Attacchi hacker in Italia, vertice al Viminale per rafforzare le difese informatiche

Data: 11 settembre 2026 | Autore: Redazione



Scuole, aeroporti e infrastrutture al centro delle verifiche sulle vulnerabilità digitali. Restano da chiarire origine e collegamenti tra le offensive degli ultimi giorni

La risposta agli **attacchi hacker in Italia**passa da una verifica dei sistemi più esposti e dal coordinamento delle indagini. Il ministro dell'Interno **Matteo Piantedosi** ha convocato per **martedì 10 novembre al Viminale**il Comitato nazionale per l'ordine e la sicurezza pubblica, con l'obiettivo di esaminare i rischi legati alla minaccia informatica e valutare le misure di protezione. adnkronos.com

Il confronto dovrà affrontare due questioni strettamente collegate: individuare le vulnerabilità che possono agevolare nuove intrusioni e ricostruire le responsabilità degli episodi recenti. La diversità degli obiettivi colpiti rende necessario distinguere i singoli casi, senza dare per accertata un'unica regia.

Falsi allarmi negli aeroporti, verifiche sulle email delle scuole

Una delle piste investigative riguarda la possibilità che alcuni **messaggi minatori indirizzati agli aeroporti**siano stati inviati attraverso caselle di posta elettronica scolastiche compromesse. L'ipotesi resta da confermare e potrebbe portare a un approfondimento sulle difese digitali degli istituti. Ansa.it

Il tema riguarda anche le conseguenze indirette di un'intrusione. Una casella violata può diventare uno strumento per inviare comunicazioni fraudolente sfruttando l'identità di un'organizzazione. La protezione della posta elettronica assume quindi un ruolo che va oltre la riservatezza dei messaggi e coinvolge l'affidabilità delle comunicazioni istituzionali.

Dai dati personali ai sistemi di refrigerazione

L'attenzione delle autorità si concentra su episodi differenti, dalla diffusione di **dati personali sul dark web** alle intrusioni nei sistemi della **catena del freddo**. In quest'ultimo caso sono stati segnalati interventi da remoto sulle centraline di frigoriferi e congelatori, con modifiche alle temperature e danni alle merci. adnkronos.com

Questi casi mostrano perché la sicurezza informatica riguardi anche il funzionamento delle attività quotidiane. Quando un dispositivo connesso controlla un processo fisico, un accesso abusivo può produrre conseguenze operative ed economiche, oltre alla perdita o alla sottrazione di informazioni.

La ricognizione delle strutture vulnerabili servirà dunque a individuare le esposizioni più urgenti e a valutare **protocolli di protezione più rigorosi**, commisurati ai servizi da tutelare.

Eventi cyber in aumento, cosa indicano i numeri

Il quadro riportato nel testo evidenzia una crescita delle segnalazioni. Nei primi nove mesi del 2026 risultano **3.271 eventi cyber**, contro i 2.729 dell'intero 2025. Di questi, **1.992 sono stati classificati come incidenti**, ossia eventi con un impatto confermato.

Nello stesso periodo sono stati individuati quasi **45 mila asset e servizi a rischio**, mentre oltre 3.200 asset sono risultati potenzialmente compromessi. Ansa.it

La distinzione è essenziale per leggere correttamente i dati: un servizio vulnerabile non coincide automaticamente con un sistema violato, così come una potenziale compromissione richiede verifiche prima di essere considerata accertata.

Responsabilità da chiarire e coordinamento europeo

Alcune azioni sono state rivendicate dal collettivo filorusso **NoName**, ma l'attribuzione dell'intera sequenza di attacchi resta aperta. Le rivendicazioni devono essere confrontate con gli elementi investigativi per stabilire eventuali collegamenti tra autori, strumenti e obiettivi. Ansa.it

La dimensione internazionale della minaccia rende centrale lo scambio di informazioni tra i Paesi coinvolti. Il confronto europeo può aiutare a riconoscere schemi comuni e a ricostruire campagne che attraversano reti e territori diversi.

Sul piano politico, **Antonio Tajani** ha chiesto una risposta condivisa del **G7**, richiamando l'attenzione sui rischi della guerra ibrida. Il ministro ha inoltre distinto la vicinanza politica dei gruppi hacker dall'eventuale responsabilità di uno Stato, che richiede prove specifiche. Sky TG24

Dal vertice del Viminale sono quindi attese valutazioni sulle priorità di intervento: protezione dei sistemi esposti, prevenzione delle intrusioni e coordinamento delle attività investigative. Le eventuali nuove misure dovranno essere definite sulla base delle verifiche, mentre prosegue l'accertamento

delle responsabilità.

Articolo scaricato da www.infooggi.it
https://www.infooggi.it/articolo/attacchi-hacker-in-italia-vertice-al-viminale-per-rafforzare-le-difese-informatiche/158044