Rapporto Clusit 2023 – Focus Healthcare

Cyber Security nella Sanità, gli attacchi continuano a crescere nel primo trimestre dell'anno

Nei primi tre mesi 2023 gli attacchi alle organizzazioni del settore sono stati il 17% del totale (contro il 12% dello scorso anno); il 71% ha avuto un impatto "critico".
In Italia gli attacchi alle strutture sanitarie sono triplicati negli ultimi quattro anni.

CLUSIT con le quattro Associazioni nazionali AIIC, AISIS, ANRA, AUSED a Healthcare Security Summit: "investire in formazione, non ci sono più scuse".

Milano, 15 giugno 2023 - È stato nel 2022 il settore più attaccato dai cyber criminali (se si esclude il fatto che la maggior parte degli attacchi è stata rivolta a "bersagli multipli"), e nel primo trimestre di quest'anno viene confermato il trend di crescita: gli attacchi sferrati alla sanità a livello globale sono stati il 17% sul totale da gennaio a marzo 2023, contro il 12% del 2022.
Non fa eccezione il nostro Paese, dove i cyber attacchi negli ultimi quattro anni sono triplicati.

I dati emergono dal **focus "Healthcare" del Rapporto Clusit** relativo al primo trimestre 2023[1] presentato questa mattina dai ricercatori del Comitato Direttivo di Clusit, Sofia Scozzari e Claudio Telmon, nel corso di Healthcare Security Summit. Il convegno è stato promosso da Clusit, l'Associazione Italiana per la Sicurezza Informatica con AIIC, Associazione Italiana degli Ingegneri Clinici, AISIS, Associazione Italiana Sistemi Informativi in Sanità, ANRA, Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali, e AUSED, Associazione Utilizzatori Sistemi e tecnologie dell'Informazione, e in partnership con Microsoft, per analizzare lo stato dell'arte della cybersecurity nel settore sanitario e farmaceutico. Sono stati oltre 120 i partecipanti allo streaming.

L'obiettivo degli attacchi
Dai dati del Rapporto Clusit – e in particolare dal focus Healthcare 2023 - emerge che l'obiettivo della criminalità informatica nel settore della sanità continua ad essere la monetizzazione, piuttosto che azioni dimostrative o di spionaggio: gli attacchi nei primi tre mesi dell'anno sono stati infatti quasi tutti riferibili al "cybercrime", in linea con la tendenza dello scorso anno, eccetto per una minima percentuale (3%) riferibile ad episodi di "hacktivism".
I dati sanitari sono infatti preziosi per molti soggetti – hanno evidenziato i ricercatori di Clusit - e vanno ad alimentare un mercato nero, rintracciabile nel dark web, particolarmente fiorente.

Ancora, illustrando i dati del focus Sanità del Rapporto Clusit, Sofia Scozzari e Clauio Telmon hanno evidenziato che nel primo trimestre di quest'anno sono stati rilevati oltre un terzo degli attacchi registrati nel corso di tutto lo scorso anno.

[1] 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. Il focus Healthcare è stato compilato per il primo trimestre 2023 dal team di ricercatori Clusit che analizza e revisiona i dati relativi agli attacchi noti in Italia e nel mondo.
Le informazioni relative alla raccolta, analisi e pubblicazione dei dati sono disponibili al relativo capitolo del Rapporto Clusit 2023.

“Questa tendenza esprime la difficoltà a proteggere i sistemi informativi da parte di un settore costretto, come tanti, ad una rapida digitalizzazione e particolarmente sotto pressione dagli anni di pandemia, ma anche di un settore che è indubbiamente arrivato meno preparato di altri a questa sfida”, ha commentato Alessandro Vallega del Comitato Scientifico di Clusit.

La gravità dell’impatto
La gravità dell’impatto degli incidenti nel settore healthcare è stata complessivamente per i primi tre mesi dell’anno più bassa rispetto alla media, con il 71% di incidenti classificati come “grave” o “critico” rispetto a una media dell’80%. Tuttavia, trattandosi del settore più colpito, l’impatto globale risulta comunque estremamente alto, e le conseguenze sociali dell’interruzione di servizi in questo ambito, o la diffusione di informazioni sullo stato di salute dei cittadini sono particolarmente rilevanti.

Le tecniche di attacco
Le strutture sanitarie italiane nel primo trimestre dell’anno sono state per lo più colpite attraverso tecniche sconosciute e, in un terzo circa dei casi, da malware. L’utilizzo di vulnerabilità come punto di ingresso per violare sistemi ha rappresentato invece nel periodo il 16% dei casi. Di rilievo, secondo i ricercatori di Clusit, anche il 9% di attacchi basati su furti di identità e violazione di account, decisamente più alto della media.

Far crescere awareness e formazione
Oggi le organizzazioni sanitarie utilizzano tecnologia, rete e strumenti digitali per gran parte della loro attività: per garantire la sicurezza dell'intero sistema è necessario che ciascuno sia consapevole del loro uso, conosca i rischi informatici e le contromisure. Altrimenti si permette ai criminali di creare grandi danni alle persone e alle organizzazioni, interrompendo i servizi di cura, ricattando gli uni e gli altri e vendendo i dati rubati. “*Si tratta di minacce per le quali le organizzazioni sanitarie dovrebbero certamente attrezzarsi meglio, anche con costanti verifiche delle vulnerabilità dei sistemi, poiché le conseguenze di questi attacchi non sono solo economiche e organizzative: a rischio ci sono i cittadini e la Società”,* ha affermato Alessandro Vallega.

Tutti partecipanti alla conferenza hanno confermato la gravità della situazione fotografata dai ricercatori e indicato quale mix di formazione, organizzazione e tecnologia deve essere adottato con grande intelligenza per rendere possibile l'accelerazione necessaria e colmare il divario tra la sicurezza che c’è e quella che dovrebbe esserci.

Alessandro Vallega ha auspicato una maggior maturità del processo con il quale si decidono gli investimenti, che oggi è molto basato sugli obblighi di conformità ma che domani dovrebbe essere basato sulle migliori pratiche e sull’analisi del rischio cyber e di quello aziendale.

Purtroppo, hanno evidenziato ancora i ricercatori di Clusit, al contrario di quanto spesso si crede, non sono solo gli utenti con posizioni intermedie all'interno delle aziende sanitarie e farmaceutiche a necessitare di formazione; frequentemente accade che anche i vertici delle organizzazioni con competenze specifiche e di elevato livello in economia, in temi legali e di salute, non abbiano consapevolezza in ambito di cybersecurity. Spesso proprio a questi profili sono riservati accessi ad account privilegiati, con autorizzazioni per compiere operazioni bancarie e fornire input amministrativi: per questo sono bersagli molto interessanti per i cyber criminali.

Il PNRR prevede finanziamenti pari a 2,5 miliardi circa per il potenziamento degli strumenti digitali, dell’infrastruttura e del fascicolo sanitario; tuttavia, non sono inclusi investimenti per la formazione specifica del personale sanitario. È quindi fondamentale che le singole organizzazioni investano in programmi di sensibilizzazione e formazione per il personale e che adottino politiche e procedure di sicurezza appropriate per proteggere i dati sanitari e prevenire gli attacchi cyber.

“*Anche nel settore sanitario la migliore prevenzione è la formazione, che deve portare alla consapevolezza nell'uso delle tecnologie digitali, per operare in sicurezza e non compromettere eventuali contromisure già messe in atto*”, ha concluso Vallega a margine della tavola rotonda **"Cybersecurity in sanità: non ci sono più scusanti?" nel corso di Healthcare Security Summit** a cui hanno partecipato:

- **Alberino Battagliola,** Tesoriere ANRA
- **Giorgio Callea**, Corporate Internal Auditor, Gruppo Bracco
- **Roberto Goldoni**, Azienda Ospedaliero Universitaria di Parma
- **Stefano Longo,** Head of Sales, Cybersecurity, Compliance and Identity, Microsoft Italia
- **Mario Lugli**, Azienda Ospedaliero Universitaria di Modena, Comitato ICT AIIC
- **Andrea Provini**, Centro Diagnostico Italiano e Presidente AUSED
- **Alberto Ronchi**, Istituto Auxologico Italiano e Presidente AISIS

Healthcare Security Summit 2023 è uno degli appuntamenti di approfondimento verticale dedicati da Clusit ai settori a maggior impatto per la sicurezza di dati e informazioni di aziende e cittadini. Con l’organizzazione di Astrea, agenzia specializzata nell’organizzazione di eventi business live e digital nel mondo della sicurezza informatica, Healthcare Security Summit crea ogni anno uno spazio di approfondimento sui rischi cyber e sulla necessità di gestire gli stessi attraverso un approccio olistico con i protagonisti del mercato.

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