Rapporto Clusit, I semestre 2026: record di incidenti cyber nel mondo. In Italia il Manufacturing è il settore più colpito, segnali positivi per sanità ed energia

Nel mondo 4.911 incidenti noti, il numero più alto mai registrato in un semestre. In Italia sono 245 e la quota sul totale mondiale scende al 5%: cala l'hacktivism, cresce il cybercrime rivolto alle imprese. I primi effetti delle normative.

Verona, 28 ottobre 2026 - **Volume, frequenza, velocità le sfide della cyber security** nel primo semestre 2026: sono stati 4.911 gli incidenti cyber di particolare gravità noti a livello mondiale, il numero più alto mai registrato da Clusit - Associazione Italiana per la Sicurezza Informatica - in un semestre, più che doppio rispetto al semestre precedente (2.392, +105%) e superiore del 71% rispetto al primo semestre 2025[1].

In sei mesi si è raggiunto il 93% degli incidenti dell'intero 2025, con una media di 819 al mese (439 nel 2025, 171 nel 2021).

Sono i dati principali dell'aggiornamento semestrale del Rapporto Clusit 2026, presentato questa mattina dai ricercatori di Clusit al Security Summit di Verona.

In Italia gli incidenti noti sono stati 245, in calo rispetto al picco di 280 del primo semestre 2025, e la loro quota sul totale mondiale scende al 5% (era il 9,5% nel semestre precedente). Tuttavia, guardando al semestre precedente, si assiste ad una leggera ripresa degli incidenti nel nostro Paese, pari all'8%, verso la crescita del 105% a livello mondiale.

A cambiare è soprattutto il profilo: diminuiscono le azioni dimostrative, in particolare quelle rivolte alla Pubblica Amministrazione, e cresce il peso del cybercrime contro le imprese, con il Manufacturing che sale al primo posto tra i settori colpiti.

Sullo sfondo, il Rapporto Clusit richiama inoltre **il ruolo dell'intelligenza artificiale** come moltiplicatore di forza: rende gli incidenti più sofisticati e abbassa la barriera d'ingresso per attori poco esperti. Secondo i ricercatori, tuttavia, l'IA non può essere considerata il motore della crescita degli incidenti nel primo semestre 2026, pur in un contesto in cui emergono i primi segnali di "**agentic hacking**", che i ricercatori si aspettano in un prossimo futuro: uno scenario di attacchi interamente automatizzati, in cui gruppi di agenti IA agiranno in modo coordinato, adattando le strategie e combinando tecniche diverse e vulnerabilità anche banali per violare i sistemi delle organizzazioni.

In particolare, secondo i ricercatori Clusit, è urgente che la cyber security sia caratterizzata da una governance adattiva e da responsabilità condivise, mettendo sempre più in campo difese «AI-

[1] L'aggiornamento semestrale del Rapporto Clusit, giunto al quattordicesimo anno di pubblicazione, prevede l'analisi dei più gravi incidenti cyber avvenuti a livello globale nell'ultimo semestre, rilevati da fonti aperte, cioè di attacchi andati "a buon fine" e diventati di dominio pubblico.

specifiche», ovvero contromisure capaci di risposta rapida, automatizzata e predittiva, per compensare l'aumento di volumi e velocità.

"*I dati ci dicono che il rischio sta cambiando la sua natura: meno azioni dimostrative, più cybercrime rivolto alle imprese, e in particolare nel nostro Paese, a quelle manifatturiere. Un minore peso sul totale mondiale non deve però generare un falso senso di sicurezza: la cybersecurity va considerata il fondamento della continuità operativa e, insieme, una responsabilità collettiva a supporto della resilienza nazionale, non un costo di conformità*", afferma **Anna Vaccarelli, presidente di Clusit**

Crescono gli incidenti nel mondo, sempre meno dettagli tecnici.

Nel corso della presentazione del Rapporto Clusit, i ricercatori hanno posto l'attenzione sulla lettura dei dati relativi alla crescita degli indicenti informatici del primo semestre dell'anno: a livello globale, questa si concentra infatti interamente laddove - **sulla base di fonti pubbliche** - **non è stato possibile determinare la tecnica utilizzata** ("tecniche undisclosed"): dai 943 del primo semestre 2025 a 3.321, pari a **due terzi del campione**.

Gli incidenti con tecnica nota sono invece in calo (1.590, contro 1.930 del primo semestre 2025). Gli autori del Rapporto Clusit lo definiscono il "paradosso della trasparenza": gli obblighi di notifica, sempre più stringenti fanno emergere più incidenti, ma non hanno finalità di trasparenza verso il pubblico: le organizzazioni tendono quindi a mantenere riservati i dettagli tecnici per salvaguardare la propria reputazione e il rischio di nuovi incidenti; appare così più complesso comprendere l'evoluzione delle minacce.

I settori più colpiti a livello globale

Il **Cybercrime** è all'origine del 95,4% degli incidenti a livello globale (4.683), mentre l'**Hacktivism** scende a 62 incidenti, il 73% in meno rispetto al primo semestre 2025, a seguito – come ipotizzato dagli autori del Rapporto Clusit – della forte risposta delle forze di polizia nel corso del primo semestre 2026[2] e di un minore clamore mediatico, che ha spostato negli ultimi mesi l'interesse su obiettivi più complessi.

Tra le vittime, il **settore Governativo, Militare e delle Forze dell'Ordine** torna al primo posto, come non accadeva dal 2021, con 751 incidenti, pari al 15,3% del totale, mentre il **Commercio all'ingrosso e al dettaglio** sale dal nono al terzo posto (467 incidenti, oltre quattro volte quelli del primo semestre 2025).

In Italia cambia il profilo degli incidenti: cause, tecniche d'attacco e settori più colpiti

L'**Hacktivism**, che nel 2025 rappresentava il 38,7% del campione italiano, scende al 17%, mentre nel primo semestre dell'anno il **Cybercrime** torna a essere la causa prevalente degli incidenti informatici, rappresentando circa l'82% del totale degli incidenti. Si ridimensiona quindi il peso delle azioni dimostrative e diminuisce sul totale la percentuale degli incidenti nel settore Governativo

[2] Ad esempio, Operation Talent, ad opera delle forze di polizia tedesche con il supporto dell'Europol (https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-takes-down-two-largest-cybercrime-forums-in-world) o e Operation Endgame, che in modo permanente ormai da tempo con azioni successive (l'ultima a maggio 2026 - https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-strikes-again-ransomware-kill-chain-broken-its-source) mira a smantellare le principali botnet che colpiscono le organizzazioni europee.

/Militare e Forze dell'Ordine, che passa dal 28,4% all'11%, oltre a dimezzarsi l'incidenza delle tecniche di DDOS, che scende dal 38,5% al 17%, coerentemente con la diminuzione degli incidenti nella Pubblica Amministrazione, che generalmente è la vittima preferita per gli attacchi DDOS, con finalità dimostrativa.

I ricercatori di Clusit hanno quindi evidenziato tra le possibili ragioni di calo dei fenomeni di Hacktivism, il miglioramento di procedure e difese, a seguito dell'entrata in vigore della Legge 90/2024 e della normativa NIS2, oltre al ripristino sempre più rapido dell'operatività dei servizi a seguito di incidenti, anche grazie alle segnalazioni al CSIRT Nazionale. Infine, va certamente indicato il minore interesse mediatico verso gli incidenti nel settore Governativo /Militare /Forze dell'Ordine. La tendenza – confermano gli autori del Rapporto Clusit - potrà però essere consolidata soltanto con l'analisi dei dati completi del 2026.

Il **Malware** torna a essere la tecnica più frequente degli incidenti nel nostro Paese, con il 43% dei casi (22,7% nel 2025), e il **settore Manufacturing** sale al primo posto con il 18,4% degli incidenti (11,7% nel 2025). In questo settore, le vittime italiane sono il **17% di quelle mondiali**, a fronte del 5% sul totale. Se confrontato con l'andamento a livello mondiale, dove il settore è soltanto ottavo in classifica, il dato che conferma come in Italia le piccole e medie imprese produttive restino tra i bersagli più attenzionati da un cybercrime sempre più efficiente e automatizzato.

Seguono, a breve distanza, gli incidenti che colpiscono "**Obiettivi Multipli**" (18%). Crescono anche gli incidenti nel settore **Informatico e delle Telecomunicazioni** (8,6%, +4,4 punti percentuali), evidenziando l'interesse degli attaccanti di colpire i fornitori per generare un impatto a cascata sulle organizzazioni clienti che utilizzano servizi informatici. Anche gli incidenti nel settore **Commercio all'ingrosso e al dettaglio** si attestano all'8,6% del totale, a pari merito con il settore ICT.

"*Nel nostro Paese sarà sempre più necessario gestire il rischio sistemico*", commenta **Luca Bechelli, del Comitato Direttivo Clusit**. "*Superata una certa soglia di frequenza, i settori più colpiti, quali manifatturiero, governo centrale e locale, infrastrutture critiche, fornitori di servizi ICT, potrebbero trovarsi in una condizione di sofferenza costante, con ricadute anche importanti sul loro buon funzionamento e, di conseguenza, sul sistema economico nazionale*", conclude Bechelli.

Non mancano, secondo i ricercatori di Clusit, segnali incoraggianti: il settore **Energia e Utilities** dimezza la propria quota (dal 2,4% degli incidenti complessivi nel 2025 all'1,2% del primo semestre 2026) e gli incidenti nella **Sanità** diminuiscono ulteriormente rispetto all'intero 2025, collocando il settore all'ultimo posto della classifica. Un segnale molto positivo, che i ricercatori di Clusit invitano tuttavia a leggere con prudenza, perché il confronto con altri rapporti nazionali e internazionali disegna ancora un quadro incerto.
Se trovasse conferma anche nel secondo semestre, potrebbe essere collegato all'attuazione delle iniziative del PNRR in ambito pubblico e all'effetto di normative come la NIS2, secondo gli esperti.

La gravità degli incidenti in Italia

Sul piano della severity il dato italiano nel primo semestre del 2026 è lievemente peggiorativo rispetto a quello globale: gli incidenti di livello "**elevato**" salgono di quasi 20 punti percentuali, rappresentando il **57% del totale**, mentre quelli di livello "**medio-basso**" scendono al **35%**; gli incidenti di livello "**critico**" si assestano su una quota molto bassa, all'**8%** del campione[3]. Secondo

[3] La gravità degli incidenti cyber nel Rapporto Clusit viene classificata dagli autori sulla base dell'impatto economico, sociale e reputazionale sulle vittime. Nel 2025 tale classificazione è stata rimodulata, comprendendo anche i dati degli ultimi cinque anni, a causa della recrudescenza dello scenario cyber e della sostanziale sparizione degli impatti di livello più basso a partire dal 2022. Nel 2025 è stata introdotta una nuova categoria di severità, di livello massimo, per rappresentare gli incidenti, caratterizzati da conseguenze particolarmente gravi e sistemiche.

i ricercatori di Clusit, questo è coerente con il minor peso degli incidenti dimostrativi e con la maggiore incidenza del cybercrime, che determina conseguenze più significative per le vittime.

"*Un segnale positivo emerge dalla distribuzione degli incidenti per gravità: in Italia, la quota di quelli con impatto medio o basso resta quasi tre volte superiore al dato globale del 2025. Se confermata nel tempo, questa tendenza potrebbe indicare una crescente capacità delle organizzazioni italiane di contenere le conseguenze degli attacchi, attraverso misure di risposta sul piano tecnico, organizzativo e procedurale*", conclude **Luca Bechelli**.

Clusit è l'Associazione Italiana per la Sicurezza Informatica. Nata nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, rappresenta oggi oltre 700 organizzazioni, appartenenti a tutti i settori del Sistema-Paese. Clusit collabora con la Presidenza del Consiglio, con diversi Ministeri, Authority, Istituzioni e organismi di controllo, tra cui ACN, Polizia Postale e per la Sicurezza Cibernetica, Arma dei Carabinieri e Guardia di Finanza, Agenzia per l'Italia Digitale, Autorità Garante per la tutela dei dati personali. Svolge inoltre un'intensa attività di supporto e di scambio con Cyber 4.0 e START 4.0, centri di Competenza nazionale e con Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA, con Università e Centri di Ricerca. In ambito internazionale, Clusit partecipa a diverse iniziative in collaborazione con i CERT, i CLUSI, con la Commissione Europea, ENISA (European Union Agency for Cybersecurity), ITU (International Telecommunication Union), OCSE, UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale), con le principali Associazioni Professionali del settore, con Università e Centri di Ricerca in oltre 20 paesi. Ulteriori informazioni sulle attività di Clusit sono disponibili sul sito www.clusit.it.

Per ulteriori informazioni si prega di contattare:
Daniela Sarti
Ufficio Stampa Security Summit | Clusit
press@securitysummit.it - dsarti@clusit.it
Tel. 335 459432