04-NOV-2026
da pag. 1-15 /foglio 1 / 2

Il Sole 24 ORE
Quotidiano - Dir. Resp.: Fabio Tamburini
Tiratura: 50225 Diffusione: 103693 Lettori: 715000 (Data Stampa 0006901)

DATA STAMPA
45° Anniversario

VERTICE A PALAZZO CHIGI

Hacker nella Gdo, il governo: nessun allarme ma sistemi da aggiornare

—Servizi a pag. 15

Il governo sugli hacker dei frigo: «Le aziende aggiornino i sistemi»

Il ministro dell'Interno Matteo Piantedosi parla del rischio di una «azione coordinata a livello europeo»

Cybersicurezza

Vertice a Palazzo Chigi con Mantovano: no allarmi ma adeguare i software

Inascoltato l'alert Acn del 13 ottobre dopo il caso francese

Ivan Cimmarusti
Manuela Perrone
ROMA

Il primo messaggio del Governo è una rassicurazione ai cittadini: l'impatto degli attacchi hacker ad alcuni sistemi di refrigerazione commerciale in Italia «è al momento fortemente limitato» e non è emerso alcun caso di rischio per la salute collegato a fenomeni di scongelamento dei prodotti. Il secondo suona invece come un monito alle imprese: i cyberattacchi hanno interessato «poche unità commerciali, per lo più munite di sistemi di sicurezza obsoleti, con interfacce esposte direttamente su Internet e carenze nei meccanismi di autenticazione».

A chi non si è adeguatamente preparato a fronteggiare le minacce è indirizzato l'alert emerso al vertice convocato ieri a Palazzo Chigi dal sottosegretario alla presidenza del Consiglio, Alfredo Mantovano, con il ministro dell'Agricoltura, Francesco Lollobrigida, il direttore dell'Agenzia per la cybersicurezza nazionale, Andrea Quacivi, e i numeri uno delle agenzie di intelligence, Bruno Valensise dell'Aisi e Giovanni Caravelli dell'Aise.

«Le aziende devono aggiornare i sistemi di protezione», sintetizza senza mezzi termini una fonte governativa. Perché gli attacchi di due giorni fa hanno dimostrato che la gran parte della catena di distribuzione risulta dotata di software aggiornati, in grado di respingere intrusioni malevole. Ma dove c'è l'inadempienza, là si aprono falle in grado di minare la sicurezza. Vale per il settore alimentare, ma non solo.

L'Esecutivo non ritiene dunque, almeno per ora, di dover intervenire con modifiche legislative o amministrative. Promette però di continuare a muoversi lungo quattro direttrici. Si va dal monitoraggio e analisi della minaccia, attività che il Governo segnala essere stata avviata «da mesi», al dialogo costante con i fornitori e i venditori della filiera alimentare; dall'individuazione e tempestiva notifica dei soggetti esposti alla diffusione su larga scala di comunicazioni preventive alle indicazioni per mitigare i rischi negli ambiti interessati.

«Non sussiste alcun allarme», è la conclusione, «ma permane la massima attenzione da parte di tutti i soggetti istituzionali competenti».

L'esortazione alle imprese ad aggiornare i software non nasce dal nulla. Ha una data: 13 ottobre, all'indomani delle incursioni cyber ai frigoriferi dei supermercati francesi. L'Agenzia per la cybersicurezza nazionale aveva già indicato il rischio. E la contromisura era chiara: mettere in sicurezza e aggiornare i sistemi che governano la catena del freddo. Un avvertimento arrivato in anticipo. Ventuno giorni dopo emerge che alcune aziende non hanno adeguato i sistemi né adottato le contromisure suggerite.

Il bollettino parlava direttamente a supermercati, operatori della logistica alimentare, aziende della refrigerazione industriale e manutentori. E descriveva uno scenario che, tre settimane dopo, si sarebbe riproposto in Italia. In Francia gli hacker avevano trovato la porta aperta nei punti più fragili: impianti obsoleti, pannelli di comando esposti direttamente su Internet, password deboli o addirittura predefinite. Una volta dentro, avevano azionato da remoto lo sbrinamento, modificato le temperature e interrotto la corretta conservazione delle merci. Il risultato: prodotti compromessi e danni economici ingenti.

La minaccia sul ciclo del freddo resta comunque sotto osservazione. Il ministro dell'Interno Matteo Piantedosi ha parlato di un'azione «coordinata a livello europeo da parte di qualcuno che ha un contenuto di ostilità evidente». E il dossier è entrato anche nell'audizione al Copasir del direttore dell'Aisi Bruno Valensise. Il quadro nel quale si inseriscono gli attacchi alla catena del freddo è, del resto, più ampio. L'Italia è tra i Paesi europei maggiormente esposti alle incursioni informatiche e il rapporto Clusit relativo al secondo semestre 2026 (si veda il grafico) segnala soprattutto un salto nella gravità degli incidenti: una parte consistente degli eventi si è spostata dalle categorie «Medium/Low» verso il livello «High».





ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS6901 - S.30524 - L.1956 - T.1991

Il Sole 24 ORE
Quotidiano - Dir. Resp.: Fabio Tamburini
Tiratura: 50225 Diffusione: 103693 Lettori: 715000 (Data Stampa 0006901)

DATA STAMPA
45° Anniversario

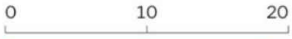
È anche per questo che ieri il direttore generale dell'Acn, Andrea Quacivi, ha incontrato rappresentanti del ministero dell'Agricoltura e alcuni tra i principali operatori della distribuzione e dell'industria alimentare: Coop, Conad, Federdistribuzione, Barilla, Gros, Galbani, Esselunga, Gs, Metro e Pam Panorama. Sul tavolo anche l'ipotesi di un Isac di settore, una rete per condividere in tempo reale informazioni sulle minacce cyber, collegata all'Isac Italia dell'Acn. L'obiettivo è rafforzare la capacità di risposta di un comparto strategico per il Paese.

© RIPRODUZIONE RISERVATA

I settori colpiti

Vittime in Italia - I semestre 2026

SETTORE	QUOTA %
Manifatturiero	18,4
Obiettivi multipli	18,0
Governo, difesa e forze dell'ordine	11,0
Commercio	8,6
ICT	8,6
Trasporti e logistica	5,3
Servizi professionali	4,1
Istruzione	4,1
Ricettività e ristorazione	3,7
Telecomunicazioni	2,9
Finanza e assicurazioni	2,9
Arte e intrattenimento	2,9
Altri servizi	2,4
Informazione e multimedia	2,0
Organizzazioni	1,6
Edilizia	1,6
Energia e utility	1,2
Sanità	0,8



Fonte: © Clusit - Rapporto 2026 sulla Cybersecurity - Aggiornamento giugno 2026

ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS6901 - S.30524 - L.1956 - T.1991