Rapporto Clusit – Focus Pubblica Amministrazione e Sanità

Clusit, crescono gli attacchi alla Sanità in Europa e aumenta la gravità; attacchi alla PA italiana sempre più di matrice politico-ideologica.

I dati relativi all'andamento della cyber security nel primo trimestre dell'anno illustrati oggi nel corso di Security Summit a Roma.

Milano, 19 giugno 2024 – Gli attacchi condotti dalla criminalità organizzata verso l'Italia sono in aumento più che nel resto del mondo, con una percentuale del 65% tra il 2022 e il 2023 (verso una crescita del 12% a livello globale). A questi dati, già evidenziati dal Rapporto Clusit[1] per il 2023, si aggiunge ora il quadro specifico sulla cyber security nella **Pubblica Amministrazione** e nella **Sanità**.

I **Focus "Rapporto Clusit Italia e PA" e "Sanità"** sono stati illustrati oggi nel corso dell'edizione romana di Security Summit, il convegno organizzata da **Clusit**, l'Associazione Italiana per la Sicurezza Informatica, con **Astrea**, Agenzia di Comunicazione ed Eventi specializzata nel settore della Sicurezza Informatica, a cui hanno partecipato circa 250 professionisti e rappresentanti del mondo accademico e delle istituzioni.

Nel 2023 ben l'11% degli attacchi registrati nel mondo ha avuto luogo nel nostro Paese, mentre nel 2012 erano meno dell'8% e nel 2011 meno del 3,5%. Complessivamente, nell'ultimo quinquennio gli attacchi significativi registrati nel nostro Paese sono decuplicati

La Pubblica Amministrazione
Si conferma particolarmente critica la situazione della Pubblica Amministrazione italiana, verso cui si è registrato un aumento degli attacchi di oltre sei volte, passando da meno di dieci attacchi significativi nel 2019 a quasi sessanta nel 2023.

"*L'Italia sta subendo un attacco sistematico e senza precedenti, le cui concause possono verosimilmente essere identificate sia in una digitalizzazione tardiva e affrettata delle nostre imprese ed amministrazioni, sia - e soprattutto - nella atavica mancanza di una corretta e consolidata cultura della sicurezza nella maggior parte degli operatori economici e produttivi nazionali, che sono costituiti da imprese e pubbliche amministrazioni di dimensioni piccole e piccolissime*", ha affermato **Corrado Giustozzi**, del comitato direttivo di Clusit nel corso della presentazione dei dati a Security Summit Roma.

Dall'analisi dei ricercatori di Clusit emerge che gli attacchi compiuti nel primo trimestre 2024 ai danni della Pubblica Amministrazione italiana comprendono nello specifico un ristretto numero di casi di attivismo di matrice politico-ideologica, condotti con tecniche DDoS.

---

[1] Frutto della collaborazione continuativa di oltre cento professionisti nell'ambito di Clusit, il Rapporto Clusit fornisce da quattordici anni 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. L'edizione 2024 del Rapporto Clusit è stata presentata a Security Summit di Milano il 19 marzo. Nel corso dell'anno, in concomitanza con gli appuntamenti "verticali" di Security Summit, vengono analizzati gli scenari di settore.

La nostra Pubblica Amministrazione è stata colpita da una ondata di attacchi cyber in anticipo rispetto ad altri settori, a partire dal 2018: un fenomeno che era stato largamente previsto negli anni precedenti da molti analisti, i quali avevano correttamente indicato il settore pubblico come maggiormente a rischio rispetto a quello privato.
Attualmente, tuttavia, il numero di attacchi verso la Pubblica Amministrazione sembra crescere ad un ritmo leggermente inferiore rispetto agli altri settori, i quali sono probabilmente considerati maggiormente lucrativi da parte delle organizzazioni criminali in cerca di profitto immediato.

I ricercatori di Clusit hanno quindi approfondito lo scenario che ha portato alle prime evidenze del 2024: nello specifico, nel 2023 gli attacchi verso il settore pubblico italiano hanno rappresentato una percentuale compresa tra il 15% e il 30% del totale. In pratica, il settore pubblico ha raccolto in media da un attacco su tre a un attacco su sei; nell'anno si è registrato un picco di azioni dimostrative verso obiettivi governativi a seguito della situazione geo-politica internazionale.

Le modalità di attacco verso il settore sono state prevalentemente attraverso malware, tecnica che tuttavia ha visto una flessione nel 2023 a favore di un incremento di attività DDOS. Questa variazione è stata spiegata dagli esperti di Clusit con il recente e forte spostamento dal piano puramente criminale a quello dimostrativo-ideologico degli attacchi. Sono invece stati relativamente poco significativi gli attacchi basati su tecniche di social engineering, le quali sembrano invece essere generalmente più utilizzate nei confronti delle vittime appartenenti al settore privato.

Anche l'analisi della "severity" degli attacchi riflette, secondo gli esperti di Clusit la natura ideologica e dimostrativa dei cyber criminali nel settore Pubblico: nel 2023 si è assistito ad una forte diminuzione degli attacchi aventi severità critica ed un corrispondente incremento di quelli aventi severità alta e media, intrinsecamente meno gravi rispetto ad attacchi criminali veri e propri.

La Sanità

Nel contesto dell'edizione romana di Security Summit si è svolto anche il tradizionale focus sul settore Healthcare, organizzato da Clusit in collaborazione con AIIC, Associazione Italiana Ingegneri Clinici, AISIS, Associazione Italiana Sistemi Informativi in Sanità, AUSED, Associazione di Utilizzatori Sistemi e Tecnologie dell'Informazione.
Nell'occasione, è stato presentato il **Rapporto Clusit Healthcare**, con i dati relativi agli attacchi cyber in ambito sanitario per il primo trimestre 2024.

L'incremento degli attacchi al settore nel nostro Paese è stato graduale, negli anni, ma non per questo meno significativo; i cyber attacchi di successo e di pubblico dominio verso il comparto healthcare sono aumentati nel 2023 fino quasi a raddoppiare rispetto al 2018, dopo la stasi dei due anni precedenti. Tuttavia, almeno per il primo trimestre del 2024 si è osservata una riduzione della percentuale di crescita rispetto al totale mondiale.

Da gennaio a marzo 2024 gli attacchi alla sanità sono stati esclusivamente perpetrati con finalità di cybercrime e, a differenza di altri settori, gli attacchi di DDOS sono stati marginali rispetto a quelli che puntano all'accesso ai sistemi e soprattutto alla sottrazione di dati. Le più utilizzate, sono state tecniche "sconosciute" (nel 50% dei casi), malware (33% dei casi), vulnerabilità generiche (14% dei casi).

La maggior parte degli attacchi ha colpito, come in passato, vittime nell'area delle Americhe (63% nel primo trimestre 2024, contro l'84% nel 2023); tuttavia, da gennaio a marzo 2024 si è verificato un aumento preoccupante della percentuale di incidenti in Europa: dal 10% del 2023 al 33% del 2024.

Nel primo trimestre dell'anno la "severity" degli attacchi compiuti ai danni del settore sanitario italiano è stata "critica" nel 40% dei casi, "elevata" nel 53%. Le percentuali erano rispettivamente del 37% e del 47% nel 2023. Si tratta di piccole oscillazioni, che non fanno che confermare la

gravità elevata degli incidenti nel settore, maggiore rispetto alla media, secondo i ricercatori di Clusit: l'impatto complessivo degli incidenti del comparto rimane decisamente grave, e questo appare coerente con le finalità dei cybercriminali, che mirano in maniera aggressiva alla monetizzazione derivante dal furto dei dati sanitari.

"*L'incremento della gravità degli attacchi nel settore sanitario nel primo trimestre di quest'anno è un indice significativo*", ha commentato Claudio Telmon, del comitato direttivo di Clusit, che ha presentato i dati. "*L'aumento degli attacchi registrati da Clusit nel settore sanitario in maniera costante è iniziato già diversi anni fa; la criminalità informatica è, infatti, decisamente consapevole che l'Healthcare deve minimizzare i disservizi in modo da poter offrire continuità nella sua funzione; d'altro canto, i sistemi informativi della sanità sono particolarmente complessi, critici ma con problemi anche di obsolescenza importanti, e richiederebbero certamente maggiori investimenti per quanto riguarda la cyber security*", ha concluso Telmon. "*Ci auguriamo che l'analisi del Rapporto Clusit contribuisca ad orientare, almeno in parte, le prossime scelte di investimento del settore*".

Security Summit

Dopo le tappe di Milano e Roma, nel 2024 Security Summit sarà a Cagliari (18 settembre) e Verona (24 ottobre); è prevista inoltre una "Streaming Edition Autumn" (7 novembre). Oltre agli appuntamenti dedicati ai settori verticali, come Energy & Utilities ed Healthcare, è in programma un approfondimento in ambito Manufacturing (7 novembre).

Security Summit è un'iniziativa di:

Clusit, 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.

Astrea, Agenzia di Comunicazione e Marketing, specializzata nell'organizzazione di eventi business nel mondo della tecnologia, e in particolare della Sicurezza Informatica. Con sede operativa a Milano, Astrea mette le competenze dei propri professionisti a disposizione delle organizzazioni per sviluppare soluzioni creative ed innovative volte a incrementare visibilità e ad acquisire autorevolezza sui mercati di riferimento. www.astrea.pro

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