Il contesto di riferimento
Rapporto Clusit 2024 sulla Sicurezza ICT in Italia

https://clusit.it/rapporto-clusit/

(Clusit – Associazione italiana per la sicurezza informatica)

Panoramica degli attacchi informatici in Italia

Nel periodo compreso tra il 2019 e il 2023, il campione rilevato dal report Clusit ha dichiarato 653 attacchi informatici di particolare gravità che hanno coinvolto realtà italiane. Di questi, 310 incidenti sono avvenuti solo nel 2023, rappresentando oltre il 47% del totale degli attacchi censiti a livello italiano dal 2019 in poi. Questo dato evidenzia un aumento significativo del 65% rispetto all'anno precedente, un trend preoccupante che segue un aumento del 169% registrato tra il 2021 e il 2022.

Le finalità degli attacchi

- Cybercrime: La principale motivazione è economica, con l'obiettivo di ottenere denaro attraverso attività come il ransomware, il furto di dati finanziari e le frodi online.
- Hacktivism: Gli attacchi sono spesso motivati da ragioni politiche o sociali, mirati a dimostrare un punto di vista o a protestare contro determinate organizzazioni o governi.
- Espionage: Gli attacchi di spionaggio sono guidati dalla volontà di ottenere informazioni sensibili o segreti industriali per vantaggi competitivi o strategici.
- Information Warfare: La guerra dell'informazione mira a destabilizzare governi o società, influenzare l'opinione pubblica e manipolare informazioni a favore di specifici interessi geopolitici.

In Italia la maggioranza degli attacchi noti si riferisce alla categoria Cybercrime, che rappresenta il 64% del totale.

Tipologie di attacco

Dall'analisi condotta da Fastweb e dalla Polizia Postale, emergono principalmente le seguenti tipologie di attacco informatico:

- Malware: Rimane la tecnica di attacco più comune, utilizzata nel 36% dei casi.
- Exploits di vulnerabilità: 18% degli attacchi sfrutta vulnerabilità, incluse quelle di tipo zero-day (vulnerabilità non precedentemente note).

- Phishing e Social Engineering: Rappresentano una significativa porzione degli attacchi, con un 8% del totale.
- DDoS: Incidenza in crescita del 98%, rappresentando una minaccia sempre più preoccupante.
- Furto di identità: Cracking degli account per accedere a informazioni personali o aziendali sensibili (3% degli attacchi totali).

Severità degli attacchi

In merito alla severità degli attacchi, in termini di distribuzione sul totale, gli attacchi critici e ad altro impatto nel 2023 risultano l'81% del totale (rispetto all'80% riscontrato nel 2022).

Destinatari degli attacchi

Gli attacchi informatici si concentrano su vari settori critici, con una particolare enfasi su:

- Governo e Pubblica Amministrazione: Subiscono il 47% degli attacchi globali di *hacktivism*, con un incremento significativo nel 2023.
- Sanità: Crescita del 30% degli attacchi, facendo di questo settore uno dei più bersagliati.
- Settore Finanziario e Assicurativo: Aumento del 62% degli incidenti, evidenziando la vulnerabilità di questo settore.
- Manifatturiero: Incremento del 25%, riflettendo l'attenzione dei cybercriminali su questo ambito.

Gli attacchi alle organizzazioni governative e alle pubbliche amministrazioni

Il settore pubblico ha visto un importante aumento degli attacchi fra il 2022 e il 2023, incremento spiegabile con attività dimostrative e di fiancheggiamento legate alla situazione geopolitica e ai conflitti in corso.

Tra il 2019 e il 2023 il campione rilevato dall'indagine Clusit riporta 653 attacchi noti di particolare gravità. Di questi, 310 incidenti (oltre il 47% del totale) sono avvenuti nell'ultimo anno. Se si considerano gli incidenti avvenuti a partire dal 2022 (498 su 653) la percentuale rispetto agli anni precedenti cresce al 76%, indicando una netta accelerazione rispetto al periodo 2019-2021.

Anno	Numero di Attacchi
2019	37
2020	48

2021	70
2022	188
2023	310

Distribuzione dei cyber attacchi in Italia nel periodo 2019-2023

Tendenze emergenti

Le tendenze più significative osservate includono:

- Aumento del numero di attacchi;
- Gravità degli attacchi: Oltre l'81% degli attacchi è classificato come "critico" o "grave", indicando un aumento della loro severità.
- Coinvolgimento dell'Intelligenza Artificiale: Emergenza dell'uso dell'AI per identificare target e vulnerabilità, suggerendo un futuro aumento della sofisticazione degli attacchi.