SECURITY SUMMIT

Anteprima Rapporto Clusit 2023

Clusit, l'Italia nel mirino degli hacker: +169% gli attacchi nel 2022 rispetto al 2021. A livello mondiale la crescita è del 21%.

La nuova fase di "guerra cibernetica diffusa" ha coinvolto negli ultimi dodici mesi anche il nostro Paese: a segno il 7,6% degli attacchi globali. La pressione maggiore degli attacchi sulle aziende manifatturiere del Made in Italy, nel settore tecnico-scientifico e dei servizi professionali; oltre l'80% ha avuto conseguenze molto gravi.

Milano, 7 marzo 2023 – Con **2.489 incidenti gravi[1] a livello globale**, il 2022 si caratterizza per l'ennesima volta come l'anno peggiore da sempre per la cyber security: sono stati 440 gli attacchi in più rispetto al 2021, che segnano una crescita annua del 21%; la media mensile degli incidenti è stata 207, contro i 171 dell'anno precedente. Il picco massimo dell'anno - e di sempre - si è registrato nel mese di marzo, con 238 attacchi.

Nel contesto delle crescenti tensioni internazionali tra superpotenze e di un conflitto ad alta intensità combattuto ai confini dell'Europa **anche l'Italia appare ormai in maniera evidente nel mirino**: nel 2022 nel nostro Paese è andato a segno il 7,6% degli attacchi globali (contro il 3,4% del 2021). In numero assoluto sono stati 188 gli attacchi verso il nostro Paese, dato che segna un incremento del 169% rispetto all'anno precedente. A completare il quadro italiano, la gravità elevata o critica nell'83% dei casi.

Sono i dati che emergono dal Rapporto Clusit 2023, presentato questa mattina alla stampa da Clusit, l'Associazione Italiana per la Sicurezza Informatica[2]. La presentazione del Rapporto Clusit al pubblico avverrà in apertura di Security Summit, il convegno dedicato ai temi della cyber security in programma a Milano dal 14 al 16 marzo prossimi.

Negli ultimi cinque anni si è verificato un cambiamento sostanziale nei livelli globali di cyber-insicurezza mondiali - hanno commentato i ricercatori di Clusit illustrando i trend di crescita degli incidenti - al quale non è corrisposto un incremento adeguato delle contromisure adottate dai difensori. Dal 2018 al 2022 è stata rilevata una crescita degli attacchi pari al 60%; nello stesso periodo la media mensile di attacchi gravi a livello globale è passata da 130 a 207.

---

[1] Nel Rapporto Clusit sono classificati come "gravi" gli attacchi con un impatto sistemico in ogni aspetto della società, della politica, dell'economia e della geopolitica.

[2] Frutto della collaborazione continuativa di oltre cento professionisti nell'ambito di Clusit, il Rapporto Clusit fornisce annualmente il quadro esaustivo della situazione globale della sicurezza informatica, avvalendosi anche del contributo di soggetti pubblici e privati che condividono con Clusit esperienze e ricerche sul campo con informazioni e dati inediti, tra cui quello della Polizia Postale e delle Comunicazioni; del CERT di Banca d'Italia, dell'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano, di CNA Milano e Unione Artigiani Milano e di Women For Security, oltre ai contributi di aziende che operano nel settore della cybersecurity. Nel Rapporto Clusit 2023 è inoltre pubblicata un'intervista a Domenico Ghiglia, Componente del Garante per la protezione dei dati personali.

In un contesto di cybercrime già in costante crescita, nel 2022 il conflitto tra Russia e Ucraina ha attivato capacità cibernetiche offensive utilizzate dai contendenti, dai loro alleati e in generale dai principali attori globali a supporto di attività di cyber-intelligence, di cyber-warfare e di operazioni ibride.

Secondo i ricercatori di Clusit, per quanto oggi in ambito intelligence e militare prevalgano ancora gli attacchi di natura tipicamente clandestina rispetto a quelli condotti con finalità di degrado, negazione o distruzione di sistemi e infrastrutture digitali, questa proporzione appare destinata a cambiare in un prossimo futuro: il processo di rapida adozione e messa in campo di strumenti cyber-offensivi sofisticati sarà difficilmente reversibile, e in prospettiva potrebbe causare gravi conseguenze in un mondo già fortemente digitalizzato ma sostanzialmente impreparato ad affrontare minacce di questa natura.

Commentando i dati relativi agli attacchi nel nostro Paese, il presidente di Clusit, **Gabriele Faggioli** ha dichiarato: "*È necessaria una ulteriore evoluzione nell'approccio alla cybersecurity. Occorre non solo che permanga il driver normativo, ma che si mettano in atto a tutti i livelli i processi di valutazione e gestione del rischio per il business, atti a calibrare adeguatamente gli investimenti sulla base delle reali necessità"*.

"Serve inoltre pensare in ottica di razionalizzazione degli adempimenti normativi, oltre ad evolvere in chiave di economia di scala, di condivisione della conoscenza, delle risorse e dei costi cyber, considerando che tanti piccoli investimenti autonomi non fanno una grande difesa ma solo tante inefficienti difese", ha proseguito Faggioli.

"Auspichiamo che in Italia le iniziative istituzionali siano sostenute anche dalle singole imprese e pubbliche amministrazioni, in un'ottica di collaborazione pubblico-privato, tramite la costituzione e l'evoluzione di processi adeguati di monitoraggio della sicurezza, incident management, crisis management, e servizi SOC, tra gli altri", ha concluso Faggioli.

2022, attacchi record nel mondo e in Italia

Gli attacchi cyber hanno registrato nel 2022 a livello globale e nazionale il valore più elevato di sempre e la maggior percentuale di crescita annua. Nell'illustrare i dati, i ricercatori e gli esperti di Clusit hanno evidenziato che si tratta di una fotografia esemplare, che tuttavia rappresenta soltanto la punta dell'iceberg, data la tendenza complessiva delle vittime a mantenere riservati gli attacchi cyber subìti, nonostante l'esistenza di normative ormai consolidate, come il Regolamento GDPR e la Direttiva NIS in Europa ed altre in fase di adozione come NIS2, DORA o il Cyber Resiliency Act.

Oltre che in quantità, su scala globale gli attacchi nel 2022 sono cresciuti anche in **gravità**, arrivando a livelli di **impatto elevato o critico nell'80% dei casi**, dato allineato al contesto italiano, ovvero con una ripercussione rilevante per le vittime a livello di immagine, di aspetto economico, sociale e dal punto di vista geopolitico.

Gli obiettivi degli attacchi nel mondo e in Italia

L'analisi degli incidenti cyber noti nel 2022 evidenzia una netta prevalenza di attacchi con finalità di **cybercrime**, che sono stati oltre 2.000 a livello globale, ovvero l'**82% del totale**, in crescita del

15% rispetto al 2021. Per l'Italia la percentuale sale al **93%**, **in crescita del 150% rispetto al 2021**.

Questa tipologia di attacchi, caratterizzata da significativi risvolti economici legati alla diffusione degli attacchi ransomware, mostra una tendenza di crescita costante negli ultimi cinque anni.

In valore assoluto, anche gli attacchi riconducibili ad attività di **spionaggio e sabotaggio** (11% del totale), ad **information warfare** (4% del totale) e ad **azioni di attivismo** (3% del totale) hanno raggiunto a livello mondiale i propri massimi storici nel 2022.

Gli esperti di Clusit notano che, analizzati in percentuale sul totale, i dati tra il 2022 e il 2021 crescono per **Information Warfare** del **110%** e **Hacktivism** del **320%**, principalmente a causa del conflitto europeo**.**

Nel nostro Paese sono stati invece il 7% gli incidenti classificati come "attivismo", mentre non sono stati rilevati attacchi significativi nelle categorie "Espionage / Sabotage" o "Information Warfare".

"*Supponiamo che la crescita di information warfare e soprattutto di attivismo possa essere dovuta almeno in parte alla guerra in Ucraina, che ha stimolato le azioni degli attivisti anche sulla rete e ha sollecitato la diffusione di informazioni di propaganda e contro-propaganda*", afferma **Sofia Scozzari**, membro del Comitato Direttivo Clusit, tra gli autori del Rapporto.

"*Analizzando i dati degli attaccanti, tuttavia, dobbiamo anche considerare che governi potrebbero aver perpetrato i propri attacchi con modalità attribuibili ad altri attori, senza ovviamente rivendicare pubblicamente le loro operazioni. Quanto all'hacktivism, oggi molte campagne tese a colpire la reputazione delle organizzazioni sono molto più efficaci sui social che non con defacement o tecniche analoghe*", ha proseguito Sofia Scozzari.

Chi viene attaccato, nel mondo e in Italia

A livello mondiale le principali vittime tornano ad essere i **Multiple Targets** (22%), con un aumento del 97% rispetto al 2021: si tratta di campagne di attacco non mirate, che continuano a causare effetti consistenti. Segue il **settore governativo e delle pubbliche amministrazioni** (12%) che, come fanno notare i ricercatori Clusit, nell'arco di cinque anni ha visto un incremento complessivo del 25%.

Nel 2022 il 12% degli attacchi è stato rivolto alla **Sanità**, con valori in crescita percentuale del 16% rispetto al 2021, l'11% all'**industria informatica** e l'8% al **settore scolastico e universitario**. Le ultime due categorie segnano un leggero calo (-3%) rispetto all'anno precedente e soprattutto in riferimento all'uso estensivo di smart working e didattica a distanza nel 2020.

In percentuale sono cresciuti gli attacchi ai settori **finanziario assicurativo** (+40%) e **Manufacturing**, verso cui è stato rilevato un aumento costante degli attacchi, che sono raddoppiati dal 2018 e, dal 2021, mostrano una **crescita percentuale sul totale del 79%**, probabilmente a causa della crescente diffusione dell'IoT e dalla tendenza verso l'interconnessione dei sistemi industriali, spesso non sufficientemente protetti.

Anche le vittime nel settore **News e Multimedia**, dopo un calo drastico dal 5% al 2% tra il 2018 e il 2020, sono state protagoniste di un raddoppio tra il 2020 e il 2022, arrivando a rappresentare il 5% degli obiettivi, con una **crescita percentuale del 70% dal 2021**. Una componente di questo aumento è senz'altro riferibile al conflitto in Ucraina, nell'ambito di attività di disinformazione, propaganda e disruption di media considerati nemici da colpire.

Il settore più attaccato **in Italia** nel 2022 è invece quello **governativo**, con il **20%** degli attacchi, seguito a brevissima distanza dal comparto **manifatturiero** (**19%**), che rappresenta il **27% del totale degli attacchi censiti nel settore livello globale**.

In coerenza con quanto avviene a livello globale, si ha anche in Italia la maggiore crescita percentuale anno su anno per la categoria "**Multiple Targets**" (**+900%**). Gli attacchi nel nostro Paese sembrano andare di pari passo con il grado di maturità tecnologica negli specifici ambiti: i settori **dei servizi professionali, e tecnico-scientifico** vedono un incremento del **233,3%** di incidenti gravi, l'**industria manifatturiera** il +**191,7%**. Essendo tra le più colpite, è rilevante anche la crescita per le organizzazioni del comparto informatico, (**+100%**) e governativo-militare (**+65,2%**).

La geografia delle vittime: i continenti più colpiti

I ricercatori di Clusit evidenziano come la lettura dei dati della distribuzione geografica percentuale delle vittime dia indirettamente la fotografia di come stia variando la digitalizzazione nel mondo e, allo stesso tempo, dei paesi che hanno adottato migliori azioni di difesa. In questo quadro, **gli attacchi rivolti all'Europa hanno rappresentato nel 2022 quasi un quarto (24%) degli attacchi globali**, in crescita di 3 punti percentuali rispetto al 2021 e in raddoppio rispetto a cinque anni fa.

L'**America** nel suo complesso diminuisce di 7 punti percentuali il numero di vittime rispetto all'anno precedente, con un valore di attacchi pari al 38%. Diminuiscono gli attacchi in **Asia** (8%) e rimangono stabili quelli in **Oceania** e **Africa** rispettivamente il 2% e l'1% del totale.

Le tecniche d'attacco, nel mondo e in Italia

Il **malware** rappresenta la tecnica con cui viene sferrato il 37% degli attacchi globali; seguono **vulnerabilità** (12%, escludendo la componente di attacchi basati sui cosiddetti "0-day"), **phishing e social engineering** (12%), in crescita del **52%** sul totale rispetto allo scorso anno, come gli **attacchi DDoS** (4%), che segnano una variazione percentuale annua del **+258%** e **tecniche multiple** (**+72%** la variazione percentuale annua), in virtù della natura più complessa degli attacchi.

Anche nel nostro Paese, come nel resto del mondo, prevalgono gli attacchi per mezzo di **malware**, che rappresentano il **53% del totale italiano**, un valore che supera di 6 punti percentuali il dato globale. In Italia, notano i ricercatori di Clusit, gli incidenti in questo settore hanno impatti gravi o gravissimi nel **95%** dei casi.

"*Gli attacchi nel nostro Paese vengono compiuti con tecniche quasi sempre standardizzate, ormai frutto dell'industria del cyber-crime che è la matrice prevalente delle attività malevole. Questo conferma come l'aumento degli attacchi in Italia sia con-causato da forti limiti nella capacità di difesa delle vittime*", ha commentato Alessio Pennasilico, membro del Comitato Scientifico di Clusit e coautore del Rapporto.

Nel nostro Paese hanno invece avuto un impatto minore rispetto al resto del mondo gli attacchi di phishing e di ingegneria sociale, pari all'8%, mentre resta preoccupante la percentuale di incidenti basati su vulnerabilità note – pari al 6%, comunque inferiore rispetto al dato globale - che denotano la persistente inefficacia dei processi di gestione delle vulnerabilità e degli aggiornamenti di sicurezza nelle nostre organizzazioni.

Gli attacchi DDoS rappresentano il 4%, in linea con il dato globale, in diminuzione dal 2021 come confermato anche dall'analisi Fastweb della situazione italiana in materia di cyber-crime contenuta all'interno del Rapporto Clusit.

Secondo i ricercatori di Clusit appare probabile una migliorata capacità di protezione delle organizzazioni su questo fronte, insieme alla tendenza dei cybercriminali ad adottare tecniche di attacco meno impegnative e più redditizie, come le campagne malware. Infatti, ben **il 64% degli incidenti a livello globale hanno come causa azioni "maldestre", degli utenti o del personale informatico nelle aziende**. "*Ritroviamo malware, Vulnerabilità, Phishing e Social Engineering ed Account Cracking ancora tra le tecniche più utilizzate dai criminali informatici: questo significa che ancora non sappiamo gestire correttamente i nostri account, non teniamo aggiornati i nostri dispositivi, server o servizi e clicchiamo incautamente link pericolosi nelle email*", afferma Pennasilico.

Nel Rapporto Clusit non manca inoltre il riferimento agli eventi che hanno colpito nel 2022 i singoli cittadini e le PMI, ben messi in luce dal **contributo della Polizia Postale e delle Comunicazioni**. "*Rileviamo che anche nel contesto della vita digitale sociale le minacce cyber stanno assumendo un grado di estensione sempre più preoccupante: è imprescindibile che la Scuola, l'Università, i soggetti pubblici e privati lavorino in sinergia per sviluppare una cultura della sicurezza che sia parte del patrimonio di conoscenze di tutti i cittadini, a partire dalle nuove generazioni*", ha affermato Gabriele Faggioli, presidente di Clusit.

Analisi Fastweb della situazione italiana in materia di cyber-crime

Come ogni anno, Fastweb ha contribuito al Rapporto Clusit analizzando le principali tendenze grazie alla elaborazione dei dati provenienti dal proprio Security Operation Center (SOC) attivo 24 ore su 24 e dai propri centri di competenza di sicurezza informatica. Dall'analisi sull'infrastruttura di rete di Fastweb, costituita da oltre 6,5 milioni di indirizzi IP pubblici, su ognuno dei quali possono comunicare centinaia di dispositivi e server, sono stati registrati oltre 56 milioni di eventi di sicurezza, un aumento del 25% rispetto agli eventi rilevati nel Report 2021.

I fenomeni e gli effetti legati al cybercrime osservati nel 2022 sono, per la maggior parte, in continuità con quanto visto nel 2021. Si continua ad osservare una progressiva consapevolezza da parte delle aziende rispetto ai rischi informatici: infatti, nonostante l'intensificarsi degli eventi di sicurezza e

l'elevata diversificazione delle tecniche di attacco, nel 2022 le rilevazioni rispetto agli effetti dannosi di questi eventi sono rimaste pressoché invariate. Sono state rilevate significative diminuzioni nel numero di attacchi Ddos (-25% degli eventi rispetto al 2021), dei servizi critici esposti su internet (-9%) e del numero di malware (-4%). Quest'ultimo dato, in particolare, è legato al rafforzamento del livello di cyber-resilienza delle aziende, in quanto, nonostante un deciso aumento delle famiglie di malware (+22%), si registra un numero inferiore di attacchi.

Il Rapporto Clusit 2022 sarà presentato al pubblico il prossimo 14 marzo, in apertura di Security Summit, il più importante convegno italiano sulla cybersecurity, organizzato da Clusit - Associazione Italiana per la Sicurezza Informatica – con Astrea, Agenzia di Comunicazione ed Eventi specializzata nel settore della Sicurezza Informatica. Security Summit si svolge a Milano - esclusivamente in presenza - dal 14 al 16 marzo 2023.

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 600 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 Polizia Postale e delle Comunicazioni, 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, il Centro di Competenza nazionale ad alta specializzazione per la cybersecurity 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