Il Messaggero
03-NOV-2026
da pag. 1-2 / foglio 1 / 2
Quotidiano - Dir. Resp.: Roberto Napoletano
Tiratura: 63845 Diffusione: 52069 Lettori: 638000 (Data Stampa 0006901)

DATA STAMPA
45° Anniversario

COLPITI 9 PAESI, VERTICE A PALAZZO CHIGI

Data Stampa 6901-Data Stampa 6901

Hacker in Europa attacco ai supermercati Casi anche in Italia

▶Guasti ai banchi frigo in Toscana, Emilia, Sicilia

Allegri, Troili e il focus di Chiara Bruschi alle pag. 2 e 3

L'attacco hacker all'Europa In tilt i frigo dei supermercati tra Emilia, Toscana e Sicilia

▶Le catene della grande distribuzione alimentare colpite dai blitz digitali
Casi denunciati in 9 Paesi. L'Acn: sistemi di sbrinamento interrotti da remoto

IL COMMISSARIO UE ALL'AGRICOLTURA: «VOGLIONO BLOCCARE LE NOSTRE SCORTE» LA FRANCIA GIÀ COLPITA È CORSA AI RIPARI

L'ALLARME

Il sabotaggio striscia e prende forma con frigoriferi in tilt, a 50 gradi, l'intento è depauperare gli approvvigionamenti, costringendo a buttare tonnellate di cibo. L'ultima frontiera dei cyber attacchi colpisce i supermercati di sette paesi europei, prese di mira in Italia, la Sicilia, la Toscana e L'Emilia Romagna. Nella notte tra il primo e il 2 novembre hacker hanno colpito sistemi di refrigerazione in Svezia, Danimarca, Finlandia, Belgio, Lussemburgo, Estonia, Irlanda, Olanda e Italia, alterando da remoto le temperature fino a raggiungere, in alcuni casi, i 50 gradi. Colpiti diversi supermercati in Sicilia, «in alcuni punti vendita Coop, almeno tre a Catania e uno a Palermo, si sono verificati attacchi ai sistemi di refrigerazione dei banchi alimentari», spiega Giuseppe Spadaro, direttore generale del gruppo Radenza, che gestisce supermercati a marchio Coop. L'attacco, che non è stato denunciato all'Agenzia per la Cybersicurezza, ha portato al surriscaldamento dei banchi, provocando un deperimento degli alimenti. La polizia postale sta ricostruendo la provenienza degli attacchi e se vi siano collegamenti con quanto accaduto negli altri Paesi europei. In concomitanza altre due aziende italiane sono finite nel mirino di attacchi informatici: un'impresa toscana attiva nella ristorazione collettiva ha già notificato l'incidente all'Agenzia per la cybersicurezza nazionale nell'ambito della normativa Nis, mentre un secondo attacco è stato rilevato ai danni di un'azienda emiliana che produce surgelati e non risulta ancora notificato. Dalle prime indagini dell'Agenzia per la cybersicurezza nazionale è emerso che «tramite lo sfruttamento di installazioni obsolete, interfacce di amministrazione esposte direttamente su Internet e carenze nei meccanismi di autenticazione, l'attacco ha consentito due diverse azioni. Da una parte, l'attivazione remota dei cicli di sbrinamento, dall'altra la modifica dei parametri operativi degli impianti. In entrambi i casi la conseguenza è stata l'interruzione della catena del freddo. Ingenti le quantità di cibo rovinato, con annessi danni economici». L'Agenzia raccomanda, «qualora non sia già stato fatto», di procedere con la massima urgenza alla verifica dell'eventuale esposizione su Internet dei sistemi di controllo e teleassistenza. Nonché, alla loro segregazione in ambienti protetti, separati dalle reti informatiche aziendali. Tra le ulteriori misure indicate figurano «il rafforzamento degli accessi da remoto attraverso VPN e l'autenticazione a più fattori, la verifica degli account privilegiati e l'aggiornamento o la sostituzione dei dispositivi non più supportati dai produttori». Cosa che ha da poco fat-





ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS6901 - S.30524 - L.1979 - T.1619

Il Messaggero
Quotidiano - Dir. Resp.: Roberto Napoletano
Tiratura: 63845 Diffusione: 52069 Lettori: 638000 (Data Stampa 0006901)

DATA STAMPA
45° Anniversario

to la Francia.

L'ESTERO

Il gruppo industriale danese Danfoss conferma il coinvolgimento dei propri prodotti, già colpiti a ottobre. «Siamo in stretto contatto con i clienti e li stiamo aiutando a gestire la situazione». In Belgio coinvolti decine di supermercati Delhaize, 15 punti vendita Carrefour e 5 negozi Spar. Per la tv olandese Nos, gli aggressori avrebbero attivato da remoto la modalità di sbrinamento degli impianti, provocando un aumento anomalo delle temperature, alcuni negozi hanno usato camion refrigerati per salvare la merce. Problemi anche nei supermercati Delhaize in Lussemburgo. Lo stesso in Svezia, con attacchi nei punti vendita ICA e Coop. A Böda, sull'isola di Öland, un congelatore ha raggiunto i 55 gradi. In Estonia, gli hacker hanno violato il computer che controllava l'impianto frigorifero di un supermercato Selver, impostando la temperatura a 50 gradi. In Irlanda, la catena SuperValu ha ritirato per precauzione i prodotti freschi e surgelati da 13 supermercati; in Finlandia in alcuni negozi della catena K-store sono state riscontrate anomalie di temperatura negli impianti di refrigerazione. In Italia è scattato l'alert dell'Agenzia nazionale cybersicurezza.

LE PREOCCUPAZIONI

«Il ripetersi degli attacchi informatici è profondamente preoccupante. Un tentativo deliberato di interrompere la nostra catena di approvvigionamento alimentare e di minare la fiducia dei consumatori: un monito che va preso sul serio», spiega il commissario Ue all'agricoltura, Christophe Hansen, assicurando che la «sicurezza alimentare» in Ue «non è attualmente a rischio, ma lo spreco alimentare e l'impatto sulle imprese sono reali» e che solleverà la «questione con i miei colleghi commissari nella nostra prossima riunione» del collegio Ue. Si tratta del secondo attacco in due mesi. A ottobre gli hacker hanno preso di mira centinaia di supermercati francesi sabotando i sistemi digitali che permettono di controllare a distanza frigo e congelatori: se vulnerabili, possono essere manipolati attraverso internet. Non risultano rivendicazioni e resta da chiarire se dietro questi attacchi ci sia quanto meno l'avallo di uno stato nemico, come la Russia, interessato a destabilizzare l'Unione Europea.

Raffaella Troili

© RIPRODUZIONE RISERVATA

ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS6901 - S.30524 - L.1979 - T.1619