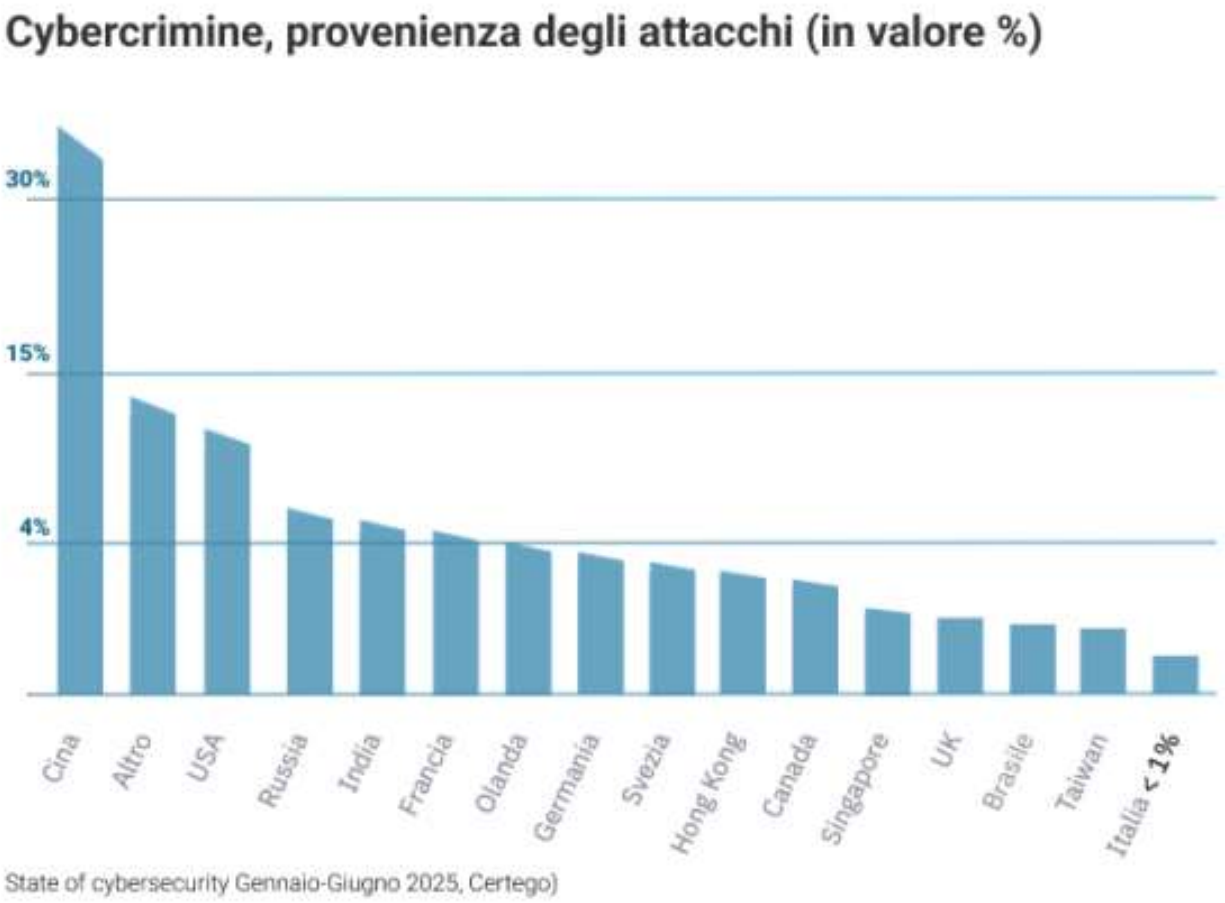
Cybercrimine, l’Italia è nel mirino: un attacco su 10 nel mondo colpisce il nostro Paese

Il report 2025 della modenese Certego rileva +16% di incidenti e il cloud come primo vettore (40%). Cina e Russia i Paesi che ci attaccano di più. Crescono pressione e vulnerabilità delle aziende italiane in tutti i settori (Fonte: https://www.corriere.it/ 7 dicembre 2025)



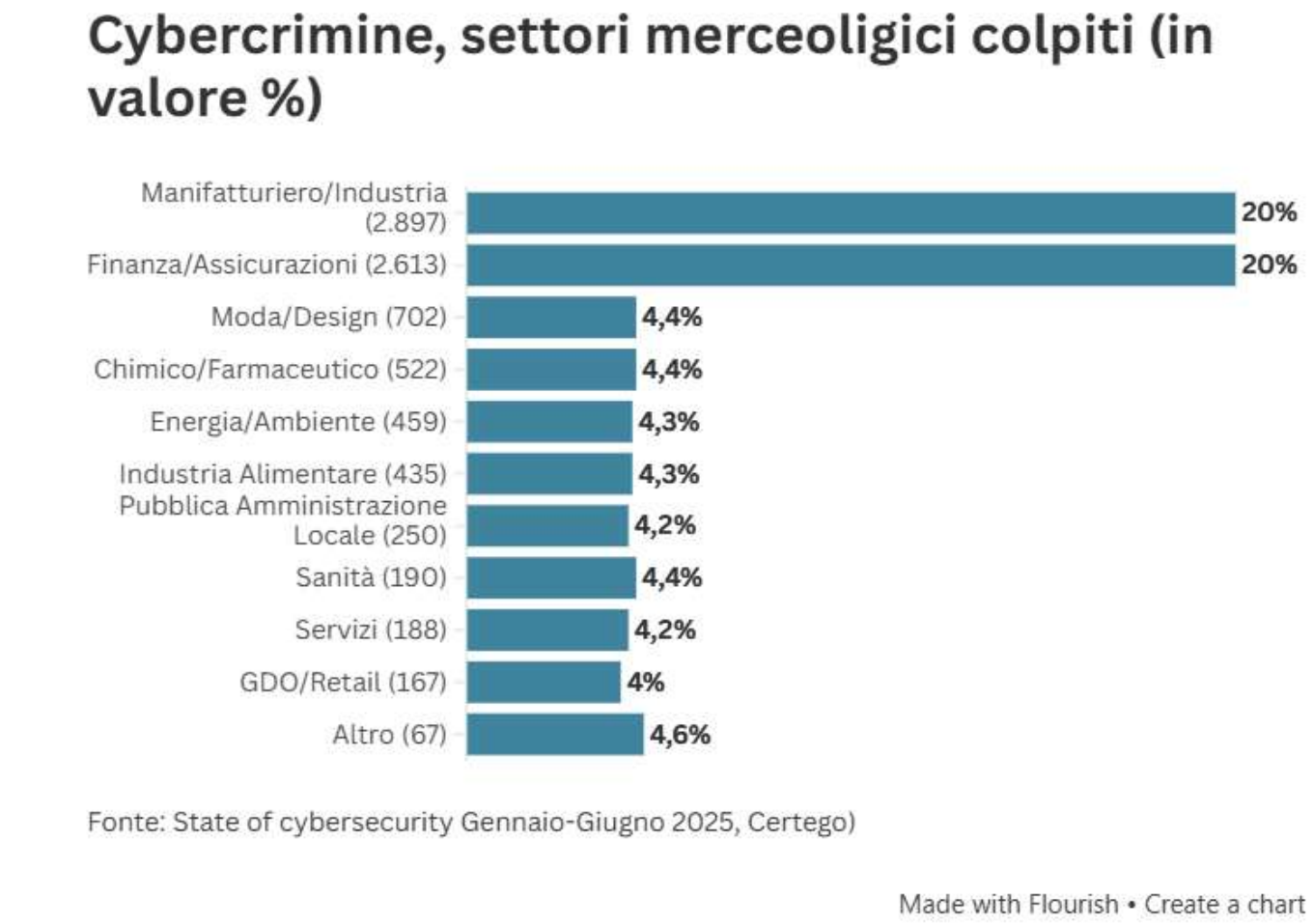
A voler usare una metafora calcistica — che in Italia non guasta mai — è come se la Nazionale del cybercrimine avesse deciso di giocare in casa nostra. E pure spesso. Perché oggi, nel panorama europeo, **siamo uno dei Paesi più colpiti dagli hacker** (e a livello globale, l’Italia risulta il quinto Paese al mondo per attacchi ransomware, dietro a Stati Uniti, Regno Unito, Canada e Germania). Come certifica infatti il **Rapporto Clusit 2024,** un incidente informatico su dieci, a livello globale, si verifica da noi, con un aumento degli attacchi, tra il 2019 e il 2024, del 110%.
A confermare l’esposizione dell’Italia è anche il nuovo ***State of Cybersecurity - Gennaio-Giugno 2025*** elaborato dalla modenese Certego, una delle realtà italiane più avanzate nella difesa digitale, basato sul monitoraggio di 1,2 milioni di asset aziendali tramite la piattaforma PanOptikon. «Siamo un Paese esposto agli attacchi hacker come pochi altri in Europa, spiega il ceo e fondatore di Certego **Bernardino Grignaffini Gregorio.** «Ed è un rapporto sproporzionato se si considera che l’Italia non è una grande potenza demografica o industriale su scala globale. Eppure, nel mirino ci finiamo noi».

L’escalation degli incidenti nel 2025

I primi mesi del 2025 raccontano un quadro in cui gli allarmi di sicurezza crescono del 10%, mentre **gli incidenti richiedono il 16% di interventi in più**. I tentativi di compromissione aumentano del 14%, e **le superfici d’attacco più sfruttate restano il cloud, gli endpoint e le reti aziendali**, in quest’ordine. «I dati del report Certego mostrano come il cloud rappresenti il 40% degli incidenti, fotografando un mutamento strutturale», spiega Grignaffini: «la sicurezza non è più una questione di perimetri, ma di comportamenti e accessi distribuiti».

Industria e finanza: i bersagli più esposti

Gli attacchi informatici colpiscono indiscriminatamente sia le aziende del settore pubblico che quelle del settore privato, entrambi accomunati da un aumento nei tentativi di attacco subiti. Ma i**l settore industriale**, ancora una volta, guida la classifica dei più colpiti: 2.897 incidenti nel solo primo semestre, **il 20% in più dell’anno precedente**. Subito dietro, **la finanza e le assicurazioni**, anch’esse in crescita del 20%. Ma a scorrere i dati completi, emerge un mosaico molto più ampio. Moda, chimica, energia, alimentare, sanità, pubblica amministrazione: **nessun comparto sembra più potersi considerare marginale nello scenario del cyber-rischio**, e la diffusione trasversale delle minacce ne è la conferma più evidente.



I «classici» del cybercrime funzionano ancora

La realtà degli attacchi è molto meno spettacolare di quanto suggerisca l’immaginario cinematografico. A colpire non sono exploit da film, ma i «classici» di sempre: malware in testa,

phishing subito dopo, e poi il furto di credenziali — che oggi rappresenta il 15% degli incidenti analizzati e continua a crescere come tecnica preferita dalle gang digitali. Nel report, la distribuzione delle tipologie mostra come basti spesso un accesso rubato per spalancare porte che nemmeno la più sofisticata infrastruttura difensiva riuscirebbe a proteggere se si parte svantaggiati dall'interno.

La mappa globale delle minacce

Il quadro geografico colloca **la Cina come origine primaria degli attacchi indirizzati verso le aziende italiane**. Seguono **Russia, India** e una costellazione di altri Paesi che contribuiscono con volumi più contenuti ma costanti. Un'indicazione evidente della natura globale del fenomeno, che non riconosce confini politici né distanze fisiche.

La pressione crescente sui team di sicurezza

Ciò che rischia di diventare insostenibile è il carico operativo che grava sui team aziendali. **La crescita degli allarmi implica un aumento dei falsi positivi, e dunque un lavoro di filtraggio sempre più complesso**. La pressione sui Security Operation Center resta uno dei punti deboli del sistema, come evidenziato nei Focus Points del report: il sovraccarico umano può diventare esso stesso una vulnerabilità, soprattutto nelle Pmi, che pure mostrano un incremento del 10% degli incidenti, mentre le grandi aziende arrivano a +19%.

Quando l'intelligenza artificiale entra nel gioco

A complicare lo scenario interviene la variabile più dirompente degli ultimi anni: **l'intelligenza artificiale**. Il report richiama le stime secondo cui almeno il 30% degli attacchi del 2025 sarà potenziato da sistemi AI, con phishing automatizzati, malware capaci di mutare struttura in tempo reale e strumenti in grado di scandagliare l'intero perimetro digitale aziendale alla ricerca di vulnerabilità ancora ignote agli stessi difensori. È la conferma che la velocità degli attaccanti rischia di superare — e in molti casi supera già — quella dei sistemi di protezione tradizionali.

La sicurezza come scelta strategica

In questo contesto, conclude **Bernardino Grignaffini Gregorio**, «la sicurezza non può più essere considerata un esercizio tecnico, ma una leva strategica. Il report insiste su un punto decisivo: le aziende devono saper comunicare ai propri board il valore della cybersecurity in termini di continuità operativa, riduzione del rischio e protezione degli asset critici. Senza una chiara comprensione al vertice, ogni investimento rischia di essere tardivo o insufficiente». Un attacco non si può prevedere, né programmare. La preparazione, invece, sì.

Leggi anche

Cybersecurity, la «trincea» italiana è a Modena: così Certego anticipa gli attacchi hacker nella guerra informatica

Italia sotto attacco hacker: +14% nel 2025, boom di cyber minacce a industria e banche