Tecnologia - *Clusit: la sanità bersaglio dei cybercriminali, nel 2025 un terzo degli incidenti ha matrice attivista*

Milano - 23 giu 2025 (Prima Notizia 24) **Si contano già 131 episodi, pressione in crescita sul settore.**

La sanità continua a essere tra gli obiettivi privilegiati degli attacchi informatici a livello mondiale. Secondo i più recenti dati Clusit, l'Associazione Italiana per la Sicurezza Informatica, nel 2024 sono stati registrati 471 incidenti cyber nel settore, pari al 13% del totale degli attacchi globalmente noti. Nel solo primo trimestre del 2025 si contano già 131 episodi – oltre un quarto di quelli rilevati nell'intero anno 2024 - a conferma di una pressione in crescita sul settore. Se il cybercrime era la principale motivazione dietro gli attacchi nel 2024, con una quota del 99%, nel 2025 si osserva un cambiamento significativo: gli attacchi di matrice criminale rappresentano circa due terzi degli eventi (66%), mentre un terzo (33%) è attribuibile a fenomeni di Hacktivism, in netta crescita e in linea con i trend globali: si tratta di attacchi che non puntano al profitto, ma a veicolare messaggi politici o sociali, rendendo più difficile prevedere i bersagli e le tempistiche, e aumentando la frequenza e la portata delle offensive, come spiegato dai ricercatori di Clusit. Le tecniche di attacco più diffuse nel settore sanitario sono quelle classificate come "Unknown" (39% nel 2024, 40% nel primo trimestre 2025) e il Malware (33% nel 2024, sceso al 20% nel 2025). I ricercatori di Clusit hanno inoltre evidenziato che molto frequentemente gli attacchi perpetrati con finalità di Hactivism vengono veicolati tramite DDoS, che mirano a saturare le risorse dei sistemi informatici, rendendo indisponibili siti web e, in particolare nel settore sanitario, portali di prenotazione, piattaforme di telemedicina e sistemi di gestione delle emergenze, con potenziali gravi conseguenze su diagnosi, cure e accesso alle informazioni critiche per i pazienti. Questa tecnica, in effetti, è stata nel primo trimestre 2025 la causa del 34% del totale degli incidenti in sanità, riflettendo il picco di attività hacktiviste. Dal punto di vista geografico, nel 2024 l'81% degli incidenti si era concentrato negli Stati Uniti, con il 13% in Europa. Nel 2025 si registra una diversificazione degli attacchi: la quota americana si riduce al 51%, mentre cresce la presenza di attacchi in Europa (18%), Oceania (dal 4% al 7%) e soprattutto in Asia, che passa dal 2% al 24%. Gli esperti di Clusit hanno poi posto l'accento sulla gravità degli incidenti: quasi un terzo degli attacchi (28%) nel 2024 ha avuto una severity critica; tuttavia, nel primo trimestre 2025 questa percentuale è scesa al 19%. Gli impatti gravi (High) riguardano però ancora oltre la metà degli incidenti di quest'anno (56% nel 2024, 47% nel 2025). "Il settore sanitario è sempre più esposto a minacce sofisticate e crescenti; per rispondere efficacemente a questo scenario, è necessario investire non solo in tecnologie avanzate, ma anche in nuovi ruoli organizzativi e in una formazione continua e specializzata. Un aspetto fondamentale è l'inclusione di settori aziendali come l'Ingegneria Clinica, finora non sempre sufficientemente coinvolti nelle strategie di sicurezza", afferma Claudio Telmon, del comitato direttivo Clusit.

“Come è stato messo in evidenza oggi a Healthcare Security Summit, la direttiva NIS2 rappresenta una grande opportunità per riportare la sicurezza al centro delle decisioni strategiche anche delle strutture sanitarie, garantendo un approccio europeo più solido e coordinato per la protezione delle infrastrutture critiche. In un momento di incertezza e tensioni geopolitiche, questa direttiva può diventare la base per costruire resilienza e fiducia nel sistema sanitario digitale”, ha concluso Telmon.

(Prima Notizia 24) Lunedì 23 Giugno 2025