PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6124 di Venerdì 17 luglio 2026

Relazione ACN 2025: cresce la minaccia cyber, aumenta la resilienza

La Relazione annuale al Parlamento dell'Agenzia per la Cybersicurezza Nazionale evidenzia l'aumento degli eventi informatici contro imprese e PA e il rafforzamento delle capacità nazionali di prevenzione, risposta e gestione degli incidenti.

La cybersicurezza nazionale continua a rappresentare un elemento strategico per la continuità operativa delle organizzazioni pubbliche e private. La Relazione annuale al Parlamento dell'Agenzia per la Cybersicurezza Nazionale (ACN), dedicata alle attività svolte nel 2025, fotografa un quadro caratterizzato da una crescita significativa delle attività malevole nel cyberspazio italiano, accompagnata tuttavia da una maggiore capacità di prevenzione, rilevazione e gestione degli incidenti.

Il documento evidenzia come il digitale sia ormai un'infrastruttura essenziale per il funzionamento dello Stato, dei servizi pubblici, del sistema produttivo e delle filiere industriali. La crescente interconnessione tra reti, sistemi informativi, servizi cloud e dispositivi tecnologici amplia però la superficie di attacco disponibile per criminali informatici, gruppi hacktivisti e attori con finalità geopolitiche.

Secondo i dati raccolti dal CSIRT Italia, nel corso del 2025 sono stati gestiti **2.729 eventi cibernetici**, con un incremento del **38% rispetto al 2024**. Gli incidenti con impatto confermato sono stati invece **615**, registrando una crescita più contenuta, pari al **7%**. Le vittime complessive hanno raggiunto quota **3.907**, con un aumento del 50% rispetto all'anno precedente.

Il dato più significativo riguarda il rapporto tra aumento degli attacchi e capacità di contenimento: la crescita degli eventi ostili non si è tradotta in un aumento proporzionale degli incidenti effettivamente dannosi. Questo andamento viene attribuito anche al rafforzamento delle attività di monitoraggio, allerta e supporto tecnico svolte dall'ACN e dal CSIRT Italia nei confronti dei soggetti potenzialmente coinvolti.

Pubblica Amministrazione nel mirino degli attacchi informatici

Tra i settori maggiormente colpiti emerge la Pubblica Amministrazione, seguita dai comparti delle telecomunicazioni e tecnologico. Gli enti pubblici rappresentano infatti obiettivi particolarmente rilevanti perché gestiscono grandi quantità di dati, erogano servizi essenziali ai cittadini e costituiscono nodi fondamentali dell'infrastruttura digitale nazionale.

Gli attacchi hanno avuto caratteristiche differenti: dalle campagne di tipo Distributed Denial of Service (DDoS), finalizzate a rendere indisponibili servizi online attraverso un sovraccarico delle infrastrutture, fino alle compromissioni di sistemi e account, al furto di informazioni e alle attività riconducibili al ransomware.

Nel corso dell'anno sono stati registrati picchi di attività ostile in particolare nei mesi di febbraio, giugno, settembre e ottobre, in corrispondenza di campagne DDoS rivendicate da gruppi hacktivisti nel contesto delle tensioni geopolitiche internazionali.

Le principali conseguenze degli incidenti cyber

L'analisi degli impatti mostra che gli attacchi non riguardano esclusivamente la disponibilità dei sistemi, ma sempre più spesso coinvolgono aspetti legati alla riservatezza e all'integrità delle informazioni.

Nel 2025 una quota rilevante degli incidenti ha determinato conseguenze sulla protezione dei dati, sulla disponibilità dei servizi digitali e sulla compromissione delle credenziali di accesso. Questo conferma come il fattore umano, la gestione delle identità digitali e la corretta configurazione dei sistemi rappresentino elementi centrali nella prevenzione degli incidenti.

Per le organizzazioni, quindi, la cybersecurity non può essere considerata soltanto un tema informatico affidato ai reparti IT, ma deve diventare parte integrante dei processi di gestione del rischio aziendale. La protezione delle informazioni, la continuità operativa e la capacità di risposta agli eventi cyber assumono un ruolo analogo alla gestione degli altri rischi organizzativi.

Il ruolo dell'ACN: prevenzione, coordinamento e sviluppo delle competenze

La Relazione evidenzia il ruolo crescente dell'Agenzia per la Cybersicurezza Nazionale come punto di riferimento per il coordinamento delle attività di sicurezza digitale del Paese. Le azioni dell'ACN comprendono il monitoraggio delle minacce, il supporto agli operatori colpiti, la diffusione di indicatori di compromissione e l'incremento delle capacità tecniche nazionali.

Nel corso del 2025 il personale tecnico dell'Agenzia è intervenuto direttamente in numerosi casi di incidente, fornendo supporto soprattutto a soggetti della Pubblica Amministrazione centrale e locale, al settore sanitario e alle organizzazioni tecnologiche.

Un altro elemento centrale riguarda la crescita delle competenze. La carenza di professionisti qualificati rappresenta infatti una delle principali criticità del settore cybersecurity. La costruzione di una cultura diffusa della sicurezza digitale richiede formazione continua, aggiornamento delle competenze e maggiore consapevolezza da parte di lavoratori, amministratori e responsabili dei processi aziendali.

Imprese e lavoratori: la cybersecurity entra nella gestione della sicurezza

L'evoluzione della minaccia cyber coinvolge direttamente anche il mondo della salute e sicurezza sul lavoro. Sebbene gli attacchi informatici siano tradizionalmente associati alla protezione dei dati e dei sistemi informativi, le conseguenze operative possono incidere sulla sicurezza complessiva delle organizzazioni.

Un blocco dei sistemi informatici può compromettere la gestione delle emergenze, la disponibilità di informazioni operative, il funzionamento di impianti industriali, la tracciabilità dei processi produttivi e l'erogazione di servizi essenziali.

Per questo motivo, la sicurezza informatica deve essere integrata nei modelli di gestione del rischio attraverso misure organizzative e tecniche:

- analisi periodica delle vulnerabilità;
- aggiornamento dei sistemi e applicazione delle patch di sicurezza;
- gestione rigorosa delle credenziali;
- autenticazione multifattore;
- formazione del personale contro phishing e tecniche di ingegneria sociale;
- procedure di backup e ripristino testate;
- piani di risposta agli incidenti.

La prevenzione diventa quindi un elemento comune tra cybersecurity e sicurezza organizzativa: ridurre la probabilità di un evento dannoso significa migliorare la resilienza complessiva del sistema.

Una minaccia in evoluzione: intelligenza artificiale e nuove tecniche di attacco

La Relazione ACN evidenzia inoltre come l'evoluzione tecnologica stia modificando rapidamente lo scenario delle minacce. Gli strumenti basati sull'intelligenza artificiale possono essere utilizzati dagli attaccanti per rendere più efficaci campagne di phishing, produzione di contenuti ingannevoli e attività di social engineering.

Parallelamente, anche le difese stanno integrando tecnologie avanzate per migliorare capacità di rilevamento, analisi automatizzata e risposta agli incidenti.

La sfida per il futuro sarà mantenere un equilibrio tra innovazione digitale e protezione dei sistemi, evitando che la crescita della trasformazione tecnologica aumenti la vulnerabilità delle infrastrutture critiche.

Conclusioni

La Relazione annuale al Parlamento dell'ACN 2025 descrive un'Italia più esposta alle minacce informatiche, ma anche più preparata rispetto al passato nel rilevare e contenere gli attacchi.

L'aumento degli eventi cyber conferma che nessuna organizzazione può considerarsi estranea al rischio informatico. La cybersecurity diventa quindi una componente strutturale della sicurezza aziendale e della resilienza nazionale.

Per imprese, enti pubblici e lavoratori la priorità non è soltanto difendersi dall'attacco, ma sviluppare una capacità permanente di prevenzione, risposta e adattamento. In un contesto digitale sempre più complesso, la sicurezza informatica rappresenta una condizione necessaria per garantire continuità, affidabilità e tutela delle persone e dei servizi.

Agenzia per la Cybersicurezza Nazionale - Relazione annuale al Parlamento 2025

RXY