Ricerca Rubrik Zero Labs: solo l'8% delle aziende italiane recupera completamente i dati dopo aver pagato il riscatto del ransomware tramite gli strumenti di decodifica degli attaccanti

- *A livello globale, il 93% delle organizzazioni ha riscontrato dei seri problemi con le proprie soluzioni di backup e recovery*
- *Nove aziende su dieci hanno confermato che gli hacker hanno tentato di accedere ai backup durante un cyberattacco, e il 73% ha avuto un successo parziale*
- *Quasi la metà (47%) dei responsabili IT e della sicurezza ritiene che il budget per la cybersecurity per il 2023 non sia sufficiente*
- *La quantità di dati protetti dalle aziende è aumentata del 25% nel 2022, rispetto all'anno precedente*

Milano, 19 aprile 2023 - Quasi tutti i responsabili IT e della sicurezza (96%) a livello globale temono che la loro organizzazione non sia in grado di mantenere la continuità operativa in seguito a un attacco informatico, secondo un nuovo studio pubblicato oggi da Rubrik, la Zero Trust Data Security™ Company. "The State of Data Security by Rubrik Zero Labs: The Hard Truths of Data Security" offre una visione approfondita del panorama della sicurezza dei dati, di ciò che i leader IT e della sicurezza hanno sperimentato nel 2022 e delle azioni che stanno compiendo per implementare una reale resilienza informatica.

Rubrik Zero Labs ha commissionato il suo secondo studio globale a Wakefield Research per raccogliere le opinioni di oltre 1.600 leader dell'IT e della sicurezza - metà dei quali erano CIO e CISO - in 10 paesi (tra cui l'Italia), integrando con dati raccolti dalla telemetria di Rubrik.

Questi alcuni dei risultati principali che emergono dalla ricerca:

La Data Security è un tema sempre più centrale, ma la realtà e i risultati variano:

- La Data Security sta diventando sempre più complessa e i dati da proteggere stanno crescendo rapidamente. I dati di Rubrik hanno rivelato che la crescita media dei dati protetti nel 2022 è stata del 25% (i dati on premise sono cresciuti del 19%, quelli cloud del 61% e quelli SaaS sono cresciuti del 236% lo scorso anno).
- Oltre la metà (56%) delle organizzazioni adotta attualmente almeno un'iniziativa "zero trust", una percentuale che in Italia sale al 61%!
- Tuttavia, solo il 56% dei responsabili IT e della sicurezza ha sviluppato o ridefinito un piano di risposta agli incidenti nel 2022 e il 54% ha testato le opzioni di backup e ripristino.

I backup legacy dei dati restano per molti l'ultima linea di difesa, ma sono insufficienti:

- Il 99% delle organizzazioni ha dichiarato di disporre di una tecnologia di backup e ripristino, ma il 93% ha riscontrato problemi significativi con la propria soluzione.
- Nove organizzazioni esterne su dieci hanno riferito che soggetti malintenzionati hanno tentato di colpire i backup dei dati durante un attacco informatico, e il 73% ha avuto un successo almeno parziale in questi tentativi.

- Quasi tre quarti (72%) delle organizzazioni hanno ammesso di aver pagato il riscatto dopo un l'attacco ransomware.
- Solo il 16% di tutte le organizzazioni globali ha recuperato tutti i propri dati attraverso gli strumenti di decriptazione degli aggressori. In Italia questo dato scende addirittura alla metà: solo l'8% ha recuperato tutti i propri dati, il valore più basso tra tutti i paesi.

Problemi nuovi e in continua evoluzione vengono affrontati secondo le modalità esistenti prima di un'intrusione:

- Quasi la metà (47%) dei responsabili IT e della sicurezza ritiene che il budget per la cybersecurity per il 2023 non sia sufficiente.
- Il 27% prevede che i budget per l'IT e la cybersecurity diminuiranno nel 2023.
- Solo il 4% ha dichiarato che quest'anno non ci sono fattori che limitano l'allineamento tra IT e sicurezza.

"È chiaro che le organizzazioni comprendono la gravità e l'impatto degli incidenti informatici, ma vediamo anche una serie di ostacoli che derivano dalla mancanza di preparazione, dal disallineamento tra i team IT e di sicurezza e dalla tendenza eccessiva a ricorrere a soluzioni di backup e ripristino non più sufficienti", ha dichiarato Steven Stone, responsabile di Rubrik Zero Labs. "Nell'attuale era della cybersecurity, il risultato migliore è garantire la resilienza informatica. Gli incidenti sono inevitabili, ed è fondamentale ridurre il rischio prima che sia necessaria una risposta, proteggendo a tutti i costi il vero patrimonio di ogni organizzazione: i dati".

"The State of Data Security" è stato realizzato da Rubrik Zero Labs, l'unità di ricerca sulla cybersecurity dell'azienda nata per analizzare il panorama globale delle minacce, fornire report sulle problematiche emergenti in materia di sicurezza dei dati e offrire alle aziende spunti di riflessione e best practice basate sulla ricerca per proteggere i propri dati dai crescenti eventi informatici.

Metodologia della ricerca
"The State of Data Security: The Hard Truths of Data Security" di Rubrik Zero Labs è stato commissionato da Rubrik e condotto da Wakefield Research tra 1.625 decision maker 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 di IT e sicurezza. La ricerca è stata condotta negli Stati Uniti, Regno Unito, Francia, Germania, Italia, Paesi Bassi, Giappone, Australia, Singapore e India tra il 10 e il 21 febbraio 2023.

Informazioni su Rubrik
Rubrik è in missione per proteggere i dati del mondo. Con la Zero Trust Data Security™, aiutiamo le organizzazioni a raggiungere la resilienza aziendale contro i cyberattacchi, gli insider malintenzionati e le interruzioni operative. Rubrik Security Cloud, basato sul machine learning, protegge i dati nelle applicazioni aziendali, cloud e SaaS. Aiutiamo le organizzazioni a mantenere l'integrità dei dati, a garantire una disponibilità dei dati che resista a condizioni avverse, a monitorare costantemente i rischi e le minacce ai dati e a ripristinare le attività con i loro dati quando l'infrastruttura viene attaccata.
Per ulteriori informazioni, visitare www.rubrik.com/it e seguire @rubrikInc su Twitter e Rubrik, Inc. su LinkedIn