Un’azienda su tre ha cambiato management a seguito di un attacco informatico, rivela una ricerca di Rubrik Zero Labs

In caso di attacco informatico:
Il 92% degli intervistati teme di non essere in grado di mantenere la continuità aziendale;
Un terzo dei consigli di amministrazione ha poca o nessuna fiducia nella capacità della propria organizzazione di recuperare i dati critici e le applicazioni aziendali;
Il 96% delle persone ha subito un impatto emotivo o psicologico

Milano, February 7, 2022 - Secondo la nuova ricerca "The State of Data Security" condotta dai Rubrik Zero Labs, i responsabili IT e della sicurezza devono affrontare in media un attacco informatico alla settimana. Rubrik, la Zero Trust Data Security™ company, ha raccolto le opinioni di oltre 1.600 responsabili della sicurezza e dell'IT, tra cui CISO, CIO, vicepresidenti e direttori di 10 paesi tra cui l’Italia. I risultati hanno messo in luce l'aumento dei rischi per la sicurezza delle aziende, con conseguenti danni diffusi alle organizzazioni e ai loro team IT e di sicurezza.

Questi alcuni dei risultati principali di "The State of Data Security" di Rubrik Zero Labs:

I cyberattacchi continuano ad aumentare in volume e impatto:

- Quasi tutti i leader intervistati hanno subito un attacco informatico nel corso dell'ultimo anno e in media hanno affrontato 47 attacchi, ovvero quasi un attacco informatico a settimana.
- Il 52% ha dichiarato di aver subito una violazione dei dati e il 51% di aver subito un attacco ransomware nell'ultimo anno.
- Solo il 5% delle organizzazioni è stato in grado di ripristinare la continuità operativa o la normale operatività entro un'ora dalla scoperta di un attacco informatico.
- Il 48% dei responsabili IT e della sicurezza ha dichiarato di essere preoccupato per le violazioni dei dati (25%) o per gli eventi ransomware (23%) come minaccia principale per l'anno a venire.

Le organizzazioni stanno perdendo fiducia nella loro capacità di resistere agli attacchi:

- Il 92% degli intervistati teme di non essere in grado di mantenere la continuità aziendale in caso di attacco informatico.
- Un terzo ritiene che il proprio consiglio di amministrazione abbia poca o nessuna fiducia nella capacità dell'organizzazione di recuperare i dati critici e le applicazioni aziendali dopo un attacco informatico.
- Secondo il 76% degli intervistati la propria organizzazione potrebbe prendere in considerazione la possibilità di pagare un riscatto in seguito a un attacco informatico.
- L'11% dei responsabili IT e della sicurezza ha dichiarato di non aver affrontato adeguatamente le vulnerabilità derivanti da precedenti eventi informatici.

Il peso della criminalità informatica si fa sentire:

- Il 96% degli intervistati ha dichiarato di aver subito conseguenze emotive o psicologiche significative in seguito a un attacco informatico, che vanno dalle preoccupazioni per la sicurezza del lavoro (43%) alla perdita di fiducia dei colleghi (37%).
- Circa un terzo degli intervistati ha dichiarato di aver registrato cambiamenti nella leadership a seguito di un attacco informatico.

- Circa un terzo dei leader intervistati ha dichiarato che i team IT e SecOps erano in qualche modo o per nulla allineati quando si trattava di difendere le loro organizzazioni.

"Da questa ricerca emerge chiaramente che i cyberattacchi continuano a produrre un forte impatto sulle organizzazioni globali, con effetti che si stanno via via aggravando", ha dichiarato Steven Stone, Head di Rubrik Zero Labs. "Oltre all'aumento della frequenza e dell'impatto degli eventi informatici, sono gli individui in prima linea che subiscono un colpo psicologico al loro benessere. La fiducia è diminuita e l'ansia è aumentata. Senza un approccio proattivo e affidabile per difendersi dalle moderne minacce informatiche e rafforzare la fiducia nella capacità di un'organizzazione di risolvere questi eventi informatici, questi impatti - sia umani che organizzativi - continueranno a peggiorare e ad alimentarsi a vicenda. La buona notizia è che stiamo assistendo anche a strategie pragmatiche e collaudate in questo stesso ambito che stanno dando i loro frutti e che possano elevare e perfezionare questo tipo di approccio."

"Spesso trascuriamo la dimensione psicologica degli attacchi informatici e il caos che tende a seguire dopo la scoperta di un incidente", ha aggiunto Chris Krebs, ex direttore del CISA e socio fondatore del Krebs Stamos Group. "Criminali e attori statali cercano di generare reazioni emotive quando attaccano, come dimostra l'aumento delle estorsioni criminali e delle campagne di hacking e leak. Alla fine, i responsabili dell'IT e della sicurezza tendono a prendersi la colpa di questi attacchi informatici. Una delle tecniche più efficaci per prepararsi a questo tipo di attacchi consiste nell'accettare che prima o poi si avrà una brutta giornata e che il proprio lavoro consiste nel fare in modo che non diventi una giornata ancora peggiore. Per questo motivo è necessario che tutti coloro che si impegnano nella difesa si uniscano, condividendo le best practice, le utili informazioni che derivano dagli attacchi, le simulazioni, i framework, in modo da rafforzare collettivamente le nostre difese e ridurre al minimo l'impatto psicologico provocato da un attacco".

"The State of Data Security" è stato realizzato da Rubrik Zero Labs, la nuova unità di ricerca sulla cybersecurity creata dall'azienda per analizzare il panorama globale delle minacce, fornire report sulle problematiche emergenti in materia di sicurezza dei dati e fornire alle organizzazioni approfondimenti e best practice basati sulla ricerca per proteggere i propri dati dai crescenti eventi informatici.

Per saperne di più su "The State of Data Security" di Rubrik Zero Labs, visitate il sito https://www.rubrik.com/it/zero-labs.

Metodologia della ricerca

"The State of Data Security" di Rubrik Zero Labs è stato commissionato da Rubrik e condotto da Wakefield Research tra 1.625 responsabili delle decisioni 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 di IT e sicurezza. La ricerca è stata condotta negli Stati Uniti, Regno Unito, Francia, Germania, Paesi Bassi, Italia, Giappone, Australia, Singapore e India tra il 18 e il 27 luglio 2022.

Informazioni su Rubrik

Rubrik è un'azienda di cybersecurity e la nostra missione è proteggere i dati del mondo. Siamo stati i pionieri della Zero Trust Data Security™ per aiutare 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