Le organizzazioni sanitarie perdono il 20% dei loro dati sensibili in ogni attacco ransomware, rivela la nuova ricerca dei Rubrik Zero Labs

- *Le organizzazioni sanitarie hanno registrato un aumento del 50% degli attacchi legati alla crittografia rispetto alla media globale nel 2023.*
- *Il passaggio al cloud aggiunge rischi intrinseci e punti ciechi per la sicurezza, con il 70% di tutti i dati che non è generalmente leggibile dalle soluzioni di sicurezza.*
- *I cyberattacchi impattano sempre più sul personale: nel 44% delle organizzazioni si è verificato un cambiamento di leadership a seguito di un attacco, in crescita rispetto al 36% del 2022.*

Milano, 8 maggio 2024 – I recenti incidenti informatici confermano il settore sanitario come obiettivo primario per gli hacker. Una nuova ricerca dei Rubrik Zero Labs rivela che gli attacchi ransomware hanno un impatto maggiore su questo specifico settore: un quinto di tutti i dati sensibili, appartenenti alle organizzazioni sanitarie, viene impattato in ogni attacco ransomware.

La nuova ricerca dei Rubrik Zero Lab "The State of Data Security: Measuring Your Data's Risk" offre approfondimenti sui rischi reali relativi alla sicurezza dei dati, in un mondo in cui il ritmo e volume degli eventi informatici continua ad aumentare a livello globale, favorito dall'esplosione dei dati nel cloud e dalla varietà degli ambienti informatici moderni. Rubrik Zero Labs studia le sfide che le organizzazioni devono affrontare per proteggere i loro asset più preziosi – i dati – e come ridurre il rischio legato alla sicurezza dei dati e prepararsi all'evoluzione del ciclo del rischio ossia prima, durante e dopo un attacco informatico.

"Nonostante le conseguenze degli attacchi informatici siano ormai di dominio pubblico, il rischio legato alla sicurezza dei dati è un tema che continua a essere oscuro, soprattutto per quanto riguarda ciò che i team di sicurezza possono effettivamente cambiare e ciò che non possono", ha dichiarato Steven Stone, Head dei Rubrik Zero Labs. "Con questa ricerca intendiamo fornire spunti misurabili che i leader dell'IT e della sicurezza possano riportare all'interno della propria organizzazione per promuovere una maggiore resilienza informatica, in particolare con i loro partner nei team di business e di governance".

L'unità di ricerca di Rubrik Zero Labs abbina la telemetria di Rubrik su più di 6.100 organizzazioni con i risultati di un sondaggio condotto da Wakefield Research su oltre 1.600 leader dell'IT e della sicurezza, la metà dei quali sono CIO e CISO. Inoltre, questo studio ha integrato i dati di due aziende partner di Rubrik e di altre cinque organizzazioni di ricerca con l'obiettivo di tracciare un quadro più completo e oggettivo. I risultati principali riguardano il panorama delle minacce informatiche nel settore sanitario, i punti oscuri della sicurezza dei dati nel cloud e il ransomware:

Il settore sanitario supera di gran lunga la media mondiale in termini di dati sensibili.

- Rubrik ha osservato che le organizzazioni sanitarie proteggono il 22% di dati in più rispetto alla media globale.
- Tipicamente, un'organizzazione sanitaria ha visto crescere il proprio patrimonio di dati del 27% lo scorso anno.
- Un'organizzazione sanitaria ha oltre 42 milioni di record di dati sensibili – il 50% in più rispetto alla media globale di 28 milioni.
- I record di dati sensibili nelle organizzazioni sanitarie osservate sono cresciuti di oltre il 63% nel 2023, un dato di gran lunga superiore a qualsiasi altro settore e più di cinque volte rispetto alla media globale (13%).

Il ransomware ha un impatto maggiore nel settore sanitario

- Gli attacchi ransomware contro le organizzazioni sanitarie osservate hanno un impatto stimato di quasi cinque volte superiore rispetto alla media globale.
- Ciò equivale a una stima del 20% del totale dei dati sensibili di un'organizzazione sanitaria tipica che subisce un impatto ogni volta che si verifica un attacco ransomware, rispetto al 6% di un'organizzazione media.
- La virtualizzazione è davvero importante per il settore sanitario: il 97% di tutti i dati crittografati nelle organizzazioni sanitarie osservate da Rubrik lo scorso anno si collocava all'interno di un'architettura virtuale, rispetto all'83% degli altri settori.

Con l'adozione sempre più diffusa del cloud, emergono nuovi punti oscuri per la sicurezza

- Le organizzazioni stanno diventando sempre più dipendenti dal cloud. Nel 2023, Rubrik ha osservato che l'architettura cloud conservava il 13% dei dati di un'organizzazione, rispetto al 9% del 2022. In confronto, l'architettura on-premise è scesa dal 77% nel 2022 al 70% nel 2023.
- Tra le organizzazioni vittime di un cyberattacco nel 2023, molte sono state attaccate su più aspetti del loro ambiente ibrido, con il 67% degli attacchi che hanno colpito i dati SaaS, il 66% il cloud e il 51% le sedi on-premise.
- Secondo la telemetria di Rubrik, il cloud comporta un rischio intrinseco basato su punti ciechi della sicurezza e dati sensibili vulnerabili:
    - Punto cieco n. 1: il 70% di tutti i dati in una tipica istanza cloud è costituito da object storage, che in genere ha una copertura di sicurezza molto inferiore rispetto ad altre aree.
    - Punto cieco n. 2: l'88% di tutti i dati nell'object storage non è verificato come leggibile o protetto da importanti tecnologie e servizi di sicurezza.
    - Punto cieco n. 3: oltre il 25% dei dati nell'object storage è soggetto a requisiti normativi o legali, come le informazioni sanitarie protette (PHI) e le informazioni di identificazione personale (PII).

Il ransomware continua a stravolgere le organizzazioni e i team IT e di sicurezza

- l 94% dei responsabili IT e della sicurezza ha dichiarato che l'anno scorso la propria organizzazione ha subito un attacco informatico significativo e in media ha dovuto affrontare 30 attacchi in un anno. Un terzo di queste vittime ha subito almeno un attacco ransomware.
- l 93% delle organizzazioni che hanno subito un attacco ransomware ha dichiarato di aver pagato una richiesta di riscatto, e il 58% di questi pagamenti è stato motivato principalmente dalla minaccia di diffondere i dati rubati. **In Italia la percentuale è simile con il 94%, ma sale vertiginosamente la percentuale della motivazione della minaccia di diffondere i dati rubati che arriva al 74%**
- Il 96% dei leader senior del settore IT e della sicurezza ha riferito di aver subito un impatto emotivo e/o psicologico come conseguenza diretta di un attacco informatico, con il 38% che si è preoccupato della sicurezza del proprio posto di lavoro.
- Il 44% delle organizzazioni ha segnalato di aver registrato cambiamenti nella leadership a seguito di un attacco informatico, rispetto al 36% della ricerca dei Rubrik Zero Labs dell'autunno 2022 "The State of Data Security: The Human Impact of Cybercrime".

Per leggere la ricerca completa, visitare il sito https://rubrik.com/zero-labs

Metodologia della ricerca

La ricerca "The State of Data Security: Measuring Your Data's Risk" di Rubrik Zero Labs è stata commissionata da Rubrik e condotta da Wakefield Research tra 1.625 decision maker in materia di IT e sicurezza di aziende con almeno 500 dipendenti. Gli intervistati erano composti per circa la metà da CIO e CISO e per l'altra metà da vicepresidenti e direttori IT e di sicurezza. La ricerca è stata condotta negli Stati Uniti, Regno Unito, Francia, Germania, Italia, Paesi Bassi, Giappone, Australia, Singapore e India tra il 18 e il 30 gennaio 2024. Nessuna di queste organizzazioni è già cliente di Rubrik. L'indagine ha integrato la telemetria di Rubrik, prendendo in esame oltre 6.000 clienti in 22 settori e 68 Paesi. I dati comprendono oltre 42 exabyte di storage logico protetto e più di 38 miliardi di record di dati sensibili da gennaio a dicembre 2023.