CYBERSECURITY IN ITALIA: ANALISI DEL RAPPORTO CLUSIT 2024 E PROSPETTIVE

Il Rapporto Clusit 2024 evidenzia un incremento significativo degli attacchi informatici nel primo semestre dell'anno, con l'Italia particolarmente bersagliata. Questo articolo analizza le tendenze emergenti, i settori più colpiti e le strategie per rafforzare la sicurezza informatica nel paese.

A cura della Redazione

Sommario

Introduzione

Negli ultimi anni, la sicurezza informatica è emersa come uno dei temi più rilevanti a livello globale, influenzando non solo l'economia e la politica, ma anche aspetti fondamentali della vita quotidiana. Il 2024 si è rivelato un anno cruciale per comprendere l'evoluzione di questa minaccia, con l'Italia che ha assunto un ruolo centrale nel panorama internazionale degli attacchi cyber. I dati del Rapporto Clusit 2024 mettono in evidenza non solo l'aumento degli attacchi gravi, ma anche l'evoluzione delle strategie adottate dai cybercriminali, spesso supportate da un accesso sempre più semplice a strumenti sofisticati grazie al cybercrime-as-a-service.

Questo scenario si inserisce in un contesto globale già di per sé complesso, caratterizzato da una digitalizzazione accelerata e dalla crescente interconnessione delle infrastrutture critiche. Settori come l'energia, le utility e la sanità sono sempre più bersagliati, evidenziando un pericoloso squilibrio tra l'avanzamento tecnologico e le capacità di protezione delle organizzazioni. Le vulnerabilità non risiedono solo nelle tecnologie obsolete o mal configurate, ma anche nella componente umana, spesso sottovalutata in termini di sensibilizzazione e formazione.

L'Italia, nello specifico, si trova a un crocevia, dove il rischio di attacchi informatici si intreccia con l'urgenza di innovare e adottare strategie difensive avanzate. La crescente consapevolezza della gravità della situazione è testimoniata dall'interesse mediatico e dalle iniziative intraprese, come il recente Security Summit Streaming Edition, un evento chiave che ha messo in evidenza le sfide e le opportunità del settore. Durante questo appuntamento, esperti e istituzioni hanno sottolineato come la minaccia cyber non sia più confinata a settori isolati, ma rappresenti un rischio sistemico che richiede interventi urgenti e coordinati.

Allo stesso tempo, emerge la necessità di un cambio di paradigma nella percezione della sicurezza informatica: non più vista come un costo o una semplice misura di prevenzione, ma come un investimento strategico per garantire la continuità operativa, proteggere i dati sensibili e preservare la fiducia dei cittadini e delle imprese. In un contesto in cui la reputazione digitale di un'organizzazione può essere distrutta in pochi secondi da un attacco ben orchestrato, l'adozione di misure proattive e innovative diventa non solo auspicabile, ma imprescindibile.

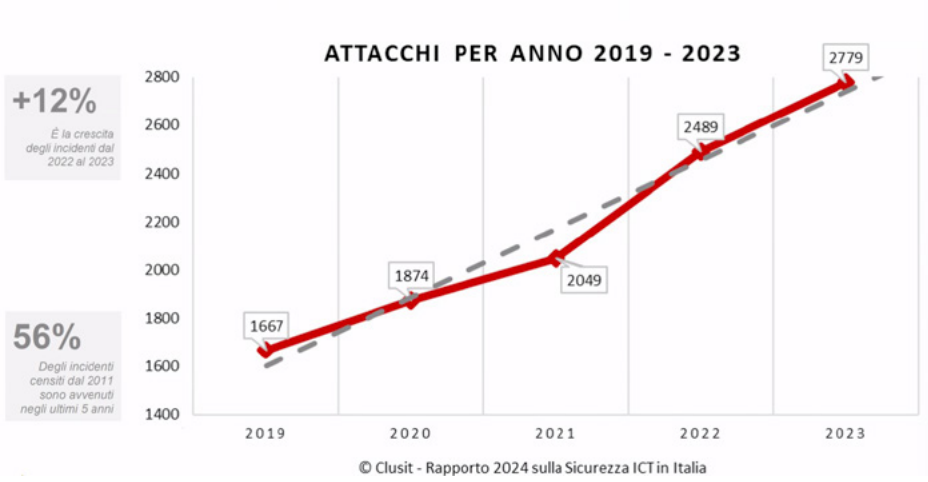
Panorama degli attacchi informatici nel 2024

Nel primo semestre del 2024, gli attacchi informatici a livello globale hanno registrato un incremento del 23% rispetto al semestre precedente, con una media di 9 attacchi gravi al giorno. In Italia, il 7,6% degli incidenti globali ha avuto luogo, posizionando il paese tra i più colpiti.

Questo aumento non è solo quantitativo ma anche qualitativo: l'81% degli incidenti è stato classificato come "critico" o "grave", rispetto al 47% del 2019. Il cybercrime si conferma la principale fonte di minaccia, rappresentando l'88% del totale degli attacchi, con un aumento di oltre 5 punti percentuali rispetto al 2023.

La media mensile degli incidenti ha raggiunto quota 273, più del doppio rispetto al primo semestre del 2019, quando si attestava a 139. In termini pratici, ciò si traduce in circa 9 attacchi significativi al giorno, contro i 4,5 di cinque anni fa.

L'evoluzione delle minacce vede una crescente sofisticazione delle tecniche di attacco e la diffusione di modelli "as-a-Service" che rendono accessibili strumenti avanzati anche a criminali meno esperti. Parallelamente, si è osservata una diminuzione degli attacchi classificati come Espionage (-2%) e Hacktivism (-3%), che tuttavia non deve essere interpretata come un allentamento della tensione in questi ambiti.



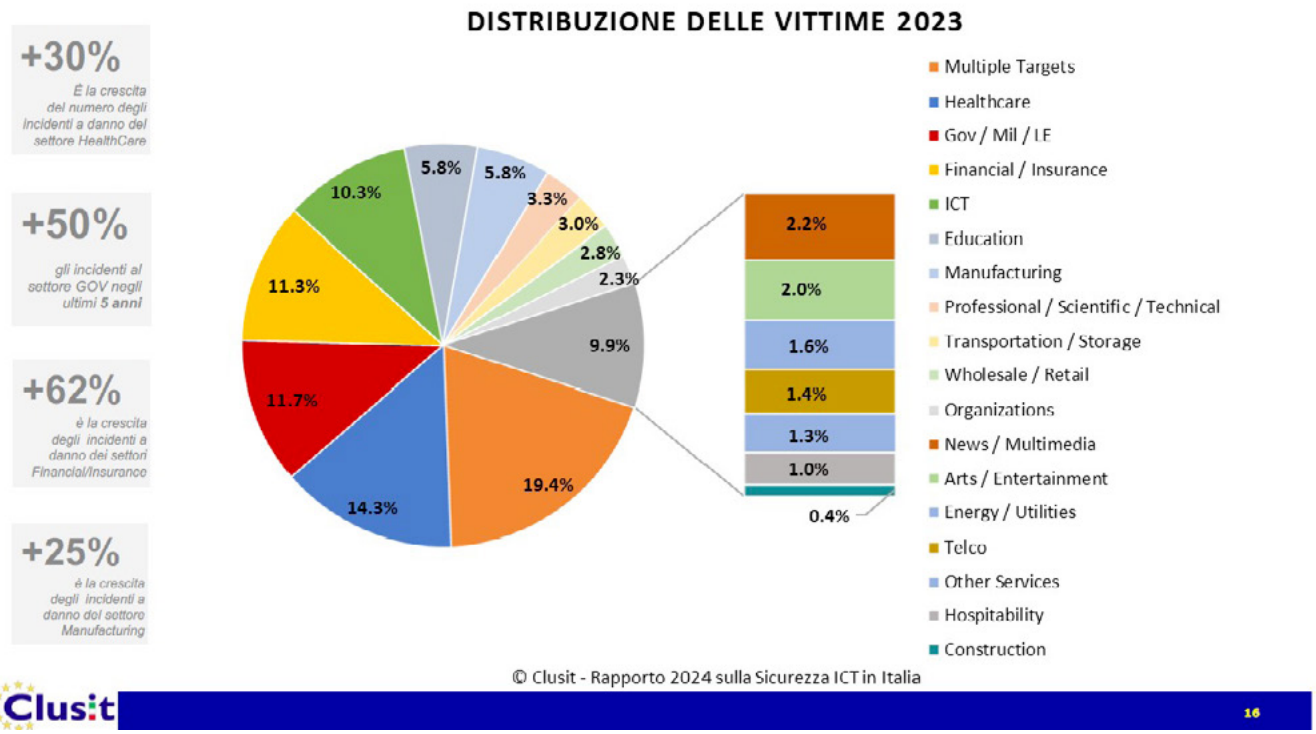
Attacchi in Italia 2019-2023

Settori più colpiti

A livello globale, il settore sanitario è stato il più bersagliato, rappresentando quasi il 20% degli incidenti totali nei primi sei mesi del 2024. In Italia, oltre al comparto sanitario, anche il settore manifatturiero è stato gravemente colpito, con un incremento dell'83% rispetto al 2023.
Il settore sanitario ha subito un aumento del 18% degli attacchi rispetto al semestre precedente, evidenziando una crescente vulnerabilità in un'area critica per la società. Anche il settore dell'educazione ha registrato un incremento significativo, con un aumento del 15% degli attacchi.
Il settore governativo e militare ha visto un aumento del 13% degli attacchi, sottolineando la necessità di rafforzare le difese cibernetiche nelle infrastrutture critiche dello Stato. Il settore dei servizi online e cloud ha registrato un incremento del 12% degli attacchi, evidenziando la crescente attrattività di questi servizi per i cybercriminali.
subiti nel primo semestre del 2024.
Gli attacchi basati su phishing e social engineering rappresentano il 20% delle tecniche utilizzate, evidenziando l'importanza della componente umana nella catena della sicurezza. Le vulnerabilità note ma non patchate sono state sfruttate nel 15% degli attacchi, sottolineando la necessità di una gestione efficace delle patch.
Gli attacchi DDoS (Distributed Denial of Service) hanno rappresentato il 10% delle tecniche utilizzate, causando interruzioni significative nei servizi online. Le tecniche di credential stuffing, che sfruttano credenziali rubate, sono state utilizzate nel 8% degli attacchi, evidenziando l'importanza di una gestione sicura delle password.

Strategie per rafforzare la Cybersecurity

L'Italia è particolarmente colpita da attacchi informatici e nel 2023 ha subito il 71% degli incidenti informatici globali legati al cybercrime.

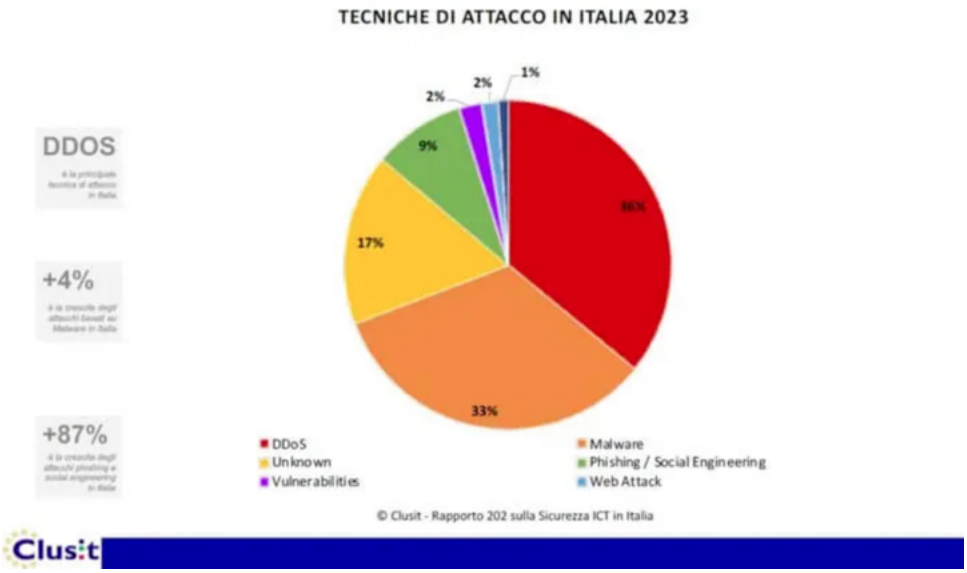


Distribuzione delle vittime

Tecniche di attacco

Il malware continua a essere la tecnica di attacco prediletta dai cybercriminali, rappresentando il 34% degli incidenti globali. Tra i diversi tipi di malware, il ransomware rimane una delle minacce più diffuse e dannose, con un impatto economico rilevante per le organizzazioni colpite. Anche l'Italia ha visto una crescita del malware, che rappresenta il 51% degli attacchi

Anche se nel 2024 si nota un lieve calo complessivo degli attacchi critici, l'impatto sugli aspetti finanziari, reputazionali e di sicurezza nazionale è elevato, richiedendo una maggiore attenzione e investimento nelle soluzioni di cybersecurity.
Per affrontare le crescenti minacce informatiche evidenziate dal Rapporto Clusit 2024, l'Italia deve adottare un approccio strategico e



Tecniche di attacco

coordinato che integri sensibilizzazione, innovazione tecnologica e collaborazioni efficaci. Un elemento cruciale è rappresentato dalla promozione della cultura della sicurezza informatica a tutti i livelli della società. È necessario investire in programmi educativi che, fin dalle scuole, sensibilizzino i giovani sui rischi cibernetici e sulle buone pratiche da adottare. Parallelamente, le università e i centri di formazione professionale dovrebbero integrare nei loro percorsi accademici corsi specifici sulla cybersecurity, formando esperti qualificati in grado di fronteggiare le sfide del settore.

Anche il rafforzamento delle partnership tra pubblico e privato riveste un ruolo strategico. Le istituzioni governative, le aziende e le organizzazioni non profit devono collaborare per condividere informazioni sulle minacce emergenti, migliorare la resilienza delle infrastrutture critiche e sviluppare soluzioni innovative. In questo contesto, l'adozione di tecnologie avanzate come l'intelligenza artificiale e il machine learning può fare la differenza, permettendo di analizzare grandi quantità di dati in tempo reale, individuare comportamenti anomali e prevenire gli attacchi prima che abbiano un impatto significativo.

Inoltre, l'Italia deve continuare a sviluppare un quadro normativo robusto che obblighi le organizzazioni a rispettare standard elevati di sicurezza e a implementare piani di risposta rapidi in caso di incidenti. La regolamentazione dovrebbe includere misure per garantire una gestione efficace delle vulnerabilità e incentivare le aziende ad adottare un approccio proattivo nella protezione dei loro sistemi. Un aspetto fondamentale è rappresentato anche dall'incremento degli investimenti statali nel settore, volti a sostenere sia le imprese innovative che le iniziative di ricerca e sviluppo.

Infine, la sensibilizzazione deve essere accompagnata da azioni concrete per migliorare la resilienza delle infrastrutture critiche del paese, che sono particolarmente esposte ad attacchi informatici. Questo richiede non solo risorse finanziarie, ma anche la creazione di un ecosistema collaborativo che coinvolga attori nazionali e internazionali, favorendo la condivisione delle conoscenze e l'allineamento delle strategie. Solo attraverso un approccio integrato e coordinato l'Italia potrà ridurre la propria vulnerabilità e affrontare con efficacia le sfide della cybersecurity del futuro.

La Nomina di Anna Vaccarelli

Il 12 dicembre 2024, Anna Vaccarelli è stata nominata presidente del Clusit, succedendo a Gabriele Faggioli, che ha assunto il ruolo di presidente onorario. Vaccarelli, dirigente tecnologo presso l'Istituto di Informatica e Telematica del CNR di Pisa e responsabile delle relazioni esterne di Registro.it, porta con sé una vasta esperienza nel campo della cybersecurity e della divulgazione scientifica. La sua nomina rappresenta un passo significativo verso un rafforzamento delle iniziative di sensibilizzazione e formazione in materia di sicurezza informatica in Italia.

Anna Vaccareli, neo nominata presidente Clusit

Il Rapporto

Il Rapporto Clusit 2024 evidenzia una situazione preoccupante per la cybersecurity in Italia, con un aumento significativo degli attacchi informatici e una crescente sofisticazione delle tecniche utilizzate dai cybercriminali. È essenziale che tutti gli stakeholder, dalle istituzioni alle aziende, collaborino attivamente per implementare strategie efficaci volte a proteggere le infrastrutture digitali e garantire la sicurezza dei cittadini nel mondo digitale.
Per un approfondimento dettagliato e per scaricare il Rapporto Clusit 2024 completo, è possibile visitare il sito ufficiale del Clusit.

Rapporto Clusit 2024

https://clusit.it

Keywords: Cybersecurity; Rapporto Clusit 2024; attacchi informatici; cybercrime; ransomware; phishing; malware; social engineering; settori critici; infrastrutture critiche; sanità; manifatturiero; energia; utility; sensibilizzazione; formazione; intelligenza artificiale; machine learning; partnership pubblico-privato; vulnerabilità; patch management; DDoS; credential stuffing; reputazione digitale; Anna Vaccarelli; protezione dati; Security Summit Streaming Edition; continuità operativa.

CYBERSECURITY IN ITALY: ANALYSIS OF THE CLUSIT 2024 REPORT AND OUTLOOK

The Clusit 2024 Report highlights a significant increase in cyberattacks during the first half of the year, with Italy being particularly targeted. This article analyzes emerging trends, the most affected sectors, and strategies to strengthen cybersecurity in the country.

By Editorial Staff

Summary

Introduction

In recent years, cybersecurity has emerged as one of the most pressing global issues, influencing not only the economy and politics but also fundamental aspects of daily life. The year 2024 has proven to be pivotal in understanding the evolution of this threat, with Italy playing a central role in the international landscape of cyberattacks. The data from the Clusit 2024 Report highlight not only an increase in severe attacks but also the evolution of strategies employed by cybercriminals, often aided by increasingly easy access to sophisticated tools through cybercrime-as-a-service.
This scenario fits within a globally complex context, characterized by accelerated digitalization and growing interconnection of critical infrastructures. Sectors such as energy, utilities, and healthcare are increasingly targeted, exposing a dangerous imbalance between technological advancements and organizations' protection capabilities. Vulnerabilities are not only present in outdated or poorly configured technologies but also in the human component, often underestimated in terms of awareness and training.
Italy, specifically, finds itself at a crossroads, where the risk of cyberattacks intersects with the urgent need to innovate and adopt advanced defensive strategies. The growing awareness

of the severity of the situation is evidenced by media interest and initiatives undertaken, such as the recent Security Summit Streaming Edition, a key event that highlighted the challenges and opportunities in the sector. During this event, experts and institutions emphasized how the cyber threat is no longer confined to isolated sectors but represents a systemic risk that requires urgent and coordinated action.
At the same time, there is a need for a paradigm shift in the perception of cybersecurity: no longer seen as a cost or a simple preventive measure but as a strategic investment to ensure operational continuity, protect sensitive data, and preserve the trust of citizens and businesses. In a context where the digital reputation of an organization can be destroyed in seconds by a well-orchestrated attack, the adoption of proactive and innovative measures becomes not only desirable but essential.

Cyberattack Landscape in 2024
In the first half of 2024, global cyberattacks increased by 23% compared to the previous semester, with an average of 9 severe attacks per day. In Italy, 7.6% of global incidents occurred, positioning the country among the most affected.
This increase is not only quantitative but also qualitative: 81% of incidents were classified as "critical" or "severe," compared to 47% in 2019. Cybercrime remains the primary source of threat, accounting for 88% of all attacks, up more than 5 percentage points from 2023.
The average monthly number of incidents reached 273, more than double compared to the first half of 2019, when it stood at 139. Practically speaking, this translates into about 9 significant attacks per day, compared to 4.5 five years ago.
The evolution of threats shows a growing sophistication in attack techniques and the spread of "as-a-Service" models that make advanced tools accessible to less experienced criminals. At the same time, there has been a decrease in attacks classified as Espionage (-2%) and Hacktivism (-3%), although this should not be interpreted as a relaxation of tension in these areas.

Most Affected Sectors
Globally, the healthcare sector was the most targeted, accounting for nearly 20% of all incidents in the first half of 2024. In Italy, in addition to the healthcare sector, the manufacturing sector was heavily impacted, with an 83% increase compared to 2023.
The healthcare sector saw an 18% increase in attacks compared to the previous semester, highlighting the growing vulnerability of this critical area for society. The education sector also recorded a significant increase, with a 15% rise in attacks.
The government and military sectors saw a 13% increase in attacks, emphasizing the need to strengthen cyber defenses in the state's critical infrastructures. The online services and cloud sector experienced a 12% rise in attacks, highlighting the increasing attractiveness of these services for cybercriminals.

Attack Techniques
Malware remains the attack technique of choice for cybercriminals, accounting for 34% of global incidents. Among the various types of malware, ransomware remains one of the most widespread and damaging threats, with significant economic impact on affected organizations. Italy also saw an increase in malware, which accounted for 51% of the attacks suffered in the first half of 2024.
Phishing and social engineering-based attacks accounted for 20% of the techniques used, highlighting the importance of the human component in the security chain. Unpatched but known vulnerabilities were exploited in 15% of attacks, underscoring the need for effective patch management.
DDoS (Distributed Denial of Service) attacks accounted for 10% of techniques used, causing significant service disruptions. Credential stuffing attacks, which exploit stolen credentials, were used in 8% of attacks, highlighting the importance of secure password management.

Strategies to Strengthen Cybersecurity
Italy is particularly impacted by cyberattacks, having suffered 71% of global cybercrime-related incidents in 2023. Although there is a slight decrease in critical attacks overall in 2024, the financial, reputational, and national security impacts remain high, requiring increased attention and investment in cybersecurity solutions.
To address the growing cyber threats highlighted by the Clusit 2024 Report, Italy must adopt a strategic and coordinated approach that integrates awareness, technological innovation, and effective collaborations. A crucial element is the promotion of a cybersecurity culture at

all levels of society. It is necessary to invest in educational programs that raise awareness of cyber risks and best practices from an early age. Universities and vocational training centers should also integrate cybersecurity courses into their academic programs, training qualified experts capable of tackling the sector's challenges.

Strengthening public-private partnerships plays a strategic role. Government institutions, businesses, and non-profit organizations must collaborate to share information on emerging threats, improve the resilience of critical infrastructures, and develop innovative solutions. In this context, the adoption of advanced technologies such as artificial intelligence and machine learning can make a difference, enabling real-time data analysis, anomaly detection, and prevention of attacks before they have a significant impact.

Moreover, Italy must continue to develop a robust regulatory framework that requires organizations to adhere to high-security standards and implement rapid response plans in case of incidents. The regulation should include measures to ensure effective vulnerability management and encourage companies to adopt a proactive approach to protecting their systems. A key aspect is also increasing state investments in the sector, supporting both innovative businesses and research and development initiatives.

Finally, awareness must be accompanied by concrete actions to improve the resilience of the country's critical infrastructures, which are particularly vulnerable to cyberattacks. This requires not only financial resources but also the creation of a collaborative ecosystem that involves national and international actors, promoting knowledge sharing and strategy alignment. Only through an integrated and coordinated approach can Italy reduce its vulnerability and effectively tackle the cybersecurity challenges of the future.

The Appointment of Anna Vaccarelli

On December 12, 2024, Anna Vaccarelli was appointed president of Clusit, succeeding Gabriele Faggioli, who assumed the role of honorary president. Vaccarelli, a technology manager at the Institute of Informatics and Telematics of CNR in Pisa and head of external relations at Registro.it, brings extensive experience in cybersecurity and scientific outreach. Her appointment marks a significant step towards strengthening awareness and training initiatives in Italy's cybersecurity landscape.

The Report

The Clusit 2024 Report highlights a concerning cybersecurity situation in Italy, with a significant increase in cyberattacks and growing sophistication in the techniques used by cybercriminals. It is essential for all stakeholders, from institutions to businesses, to collaborate actively to implement effective strategies to protect digital infrastructures and ensure the safety of citizens in the digital world. For a detailed analysis and to download the full Clusit 2024 Report, visit the official Clusit website.

https://clusit.it

Keywords: Cybersecurity; Clusit 2024 Report; cyberattacks; cybercrime; ransomware; phishing; malware; social engineering; critical sectors; critical infrastructures; healthcare; manufacturing; energy; utilities; awareness; training; artificial intelligence; machine learning; public-private partnerships; vulnerabilities; patch management; DDoS; credential stuffing; digital reputation; Anna Vaccarelli; data protection; Security Summit Streaming Edition; operational continuity.