veeam Insights

Dal rischio alla resilienza

Tendenze del ransomware nel 2025 e strategie proattive

Executive Summary:

Valutare le minacce ransomware e le difese nel 2025

Gli attacchi ransomware si evolvono, crescono più velocemente e sono più sofisticati che mai. Una cosa è certa: **la minaccia pervasiva del ransomware continuerà ad affliggere le organizzazioni per tutto il 2025 e oltre.** Indipendentemente dal fatto che questi attacchi provengano da gruppi consolidati o dal numero crescente di "lupi solitari", non prepararsi accuratamente può costare a un'organizzazione tempo e denaro significativi, oltre alla fiducia degli stakeholder.

Per contribuire ad affrontare queste minacce informatiche persistenti, il nostro report sui rischi per la resilienza del 2025 mostra diverse azioni che le organizzazioni possono intraprendere per mitigare i rischi e ripristinare più rapidamente da un attacco. **Abbiamo intervistato 1.300 organizzazioni a livello globale** per valutare come i Chief Information Security Officer (CISO), i professionisti della sicurezza e i leader IT stanno implementando il ripristino dalle minacce informatiche.

Le strategie testate sul campo dalle aziende che si sono riprese più velocemente dagli attacchi riflettono una serie di best practice per la resilienza informatica che tutte le organizzazioni dovrebbero considerare di implementare.

C'è una buona notizia. Rispetto al nostro sondaggio del 2024,[1] **la percentuale di aziende colpite da almeno un attacco ransomware con conseguente crittografia o esfiltrazione di dati è leggermente diminuita, passando dal 75% al 69%.** Questa diminuzione deriva probabilmente dal continuo miglioramento delle pratiche di preparazione e resilienza da parte delle organizzazioni, nonché dalla maggiore collaborazione tra i team IT e di sicurezza. I governi si sono anche alleati per abbattere i principali gruppi di ransomware, portando gli attori delle minacce ad adattarsi e modificare dinamiche di attacco più ampie.

La nostra analisi rivela **sei tendenze chiave che plasmeranno il panorama delle minacce ransomware nel 2025** e le informazioni supportate dai dati che possono aiutare le aziende a migliorare la resilienza. Dalle tattiche di inseguimento e dalla crescita delle esfiltrazioni, fino al calo dei pagamenti dei riscatti e alla crescente collaborazione tra gli stakeholder, esaminiamo il panorama delle minacce persistenti e il modo in cui le organizzazioni di successo riducono i rischi e gli impatti del ransomware.

1.300

organizzazioni di tutto il mondo intervistate da Veeam

6%

in meno di aziende colpite da almeno un attacco ransomware

Le organizzazioni devono passare dalla sicurezza reattiva a strategie **di resilienza informatica proattiva** per affrontare le sfide del ransomware, sfruttando la preparazione, la risposta rapida e le misure di ripristino sicuro per ridurre i rischi.

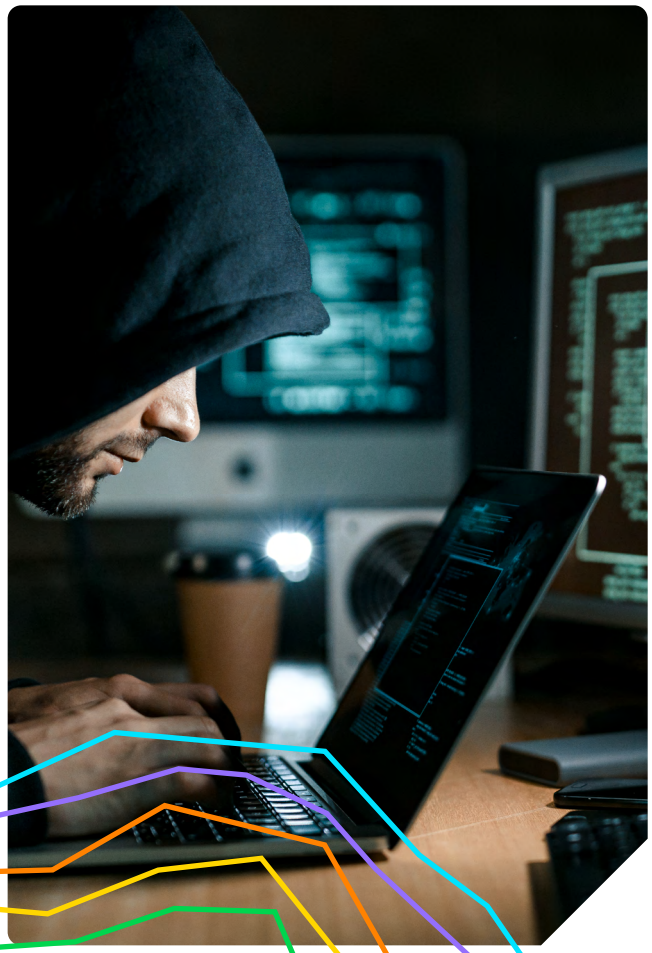
Le 6 principali tendenze nel ransomware da tenere d'occhio nel 2025

1. **Le forze dell'ordine costringono gli attori delle minacce ad adattarsi**
2. **Gli attacchi di esfiltrazione dei dati crescono**
3. **I pagamenti per il ransomware stanno diminuendo**
4. **Conseguenze legali emergenti dei pagamenti del riscatto**
5. **La collaborazione rafforza la resilienza contro il ransomware**
6. **I budget per la sicurezza e il ripristino aumentano, ma occorre fare di più**

Le forze dell'ordine costringono gli attori delle minacce ad adattarsi

TENDENZA 1

Il 2024 ha visto le autorità lanciare diverse operazioni di successo per abbattere importanti gruppi di minacce informatiche. L'eliminazione di questi gruppi più grandi è ovviamente uno sviluppo positivo per la difesa dalle minacce. Tuttavia, **il numero di gruppi più piccoli e di "lupi solitari" che propagano attacchi è aumentato.** Alcuni gruppi hanno anche spostato il loro obiettivo a valle, evitando le infrastrutture critiche per ridurre il controllo da parte delle forze dell'ordine e prendendo di mira le piccole e medie imprese (PMI) che spesso hanno difese informatiche più deboli.



Alcuni dei gruppi più grandi che sono stati chiusi, sono scomparsi o hanno cessato l'attività includono:

- **LockBit**, un gruppo di ransomware-as-a-service (RaaS), smantellato dagli sforzi delle forze dell'ordine diretti dalla National Crime Agency del Regno Unito in collaborazione con l'FBI e l'Europol.[2]
- **BlackCat**, un gruppo RaaS, che l'FBI aveva precedentemente interrotto nel 2023,[3] ha terminato le operazioni nel marzo 2024 in seguito al successo dell'attacco contro Change Healthcare e, secondo quanto riferito, a un pagamento di riscatto del valore di oltre 22 milioni di dollari USA.[4]
- **Black Basta**, che sembra aver interrotto le operazioni nel 2025 dopo che i registri delle chat trapelati hanno rivelato preoccupazioni sui controlli da parte delle forze dell'ordine dopo un attacco al sistema sanitario statunitense Ascension, che comprendeva 140 ospedali in 19 stati.[5]

Gli attacchi di esfiltrazione dei dati crescono

TENDENZA 2

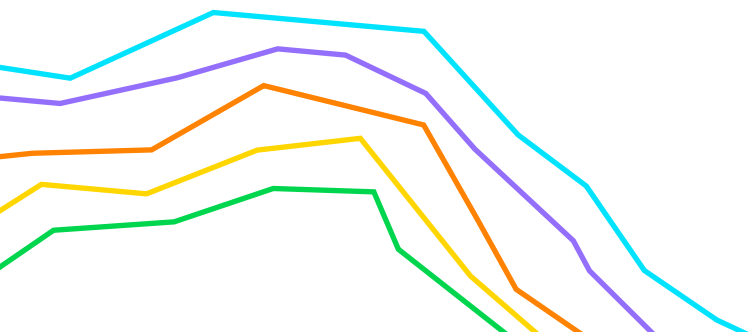
Man mano che il panorama delle minacce si evolve, gli autori delle minacce continuano a modificare le loro tattiche. In particolare, mentre le tattiche di esfiltrazione sono tipicamente utilizzate in combinazione con la crittografia dei dati, il numero di vittime di sola esfiltrazione che hanno pagato un riscatto è aumentato durante il quarto trimestre.[6]

L'esfiltrazione riflette un approccio "smash and grab" comune negli attacchi ransomware tradizionali prima della crittografia. Essa si verifica inoltre con applicazioni basate su cloud e infrastrutture cloud scarsamente protette. Insieme a questo passaggio verso l'esfiltrazione dei dati, così come verso la doppia estorsione che combina sia la crittografia per limitare l'accesso, sia la pubblicazione dei dati sensibili esfiltrati, **si è inoltre assistito a una riduzione del tempo di attesa, il tempo che intercorre tra la compromissione e il lancio dell'attacco, con molti attacchi che si verificano nel giro di poche ore.**

Nel secondo trimestre del 2024, Coveware by Veeam ha rilevato che due dei tre principali avversari del ransomware in quel trimestre avevano un tempo di permanenza medio inferiore a 24 ore.[7] Si tratta di un netto calo rispetto ai trimestri precedenti e la tendenza è continuata anche nel quarto trimestre.

Quando gli autori delle minacce ottengono l'accesso alle reti delle vittime, tendono a utilizzare tecniche di movimento laterale. Cercano la facilità di esfiltrazione o un obiettivo specifico, come compromettere gli hypervisor VMware ESXi, per costringere le vittime a pagare il riscatto. Queste strategie efficienti e ben collaudate spesso si traducono in attacchi più rapidi che possono essere difficili da rilevare e contenere.

Troppo spesso, le organizzazioni che hanno una debole strategia di sicurezza informatica e architetture di rete complesse sono particolarmente vulnerabili all'esfiltrazione dei dati e alle minacce informatiche correlate.



I pagamenti per il ransomware stanno diminuendo

TENDENZA 3

Fortunatamente, nel corso del 2024 il valore totale dei pagamenti del ransomware è diminuito rispetto al 2023.[8] Più di un terzo delle organizzazioni colpite da un attacco ransomware (36%) non ha pagato un riscatto e il 25% non ha pagato ma è stato comunque in grado di ripristinare i propri dati.

Tra coloro che hanno pagato, l'82% ha pagato meno del riscatto iniziale e il 60% ha pagato meno della metà di tale somma. Questi dati sono inoltre in linea con quelli che Coveware by Veeam ha potuto constatare in prima persona durante il suo lavoro con le aziende colpite nel 2024, quando il **pagamento mediano si è ridotto del 45% nel quarto trimestre** a circa 110.000 dollari, un minimo storico.

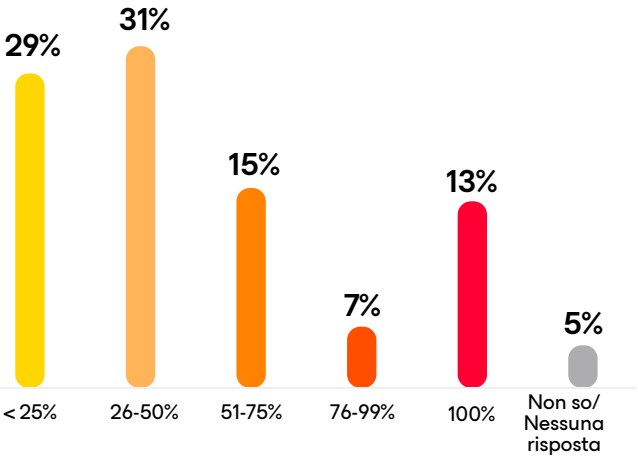
Solo il 25% delle aziende che lavorano con una risposta esperta agli incidenti di Coveware by Veeam ha pagato un riscatto, segnando una "pietra miliare significativa nella lotta contro il ransomware".[9]

Rispetto alle aziende che hanno utilizzato i servizi di risposta agli incidenti di Coveware by Veeam, le altre organizzazioni hanno avuto il 156% di probabilità in più di pagare un riscatto. Ciò suggerisce che **la collaborazione con terze parti esperte per la risposta agli incidenti è correlata a un minor numero di pagamenti di riscatti, a pagamenti di riscatti inferiori e a pratiche complessivamente più resilienti.**

Le vittime sono sempre più riluttanti a pagare i riscatti perché non possono fidarsi che gli aggressori rilascino i loro dati. Le organizzazioni hanno inoltre migliorato in modo proattivo i propri piani di risposta agli incidenti, anche attraverso l'uso di backup immutabili.

La vostra organizzazione ha pagato un riscatto per ripristinare i dati?

Percentuale del riscatto pagato



Conseguenze legali emergenti dei pagamenti del riscatto

TENDENZA 4

Pagare un riscatto può rivelarsi molto costoso, in quanto incentiva gli aggressori e conferma che un'organizzazione vulnerabile è disposta a pagare. Infatti, **tra coloro che hanno pagato un riscatto, il 69% è stato attaccato più di una volta.** Le organizzazioni che non adottano misure per rafforzare la loro capacità di difesa e risposta si lasciano con meno opzioni quando si verifica un attacco.

69%

delle organizzazioni che hanno pagato un riscatto, sono state attaccate più di una volta

L'evoluzione delle iniziative normative e di segnalazione, nonché l'attuazione coordinata da parte delle autorità in tutte le giurisdizioni, hanno inoltre contribuito a ridurre i pagamenti dei riscatti. In particolare, l'International Counter Ransomware Initiative (CRI), lanciata dal governo degli Stati Uniti nel 2021, e la task force ad essa affiliata riuniscono 68 paesi con l'obiettivo di sconvolgere l'ecosistema del ransomware e sviluppare approcci politici comuni.[10]

Nel 2023, 40 membri della CRI hanno firmato un impegno governativo congiunto per "scoraggiare fortemente chiunque dal pagare una richiesta di ransomware".[11] Alcuni paesi hanno anche proposto una legislazione che vieta alle organizzazioni del settore pubblico di pagare riscatti, come il Regno Unito nel gennaio 2025[12], e due stati degli Stati Uniti (Florida e Carolina del Nord) hanno approvato tali leggi.[13]

L'FBI scoraggia le organizzazioni dal pagare i riscatti[14] e il Dipartimento del Tesoro degli Stati Uniti avverte che potrebbero esserci rischi di sanzioni associati ai pagamenti effettuati a entità bloccate dall'Office of Foreign Asset Control (OFAC).[15] Le organizzazioni globali devono considerare anche altri rischi di pagamento e requisiti di conformità.

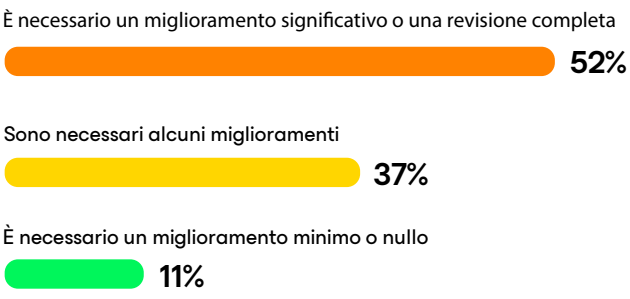
La collaborazione rafforza la resilienza contro il ransomware

TENDENZA 5

Anche il miglioramento della collaborazione e della comunicazione tra le operazioni IT e i team di sicurezza ha aiutato le organizzazioni ad aumentare la loro resilienza informatica. Tuttavia, la maggior parte degli intervistati (52%) ha affermato che è necessario un miglioramento significativo o una revisione completa per allineare questi team. E solo l'11% ha affermato che è necessario un piccolo miglioramento o nessun miglioramento.

Allo stesso tempo, gli attori della piattaforma e della tecnologia stanno collaborando per aggregare le informazioni sul ransomware e per fornire servizi che aiutino le organizzazioni a potenziare le difese. La segnalazione di ransomware e altri attacchi informatici alle forze dell'ordine e alle autorità di regolamentazione, nonché alle reti di partner emergenti e agli scambi di condivisione delle informazioni del settore, rafforza le difese collettive.

Allineamento dei team IT di Operazioni e Sicurezza



> "Abbiamo un obiettivo condiviso di sicurezza e dobbiamo farlo insieme. Quindi, non credo che ci sia modo di arrivare a un futuro sicuro dal punto di vista informatico senza che sia gli enti pubblici che quelli privati, e le loro proposte di valore, si uniscano per trovare alcune soluzioni."[16]

Sue Gordon

ex vicedirettore principale dell'intelligence nazionale degli Stati Uniti

Guarda l'intervista completa con Sue Gordon e il CISO di Veeam Gil Vega, qui

I budget per la sicurezza e il ripristino aumentano, ma occorre fare di più

TENDENZA 6

Fondamentalmente, consente ai fornitori e alle agenzie di fornire indicatori di compromissione e strategie di mitigazione ad altri nell'ecosistema.

Sebbene molte tecniche di difesa dal ransomware abbiano mostrato segni di miglioramento, **alcune organizzazioni non stanno aumentando i budget per la sicurezza e il ripristino abbastanza velocemente** da tenere il passo con il crescente panorama delle minacce. I team di sicurezza sono inoltre dispersi a causa dell'ampia gamma di ransomware e altri vettori di attacco che devono affrontare.

Nel complesso, le organizzazioni tendono a dedicare un po' più di risorse alla sicurezza (in media il 31% del budget IT) piuttosto che al ripristino (28% in media), il che suggerisce una potenziale vulnerabilità nella creazione di una resilienza proattiva. I Chief Information Officer (CIO) e i Chief Information Security Officer (CISO) devono trovare l'equilibrio adeguato in base alle esigenze della loro organizzazione quando destinano il budget per ogni area. I risultati del sondaggio indicano che **investimenti insufficienti nella sicurezza o nel ripristino possono indebolire le capacità delle organizzazioni di proteggersi dagli attacchi ransomware e di reagire.** La mancanza di attenzione al ripristino, in particolare, può costare tempo e risorse preziose, in particolare quando gli autori delle minacce prendono di mira i repository di backup.

Un aspetto positivo è che il **94% delle organizzazioni ha aumentato il budget per il ripristino per il 2025 e il 95% lo ha aumentato per la prevenzione,** il che indica una crescente priorità per aumentare la resilienza informatica.

94%

delle organizzazioni hanno aumentato il budget per il ripristino per il 2025

95%

delle organizzazioni hanno aumentato il budget per il ripristino a scopo di prevenzione

Domande che il consiglio di amministrazione porrà dopo un attacco ransomware

Come è avvenuto l'attacco?

Descrivere in dettaglio la causa, la portata e l'impatto dell'attacco.

Che cosa è stato fatto per eliminare la minaccia?

Descrivere se è stato pagato un riscatto (in caso affermativo, come) e le misure intraprese per eliminare la minaccia e ripristinare.

Quali sistemi, dati e operazioni aziendali sono stati interessati?

Delineare gli impatti dell'attacco, comprese le eventuali conseguenze finanziarie e reputazionali.

Cosa è stato fatto per migliorare la resilienza informatica e prevenire attacchi futuri?

Identifica le misure adottate per rafforzare la sicurezza e il ripristino, come i cambiamenti nelle misure di governance o le priorità di investimento nella sicurezza informatica.

Fattori chiave di successo:

Cosa hanno in comune le organizzazioni con risultati migliori

Quando si affronta improvvisamente un attacco ransomware, le organizzazioni devono agire immediatamente e in modo coordinato. Il tempo è essenziale, quindi è fondamentale valutare la portata della violazione, contenere la minaccia e avviare la risposta all'incidente nel giro di pochi minuti.

L'analisi degli aspetti comuni delle organizzazioni con esiti di maggior e minore successo da un attacco ransomware può fornire spunti per potenziare le tue difese informatiche.

Questo ampio divario nel successo solleva la domanda:

Perché così tante organizzazioni hanno faticato ad affrontare una minaccia informatica così diffusa?

Esaminando i risultati del sondaggio, diverse aree di carenza sono correlate a una minore resilienza al ransomware. Inoltre, osservando quali lezioni le organizzazioni hanno dichiarato di aver appreso nell'ultimo anno dopo essere state attaccate, emergono diversi modelli che possono essere applicati per una migliore difesa e ripristino dal ransomware.

Un'organizzazione è stata considerata di maggior successo se sono stati soddisfatti cinque dei nove dei seguenti criteri.

- ✔ L'organizzazione non ha pagato alcun riscatto ed è riuscita a ripristinare i propri dati.
- ✔ L'organizzazione non è stata attaccata più volte.
- ✔ L'organizzazione non ha subito impatti significativi.
- ✔ L'organizzazione non ha avuto i dati di produzione crittografati.
- ✔ L'organizzazione è stata valutata come preparata o completamente preparata dopo l'attacco.
- ✔ L'organizzazione ha ripristinato la funzionalità per oltre l'80% dei suoi server.
- ✔ Oltre il 90% dei dati dell'organizzazione interessata è stato ripristinato.
- ✔ Meno del 20% delle piattaforme di produzione dell'organizzazione sono state colpite.
- ✔ Meno del 10% dei repository di backup sono stati modificati o eliminati durante il tentativo compiuto dall'autore della minaccia.

Le linee guida sul ransomware migliorano la preparazione agli attacchi

La fiducia prima dell'attacco non sempre corrisponde alla realtà: **il 69% delle vittime di ransomware ha dichiarato di ritenere di essere preparato prima di essere attaccato, ma tale fiducia è diminuita di oltre il 20% dopo l'attacco,** evidenziando lacune critiche nella pianificazione.

Anche il divario nella percezione della preparazione rispetto alla realtà era più ampio per alcuni ruoli. In particolare, il livello di preparazione dei CIO è diminuito del 30% dopo l'attacco rispetto a un calo del 15% per i CISO, indicando che i CISO hanno una comprensione più accurata dell'approccio alla sicurezza della loro organizzazione.

Nel complesso, è fondamentale promuovere l'allineamento organizzativo in merito alla resilienza informatica, alle misure di preparazione e alle procedure di risposta agli incidenti. Ciò dovrebbe includere corsi di formazione ed esercitazioni in tutti i gruppi applicabili per supportare una risposta coerente e coordinata durante e dopo un attacco.

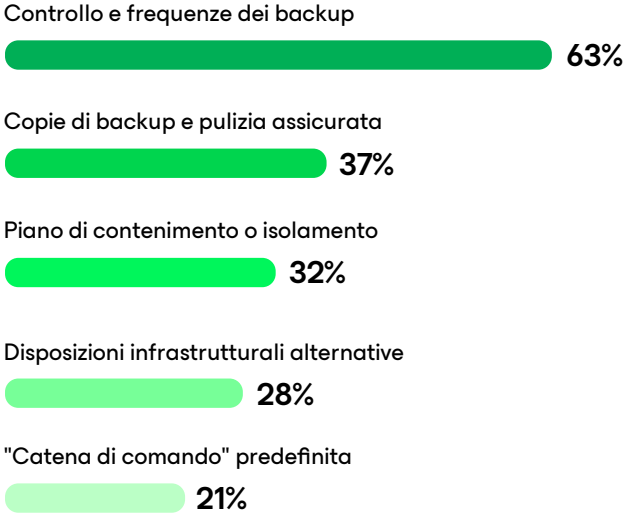
Mentre il 98% degli intervistati disponeva di un playbook sul ransomware, **meno della metà delle organizzazioni disponeva di elementi tecnici chiave,** come le verifiche e la frequenza dei backup (44%), le copie del backup e la garanzia di pulizia (44%), le disposizioni infrastrutturali alternative (37%), i piani di contenimento o isolamento (32%) e una "catena di comando" predefinita (30%).

Le organizzazioni con **risultati di maggior successo hanno avuto un'incidenza molto più elevata nell'includere questi cinque elementi tecnici chiave nelle loro linee guida.**

erano fiduciose nella propria preparazione prima di un attacco ransomware

di calo di fiducia nella preparazione della propria organizzazione dopo un attacco

Elementi chiave del playbook per organizzazioni di maggior successo



Il ripristino proattivo del backup aumenta la resilienza

Il ripristino sicuro del backup è fondamentale, ma è più impegnativo di quanto ci si possa aspettare. Infatti, **l'89% delle organizzazioni ha avuto i propri repository di backup presi di mira dall'autore della minaccia.**

Peggio ancora, hanno avuto una media del 34% dei repository di backup modificati o eliminati. Meno del 10% è riuscito a ripristinare più del 90% dei propri server entro le aspettative e solo il 51% ha ripristinato la maggior parte dei propri server.

La pianificazione del ripristino è fondamentale e si articola in più fasi. I team di sicurezza e IT devono contenere o eliminare la minaccia informatica, quindi porre rimedio all'accesso con strumenti come Identity and Access Management e altre soluzioni di sicurezza informatica, prima di ripristinare i dati in un ambiente sicuro.

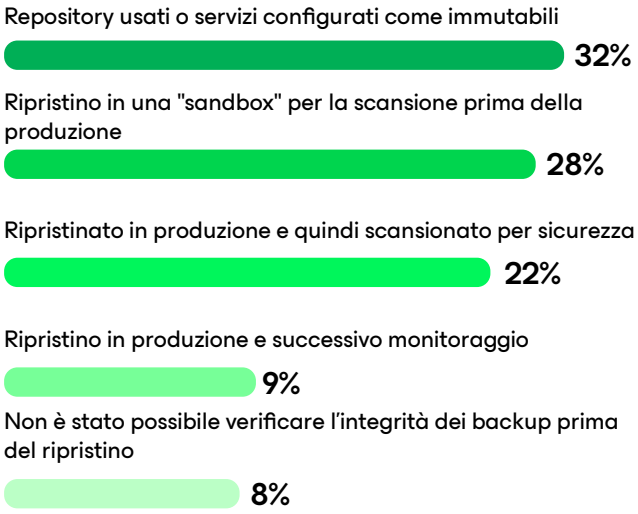
Anche i backup sicuri sono stati sottoutilizzati come misura proattiva. **Solo il 32% degli intervistati ha utilizzato repository o servizi configurati come immutabili,** mentre solo il 28% ha ripristinato i dati in un ambiente "sandbox" e ne ha eseguito una scansione per verificarne l'integrità. **Il 39% degli intervistati ha dovuto ripristinare i dati direttamente nell'ambiente di produzione e l'8% non ha potuto verificare l'integrità del backup prima del ripristino.**

Per ridurre il rischio aziendale, i responsabili IT e aziendali devono garantire che i dati e i backup siano scansionati e privi di malware prima di ripristinare in produzione. In caso contrario, potrebbero dover affrontare una serie di gravi conseguenze, tra cui: reinfezione rapida, movimento laterale, meccanismi di persistenza, detonazione ritardata, interruzione prolungata dell'attività, violazioni della conformità e altro ancora.

89%

delle organizzazioni hanno avuto i propri repository di backup presi di mira dall'autore della minaccia

Metodo di verifica dell'integrità del backup



Il potere delle "persone" nella resilienza al ransomware

Sebbene questi aspetti tecnici del ripristino siano essenziali, troppe organizzazioni trascurano gli elementi relativi alle "persone" cruciali nelle loro linee guida sul ransomware.

Solo il 26% delle organizzazioni disponeva di un processo decisionale di pagamento del riscatto per guidare una risposta rapida alle richieste di pagamento in base al potenziale impatto. Inoltre, in molti casi mancano le procedure per informare le forze dell'ordine, il che potrebbe aiutare nel ripristino e nella conformità.

Oltre un terzo delle organizzazioni ha utilizzato membri del team interno per comunicare con gli autori delle minacce. Il resto si è affidato all'assistenza di terze parti, inclusi specialisti di risposta agli incidenti e specialisti nella negoziazione dei riscatti. Questi specialisti sono indispensabili per guidare l'impegno sulla base di una comprensione dettagliata del comportamento degli attori delle minacce, che aiuta a supportare risultati più positivi. La comunicazione tra i membri del team interno e gli autori delle minacce può anche esporre inavvertitamente un'organizzazione a ulteriori rischi e minacce.

Infine, solo il 30% delle organizzazioni disponeva di una catena di comando predefinita per gestire gli attacchi. La catena di comando aiuta a garantire le scale di autorizzazione e le approvazioni appropriate per le decisioni critiche durante la risposta agli incidenti, fino al coinvolgimento con gli autori delle minacce o al pagamento di un riscatto.

Indipendentemente dal giorno o dall'ora, è sempre un brutto momento per subire un attacco ransomware, motivo per cui è così importante disporre di una roadmap per rispondere a minacce così stressanti e urgenti.

26%

delle organizzazioni hanno intrapreso un processo decisionale per il pagamento del riscatto

Mettendo assieme il tutto

Se considerate nel loro insieme, queste misure indicano una differenza fondamentale di mentalità tra le organizzazioni che hanno dimostrato resilienza agli attacchi ransomware nell'ultimo anno e quelle che non l'hanno fatto:

Le organizzazioni di successo fanno della resilienza informatica una parte della loro disciplina quotidiana. Integrano strategie proattive in tutte le loro operazioni IT quotidiane.

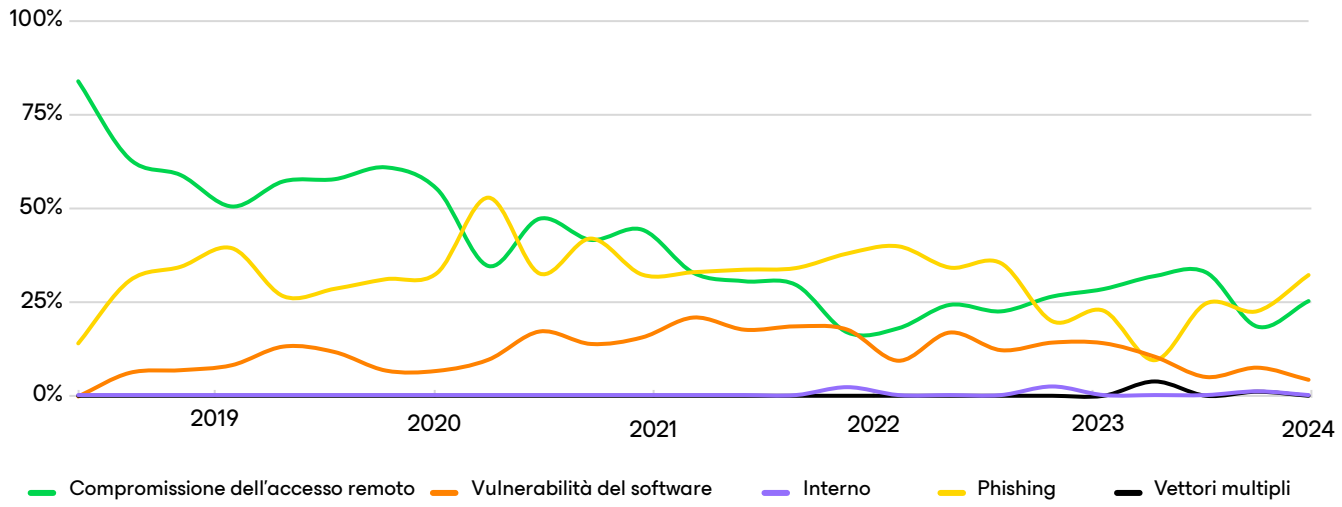
Dopo l'attacco, le organizzazioni di maggior successo erano anche più propense a rafforzare i programmi di formazione e sensibilizzazione dei dipendenti, che possono aiutare a mitigare gli attacchi di ingegneria sociale come il phishing. I criteri di aggiornamento del software vengono inoltre comunemente rafforzati dopo l'attacco per proteggersi dallo sfruttamento delle vulnerabilità del software su base continuativa. In particolare, **molte aziende hanno implementato nuove soluzioni di backup e ripristino e sono passate al cloud o ai servizi gestiti dopo l'attacco.** L'utilizzo di queste misure aiuta a proteggersi dai vettori di attacco comuni e migliora la resilienza.

Le organizzazioni di successo hanno implementato elementi di ripristino più proattivi dopo l'attacco rispetto alle organizzazioni di minor successo.

Queste pratiche di difesa proattiva aiutano anche ad affrontare i vettori di accesso iniziale più comuni che Coveware by Veeam ha riscontrato nel suo lavoro durante il quarto trimestre, tra cui la compromissione dell'accesso remoto, il phishing, le vulnerabilità del software e altro ancora.

Una solida difesa dagli attacchi ransomware non può essere semplicemente evocata quando si verifica un attacco. Devono essere una parte fondamentale delle operazioni quotidiane di un'organizzazione.

Fornitori di soluzioni contro attacchi ransomware



Fonte: Coveware by Veeam, "Il successo delle forze dell'ordine contro il ransomware continuerà nel 2025?"

Fare il punto della situazione e agire

Gli attacchi ransomware possono danneggiare la reputazione di un'organizzazione ed erodere la fiducia tra i suoi clienti e utenti finali. I costi legati alla gestione di un attacco possono anche avere gravi impatti finanziari, tra cui interruzioni operative, perdita di produttività e potenziali multe o cause legali.

Quando si verifica un attacco, le organizzazioni devono concentrarsi sul lavoro di squadra, sulla collaborazione e sulla comunicazione, mantenendo la calma e la compostezza mentre implementano le strategie di risposta previste dalle loro linee guida sugli attacchi ransomware. All'indomani di un attacco, le organizzazioni devono fare il punto della situazione, affrontare le cause alla radice del motivo per cui si è verificato e adottare misure per costruire la resilienza in modo da evitare che accada di nuovo.

Le organizzazioni che hanno avuto ripristini più efficaci hanno seguito queste best practice:

- ✔ Sviluppare solidi piani di risposta agli incidenti con ruoli e responsabilità chiari.
- ✔ Creare una strategia di backup e ripristino. Seguire la regola di resilienza dei dati 3-2-1-1-0 per configurare i repository come immutabili o protetti in altro modo e assicurarsi che i backup siano privi di malware prima del ripristino.[17]
- ✔ Implementare misure e processi di sicurezza proattivi, come l'architettura zero-trust, la gestione delle identità e degli accessi, le policy di aggiornamento software, le nuove soluzioni di rilevamento e risposta e i servizi cloud o gestiti.
- ✔ Aumentare la spesa in strumenti di rilevamento delle minacce per la prevenzione e in soluzioni di backup per il ripristino. Le piattaforme per la resilienza dei dati integrate con gli strumenti di sicurezza e dotate di funzionalità per prevenire o rilevare le minacce, come la Veeam Data Platform[18], contribuiscono in modo significativo a migliorare la sicurezza informatica e la resilienza.
- ✔ Organizzare programmi di formazione sulla sicurezza e sensibilizzare tutti i dipendenti.

Informazioni sul report

Il report sul ransomware di quest'anno ha intervistato 1.300 organizzazioni, 900 delle quali avevano subito almeno un attacco ransomware con conseguente crittografia o esfiltrazione negli ultimi 12 mesi. Gli intervistati erano Chief Information Security Officer (CISO) o dirigenti con responsabilità simili, nonché professionisti della sicurezza e leader IT provenienti dalle le Americhe, dall'Europa e dall'Australia.

Visita la nostra homepage per avere maggiori informazioni sulle soluzioni di sicurezza che possono migliorare la tua strategia di sicurezza informatica per aiutare ad accelerare il ripristino o per parlare con uno dei nostri esperti Veeam.

Le strategie di difesa informatica sono un problema che riguarda il consiglio di amministrazione. Non aspettare che si verifichi un attacco informatico. Adottare le misure necessarie per ridurre al minimo i rischi e mantenere la resilienza.

Note conclusive

1 https://go.veeam.com/ransomware-trends-executive-summary-2024-us

2 https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

3 https://www.justice.gov/archives/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

4 https://www.healthcareinfosecurity.com/blackcat-ransomware-group-seizure-appears-to-be-exit-scam-a-24521

5 https://www.databreachtoday.com/blogs/leaked-chat-logs-reveal-black-bastas-dark-night-soul-p-3828

6 https://www.veeam.com/blog/will-law-enforcement-success-against-ransomware-continue-in-2025.html

7 https://www.coveware.com/blog/2024/7/29/ransomware-actors-pivot-away-from-major-brands-in-q2-2024

8 https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

9 https://www.coveware.com/blog/2025/1/31/q4-report

10 https://counter-ransomware.org/aboutus

11 https://www.centerforcybersecuritypolicy.org/insights-and-research/the-international-counter-ransomware-initiative-from-forming-and-norming-to-performing

12 https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals/ransomware-legislative-proposals-reducing-payments-to-cyber-criminals-and-increasing-incident-reporting-accessible

13 https://www.databreachtoday.com/blogs/as-states-ban-ransom-payments-what-could-possibly-go-wrong-p-3273

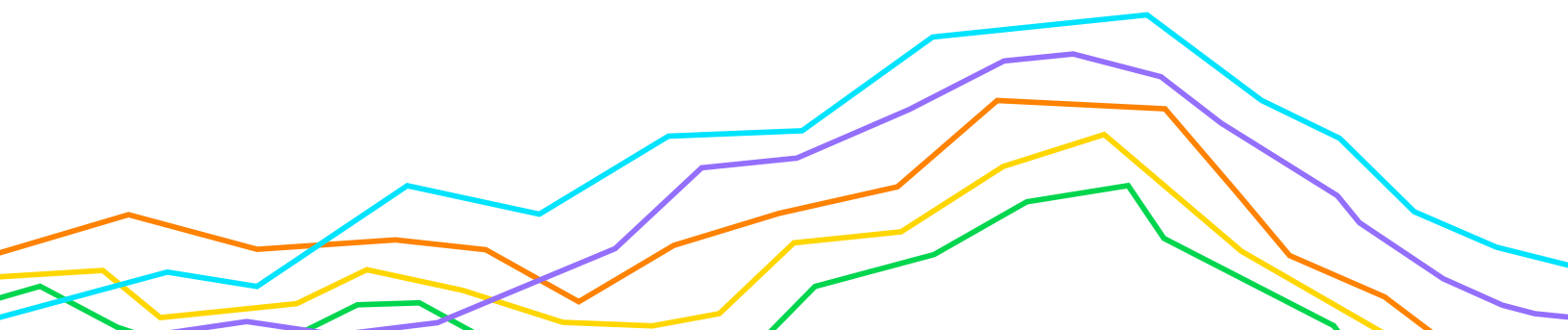
14 https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware

15 https://ofac.treasury.gov/media/912981/download?inline

16 https://www.youtube.com/watch?v=Fs2xq0pb7YQ

17 https://www.veeam.com/blog/321-backup-rule.html

18 https://www.veeam.com/products/veeam-data-platform.html



veeam Insights