Allarmi bomba e frigoriferi, l'Italia dentro la guerra ibrida. Come difendersi dagli hacker che attaccano banche, sanità, trasporti e acquedotti di Rinaldo Frignani

Gli 007, insieme con Digos, polizia postale e Agenzia per la cybersicurezza nazionale lavorano per individuare chi minaccia il nostro Paese. Un'ondata di attacchi senza precedenti per terrorizzare l'opinione pubblica (Fonte: https://www.corriere.it/ 6 novembre 2026)



Un’escalation di cyber attacchi e falsi allarmi bomba nell’arco di pochi giorni. Uno scenario senza precedenti che per la prima volta con questa intensità coinvolge l’Italia oltre che mezza Europa. E il sospetto — più volte sottolineato dal ministro della Difesa Guido Crosetto e dal capo di Stato maggiore dell’Esercito Carmine Masiello — è che si tratti di azioni da guerra ibrida e cognitiva per destabilizzare e **impaurire l’opinione pubblica alla vigilia delle elezioni del prossimo anno.** Gli 007, la Digos, la polizia postale e l’Agenzia per la cybersicurezza nazionale sono impegnate in una gigantesca caccia agli hacker. **Anche perché le minacce si susseguono e puntano sempre più in alto: sanità, trasporti, forniture idriche ed elettriche**. Ma anche al sistema bancario e assicurativo, come ha sottolineato ieri in Senato il direttore dell’Acn Andrea Quacivi parlando di «minaccia cibernetica sempre più articolata e complessa, che può produrre effetti sull’affidabilità dei servizi, sulla fiducia dei cittadini e più in generale sulla stabilità del sistema Paese».

L’allerta sanitaria

La maggiore preoccupazione riguarda gli attacchi a settori strategici per l’assistenza della popolazione, primo fra tutti quello sanitario. Le misure di sicurezza sono state rafforzate **in tutta Italia dopo che in Francia** gli hacker sono riusciti a colpire le celle frigorifere in cui vengono conservate le scorte di sangue donato, compromettendo i sistemi di monitoraggio e controllo in tre sedi. **L’Etablissement francais du sang (l’ente francese per il sangue)** ha assicurato che non è stato perduto alcun prodotto ematico. Ma il pericolo che le azioni abbiano successo non è scongiurato. Del resto negli anni scorsi la sanità italiana è stata presa di mira più volte dagli incursori informatici, fra gli episodi più gravi il ricatto milionario alla Regione Lazio che durante il Covid provocò il blocco delle prenotazioni dei vaccini.

La catena del freddo

L’infiltrazione nei sistemi informatici della grande distribuzione alimentare con modifiche a distanza della catena del freddo nelle celle frigorifere per causare **il maggior danno economico possibile ha messo in ginocchio numerose aziende in molti Paesi europei** e anche in Italia si sono registrati casi da Nord a Sud con la perdita di tonnellate di prodotti. In Liguria, Veneto, Abruzzo, Sicilia, Molise, Friuli-Venezia Giulia e anche a Roma e provincia. Gli hacker filorussi dei gruppi NoName057(16) e Z-Pentest hanno rivendicato le azioni — **anche se non ci sono conferme ufficiali** che siano stati proprio loro — annunciando altri raid «ai sistemi di approvvigionamento idrico, alle centrali elettriche, agli impianti industriali» oltre che «ai siti di stoccaggio degli alimenti».

Trasporti nel mirino

Attacchi di tipo ddos, con la saturazione e quindi il blocco dei sistemi informatici provocati da milioni di richieste d’accesso da pc zombie sparsi per il mondo, hanno preso di mira i trasporti pubblici e privati. Per gli esperti quello appena passato è stato un ottobre nero. In Italia i Noname – o presunti tali – **hanno colpito la logistica, bloccando quindi ordini, spedizioni e consegne,** e anche società partner del ministero dei Trasporti. Presa di mira anche la Farnesina. **I danni sono stati mitigati grazie alle contromisure adottate.** Ma rimangono i timori che nel mirino finiscano asset operativi con conseguenze, ad esempio, per la circolazione ferroviaria o autostradale. Per non parlare di quella aerea, sotto pressione proprio in questi giorni con le false segnalazioni di bombe a bordo arrivate per mail, in Italia, ai dipendenti di Aeroporti di Roma che hanno costretto all’atterraggio d’emergenza una decina di velivoli.

Gli acquedotti e le scuole

Ma lunedì scorso un’altra mail ha fatto scattare l’allarme in 280 istituti scolastici italiani, molti dei quali evacuati, per l’annunciata — e falsa — presenza di ordigni esplosivi. In questo caso è stato «bucato» il sistema informatico di una delle scuole e gli hacker, **presunti terroristi islamici, hanno poi ottenuto la mailing list con gli indirizzi di tutte le altre**. È stata rafforzata la vigilanza dei

sistemi che gestiscono gli acquedotti, grandi e piccoli, interessati a ottobre da una maxi esercitazione sull'impronta di quella negli Usa del mese precedente. Obiettivo: scongiurare l'alterazione a distanza i parametri chimici dell'acqua.

Le contromisure

L'Agenzia per la cybersicurezza ha diramato un'allerta chiedendo di segnalare immediatamente qualsiasi attacco o incidente alle autorità di polizia, rinforzare **le protezioni degli accessi ai sistemi informatici** (con autenticazione a due fattori anche per i canali social e per le mail, con password forti e cambiate di frequente, insieme con l'aggiornamento costante dei sistemi operativi) e la «segregazione», ovvero la separazione, di quelli strategici rispetto a quelli aziendali.