

Cyberattacchi, in Italia già 3.271 eventi nei primi nove mesi del 2026: superato il dato dell'intero 2025 di Serena Palumbo

L'Agenzia per la cybersicurezza nazionale registra 1.922 incidenti con impatto confermato e 149 vittime di ransomware. Individuate anche 45 vulnerabilità zero-day, 35 ad alta gravità (Fonte: <https://www.corriere.it/> 13 ottobre 2026)



Sono 3.271 gli eventi cyber rilevati in Italia nei primi nove mesi del 2026, contro i 2.729 registrati nell'intero anno precedente. Tra loro, 1.922 hanno avuto un impatto confermato e, perciò, sono stati classificati come incidenti. **Numeri, tutti questi, presentati oggi dal direttore generale dell'Agenzia per la [cybersicurezza nazionale](#)** durante un'audizione alla Commissione Affari esteri e Difesa del Senato sul disegno di legge per il rafforzamento delle capacità di difesa nazionale.

Un aumento delle segnalazioni legato anche all'avvio - da gennaio 2026 - degli obblighi di notifica previsti dalla direttiva Nis2. **Tra le minacce più rilevanti restano gli attacchi ransomware**, ovvero quelli condotti con sistemi che bloccano l'accesso a dispositivi elettronici e file personali, chiedendo poi un riscatto per ripristinarli. Ed ecco che - stando ai dati registrati dal Computer security incident response team Italia (Csirt) - **ad averli subiti sono state 149 vittime da inizio anno**. Nel mirino soprattutto imprese manifatturiere, operatori finanziari e aziende tecnologiche, ai quali sono state interrotte le attività e resi non disponibili i dati. Ma, in diversi casi, al blocco dei sistemi si è aggiunta anche la sottrazione di informazioni, con la minaccia di renderle pubbliche per ottenere un riscatto.

I dati raccolti, però, non si fermano qui. Nei primi nove mesi dell'anno il monitoraggio dell'Acn ha inoltre individuato **quasi 45 mila asset e servizi esposti a rischio e più di 3.200 potenzialmente compromessi**. L'Agenzia ha inviato quasi 72 mila comunicazioni di allertamento e pubblicato oltre mille alert. Le attività di scrutinio tecnologico hanno consentito di scoprire nel 2026 anche 45 vulnerabilità zero-day, 35 delle quali caratterizzate da un livello di gravità elevato. Inoltre, **le tensioni geopolitiche continuano a riflettersi nel cyberspazio, attraverso campagne hacktiviste condotte soprattutto con attacchi DDoS** (un tentativo di bloccare un sito web, un server o una rete, inondandolo con una quantità massiccia di traffico o richieste). Da inizio anno ne sono stati registrati più di 500, il 35% in meno rispetto allo stesso periodo del 2025. Secondo l'Acn, gli impatti sono stati generalmente limitati, anche grazie all'attività di allertamento tempestivo del Csirt Italia.

Nel corso dell'audizione è stato sottolineato anche il ruolo della cooperazione tra istituzioni civili e militari nella gestione delle crisi informatiche. **Per l'Agenzia, il disegno di legge è coerente con l'assetto nazionale**: l'articolo 7 definisce lo «Spazio cibernetico di interesse nazionale per la difesa e la sicurezza militare dello Stato» e le attribuzioni del Capo di Stato maggiore della Difesa, nel rispetto delle competenze del presidente del Consiglio e degli altri soggetti dell'architettura cyber, compresa l'Acn.