LO STATO DELLA SICUREZZA DEI DATI:

Misurare il

RISCHIO SUI TUOI DATI

Rubrik Zero Lab

INDICE

INTRODUZIONE 03

DATI E METODOLOGIA 04

I tuoi dati sono a
RISCHIO ATTACCO? 14

I tuoi dati
SONO A RISCHIO? 19

Quanto è
GRAVE? 28

Recovery
PER L'AZZERAMENTO 37

Azzerare
IL RISCHIO SUI DATI 41

RICONOSCIMENTI 48

Questa è una storia che parla dei

I tipi di dati che possiedi, come cambiano i dati,
e una visione pragmatica sulle minacce ai dati.

Ma è anche una storia sul rischio. Come lo misuriamo, la nostra capacità di pianificarlo, come cambia e perché è sempre presente.

Prima però, spieghiamo ***come siamo arrivati fin qui.***

DATI E METODOLOGIA

Rubrik Zero Labs punta a fornire informazioni utilizzabili e indipendenti dai vendor per ridurre i rischi di sicurezza sui dati. A questo scopo, abbiamo incorporato i risultati di quattro fonti primarie.

TELEMETRIA DI RUBRIK = ◆
Abbiamo utilizzato la telemetria di Rubrik per capire quale sia il patrimonio di dati di un'azienda media e i reali rischi.

WAKEFIELD RESEARCH = ▲
I punti di vista di oltre 1600 leader del settore IT e della sicurezza

PARTNER DI RUBRIK = ●
Ricerca e informazioni da parte di due organizzazioni partner di Rubrik

ORGANIZZAZIONI CHE HANNO CONTRIBUITO = ■
Ricerche di autorevoli organizzazioni e istituzioni di cybersecurity

TELEMETRIA DI RUBRIK = ◆

Rubrik Zero Labs pensa che se le aziende ci affidano i loro dati, è nostro obbligo essere trasparenti su ciò che quei dati ci rivelano. A proposito di trasparenza, ecco da cosa è composta la nostra telemetria e come influenza il nostro punto di vista.

Nota: questo studio contiene il primo utilizzo di dati derivati da Laminar. Laminar è una piattaforma leader nella gestione della sicurezza dei dati acquisita da Rubrik nel 2023.

LA TELEMETRIA DI RUBRIK COMPRENDE:

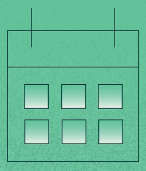
6000+ clienti

68 paesi

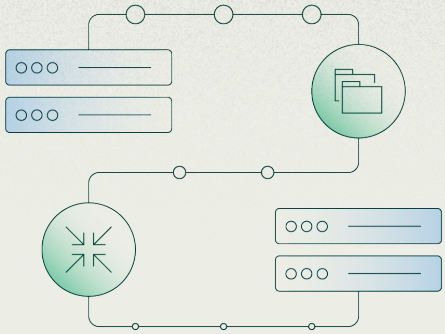
42 EB protetti con oltre 38,4 miliardi di record di dati sensibili

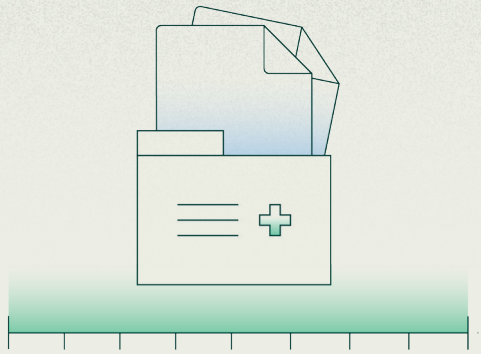
Volume totale di dati protetti:
- 42 exabyte di storage logico
- 963 petabyte di backend (BEPB) di storage fisico

38,4+ miliardi di record di dati sensibili



I dati si riferiscono al periodo compreso tra il 1° gennaio 2023 e il 31 dicembre 2023





FRONT-END vs. BACK-END

Un'osservazione degli esperti di dati: quando la maggior parte delle persone sente parlare di "dati", pensa allo storage logico, anche noto come storage front-end. Noi che ci occupiamo di dati, ci concentriamo sullo storage back-end. Rubrik prende la totalità dei dati di un'organizzazione ed esegue una serie di operazioni con tecniche diverse, tra cui deduplicazione e compressione, per ridurre la quantità di dati di front-end nello storage di back-end. In questo report utilizzeremo lo storage back-end.

Quanti sono 42 EB?

Pensa alla tua cartella clinica con tutto ciò che può contenere, immagini (radiografie, risonanze magnetiche, ecc.), note e altri dati. Se sei come la maggior parte delle persone, hai una cartella clinica di circa 80MB.

Se i 42 EB di dati protetti da Rubrik consistessero solo in cartelle cliniche, corrisponderebbero a cinque cartelle cliniche per ognuno dei 117 miliardi di persone che hanno vissuto sulla terra per tutta la storia dell'umanità. È... un'enormità.

WAKEFIELD RESEARCH

Abbiamo cooperato con Wakefield Research per uno studio che ha raccolto informazioni aggiuntive dai leader del settore IT e della sicurezza. Questi dati integrano la nostra telemetria Rubrik per darci informazioni sul punto di vista dei leader e su ciò che vedono sul campo. Per mantenere la massima neutralità, in questo set di dati non abbiamo incluso i clienti di Rubrik.

1.600+ Leader IT e della sicurezza

10 paesi

50%+ CIO o CISO

1.625

decisori di aziende con almeno 500 dipendenti in 10 paesi (Stati Uniti, Regno Unito, Francia, Germania, Italia, Paesi Bassi, Giappone, Australia, Singapore, India) in tre regioni (Americhe, EMEA e APAC).

50% CIO o CISO

50% Direttori o VP

50% Responsabili delle decisioni in ambito IT

50% Responsabili delle decisioni in ambito sicurezza

PARTNER DI RUBRIK

Abbiamo utilizzato i set di dati e ricevuto indicazioni da due partner di Rubrik al fine di migliorare la resilienza dei dati.

Microsoft ha fornito i dati del Microsoft Digital Defense Report del 2023[1], in particolare i tassi di esfiltrazione dei dati e le raccomandazioni sulla resilienza.

Aon ha fornito i dati del 2023 Aon Cyber Resilience Report[2], in particolare le realtà di backup dei dati e i risultati post-intrusione.

ORGANIZZAZIONI CHE HANNO CONTRIBUITO

Rubrik ha incluso dati chiave provenienti da varie organizzazioni che hanno una visibilità unica rispetto alla telemetria di Rubrik, nel tentativo di fornire una visione il più possibile oggettiva.

Mandiant ha fornito i tempi di permanenza osservati nei suoi eventi di risposta agli incidenti/MDR nel 2023[3].

La Unit 42 di Palo Alto Networks ha fornito i risultati relativi alle richieste e ai pagamenti di ransomware in base agli eventi di risposta agli incidenti/MDR nel 2023.

Proofpoint ha fornito informazioni sugli attacchi al cloud basate sul suo 2023 Human Factors Threat Report[4].

Recorded Future ha fornito le tendenze del ransomware riportate pubblicamente per il 2023[5].

La University of Minnesota Twin Cities - School of Public Health ha fornito gli impatti del ransomware sulle istituzioni sanitarie pubbliche sulla base della ricerca "Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients[6]", pubblicata e attualmente in fase di revisione finale.

1 https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023
2 https://www.aon.com/2023-cyber-resilience-report/
3 https://www.mandiant.com/m-trends
4 https://www.proofpoint.com/us/resources/threat-reports/human-factor
5 https://therecord.media/ransomware-tracker-the-latest-figures
6 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292

PARLIAMO DI RISCHIO

Definiamo le regole di base seguite da questo studio per l'approccio al rischio.

PRIMO

Vogliamo semplificare il "calcolo del rischio":

Quanto è probabile che i tuoi dati vengano colpiti da un'entità esterna + Qual è il rischio presente oggi nei tuoi dati + Quale impatto potrebbe produrre + Le tue decisioni in risposta agli impatti = Calcolo del rischio

ALLA FACCIA DEI CALCOLI COMPLESSI!

SECONDO

Concentriamoci sui dati.
Rubrik si occupa di sicurezza dei dati e le nostre migliori informazioni riguardano i dati delle organizzazioni, non la loro infrastruttura o architettura, quindi ci concentriamo sui rischi interni ai tuoi dati e per i tuoi dati.

Aree di interesse specifiche
Siamo onesti. Ci sono tante cose da fare. Nessuno di noi ha il tempo di approfondire tutti gli aspetti della sicurezza dei dati. Quindi abbiamo ristretto di proposito questo studio ad alcuni argomenti chiave:

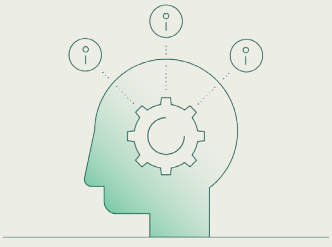
Cloud
I cloud sono disponibili in commercio ormai da decenni. Tuttavia, c'è ancora confusione riguardo alla sicurezza dei dati nel cloud. Il cloud viene preso di mira con più frequenza e successo rispetto alle sue controparti on-premise. Inoltre, presenta dei punti ciechi che ne rendono difficile la difesa.

Ransomware
Non troppo tempo fa, gli esperti avevano previsto il declino del ransomware. Non è mai realmente accaduto, e il ransomware semina ancora il caos in aziende di tutti i tipi.

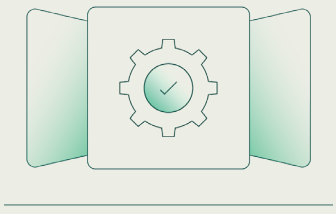
Sanità
Escluse poche eccezioni, le organizzazioni sanitarie producono e conservano più dati sensibili e sono soggette a un maggiore controllo normativo rispetto ad altri settori. Un vantaggio secondario delle restrizioni normative sulla sanità è la maggiore disponibilità di dati pubblici da studiare.

TERZO

A chi si rivolge questo studio?



L'intelligence deve dare informazioni al giusto decisore, e le decisioni sui rischi avvengono di solito a livello di senior leader.



Il nostro obiettivo è fornire informazioni e favorire queste discussioni tra i senior leader delle funzioni aziendali, della cybersecurity e dell'IT.

Dando a questi decisori un punto di partenza comune, saranno meglio preparati ad affrontare i rischi insieme.

ORA PARLIAMO UN PO' DI COME LE PERSONE PERCEPISCONO IL RISCHIO.

Gli esseri umani non sanno gestire bene le incertezze. Quando siamo di fronte alla possibilità che qualcosa accada, di solito pensiamo:

Se un meteorologo ti dice che c'è il 52% di probabilità di pioggia nella tua zona, non ti sta dicendo in modo definitivo: "Sì, pioverà" o "No, non pioverà".

Poi ci sono i dettagli che vogliamo sapere: Quanta pioggia? Pioverà o sarà un diluvio? Devo rimanere a casa? Perché comunque non ho voglia di andare in ufficio.

Queste decisioni sono tue e solo tue.

Sarebbe bello se dovessi prendere queste decisioni solo una volta.

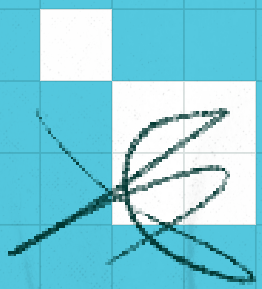
Ma... non funziona così.

La reazione di oggi alla pioggia influisce sul modo in cui penseremo alle previsioni del tempo di domani e può fornirci spunti su come gestire la pioggia.

Questi fattori si combinano per creare nuove condizioni la prossima volta che ci ritroveremo ad affrontare un temporale. Questo vale per la pioggia e per il rischio informatico.

Cominciamo con le minacce esterne che devi prendere in considerazione.

I tuoi dati sono a
RISCHIO ATTACCO?



Iniziamo con una domanda di base:

È probabile che gli aggressori prendano di mira *i miei dati?*

Il tuo frigorifero connesso sta cercando di ucciderti?

Il passaggio degli attacchi ransomware a ESXi rappresenta un'evoluzione enorme

In che modo gli aggressori usano realmente l'AI

QUANTA PARTE DEL TUO NEWSFEED È REALE E QUANTA FUD?

Sarà il prossimo Solarwinds?

(FUD = paura, incertezza, dubbio)

La madre di tutte le violazioni dati: la più grande perdita di dati di sempre

Perché Strawberry Tempest è peggio di Lapsus$

Nessuno può dirti al 100% se subirai un attacco informatico, ma possiamo dirti cosa è successo ad altre persone e aziende come la tua lo scorso anno.

Quasi ogni leader come te ha subito attacchi informatici circa ogni due settimane.

Ecco come è andato lo scorso anno per i leader del settore IT e della sicurezza: ▲

94% dei leader IT e della sicurezza ha dichiarato che l'anno scorso la sua organizzazione ha subito un attacco informatico significativo.

30 La frequenza media è stata di 30 eventi dannosi portati all'attenzione dei leader senior nel corso del 2023.

93% delle organizzazioni esterne ha inviato una notifica formale a un'organizzazione governativa per una perdita di dati.

Gli attacchi informatici sono molto più probabili di un *furto fisico o un incendio.*

Per mettere in prospettiva la probabilità di attacchi informatici, una Compagnia assicurativa europea[1] ha messo a confronto gli attacchi informatici alle minacce tradizionali nello stesso periodo di tempo e ha rilevato che:

67% Le organizzazioni hanno il 67% di probabilità in più di subire un attacco informatico rispetto a un furto fisico.

5x Le organizzazioni hanno cinque volte più probabilità di subire un attacco informatico rispetto a un incendio.

20% delle organizzazioni non sa quali azioni intraprendere in caso di attacco informatico.

1 https://www.aviva.com/newsroom/news-releases/2023/12/One-in-five-businesses-have-been-victims-of-cyber-attack-in-the-last-year/

Gli aggressori attaccano volentieri gli *ambienti ibridi*.

Quindi, se ci sono probabilità che tu subisca un attacco, è utile capire dove e cosa succederà. Sul 94% delle organizzazioni vittime di un attacco informatico, molte sono state colpite in diversi tipi di ambiente: ▲

67%
SaaS

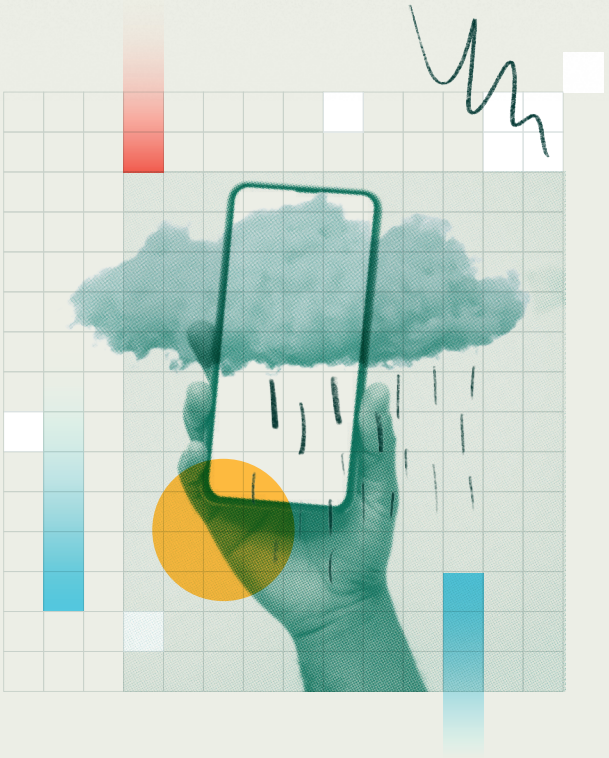
66%
Cloud

51%
On-Premise

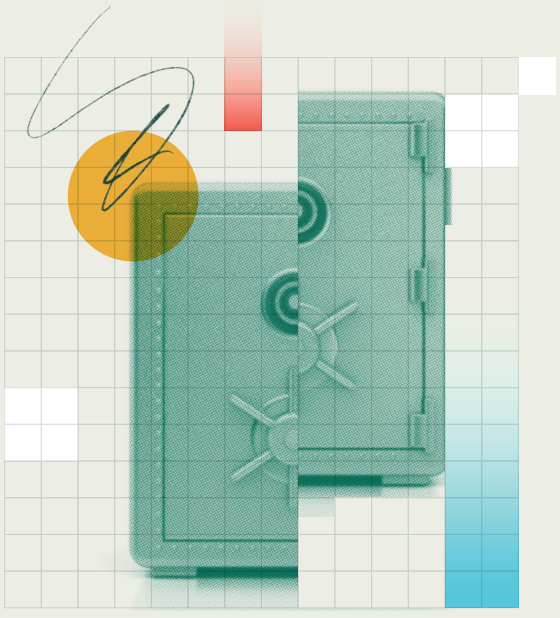
Ecco alcuni dati sui due tipi di attacchi più comuni in questi ambienti: ▲

38%
di queste organizzazioni ha subito almeno una violazione dei dati a causa di un attacco informatico.

33%
di queste vittime ha subito almeno un attacco ransomware.



Quasi tutti i cloud tenant sono stati attaccati nel 2023 e 2 su 3 sono stati compromessi.



Non l'abbiamo scoperto solo con le nostre ricerche. Proofpoint ha segnalato[1]: ■

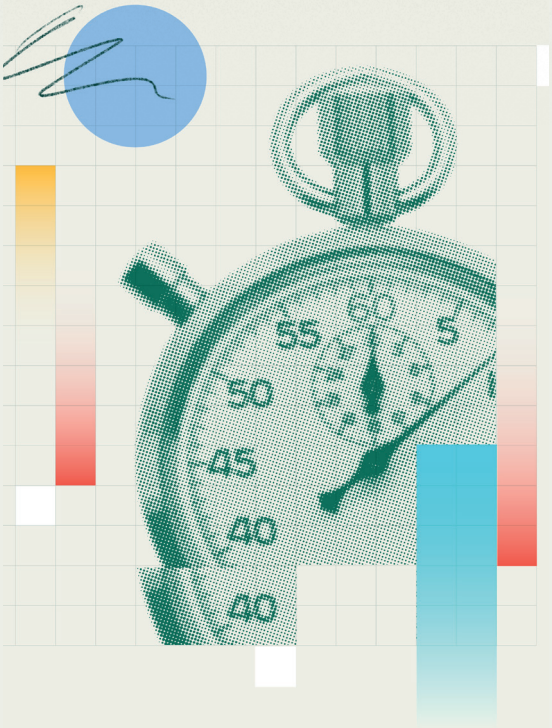
94%
dei cloud tenant sono stati presi di mira ogni mese lo scorso anno.

62%
dei cloud tenant presi di mira sono stati compromessi con successo.

1 https://www.proofpoint.com/us/resources/threat-reports/human-factor

Gli aggressori hanno *accesso ai tuoi dati* per vari giorni prima di essere individuati

Mandiant misura il tempo di permanenza[1] come il numero di giorni in cui un aggressore è presente nell'ambiente di una vittima prima di essere individuato.



10 GIORNI

Lo scorso anno il tempo di permanenza medio globale per tutti gli eventi è stato di 10 giorni.

5 GIORNI

Il tempo di permanenza medio globale di un evento ransomware è di 5 giorni.

LA BUONA NOTIZIA:

Questi sono i tempi di permanenza più brevi mai osservati da Mandiant.

LA CATTIVA NOTIZIA:

È comunque una durata significativa per degli aggressori determinati a raggiungere i loro obiettivi.

QUALCOSA DI IMPREVISTO. IL RANSOMWARE È CRESCIUTO (70% IN PIÙ).

Recorded Future ha rilevato un significativo incremento degli attacchi ransomware segnalati pubblicamente lo scorso anno:

46%

358 attacchi ransomware segnalati contro il settore sanitario (+46% rispetto all'anno precedente).

70%

4.399 attacchi segnalati in tutti i settori (+70% rispetto all'anno precedente).

Diamo ora un'occhiata ai tuoi dati.

1 https://www.mandiant.com/m-trends

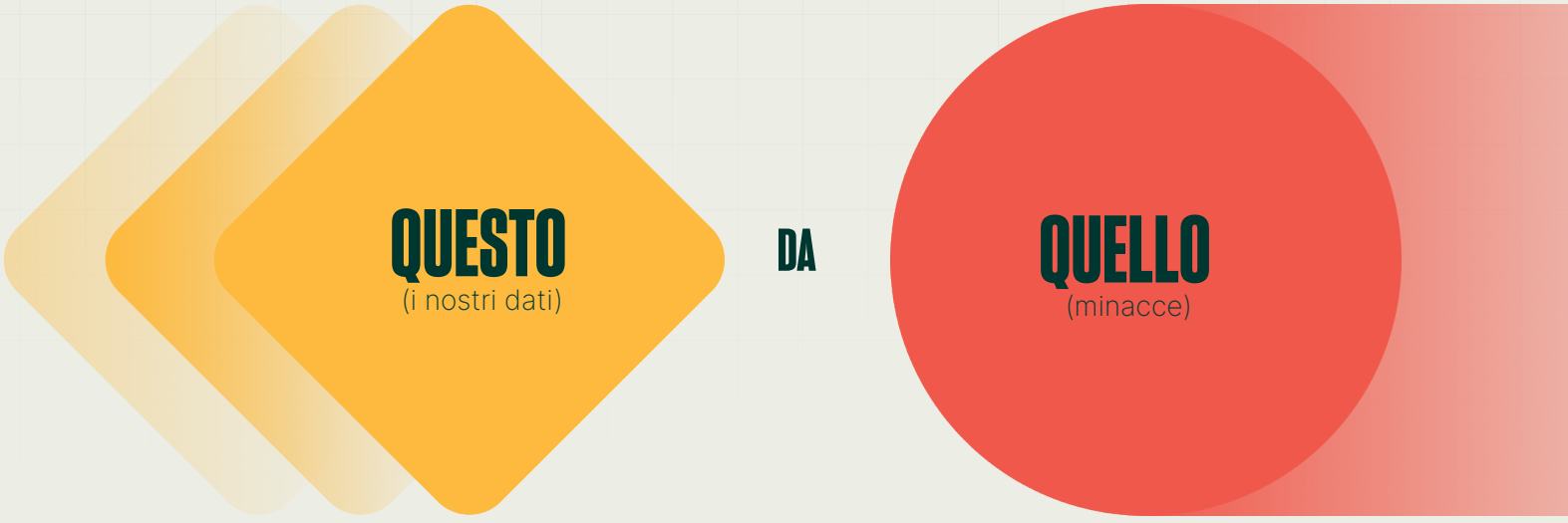
I tuoi dati
SONO A RISCHIO?

Se conosci le probabilità di un attacco (che in realtà non sono elevate), ha senso fare tutto il possibile per diminuire i tuoi rischi riducendo:

LA PROBABILITÀ CHE UN ATTACCO VADA A BUON FINE

LE RICADUTE DI UN ATTACCO

In fin dei conti, ciò che stiamo cercando di fare è apparentemente semplice (sulla carta). Stiamo cercando di proteggere:



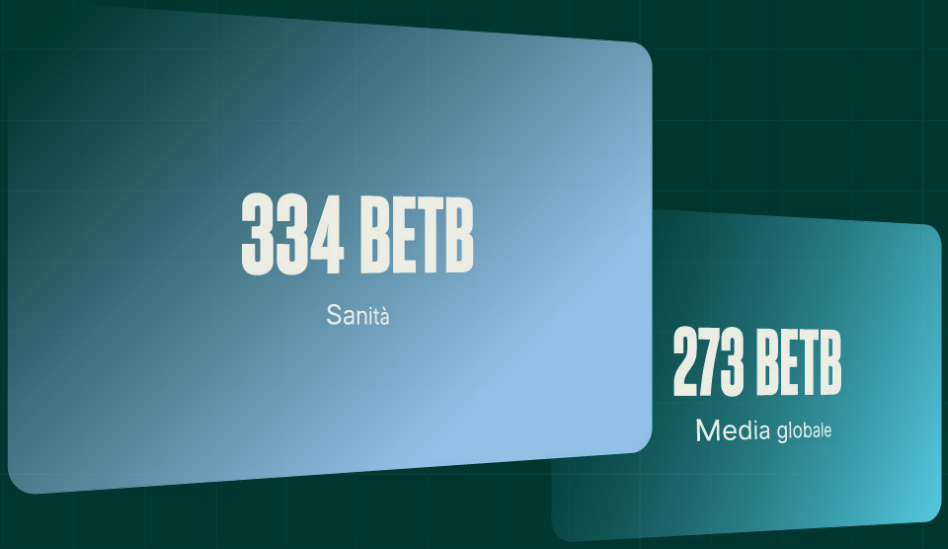
Dobbiamo esaminare entrambi i lati della questione. Vediamo cosa si aspettano i team operativi dalle difese per garantire la sicurezza.

DATI

stanno crescendo rapidamente e stanno ampliando i confini delle difese.

I responsabili delle difese nel settore sanitario devono proteggere una superficie di dati più ampia, con un numero maggiore di dati sensibili e una crescita più rapida rispetto alla media globale. ◆

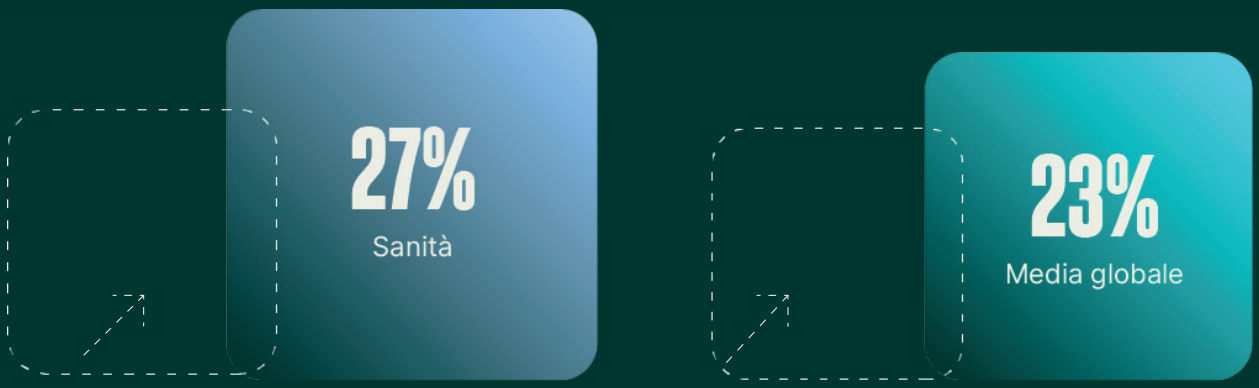
Le organizzazioni sanitarie proteggono il 22% di dati in più rispetto alla media mondiale.



COS'È QUINDI UN BETB?

FRONT-END vs. BACK-END
Un promemoria dagli esperti di dati: quando la maggior parte delle persone sente parlare di "dati", pensa allo storage logico, anche noto come storage front-end. Noi che ci occupiamo di dati, ci concentriamo sullo storage back-end. Rubrik prende la totalità dei dati di un'organizzazione ed esegue una serie di operazioni con tecniche diverse, tra cui deduplicazione e compressione, per ridurre la quantità di dati di front-end nello storage di back-end. In questo report utilizzeremo lo storage back-end.

L'organizzazione sanitaria media ha visto crescere il proprio patrimonio di dati del 27% lo scorso anno (23% per un'organizzazione globale).



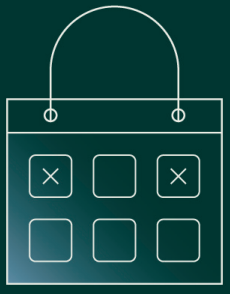
Un'organizzazione sanitaria media possiede il 50% in più di dati sensibili rispetto alla media mondiale.

I record di dati sensibili nel settore sanitario sono cresciuti di oltre il 63% nel 2023, superando di gran lunga qualsiasi altro settore e più di cinque volte la media globale (13%).

LO SCORSO ANNO LE ORGANIZZAZIONI HANNO DOVUTO AFFRONTARE UN NUMERO RECORD DI PROBLEMI.

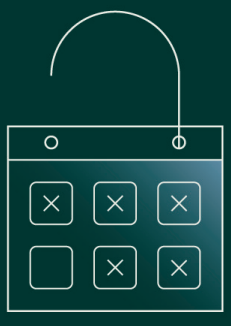
Le vulnerabilità non sono una misura perfetta dell'esposizione, ma forniscono una visione chiara della portata ed entità del rischio ereditato dai fornitori.

Il 2022 è stato un anno di vulnerabilità record con il più alto numero di segnalazioni di sempre:



25.083
vulnerabilità scoperte

Il 2023 ha stabilito un nuovo record, un incremento del 16% rispetto al record precedente.

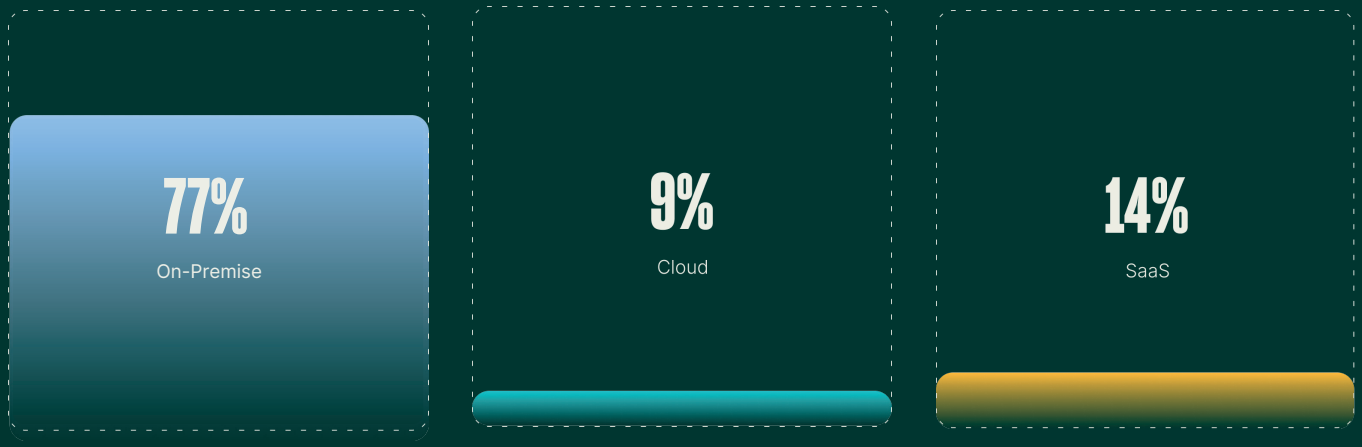


29.065
vulnerabilità scoperte

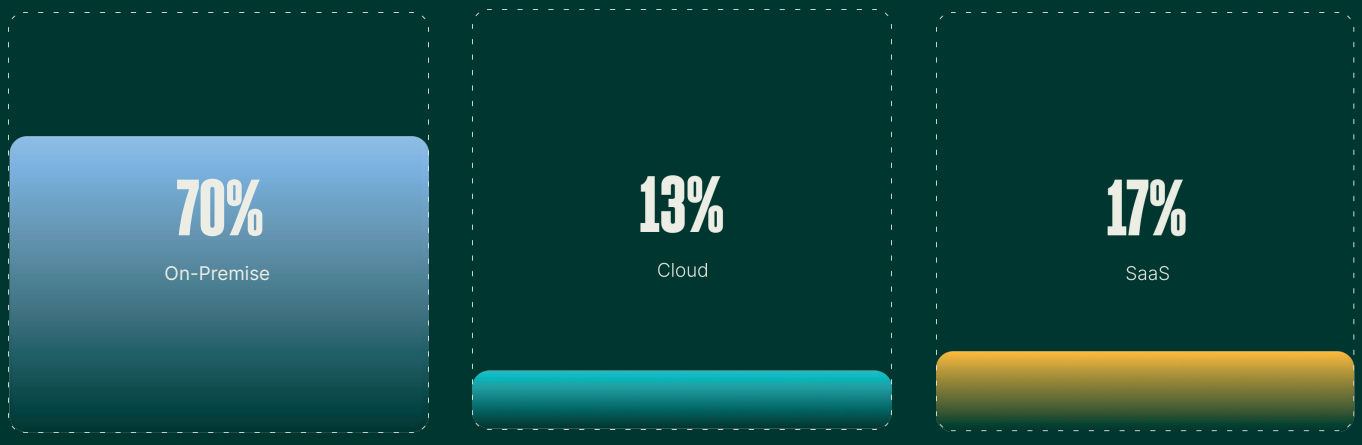
LE ORGANIZZAZIONI STANNO DIVENTANDO SEMPRE PIÙ DIPENDENTI DAL CLOUD E DAL SAAS ◆

Le esigenze di un'azienda moderna richiedono un maggiore orientamento verso il cloud. Vediamo che la natura degli ambienti ibridi si sposta regolarmente verso il cloud e il SaaS, mentre si sta riducendo la crescita dell'architettura on-premise.

2022:



2023:



LA SICUREZZA DEL CLOUD HA ALCUNI PUNTI CIECHI

Sicurezza dei dati nel cloud

PUNTO CIECO N. 1:

Il 70% di tutti i dati in una tipica istanza cloud è costituito da storage di oggetti.

Lo storage ad oggetti rappresenta un punto cieco comune per la maggior parte delle appliance di sicurezza, perché in genere non è leggibile da queste tecnologie.

Sicurezza dei dati nel cloud

PUNTO CIECO N. 2:

L'88% di tutti i dati presenti nello storage ad oggetti è costituito da file di testo o semi-strutturati, come CSV, JSON e XML.

Supponiamo che i tuoi strumenti e i tuoi processi siano in grado di vedere lo storage ad oggetti. Ecco un altro problema: I dati non strutturati (come i file di testo) e i dati semi-strutturati rappresentano un altro punto cieco per la sicurezza, perché la variazione significativa a cui sono spesso sottoposti ne impattano leggibilità e/o copertura da parte delle principali tecnologie e servizi di sicurezza.

Sicurezza dei dati nel cloud

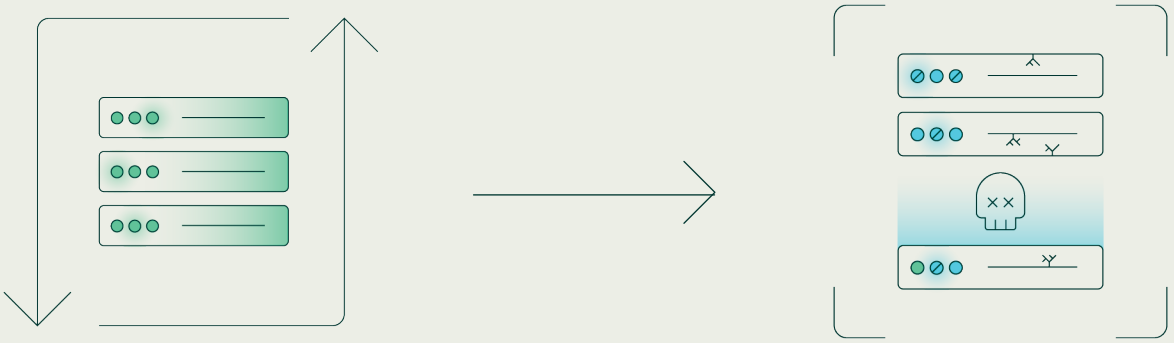
PUNTO CIECO N. 3:

Oltre il 25% di tutti gli archivi di oggetti contiene dati soggetti a requisiti normativi o legali, come informazioni sanitarie protette (PHI) e informazioni di identificazione personale (PII).

In parole povere, il cloud comporta rischi intrinseci perché le aziende ne hanno bisogno per operare, ma conserva anche dati regolamentati con meno funzionalità di sicurezza e meno visibilità rispetto agli asset on-premise.

LA MAGGIOR PARTE DELLE SOLUZIONI DI BACKUP NON È ALL'ALTEZZA.

Le tecnologie di backup e recovery sono componenti fondamentali per quasi tutte le organizzazioni. Vengono utilizzate ormai da decenni per il disaster recovery e la conformità aziendale. Tuttavia, la maggior parte delle organizzazioni ha difficoltà a far funzionare bene queste soluzioni.

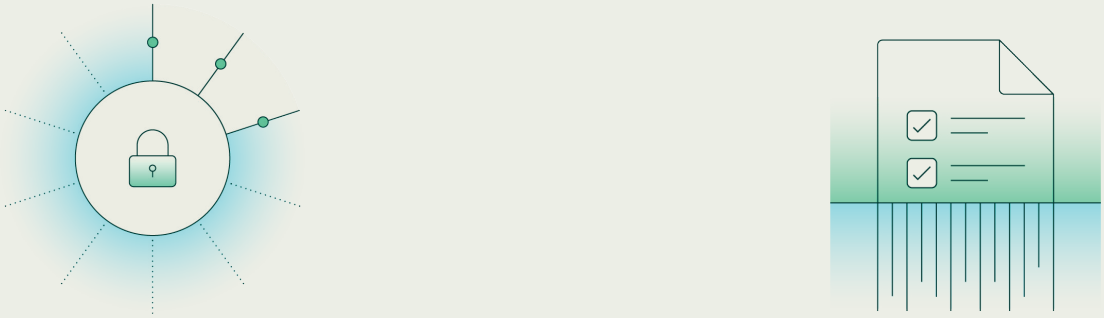


99%

Rubrik Zero Labs ha dichiarato in precedenza[1] che oltre il 99% delle organizzazioni esterne ha specificato di avere una soluzione di backup. ◆

93%+

Tuttavia, oltre il 93% di queste organizzazioni ha riscontrato problemi significativi con la soluzione esistente. ◆



70%

Aon ha segnalato[2] che il 70% delle organizzazioni non archivia i backup fuori sede o che i loro backup non sono immutabili. ●

40%

Quasi il 40% delle organizzazioni osservate da Rubrik non ha impostato policy di conformità per i backup dei dati. ◆

1 https://www.rubrik.com/zero-labs/2023-spring
2 https://www.aon.com/2023-cyber-resilience-report/

LE CATTIVE NOTIZIE:

I criminali informatici si sono abituati al gioco dei backup e li prendono abitualmente di mira.

Gli aggressori hanno quasi universalmente tentato di rimuovere le opzioni di backup e ripristino dei sistemi di difesa. **Le organizzazioni esterne che hanno segnalato un attacco riuscito indicano che:** ▲

96%

Gli aggressori hanno tentato di compromettere i backup nel 96% di questi attacchi.

74%

E hanno avuto un successo almeno parziale nel 74% dei tentativi.

I criminali informatici si prendono un'ulteriore garanzia contro i recovery efficaci

Gli aggressori stanno facendo evolvere il loro approccio al ransomware in base alle azioni dei difensori. Invece di limitarsi a crittografare i dati, li rubano e minacciano di pubblicarli. Se il loro target riesce a contrastare l'evento di crittografia con un recovery rapido, gli autori del ransomware hanno un altro modo per ottenere un pagamento.

2x

Microsoft ha determinato che il numero di volte in cui gli autori delle minacce hanno potenzialmente esfiltrato i dati dopo una compromissione iniziale è raddoppiato dal novembre 2022. ●

12%

Secondo Aon, le violazioni dei dati hanno un impatto complessivo sulle organizzazioni superiore del 12% rispetto al solo ransomware. ●

93%

Il 93% delle organizzazioni esterne che hanno subito un attacco ransomware ha dichiarato di aver pagato una richiesta di riscatto e il 58% di questi pagamenti è stato motivato dalla minaccia di diffondere i dati rubati. ▲

Ora che conosciamo le probabilità, diamo un'occhiata all'impatto.

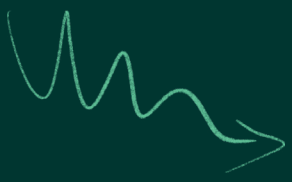
Quanto è GRAVE?

Spesso si pensa che l'attacco informatico sia la fine della storia.

Ma in realtà è la parte centrale.

Tornando all'esempio delle previsioni del tempo, la storia della tua giornata *non finisce quando piove.*

Devi comunque vivere la tua vita. Ma ora devi adattarti alle nuove condizioni. Come farai a non bagnarti? Il cane è stato portato fuori con la pioggia? Cosa succede quando ti ritrovi sotto la pioggia?



Allo stesso modo, un attacco informatico avvia tutta una serie di attività di remediation, recovery e reporting.

Il grado di difficoltà di queste attività dipende dalla preparazione iniziale a questi risultati.

Analizziamo le conseguenze degli attacchi informatici dello scorso anno, e in particolare del ransomware, contro le organizzazioni sanitarie.

QUESTO È CIÒ CHE ACCADE DOPO UN ATTACCO INFORMATICO.

L'anno scorso circa un americano su tre, ha subito una compromissione dei suoi dati personali nel corso di intrusioni nel settore sanitario[1].

244mila+

persone (in media) colpite durante un singolo attacco a un sistema sanitario lo scorso anno.

186%

Aumento dal 2022

133 mil+

Le persone che hanno subito una compromissione di dati durante attacchi informatici contro organizzazioni sanitarie negli Stati Uniti lo scorso anno

1 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Gli attacchi ransomware alle organizzazioni sanitarie hanno un impatto quasi cinque volte superiore alla media globale. ◆

Rubrik misura sia il raggio d'azione della crittografia ransomware che i dati sensibili colpiti da questo raggio d'azione. I file interessati includono file crittografati, file eliminati e file esfiltrati.

Ecco i dati relativi a un tipico evento di crittografia ransomware in ambito sanitario in un ambiente di produzione:

Organizzazioni sanitarie:

16,8 MIL
totale dei file impattati per evento di crittografia.

8,4 MIL
record di dati sensibili all'interno di questi file impattati.

20%
del totale dei dati sensibili di un'organizzazione sanitaria media impattati ogni volta che si verifica un evento di crittografia ransomware.

Un'organizzazione globale media di grandi dimensioni subisce in genere un impatto molto minore sui propri dati sensibili.

13,7 MIL
totale dei file impattati per evento

1,7 MIL
milioni di record di dati sensibili colpiti in ogni evento di crittografia

6%
dei dati sensibili totali di un'organizzazione

La virtualizzazione è davvero importante per il settore sanitario e il ransomware.

Vediamo ora dove avviene la crittografia dei ransomware.

97%

dei dati sanitari crittografati è all'interno dell'architettura virtualizzata.

83%

dei dati crittografati di tutti i settori è all'interno di un'architettura virtualizzata.

Questo è probabilmente dovuto a due fattori.

1: Le architetture virtualizzate hanno in genere una copertura di sicurezza inferiore rispetto agli endpoint tradizionali. Ciò crea punti morti nella sicurezza e allo stesso tempo offre agli aggressori un accesso illimitato.

2: Una volta che gli aggressori hanno accesso ai pannelli di controllo della virtualizzazione, si muovono rapidamente e su larga scala usando solo credenziali compromesse.

I PAGAMENTI DEI RISCATTI VARIANO ENORMEMENTE.

Le richieste iniziali di riscatto sono spesso più alte dei pagamenti effettivi. La Unit 42 di Palo Alto Networks ha rilevato queste tendenze nei pagamenti di riscatti dell'ultimo anno: ▪

	TUTTI I SETTORI:	SANITÀ:
Richiesta media	$ 800.000	$ 200.000
Pagamento medio	$ 275.000	$ 100.000
Media dei cinque maggiori pagamenti	$ 25.000.000	$ 297.000

I backup e il furto di dati influiscono notevolmente sulle probabilità che una vittima paghi un riscatto.

La University of Twente[1] ha studiato i fattori che inducono le vittime a pagare un riscatto e, separatamente, quelli che incidono sull'entità dell'effettivo pagamento del riscatto. I risultati indicano che:

Le organizzazioni con backup recuperabili sono state

27,5x

MENO PROPENSE A PAGARE UN RISCATTO

1 https://databreaches.net/university-of-twente-maps-decision-making-process-for-ransomware-victims/#:~:text=for%20the%20best-,article,-.

L'esfiltrazione dei dati ha comportato maggiori probabilità di pagamento del riscatto e importi di riscatto più elevati.

40%

Ha pagato il riscatto con esfiltrazione dei dati.

25%

Ha pagato il riscatto senza esfiltrazione dei dati.

5,5x

Il pagamento del riscatto è stato 5,5 volte maggiore in caso di esfiltrazione dei dati, rispetto agli eventi di sola crittografia.

Sovraccarico dello storage: il lato oscuro del recovery di cui nessuno si accorge per tempo

Quando piove, ti bagni. Poche organizzazioni sono preparate al diluvio di dati causato dal ransomware.

Se un singolo evento di ransomware sanitario crittografa o modifica 16,8 milioni di file, significa che l'evento di crittografia ha creato 16,8 milioni di "nuovi" file per la vittima (rispetto a 13,7 milioni di nuovi file per un'organizzazione globale media). ◆

Questi file vengono sottoposti a backup come nuovi file, il che consuma grandi quantità di capacità di storage al momento dell'evento di crittografia.

Se lo spazio di storage pre-ransomware di una vittima supera il 70% della capacità, questi "nuovi" dati possono esaurire la capacità di recovery di un'organizzazione in una o due settimane.

Il problema si complica perché le vittime di ransomware devono spesso creare altri "nuovi dati", ad esempio: immagini forensi per l'analisi e copie immutabili per scopi legali. In molti casi, anche i flussi di lavoro di risposta/recovery richiedono dati duplicati. In parole povere, la vittima deve creare altri nuovi dati come parte del processo di risposta subito dopo che l'aggressore ha creato una grande quantità di nuovi dati.

Nelle oltre 200 operazioni di recovery effettuate dal Rubrik Ransomware Response Team, questo problema porta di solito a uno di questi due risultati. L'organizzazione ha bisogno di:

1: Aumentare rapidamente la capacità per ospitare i dati, il che richiede investimenti finanziari e pressione sulla forza lavoro.

2: Ridurre le capacità di recovery per rallentare la crescita dei dati, il che a sua volta limita le opzioni di recovery in tempi critici.

LE RIPERCUSSIONI DEL RANSOMWARE HANNO CONTRIBUITO DIRETTAMENTE AD ALMENO 42 MORTI NEGLI STATI UNITI.

In ogni evento ransomware si verifica un impatto sui dati. I rischi reali, in particolare per la sanità, si misurano anche in termini di impatto operativo e di vite umane.

La University of Minnesota Twin Cities - School of Public Health ha studiato gli impatti reali sugli ospedali e sull'assistenza ai pazienti causati da eventi ransomware tra il 2016 e il 2021[1]. Lo studio ha rilevato quanto segue:

20%

L'attività di assistenza ai pazienti è diminuita del 20% nella prima settimana di un attacco ransomware.

Questi attacchi non colpiscono più solo i dati, le aziende o la privacy dei singoli individui. Esistono prove dirette che gli attacchi informatici sono anche una questione di vita o di morte.

1 su 4

Sebbene solo il 5% degli ospedali statunitensi sia stato colpito direttamente dal ransomware nel corso dello studio, un ulteriore 20% di ospedali ha subito effetti a catena quando i pazienti sono stati trasferiti o dirottati dagli ospedali colpiti a quelli circostanti.

0,5-1%

Un ospedale medio ha perso tra lo 0,5 e l'1% del suo fatturato annuale totale come conseguenza diretta di un singolo attacco ransomware.

2-3 sett.

Gli ospedali hanno impiegato in media dalle due alle tre settimane per tornare ai livelli medi di assistenza ai pazienti dopo un attacco ransomware.

42-67 decessi

Le conseguenze degli attacchi ransomware hanno contribuito direttamente alla morte di un numero compreso tra 42 e 67 pazienti[2].

1 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292
2 https://www.statnews.com/2023/11/17/hospital-ransomware-attack-patient-deaths-study/

Recovery

PER L'AZZERAMENTO

Una volta terminata la risposta iniziale e dopo che le organizzazioni ripristinano la normale operatività, le ricadute di un attacco ransomware continuano a produrre rischi.

CI SONO CATTIVE NOTIZIE E BUONE NOTIZIE PER TUTTI NOI.

Gli attacchi informatici ***hanno un impatto*** sulle nostre organizzazioni e sulle persone.

Aon ha riferito che un grave incidente informatico ha generato un: ●

9%

di diminuzione del valore per gli azionisti per ogni evento.

Le organizzazioni esterne hanno riportato i seguenti impatti diretti dopo un attacco informatico: ▲

44%

Leadership costretta a cambiare

43%

Copertura stampa negativa e/o danni alla reputazione

37%

Perdita di ricavi

36%

Perdita di clienti

Il 96% dei senior leader del settore IT e della sicurezza ha segnalato cambiamenti del proprio stato emotivo e/o psicologico in conseguenza di un attacco informatico: ▲

53%

Aumento dell'ansia per il ruolo attualmente ricoperto

41%

Perdita di fiducia tra colleghi e membri del team

38%

Preoccupazione per la sicurezza del lavoro

33%

Perdita di sonno o difficoltà a dormire

I dirigenti devono essere certi che la loro organizzazione *possa riprendersi dal prossimo* attacco.

60% dei leader IT e della sicurezza sono molto o estremamente preoccupati per la capacità della loro organizzazione di mantenere la business continuity durante un attacco informatico. ▲

28% delle organizzazioni esterne ritiene che il proprio CdA o dirigenza abbia poca o nessuna fiducia nella capacità dell'azienda di recuperare dati e applicazioni critici in un attacco informatico. ▲

GLI ATTACCHI INFORMATICI GENERANO PROBLEMI PREVEDIBILI DA RISOLVERE.

Ecco i problemi riscontrati più di frequente durante un attacco informatico e i cambiamenti tipici che le organizzazioni devono prepararsi ad affrontare dopo un attacco:

Queste sono le maggiori limitazioni riscontrate dalle organizzazioni esterne durante un attacco informatico: ▲

- **19%** Problemi a lavorare in un ambiente ibrido
- **18%** Mancanza di allineamento tra i team
- **18%** Soluzioni di backup e recovery inefficaci
- **17%** Mancanza di coinvolgimento della leadership
- **16%** Sfide di visibilità

Questi sono i cambiamenti più comuni riscontrati dalle organizzazioni esterne per un attacco informatico: ▲

- **24%** Maggiore controllo da parte della senior leadership
- **20%** Cambiamenti nella tecnologia di cybersecurity
- **19%** Rielaborazione dei piani e delle procedure di cybersecurity
- **19%** Più attribuzioni di responsabilità individuali
- **18%** Calo del morale tra i team IT o di cybersecurity

Gli attacchi informatici possono portare risultati positivi.

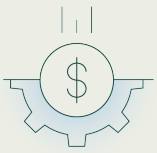
Le organizzazioni in grado di trarre vantaggio da questi momenti di crisi possono rimodellare il loro futuro.

Aon ha segnalato che le aziende che hanno superato con successo un attacco informatico hanno registrato un aumento del

valore per gli azionisti del 18%

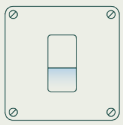
rispetto ad aziende simili. ●

Dopo un attacco informatico, le organizzazioni esterne hanno segnalato ▲



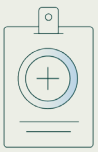
55%

Aumento della spesa per nuove tecnologie o servizi



42%

Cambiamento di fornitori o di relazioni con terze parti



37%

Assunzione di nuovo personale

Non puoi eliminare i rischi, ma puoi intervenire sul ciclo del rischio e avere una nuova linea di base del rischio.

Azzerare

Il RISCHIO SUI DATI

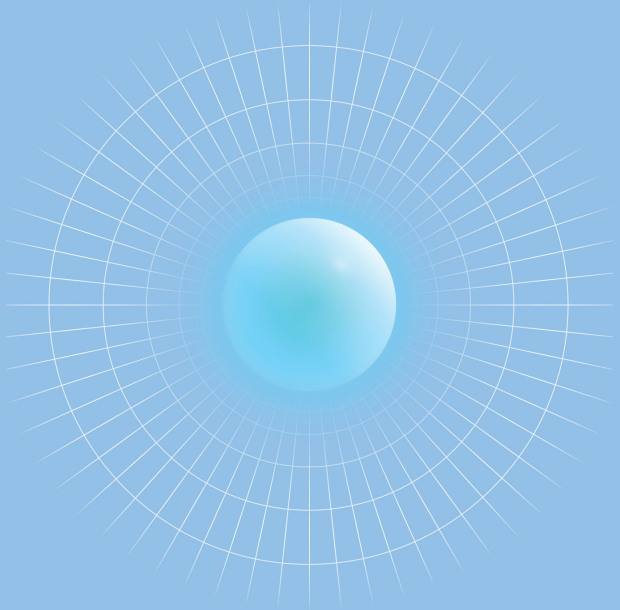
Vorremmo poter dire
che questi risultati finali
pongono fine alla storia,

ma in verità questo
è l'inizio di un nuovo
capitolo.

IL FATTO CHE SIA STATA SUPERATA UNA TEMPESTA NON SIGNIFICA CHE SARÀ L'ULTIMA CHE SI AFFRONTERÀ.

Infatti, è quasi certo che se ne incontrerà un'altra che porterà con sé nuovi rischi, forse imprevisti, che potrebbero cogliere di sorpresa.

Ci piacerebbe anche dire che ci sono opzioni per modificare i fattori di rischio controllati dagli aggressori, ma purtroppo la nostra analisi ci dice che questo approccio è inutile quanto cercare di controllare il clima.

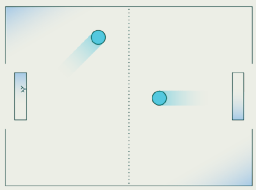


Come nella maggior parte dei casi della vita, non puoi controllare ciò che accade, ma la buona notizia è che puoi controllare l'azzeramento del rischio e i conseguenti impatti.

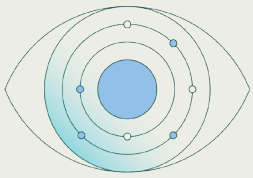
Esaminiamo i dati su come gestire al meglio l'azzeramento del rischio. Ogni raccomandazione sui rischi deriva da risultati relativi agli attacchi informatici, agli impatti sui dati o ai risultati attesi.

COSA INFLUISCE EFFETTIVAMENTE SUL NUOVO RISCHIO DEI DATI?

Ecco le azioni di maggior impatto che puoi sfruttare per migliorare significativamente il rischio dei tuoi dati:

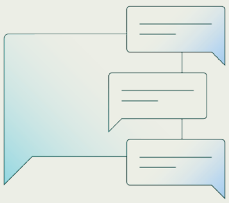


Preparati a sfidare gli aggressori in ogni parte di un ambiente ibrido. Gli aggressori stanno già operando con successo negli ambienti ibridi e le nostre organizzazioni stanno andando in quella direzione.

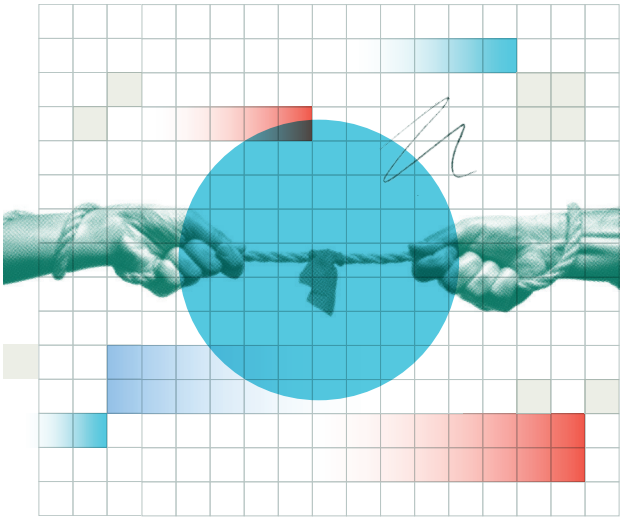


Aumenta la tua ***visibilità sui dati***, in particolare:

- Espandi la tua visione su tutti gli aspetti degli ambienti ibridi.
- Scopri dove si trovano i tuoi dati sensibili e quali aspetti normativi si applicano a specifici elementi dei dati.
- Preparati a rispondere alle nuove verifiche del management e dimostra perché i recenti investimenti porteranno ai risultati attesi.



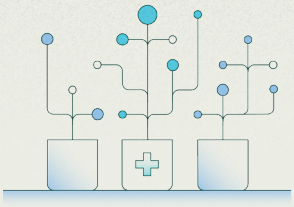
Anticipa l'aumento di controllo da parte del management e comunica in modo proattivo le tue iniziative dopo un attacco informatico.



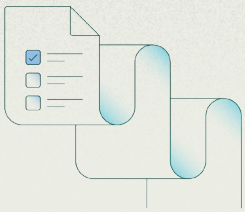
Preparati al recovery e alla *reazione degli aggressori al tuo recovery*.

Questa parte include:

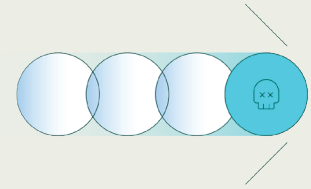
- Verificare che i backup siano del tutto immutabili e disponibili durante un attacco informatico.
- Automatizzare il più possibile il processo di recovery.
- Testare i risultati di recovery negli ambienti ibridi.
- Sfruttare i servizi e le tecnologie di sicurezza esistenti per testare l'immutabilità e l'integrazione delle tecnologie di backup.



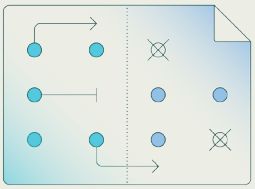
Ricorda che i tuoi dati (soprattutto quelli sensibili) stanno crescendo. Impara a controllare questa crescita e a dare priorità alla difesa dei dati critici.



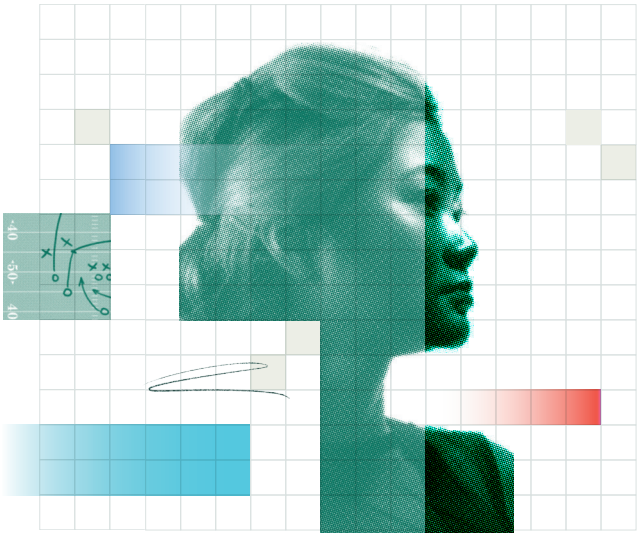
Preparati a rispondere a domande di carattere normativo e legale durante un evento ransomware, in un contesto in cui l'ambiente è attivamente crittografato e gli aggressori minacciano di divulgare i dati rubati.



Ricorda che gli attacchi informatici spesso portano all'introduzione di nuove tecnologie, all'aumento del personale e al cambio di fornitori o partner. Preparati a sfruttare questi periodi di cambiamento per ottenere il massimo impatto.



Comunica regolarmente piani e risultati all'intera organizzazione per gestire il calo del morale causato dagli attacchi informatici e ripristinare la fiducia tra i team.



Trova modi per *unire team diversi* prima, durante e dopo un attacco informatico.

Questa parte include:

- Creare playbook combinati ed eseguire esercitazioni a tavolino.
- Determinare quale team è più adatto a prendere decisioni specifiche sul rischio.
- Stabilire il modo migliore per far pervenire i dati giusti al titolare di uno specifico rischio.
- Verificare che tutti i team abbiano la stessa vista sui dati per velocizzare le decisioni e ridurre la potenziale resistenza causata da punti di vista discordanti.

UN'ALTRA PROSPETTIVA

In effetti, Rubrik Zero Labs esamina i rischi da una prospettiva basata sui dati. Ampliamo ora la nostra visione per includere i principali consigli sulla resilienza contenuti nel 2023 Digital Defense Report di Microsoft.[1] Il punto di vista di Microsoft è decisamente diverso da quello di Rubrik, e ci auguriamo che questo ci porti a migliorare le attività di riduzione del rischio.

99% Microsoft ritiene che l'igiene di base della sicurezza dei dati protegga dal 99% degli attacchi.•

Le raccomandazioni specifiche sono: •

- Abilitare l'autenticazione a più fattori
- Applicare i principi Zero Trust, in particolare per gli asset che proteggono i dati e le funzioni critiche
- Utilizzare il rilevamento esteso e l'antimalware per le parti critiche degli ambienti ibridi
- Mantenere un patching regolare su sistemi e applicazioni chiave
- Proteggere i dati sapendo quali sono e dove si trovano quelli critici, implementando inoltre misure difensive adeguate per queste enclavi

Un ulteriore approfondimento della visione Microsoft sul ransomware indica che "The Foundational Five" è il percorso migliore per eliminare l'impatto del ransomware: •

1 Autenticazioni moderne con credenziali resistenti al phishing

2 Accesso con privilegi minimi applicato all'intero stack tecnologico

3 Ambienti protetti da minacce e rischi

4 Gestione della postura per la conformità e l'integrità di dispositivi, servizi e risorse

5 Backup automatico e sincronizzazione dei file nel cloud per i dati critici di utenti e dell'azienda

1 https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

Abbiamo iniziato questo report semplificando il nostro calcolo del rischio: Dobbiamo difendere QUESTO da QUELLO.

In pratica, il rischio è un argomento incredibilmente complesso

RISCHIO

A causa dei milioni di variabili coinvolte, non sarà mai possibile definire completamente il tuo rischio, né eliminarlo del tutto. Ciò che puoi fare è gestire le leve di maggiore impatto, lavorare bene sui risultati prevedibili e intraprendere azioni specifiche per modificare il calcolo del rischio a tuo favore.

Ci auguriamo che questo studio ti abbia fornito indicazioni utili sulla riduzione del rischio relativo ai dati e che ti abbia preparato per l'evoluzione del ciclo del rischio.

RICONOSCIMENTI

Rubrik desidera estendere il proprio riconoscimento alle organizzazioni che hanno fornito i loro dati, raccolti con grande sforzo, per questo studio.

- I nostri partner Microsoft e Aon hanno fornito sia la direzione strategica che i dati di supporto.
- Le seguenti organizzazioni ci hanno concesso di usare le loro analisi fornendoci inoltre materiali di supporto per una categorizzazione appropriata:
  - Proofpoint
  - Recorded Future (Allan "Ransomware Sommelier" Liska)
  - Mandiant (Kirstie "Swiftie" Failey)
  - Palo Alto Networks Unit 42 (Ingrid Parker)
- La University of Minnesota Twin Cities School of Public Health (Hannah Neprash, Claire McGlave e Sayeh Nikpay) ci ha concesso di utilizzare i risultati da loro ottenuti, ci ha fornito approfondimenti sulla loro ricerca e ha collaborato con Rubrik Zero Labs per fare in modo che la loro ricerca accademica fosse a supporto della ricerca industriale di Rubrik Zero Labs.

Come per tutte le iniziative di Rubrik Zero Labs, è necessaria una collaborazione estesa per portare a termine questi studi. Wakefield Research ha fornito dati esterni per rendere questa ricerca il più oggettiva possibile. Shaped By ha trovato il modo di elaborare i nostri dati e renderli comprensibili. Infine, molti "Rubrikan" hanno lavorato con impegno per fornire capacità, contesto e indicazioni. Desideriamo esprimere un ringraziamento speciale ad Amanda "Danger" O'Callaghan, Linda "Taskmaster" Nguyen, Lynda "Go Niners" Hall, Ben Long, Peter "I'm the Law" Chang, Ajay Kumar Gaddam, Ryan Goss, Derek Morefield, Josh Burns, Gunakar Goswami, Prasath Mani, Ethan Hagan, Kevin Nguyen, Caleb "Social King" Tolin, Kelly Cooper, Hannah Battillo, Sindhu Nagendra, Caitlin "Plz stop letting Steve talk to reporters" O'Malley e Fareed Fityan.