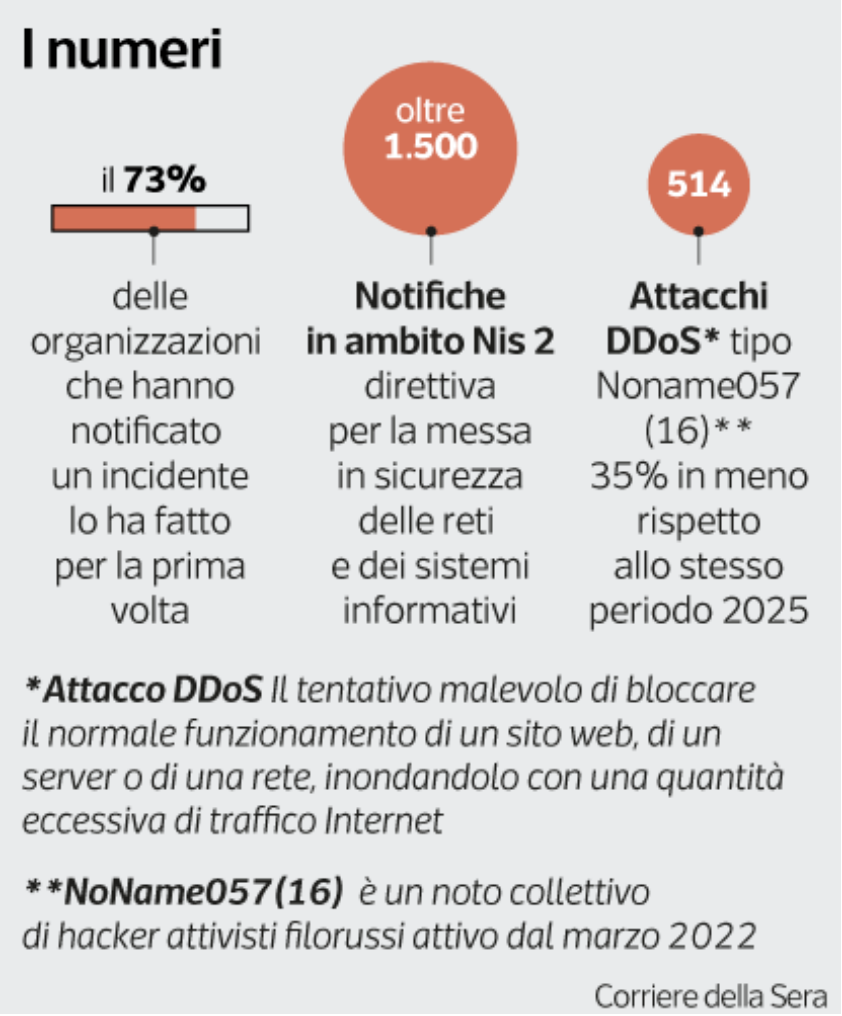
Hacker, gli asset strategici a rischio: sanità, treni, acqua di Rinaldo Frignani

Il dossier cybersicurezza: 177 strutture strategiche sotto minaccia ogni giorno.Triplicati rispetto al 2025 gli interventi per difenderle

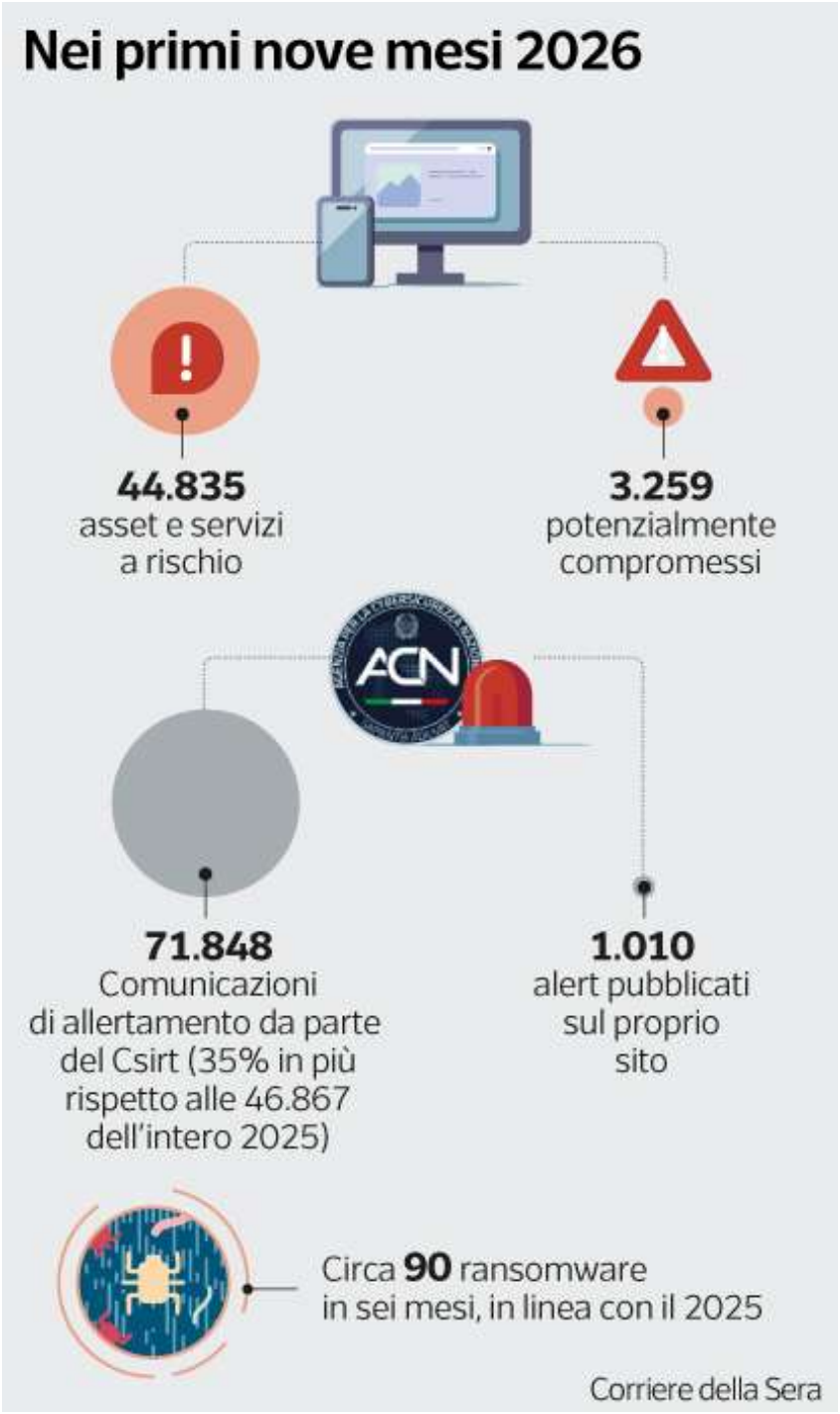
(Fonte: https://www.corriere.it/ 10 novembre 2026)

Centosessantasette asset strategici a rischio ogni giorno in Italia, 12 dei quali «potenzialmente compromessi». È la conferma che nei primi nove mesi del 2026 **l'azione degli hacker** si è intensificata nell'ambito di quella che, senza mezzi termini, il ministro della Difesa **Guido Crosetto con i vertici delle forze armate** definiscono **una guerra ibrida e cognitiva che già coinvolge il nostro Paese.** È questo forse il dato che più di tutti fotografa la situazione attuale (ottobre e forse anche novembre potrebbero peraltro riservare **altre sorprese**) e a scattarla **sono gli specialisti dello Csirt, la squadra di risposta rapida agli attacchi informatici dell'Agenzia per la cybersicurezza nazionale.** A essere presi di mira sono in particolare i servizi pubblici essenziali che rappresentano la spina dorsale nazionale e che non devono essere messi fuori gioco, pena immediate ripercussioni sulla vita di tutti i giorni.



Reti e imprese

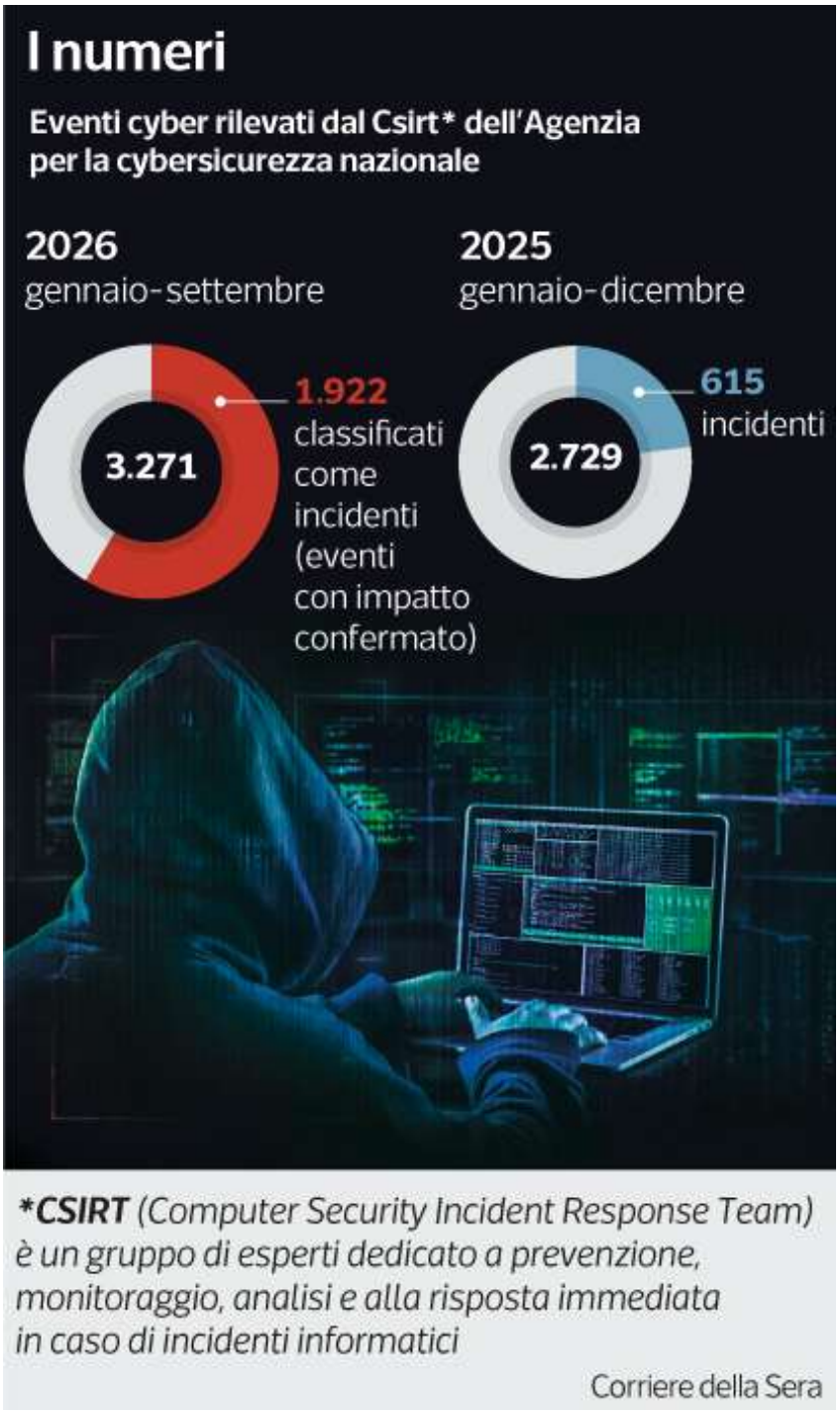
Ne abbiamo avuto una prova — anche se in Italia gli effetti sono stati minori — con **i raid alla grande distribuzione alimentare** che invece in Francia hanno messo in ginocchio intere catene di supermercati. Ma a rischio ci sono oggi **la sanità, i trasporti, le banche, la stessa sicurezza sul territorio**. Le reti idriche, al centro di esercitazioni mirate in diversi Paesi, ed elettriche. Le pubbliche amministrazioni, anche le piccole e medie imprese, i sistemi di telecomunicazione.



Gli attacchi nel 2026

Il quadro che emerge dall'analisi dei dati di 270 giorni di attività di quest'anno da parte del Csirt Italia è chiaro: gli eventi cyber rilevati dai tecnici sono stati 3.271, con 1.922 episodi classificati come «incidenti». Attacchi dunque con «impatto confermato». **Più del triplo rispetto ai 615 del 2025 su un totale di rivelazioni — in dodici mesi — di 2.729 situazioni che hanno richiesto l'intervento della squadra dell'Acn**. Ma se da una parte l'allerta aumenta, dall'altra si rileva anche — e finalmente, si potrebbe dire — una maggiore sensibilità da parte delle aziende, grandi e piccole, pubbliche e private, sul tema della cybersicurezza, forse anche sull'onda delle notizie che a ritmo quotidiano descrivono scenari sempre più preoccupanti. Il 73 per cento delle oltre 1.500 società ed enti italiani che fino al 30 settembre hanno inviato notifiche — nell'ambito della direttiva che obbliga per legge le imprese a proteggere le reti e i sistemi informatici — lo ha fatto **per la prima volta**. Un'attività di prevenzione indispensabile perché **gli attacchi sono continui**: in

calo comunque quelli ddos (514), cioè con il blocco dei sistemi, stabili i ricatti ransomware (una novantina fino a giugno). Come detto nel 2026 asset e servizi individuati a rischio sono stati 44.835, mentre quelli compromessi, a fine settembre, erano 3.259.



Gli elettrodomestici

Il Csirt ha quindi inviato quasi **72mila alert — più del doppio rispetto al primo semestre 2025 —** pubblicando sul proprio sito internet 1.010 avvertimenti pubblici generici destinati a «soggetti che non vengono raggiunti da comunicazioni puntuali, in quanto non espongono criticità». Che tuttavia sono imprevedibili, perché le azioni dei gruppi hacker — filorussi, filoiraniani, statuali e non, indipendenti oppure appartenenti ad altre sfere, che secondo gli esperti arrivano anche a crew vicine alla Corea del Nord e alla Cina — dimostrano che **nessun settore è immune dal rischio di essere attaccato**. Proprio ieri ad esempio Juhan Lepassaar, direttore esecutivo dell'Enisa — l'agenzia per la cybersicurezza dell'Ue — ha lanciato l'allarme anche sugli elettrodomestici e sui

routers domestici dopo che sono state colpite le celle frigorifere dei supermercati. «**Tutti gli incidenti possono essere evitati** — avverte — ma la questione è se siamo disposti a investire per farlo, perché la sicurezza informatica non è a buon mercato e deve essere prevista fin dalla fase di progettazione dei prodotti interconnessi, che ormai sono ovunque, comprese le nostre cucine o le nostre camere da letto».

Invece il Csirt Italia mette in guardia su **attacchi hacker destinati ai fornitori delle imprese che a loro volta potrebbero rimanere vittime di campagne di phishing** (cioè con delle mail trappola) e di azioni contro hardware e software non aggiornati. A dimostrazione che gli hacker sanno bene dove colpire, perché il fattore umano è a oggi ancora fondamentale. E quello è spesso il punto debole.

