▶ I PIRATI DELLA RETE

Treni, dighe e istituzioni L'Occidente si scopre indifeso davanti alla minaccia hacker

Allerta sulla sicurezza dei trasporti negli Stati Uniti. Mentre in Norvegia un gruppo filorusso ha dato una dimostrazione di forza. Corsa contro il tempo per proteggersi

di **STEFANO PIAZZA**

■ Negli ultimi mesi si è andato delineando un quadro allarmante che attraversa gli Stati Uniti e l'Europa: le infrastrutture critiche, dai treni alle dighe fino alle reti elettriche, sono sempre più esposte a intrusioni informatiche e operazioni ibride che mirano non soltanto a causare danni materiali, ma soprattutto a generare panico, disordini e perdita di fiducia nei sistemi statali.

La scorsa settimana la Cisa (Cybersecurity and infrastructure security agency) statunitense ha diffuso un avviso riguardante la vulnerabilità Cve-2025-1727, una falla che colpisce i sistemi di comunicazione ferroviaria. In particolare, il problema interessa i dispositivi End-of-train (Eot) e Head-of-train (Hot), collegati tramite un protocollo radio che, per ragioni storiche, non prevede né cifratura, né autenticazione. In altre parole, chiunque disponga di una radio software-defined può intercettare e inviare pacchetti malevoli, fino a impartire comandi ai freni di un convoglio.

Secondo l'avviso di Cisa, «lo sfruttamento di questa vulnerabilità potrebbe consentire a un aggressore di impartire comandi di frenata al dispositivo di fine treno, causando un arresto improvviso con possibili guasti o interruzioni operative». Il rischio non è teorico: **Neil Smith**, uno dei ricercatori che già nel 2012 individuò la falla, ha dichiarato che con meno di 500 dollari di attrezzatura è possibile fermare un treno merci o passeggeri a distanza, creando condizioni pericolose e, potenzialmente, deragliamenti.

Nonostante i ripetuti allarmi, l'Association of american railroads (Aar) ha per anni minimizzato la questione, respingendo anche un'inchiesta della *Boston Review*, che denunciava la scelta dell'industria di privilegiare i profitti rispetto alla sicurezza. Solo oggi l'associazione ammette la necessità di agire: dal 2026 dovranno essere sostituiti o aggiornati circa 70.000 dispositivi Eot e Hot.

Se negli Stati Uniti l'attenzione si concentra sui sistemi ferroviari, l'Europa ha già vissuto un episodio che ha reso tangibile la portata della minaccia. Lo scorso 7 aprile, in Norvegia, un gruppo di hacker filorussi ha preso il controllo di una diga a Bremanger, nella regione occidentale del Paese. Per quattro ore è stata aperta una paratoia che ha rilasciato circa 500 litri d'acqua al secondo, prima che i tecnici riuscissero a ripristinare il controllo. Non ci sono state vittime, ma l'incidente ha mostrato quanto siano fragili le infrastrutture energetiche di un Paese che dipende in larga parte dall'idroelettrico. Il direttore del servizio di sicurezza Pst, **Beate Gangas**, ha parlato di «operazione dimostrativa», chiarendo che l'obiettivo non era distruggere ma «mostrare capacità, influenzare e instillare paura o malcontento nella popolazione». Non un caso isolato: dal 2023, in Europa, sono state registrate decine di azioni attribuite a reti vicine a Mosca, dai sabotaggi agli incendi dolosi, tutte riconducibili a quella che gli analisti definiscono guerra ibrida. L'ambasciata russa a Oslo ha bollato le accuse come «infondate», ma l'intelligence norvegese considera Mosca la minaccia più pericolosa e imprevedibile per il Paese. L'episodio norvegese si inserisce in un mosaico più ampio che riguarda l'intero continente. A rendere ancora più evidente la fragilità delle infrastrutture europee sono stati i recenti blackout in Francia, che hanno lasciato intere regioni senza energia elettrica per ore. Sebbene le autorità abbiano attribuito gli episodi a guasti tecnici e sovraccarichi della rete, diversi esperti non escludono l'ipotesi di test ostili volti a mettere sotto pressione il sistema energetico nazionale. In un Paese che basa gran parte della sua produzione sull'energia nucleare e su una rete interconnessa con i vicini, un attacco mirato al sistema di distribuzione elettrica potrebbe avere conseguenze devastanti.

Anche la Germania non è rimasta immune. Negli ultimi anni Berlino è stata più volte bersaglio di attacchi informatici contro infrastrutture sensibili, con conseguenze dirette sulla sicurezza nazionale. Uno degli episodi più noti resta l'hackeraggio al Bundestag nel 2015, attribuito al gruppo russo Fancy Bear, che paralizzò i sistemi parlamentari e portò al furto di dati riservati. Ancora più drammatico fu l'attacco ransomware del 2020 contro l'ospedale universitario di Düsseldorf: il blocco dei sistemi informatici costrinse a deviare un'ambulanza e una paziente perse la vita, segnando il primo decesso collegato a un cyberattacco in Europa. Sul fronte energetico, il sabotaggio dei gasdotti Nord Stream nel 2022 ha rappresentato un colpo diretto alla sicurezza energetica europea, con indagini ancora aperte e recenti arresti. Nel 2024, inoltre, i servizi di intelligence hanno registrato una crescita di incursioni contro centrali elettriche e reti di distribuzione, spingendo la Germania ad avviare il progetto «Cyber dome» per rafforzare le proprie difese.

La combinazione di eventi - vulnerabilità dei sistemi ferroviari negli Stati Uniti, presa di controllo di una diga in Norvegia, blackout in Francia e attacchi in Germania - delinea un'unica tendenza: la guerra informatica non è più confinata agli scenari militari, ma si sposta sempre di più verso infrastrutture civili con lo scopo di colpire la vita quotidiana dei cittadini. Gli attori ostili, spesso legati a Stati o a gruppi filogovernativi, non mirano soltanto a danneggiare fisicamente, ma a produrre insicurezza diffusa, disagi economici e pressioni politiche. Il pericolo, spiegano gli analisti, è che la prossima escalation non riguardi più soltanto incidenti dimostrativi o blackout temporanei, ma vere e proprie operazioni coordinate. Un attacco simultaneo che combinasse l'arresto dei treni, l'apertura incontrollata di dighe e il blocco delle reti elettriche avrebbe l'effetto di paralizzare interi Paesi, generando caos e rendendo difficile distinguere tra sabotaggio e guerra convenzionale. In Europa molte infrastrutture critiche utilizzano ancora protocolli obsoleti, progettati in epoche in cui la minaccia cyber era inesistente. Gli ultimi episodi, mostrano che l'Occidente si trova davanti a una sfida sistemica. Non bastano più investimenti settoriali o risposte emergenziali: occorre un coordinamento europeo e transatlantico che unisca norme di sicurezza, investimenti tecnologici e capacità di risposta rapida.

PERICOLI In alto, la famosa Grand Central, snodo ferroviario che si trova proprio nel cuore di New York [iStock]. A sinistra, la diga di Bremanger, in Norvegia, usata per una prova di forza dagli hacker russi lo scorso 7 aprile: 500 litri d'acqua sono andati dispersi, ma poteva andare molto peggio

Pure in Italia si stanno moltiplicando i «colpi» informatici di alto livello

Impennata del 18% nel 2024. Il settore maggiormente bucato è la sanità (+83%)

■ Negli ultimi due anni l'Italia ha subito una crescita significativa di cyberattacchi contro infrastrutture strategiche, aziende e servizi pubblici. I dati diffusi dal Clusit e dall'Agenzia per la cybersicurezza nazionale (Acn) confermano che tra 2024 e 2025 la minaccia è aumentata in numero, intensità e sofisticazione, con impatti concreti sulla sicurezza nazionale. Nel 2024 sono stati registrati oltre 1.900 attacchi, +18% rispetto al 2023, di cui 467 classificati come incidenti gravi. La sanità è risultata il settore più vulnerabile, con un incremento dell'83%. Diversi ospedali hanno subito *ransomware* che hanno bloccato reparti e sottratto dati sensibili, poi comparsi nel dark Web.

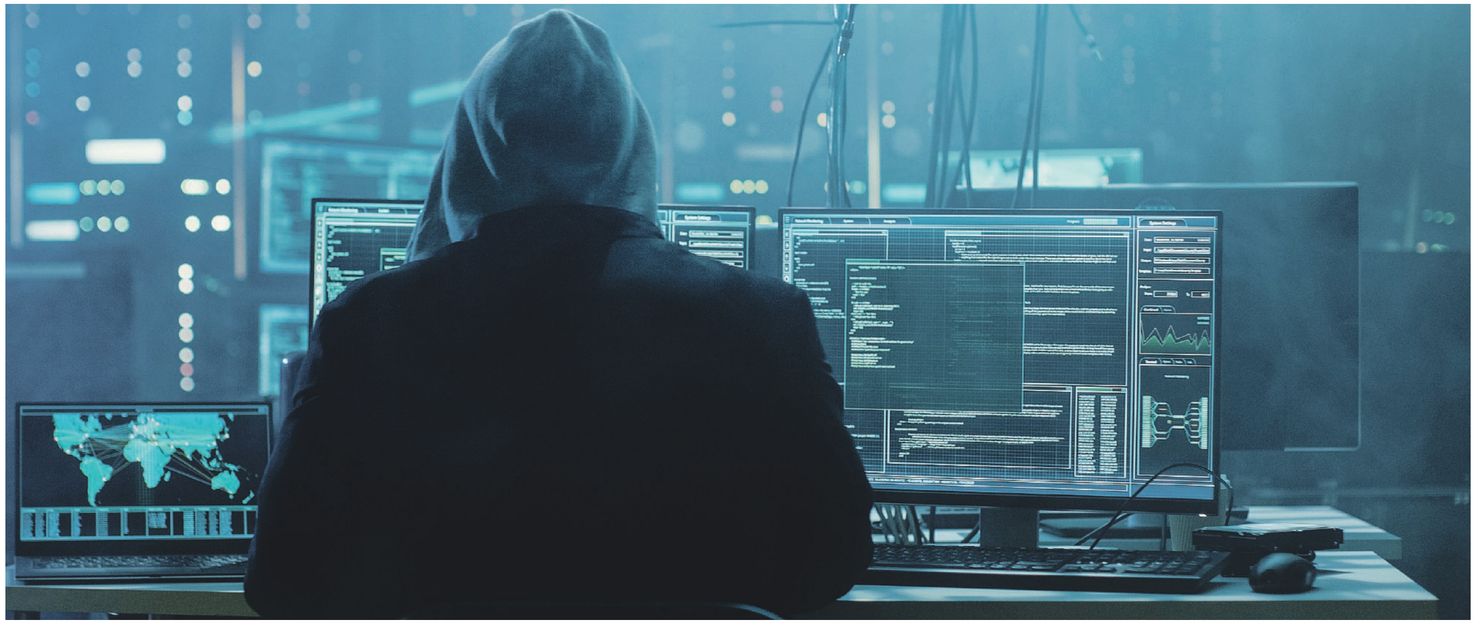
Il comparto manifatturiero ha pagato la scarsa protezione dei sistemi industriali, mentre reti energetiche e centrali elettriche hanno registrato intrusioni e tentativi di sabotaggio. Aumentato anche il furto di credenziali e di informazioni riservate: l'Italia si è collocata al quinto posto mondiale per e-mail compromesse. Il 2024 ha visto il boom di campagne di phishing alimentate da testi generati con Intelligenza artificiale, capaci di ingannare anche utenti esperti. In parallelo, dispositivi IoT non protetti - telecamere, router, sistemi di domotica - sono stati arruolati in botnet per attacchi DDoS contro portali pubblici e siti aziendali. Il 2025 segna un salto di qualità. Nel solo primo semestre sono stati censiti oltre 1.500 attacchi (+53%), con 346 incidenti gravi (+98%).

Non si tratta più soltanto di criminalità informatica, ma anche di offensive a carattere politico. Il collettivo filorusso NoName057(16) ha rivendicato azioni DDoS tra febbraio e marzo contro aeroporti (Linate, Malpensa), porti (Trieste, Taranto), ministeri, Guardia di finanza e persino Banca d'Italia. Attacchi spesso temporanei, ma dal forte valore simbolico: dimostrare la vulnerabilità dell'Italia, Paese Nato impegnato nel sostegno a Kiev.

Parallelamente, la Pubblica amministrazione è stata colpita da campagne di intrusione e blocchi dei sistemi digitali. Colpiti anche i servizi di telecomunicazione, con tentativi di rallentamento delle reti e intercettazione dei dati. Secondo il Rapporto Clusit 2025, quasi l'80% degli attacchi in Italia presenta un livello di gravità alto o critico. Non più episodi isolati, ma una minaccia sistemica che combina criminalità, hacktivismo e operazioni di influenza geopolitica. Sanità, energia, telecomunicazioni e Pubblica amministrazione sono ormai bersagli costanti. Per contrastare la crescita degli attacchi, l'Acn ha rafforzato le misure di prevenzione e coordinamento, con investimenti nei centri di monitoraggio e nella formazione. La Polizia postale ha avviato operazioni internazionali che a luglio 2025 hanno portato all'arresto di membri di NoName057(16) e al sequestro di server. Resta però il problema della resilienza complessiva. Molte aziende italiane, soprattutto pmi, non dispongono di adeguati sistemi di difesa. La sfida sarà migliorare la protezione delle infrastrutture critiche e diffondere una cultura della sicurezza informatica anche nei settori meno strutturati.

S. Pia.

SEGNALE La Banca d'Italia è già stata danneggiata [Ansa]



L'INTERVISTA **PIERLUIGI PAGANINI**

«Il tallone d'Achille del nostro Paese è il sistema energetico a 360 gradi»

L'esperto di cybersecurity: «Gli attacchi si stanno moltiplicando e gli investimenti continuano a essere insufficienti. Lo scudo tedesco è avanzato e si ispira a Israele, noi abbiamo ancora un approccio diverso»

■ Pierluigi Paganini è analista di sicurezza informatica in materia di cybersecurity e cyber intelligence.

Le ferrovie italiane presentano vulnerabilità simili a quelle emerse negli Usa sui sistemi ferroviari?

«Le reti ferroviarie in tutto il mondo si compongono di sistemi complessi per la gestione del traffico, la sicurezza e i servizi ai passeggeri. Sebbene negli Usa siano emerse vulnerabilità presenti in alcune di queste componenti, non abbiamo informazioni pubbliche relative a rapporti che indichino vulnerabilità simili nella nostra rete nazionale. Fatta questa premessa, è tecnicamente possibile che vi siano falle simili all'interno dei sistemi presenti nella nostra rete ferroviaria. I principali rischi sono legati al largo impiego di Scada (sistemi di controllo) e sistemi Ot spesso con componenti datate, l'integrazione di sistemi It-Ot (reti aziendali e reti industriali) che aumenta la superficie d'attacco, la presenza di fornitori esterni e appaltatori che utilizzano processi di sicurezza poco sicuri».

Quanto è esposto il sistema energetico italiano a cyberattacchi o sabotaggi come in Norvegia e Francia?

«Il sistema energetico italiano è esposto a minacce informatiche significative, analoghe a quelle che hanno colpito Norvegia e Francia. Gli attacchi informatici nel settore Energy & utilities sono aumentati negli ultimi anni. In risposta, l'Italia ha adottato normative come la direttiva NIS2 e la direttiva Cer, che impongono obblighi di sicurezza più stringenti per le entità critiche nel settore energetico. Tuttavia, la consapevolezza e gli investimenti in cybersecurity rimangono insufficienti, con molte organizzazioni che non dispongono di risorse adeguate ad affrontare le minacce emergenti».

L'Italia dispone di un piano di difesa delle infrastrutture critiche paragonabile al «Cyber dome» tedesco?

«L'Italia dispone di un Piano nazionale per la protezione cibernetica e la sicurezza informatica che coinvolge molteplici ministeri e agenzie, con l'obiettivo di rafforzare la difesa delle infrastrutture critiche, migliorare la risposta alle minacce cibernetiche, promuovere cooperazione pubblico-privato e cultura della sicurezza. Il piano è ovviamente in continua evoluzione. Rispetto al "Cyber dome", l'Italia ha un approccio strutturato ma non dispone ancora di un sistema così specifico e centralizzato. Il modello tedesco mira a integrare difesa militare e civile con sistemi di allerta rapida ispirati a Israele, mentre l'Italia punta soprattutto a integrare e coordinare le capacità nazionali in modo più orizzontale tra istituzioni e aziende, in linea con le direttive Ue».

> *Il livello di esposizione è sicuramente elevato Un'aggressione simultanea potrebbe essere fatale*

Qual è oggi il livello di esposizione dell'Italia agli attacchi ibridi attribuiti a reti filorusse, iraniane o cinesi?

«Il livello di esposizione per il nostro Paese è sicuramente elevato. L'Italia è esposta a una significativa minaccia ibrida attribuita a reti filorusse, iraniane e cinesi. Gruppi filorussi come Noname057(16) e Killnet continuano a condurre attacchi DDoS e campagne di disinformazione mirate a destabilizzare istituzioni e organizzazioni italiane, spesso legate al sostegno italiano all'Ucraina. La Cina invece si distingue per le attività di spionaggio cyber nei confronti delle nostre imprese e istituzioni. Infine, le operazioni riconducibili al governo iraniano sono principalmente di sabotaggio, soprattutto in Medio Oriente, ma con rischi per infrastrutture critiche europee, inclusa l'Italia».

In caso di attacco simultaneo a trasporti, dighe ed energia, quali sarebbero i punti più deboli dell'Italia?

«L'Italia, come altri Paesi, presenta diversi punti deboli in caso di attacco simultaneo a infrastrutture critiche. La forte interconnessione tra sistemi operativi industriali (Ot) e informatici (It) facilita la propagazione delle minacce tra settori critici. Inoltre, la diffusione di dispositivi IoT vulnerabili amplia la superficie d'attacco. Le supply chain digitali complesse rappresentano un ulteriore rischio. Mancano piani di risposta agli incidenti maturi in molte pmi coinvolte e la risposta stessa resta lenta e poco coordinata. È auspicabile un miglior coordinamento pubblico-privato per garantire una risposta efficace e tempestiva, riducendo così il rischio di interruzioni significative e danni economici e sociali».

> *Dalla Cina bisogna temere lo spionaggio Dall'Iran operazioni di sabotaggio*

S. Pia.

ALLARME ROSSO Pierluigi Paganini, analista [Imagoeconomica]