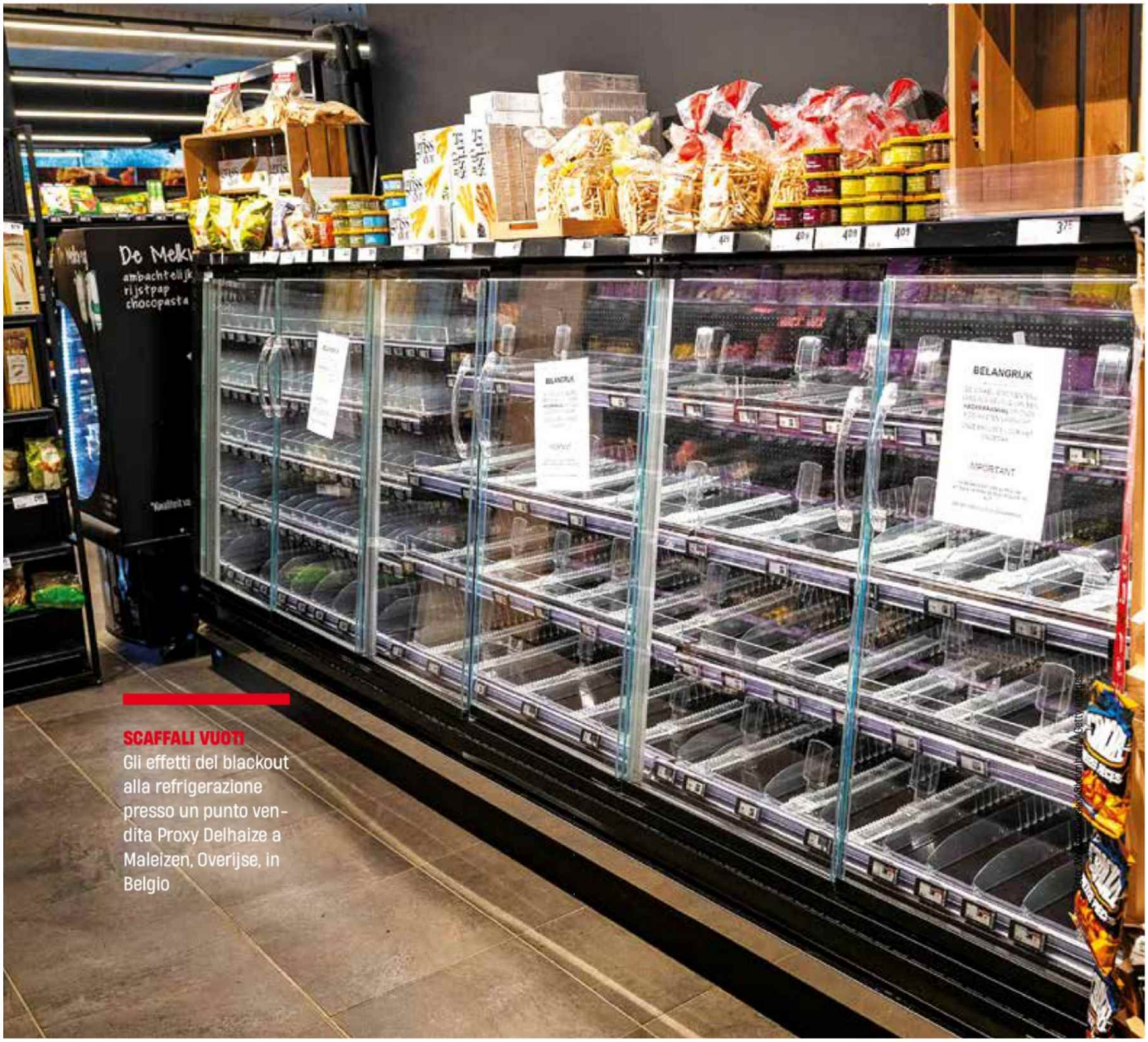
13-NOV-2026
da pag. 42 / foglio 1 / 4

l'Espresso
Settimanale - Dir. Resp.: Emilio Carelli
Tiratura: 43178 Diffusione: 33007 Lettori: 944000 (Data Stampa 0006901)

DATA STAMPA
45° Anniversario

Data Stampa 6901-Data Stampa 6901
Data Stampa 6901-Data Stampa 6901

Il terrore hacker corre sul frigo E ci trova fragili



SCAFFALI VUOTI
Gli effetti del blackout alla refrigerazione presso un punto vendita Proxy Delhaize a Maleizen, Overijse, in Belgio

ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS6901 - S.30524 - L.1992 - T.1733

l'Espresso
Settimanale - Dir. Resp.: Emilio Carelli
Tiratura: 43178 Diffusione: 33007 Lettori: 944000 (Data Stampa 0006901)

DATA STAMPA
45° Anniversario

ALESSANDRO LONGO

Con un tessuto di piccole e medie imprese la vulnerabilità italiana è maggiore quando la minaccia punta a colpire le nostre abitudini quotidiane. Perché siamo indietro

Intorno alle 6 di mattina del 2 novembre, ai primi dipendenti che entrano in una Coop di Palermo si presenta una scena mai vista. «Nei frigoriferi, appaiono scongelati i pacchi di piselli. Idem i bastoncini di pesce. I gelati sono sciolti. Su quei frigoriferi, che di solito sono a meno 20 gradi, qualcuno aveva attivato a distanza comandi per portarli a 20 gradi sopra lo zero», racconta a *L'Espresso* **Giuseppe Spadaro**, direttore generale della Coop Gruppo Radenza in Sicilia. «Chiamano subito in direzione generale per lanciare l'allarme. Allora si scopre che altri tre supermercati, a Catania e Ragusa, hanno vissuto lo stesso orrore mattutino», aggiunge. Non solo Coop, non solo Sicilia. Nelle stesse ore – e poi anche nei giorni successivi – emergono casi simili in una dozzina di regioni italiane: ne abbiamo censiti una quarantina emersi su testate locali, tra supermercati, bar, mense, produttori di alimenti. Non solo Italia: l'incidente riguarda quasi tutti i Paesi europei, circa una ventina quelli colpiti, dalla Francia alla Grecia, alla Scandinavia. Ma che sta succedendo? Soprattutto: che altro potrebbe succedere, ancora di più grave? Gli esperti concordano. «Non sono stati ragazzini ad avere colpito via Internet i frigoriferi in Europa. È un attacco informatico coordinato su molti Paesi. Certo sono esperti che hanno alle spalle uno Stato nazione nemico dell'Occidente. La Russia è il principale indiziato», dice **Sven Herpig**, esperto internazionale di politiche di cybersecurity, presso il think tank europeo Interface. «Sono partite indagini, coordinate con le autorità di tutta l'Europa. Hacker filo russi hanno rivendicato l'attacco ed è plausibile siano loro», aggiunge **Ivano Gabrielli**, direttore del Servizio Polizia Postale e per la Sicurezza Cibernetica.



Siamo entrati in una nuova, pericolosa era: attacchi informatici causano danni ad apparati fisici, in settori importanti. «Un salto di qualità della minaccia. Fino a ieri, almeno in Italia, gli hacker di Paesi avversari si limitavano ad attacchi superficiali che al massimo bloccavano un sito o un servizio digitale per qualche ora», aggiunge **Gabriele Faggioli**, presidente onorario del Clusit, l'associazione italiana della sicurezza informatica. Ma ad avere software ed essere connessi a Internet, e quindi essere vulnerabili ad attacchi informatici, sono tantissime cose, ormai: impianti industriali, pompe di benzina, centrali energetiche; frigoriferi, appunto.

Significa che disastri devastanti sono in agguato nelle nostre città? Blackout, assenza di carburante, esplosioni? A questo punto è importante restare con i piedi per terra. Cadere in un eccesso di allarmismo significa fare il gioco degli avversari. Interessati, con queste azioni così come con le varie campagne di disinformazione, appunto «a seminare caos e paura, per minare un pilastro dei nostri Stati democratici: la fiducia dei cittadini nella capacità dei Governi di proteggerli», dice Herpig.

La maggior parte degli esperti, come Herpig e Faggioli, concorda: i prossimi attacchi saranno simili a questi, quindi di basso livello, con danni tutto sommato limitati – come ha commentato una nota di Palazzo Chigi. Vedi anche gli attacchi (falliti) a celle frigorifere con sangue dei donatori, sempre a novembre, in Francia. «Questi attacchi continueranno perché funzionano e sono più compatibili con l'attuale livello del conflitto in Europa. Causare un blackout, per hacker al soldo della Russia, segnerebbe invece una pericolosa escalation diplomatica», dice Faggioli. Però, un attimo: non significa che si possa dormire tranquilli. Intanto, gli ultimi attacchi sul piano economico non sono trascurabili. Ciascuna azienda riporta danni alle merci di migliaia o ▶

ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS6901 - S.30524 - L.1992 - T.1733

l'Espresso
Settimanale - Dir. Resp.: Emilio Carelli
Tiratura: 43178 Diffusione: 33007 Lettori: 944000 (Data Stampa 0006901)

DATA STAMPA
45° Anniversario





AL MACERO
Prodotti al macero dopo l'attacco a un supermercato di Stoccolma, in Svezia. A destra, la sessione sulla cybersicurezza alle "Olimpiadi della Tecnologia" iraniane del 2025

► decine di migliaia di euro. Il danno più grave l'ha subito una catena commerciale di Roma in zona Tiburtina, circa 500 mila euro. I danni in termini di minori vendite sono molto più grandi, fino a milioni di euro in Sicilia (la regione più colpita), prevede Federdistribuzione. In Europa la vittima maggiore è forse il colosso della grande distribuzione Ahold Delhaize, che ha subito danni a supermercati in Francia (già a ottobre, quando c'è stata la prima ondata europea, per la quale Parigi accusa l'Iran), Belgio e Lussemburgo. Qualche giorno fa ha previsto minori vendite per 200-250 milioni di euro a causa degli attacchi.

Il possibile parco delle vittime, poi, è abbastanza ampio, «soprattutto in Italia dove abbiamo pmi molto vulnerabili agli attacchi informatici che sono anche centrali per filiere di importanti settori come gli alimentari, i trasporti, l'energia», spiega **Stefano Zanero**, ordinario di cybersecurity al Politecnico di Milano. Tasselli fragili che possono spezzare una catena strategica, con impatti anche sulla popolazione. Ad esempio su distribuzione e costi di alimenti. Gli stessi attacchi ai frigoriferi sono tesi a «danneggiare il nostro approvvigionamento alimentare», ha commentato il commissario Ue all'agricoltura **Christophe Hansen**. «La nostra manifattura, la nostra Sanità sono molto esposti a questi attacchi», aggiunge **Pierluigi Paganini**, già esperto Enisa, l'agenzia Ue per la cybersecurity. «Se per un attacco esplode una fabbrica, ci saranno danni a persone e cose: inutile nascondersi dietro un dito», aggiunge. «Le norme europee già impongono misure di sicurezza alle aziende, in ambiti di importanza critica, anche se non a negozi al detta-

ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS6901 - S.30524 - L.1992 - T.1733

l'Espresso
Settimanale - Dir. Resp.: Emilio Carelli
Tiratura: 43178 Diffusione: 33007 Lettori: 944000 (Data Stampa 0006901)

DATA STAMPA
45° Anniversario



Foto: M. Nikoubazl / NurPhoto / Getty Images. F. Sandberg – Afp / Getty Images

glio – aggiunge Herpig. Ma il punto è far sì che le aziende adottino misure di base, nei loro stessi interessi».

Per capire quanto sia difficile, torniamo in Sicilia. «Sapevamo di essere a rischio, avevamo letto dell'attacco ai frigoriferi francesi a ottobre», dice Spadaro. L'Agenzia per la cybersecurity nazionale, del resto, aveva già mandato l'allarme due settimane prima. «Avevamo cominciato ad applicare le misure di sicurezza previste in questo caso, ma non siamo riusciti a farlo in tutti i supermercati: è una procedura lenta. Non pensavamo che potesse capitare così presto anche a noi», aggiunge. «Caso tipico di una pmi: non ha piena consapevolezza del rischio. Se l'avesse avuta, avrebbe accelerato le azioni e nel frattempo staccato da Internet i frigoriferi ancora esposti», dice Herpig. Stessa misura che ha consigliato il governo americano nei giorni scorsi, pure allarmato da quanto sta capitando in Europa. Enisa, governo italiano, agenzia cyber sono al lavoro in questi giorni per trovare soluzioni, sensibilizzare il settore.

«Sì, le autorità si danno da fare per rendere il Paese più sicuro sulla cyber, ma quest'attività va potenziata: la minaccia sta crescendo più veloce delle difese», dice Zanero. «I fondi pubblici disponibili non sono abbastanza», aggiunge. Nemmeno le aziende spendono quanto serve, in media: «la spesa in cyber in Italia è 2,7 miliardi di euro nel 2025. In rapporto al Pil è un terzo rispetto a Usa e Regno Unito», dice Faggioli, con dati Clusit e Politecnico di Milano. «A quanto risulta dalle prime stime sul 2026, che pubblicheremo, il divario con il resto d'Europa si sta riducendo ma solo di poco. Il ritardo accumulato in anni di sottovalutazione del pericolo è ancora grande», aggiunge. Le previsioni Mordor Intelligence sul 2026 confermano che l'Italia è ultima per spesa cyber in rapporto al Pil tra i grandi Paesi europei (sotto Germania, Francia, Spagna). «Importante che l'Italia si fortifichi nella cyber così come sta facendo sul piano militare. Il governo l'ha capito ma non ha chiaro cosa fare di preciso», dice Zanero. «Le nostre tante pmi non ce la fanno da sole: hanno bisogno di un supporto più forte dallo Stato», aggiunge. Su questo fronte, secondo gli esperti, lo scatto non è ancora avvenuto. Vale per tutti i Paesi Ue, ma in Italia è un problema più grande a causa del nostro tessuto fatto di pmi. Adesso la speranza è che la svolta avvenga prima di un attacco più devastante. «Ma limitarsi a sperare che non capiti qualcosa di brutto è il tipico e peggiore errore che si possa fare, nella cybersecurity», dice Herpig. In Sicilia, e non solo lì, l'hanno ormai capito. 'E

I danni sono comunque ingenti tra merci deteriorate e crollo di consumi. Sulla prevenzione dei danni si fa ancora poco. "E le risorse pubbliche sono insufficienti", dicono gli esperti

© RIPRODUZIONE RISERVATA

ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS6901 - S.30524 - L.1992 - T.1733