. Sono state considerate anche piste riconducibili ad attori statali o filostatali, compresi gruppi legati alla Russia o alla Cina, ma non esistono elementi pubblici sufficienti per confermare alcuna responsabilità. Le autorità belghe hanno avvertito che potrebbe persino non essere possibile identificare gli autori.

Alterare contemporaneamente sistemi apparentemente marginali significa dimostrare che una componente della catena alimentare può essere trasformata in un punto di pressione senza colpire direttamente reti energetiche, infrastrutture militari o grandi centri dati.

È questo il possibile salto di scala. Lo stesso principio può essere applicato a impianti di climatizzazione, magazzini refrigerati, sistemi logistici e altre apparecchiature di tecnologia operativa collegate alla rete. La vulnerabilità nasce spesso dalla combinazione di dispositivi obsoleti, software non aggiornati, accessi remoti e collegamenti affidati a fornitori esterni.

Per l'Europa e in particolare per l'italia il problema diventa quindi duplice. Da una parte occorre impedire che sistemi industriali progettati per essere facilmente amministrabili diventino porte d'ingresso; dall'altra bisogna evitare che episodi circoscritti producano una percezione generalizzata di vulnerabilità della catena alimentare. Questi attacchi sono un tentativo deliberato di interrompere la catena di approvvigionamento e minare la fiducia dei consumatori. E la seconda ondata dimostra che il fenomeno non è più confinato a un singolo Paese. In una guerra ibrida, la capacità di provocare un danno può contare meno della capacità di dimostrare che quel danno è possibile.

€ 2,00 in Italia
solo per gli acquirenti in edicola
e fino ad esaurimento copie

Redazione e amministrazione
via di Pallacorda 7 - Roma - Tel 06 32876214
Sped. Abb. Post., Art. 1, Legge 46/04 del 27/02/2004 - Roma

9 772704 688006 61104