SOPHOS

LA VERA STORIA DEL RANSOMWARE NEL RETAIL 2025

I risultati di uno studio indipendente a cui hanno partecipato 3.400 IT e Cybersecurity Manager in 16 paesi, inclusi 361 professionisti del settore retail, le cui organizzazioni sono state colpite dal ransomware l'anno scorso.

Whitepaper Sophos. 2025 ago

Introduzione

Ti diamo il benvenuto alla quinta edizione del report annuale di Sophos "La Vera Storia del Ransomware nel Retail" che rivela le dinamiche del malware nel 2025 per le organizzazioni che operano in tale settore.

Il report di quest'anno mostra come si sono evolute le esperienze con il ransomware (tanto le cause, quanto le conseguenze) delle organizzazioni nel corso degli ultimi 12 mesi. Inoltre, offre una nuova prospettiva su ambiti precedentemente inesplorati, inclusi i fattori operativi che hanno esposto le organizzazioni agli attacchi, nonché l'impatto umano degli incidenti sul team IT/di cybersecurity nel retail.

Prendendo spunto dalle esperienze reali vissute in prima persona da 361 IT e Cybersecurity Manager in 16 paesi, che lavorano per organizzazioni nel settore del retail cadute vittima del ransomware l'anno scorso, questo report offre approfondimenti esclusivi su argomenti quali:

- perché le organizzazioni in ambito retail vengono colpite dal ransomware
- cosa succede ai dati
- i riscatti: richieste e pagamenti
- l'impatto commerciale del ransomware
- l'impatto umano del ransomware

Una nota sul periodo di riferimento del report

Per facilitare il confronto delle statistiche dei nostri sondaggi annuali, i nostri report vengono nominati in base all'anno in cui viene condotto il sondaggio, in questo caso il 2025. Siamo consapevoli del fatto che i partecipanti condividono le loro esperienze nel corso dell'anno precedente, per cui molti degli attacchi menzionati si sono verificati nel 2024.

Informazioni sul sondaggio

Il report è basato sui risultati di una ricerca indipendente e vendor-agnostic che valuta le esperienze delle organizzazioni con il ransomware. È stato condotto per conto di Sophos da specialisti di terze parti nel periodo tra gennaio e marzo 2025. A tutti i partecipanti, che lavorano in organizzazioni con un numero di dipendenti compreso tra 100 e 5.000, è stato chiesto di rispondere tenendo in considerazione le proprie esperienze nei 12 mesi precedenti.

I 361 intervistati nel settore del retail inclusi nel report provengono da 16 paesi, per garantire che i risultati del sondaggio riflettano una selezione ampia e diversificata di esperienze. Il report include comparazioni con i risultati dei nostri studi di ricerca precedenti, per un raffronto annuo. Tutti i dati finanziari sono espressi in dollari U.S.A.

i risultati più salienti

perché le organizzazioni vengono colpite dal ransomware

- per il terzo anno consecutivo, le vittime nel settore retail identificano le **vulnerabilità soggette a exploit** come la più comune causa originaria di un attacco, essendo state sfruttate nel 30% degli incidenti.
- Le organizzazioni che operano in ambito retail sono state colpite dal ransomware a causa di molteplici fattori operativi, il più ricorrente dei quali è stata la presenza di una **lacuna di sicurezza di cui l'organizzazione non era a conoscenza**, segnalata dal 46% delle vittime. Al secondo posto segue a distanza ravvicinata la **mancanza di competenze**, che è stata un fattore che ha contribuito all'attacco nel 45% dei casi (il tasso più alto tra tutti i settori analizzati). Al terzo posto si trova la **mancanza di protezione**, che è risultata significativa nel 44% degli attacchi.

Cosa succede ai dati

- La **crittografia dei dati** come conseguenza degli attacchi nel settore del retail è scesa al livello più basso in cinque anni, in quanto è stata riscontrata nel 48% dei casi: una percentuale in calo rispetto al picco del 71% del 2023.
- Il 29% delle organizzazioni che operano in ambito retail che avevano subito la crittografia non autorizzata dei dati sono cadute vittima anche dell'**esfiltrazione dei dati**.
- Il 98% delle organizzazioni in ambito retail i cui dati erano stati crittografati è stato in grado di recuperarli.
- L'utilizzo di **backup** da parte delle organizzazioni che operano nel retail per ripristinare i dati crittografati ha toccato il punto più basso negli ultimi sei anni, essendo stato osservato nel 62% degli incidenti.
- Nel 58% dei casi riscontrati nel retail, le vittime hanno **pagato il riscatto** per recuperare i dati sottratti. Sebbene sia una leggera diminuzione rispetto al 60% dell'anno precedente, è pur sempre una percentuale che si colloca al secondo posto nella classifica dei più alti tassi di pagamento del riscatto osservati negli ultimi cinque anni.

Riscatti: le richieste e i pagamenti

- La somma media (mediana) delle **richieste di riscatto** nei confronti delle organizzazioni retail è raddoppiata negli ultimi 12 mesi: nel 2025 ammonta infatti a 2 milioni di $, mentre nel 2024 era di 1 milione di $. La principale causa di questa impennata è un aumento del 59% nel tasso dei pagamenti del riscatto pari a 5 o più milioni di $, che è passato dal 17% dei pagamenti nel 2024 al 27% nel 2025.
- Ciononostante, l'anno scorso la media (mediana) dei **pagamenti del riscatto** è salita di appena il 5%, raggiungendo 1 milione di $ nel 2025, in aumento rispetto ai 950.000 $ del 2024. Questo suggerisce che le organizzazioni del retail potrebbero essere sempre più restie a pagare riscatti gonfiati.
- La **percentuale delle richieste di riscatto che sono state pagate** dalle aziende del retail nel 2025 è infatti scesa all'81%, rispetto all'85% del 2024.
- Analizzando attentamente **le richieste rispetto ai pagamenti**, il pagamento finale è stato pari alla richiesta iniziale solo per il 29% degli intervistati nel settore del retail. Nel 59% degli incidenti, le vittime hanno pagato meno della richiesta iniziale, mentre nell'11% dei casi hanno pagato di più.

L'impatto commerciale del ransomware

- L'anno scorso il **costo per il recovery in seguito all'attacco ransomware nel settore del retail** è sceso del 40%, con 1,65 milioni di $, in calo rispetto ai 2,73 milioni di $ del 2024.
- Analizzando il **tempo necessario per tornare alla normalità operativa**, viene rilevato che le organizzazioni del retail si riprendono dagli attacchi con maggiore rapidità, con il 51% degli intervistati che sostiene di aver ripreso le normali attività dopo una settimana nel 2025, una statistica in aumento rispetto al 46% del 2024.

L'impatto umano del ransomware

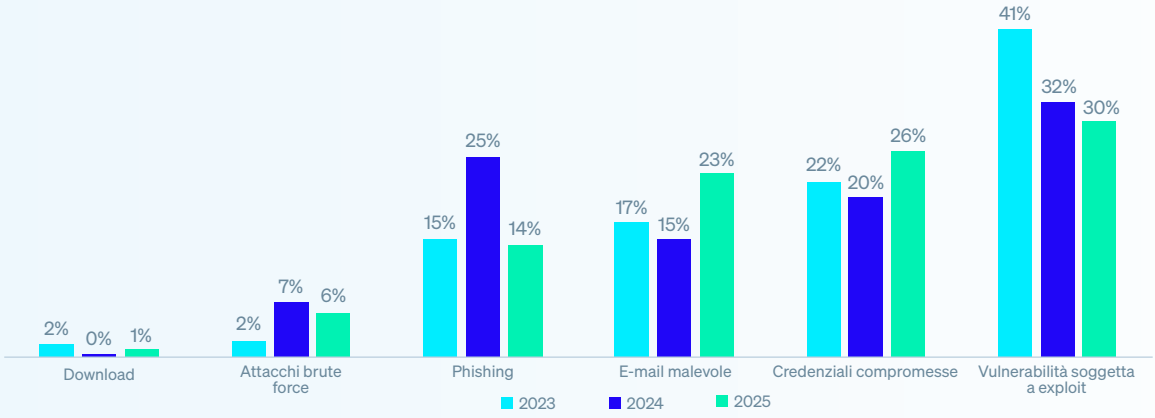
- Tutte le organizzazioni retail che avevano subito la crittografia non autorizzata dei dati confessano che ci sono state **ripercussioni dirette** sui loro team IT/di cybersecurity:
  - Quasi la metà (47%) dei team IT/di cybersecurity ha subito **maggiori pressioni** dal Senior Management, mentre il 30% ha notato un **maggior riconoscimento del proprio ruolo** da parte dei dirigenti aziendali.
  - Il 43% degli intervistati nel settore del retail ha confessato che il proprio team IT/di cybersecurity ha provato maggiore ansia o stress per paura di attacchi futuri e ha registrato un **aumento costante** del carico di lavoro.
  - Il 41% dei partecipanti al sondaggio ha notato cambiamenti nella **struttura del team/organizzativa** come conseguenza di un incidente.
  - Nel 37% dei team sono state osservate **assenze del personale** dovute a problemi di stress/salute mentale correlati all'attacco.
  - Un terzo (34%) sostiene che il team ha avuto **sensi di colpa** dovuti al fatto che l'attacco non era stato fermato in tempo.
  - In un quarto di questi casi (26%), c'è stato un **cambio di leadership** nel team come conseguenza dell'attacco.

Perché le organizzazioni vengono colpite dal ransomware

Causa tecnica all'origine degli attacchi

Per il terzo anno consecutivo, le vittime nel settore del retail identificano le vulnerabilità soggette a exploit come la più comune causa originaria degli incidenti di ransomware, essendo state utilizzate per l'infiltrazione nei sistemi delle organizzazioni nel 30% degli attacchi. Le credenziali compromesse mantengono il secondo posto nella classifica dei più comuni vettori di attacco percepiti, con una percentuale degli attacchi che utilizzano questo approccio che è salita dal 20% del 2024 al 26% del 2025. Le e-mail continuano a essere uno dei principali vettori di attacco, con il 23% degli intervistati nel retail che dichiara che la causa originaria dell'incidente è stato il phishing (in netto aumento rispetto al 15% registrato nel 2024), mentre per un ulteriore 14% si è trattato di un'e-mail malevola.

Grafico 1: Causa tecnica all'origine degli attacchi ransomware nel retail, 2023-2025



Conosci la causa all'origine dell'attacco ransomware subito l'anno scorso dalla tua organizzazione? Sì. n=359 (2025), n=261 (2024), n=243 (2023).

La ricerca rivela che, sebbene la causa originaria vari in base al settore, le vulnerabilità soggette a exploit costituiscono uno dei principali vettori di attacco per gran parte dei settori. Eccezioni significative:

- Il **phishing** è stata la più comune causa originaria sia nel settore dell'**istruzione** (22%), che in quello energetico, **petrolio/gas e utility** (29%).
- Le **credenziali compromesse** si trovano al primo posto nella classifica dei più comuni vettori di attacco percepiti per le realtà che operano nell'**amministrazione locale/pubblica**, in quanto costituiscono quasi un terzo degli incidenti (32%).

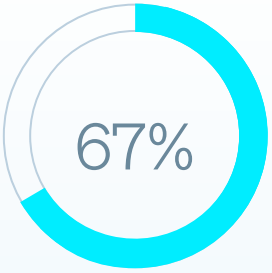
Grafico 2: Causa tecnica all'origine degli attacchi ransomware, con risultati suddivisi in base al settore

Conosci la causa all'origine dell'attacco ransomware subito l'anno scorso dalla tua organizzazione? Sì. Base di partecipanti indicata nel grafico.

Causa originaria degli incidenti nel retail inerente a fattori organizzativi

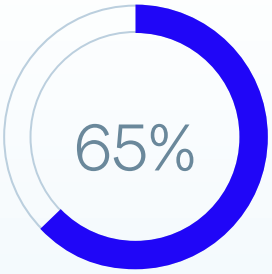
Il report di quest'anno esplora per la prima volta i fattori organizzativi che hanno esposto le organizzazioni in ambito retail agli attacchi. Dai risultati emerge che di solito le vittime nel settore del retail si trovano ad affrontare varie sfide organizzative, in quanto gli intervistati citano una media di 2,9 fattori che hanno contribuito a renderli un bersaglio per gli attacchi ransomware.

Complessivamente, le cause originarie inerenti a fattori organizzativi sono suddivise in maniera piuttosto equa tra le seguenti categorie: problemi di protezione, difficoltà in termini di risorse e lacune di sicurezza. Tuttavia, nel retail le organizzazioni hanno una probabilità leggermente maggiore di segnalare una lacuna di sicurezza (nota o sconosciuta) come fattore principale.



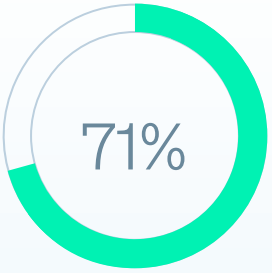
Sfide in termini di protezione

Mancanza di protezione o soluzioni di protezione di scarsa qualità, che non sono state in grado di bloccare l'attacco



Scarsa disponibilità di risorse

Mancanza delle competenze umane (capacità o conoscenze) necessarie per rilevare e bloccare l'attacco in tempo



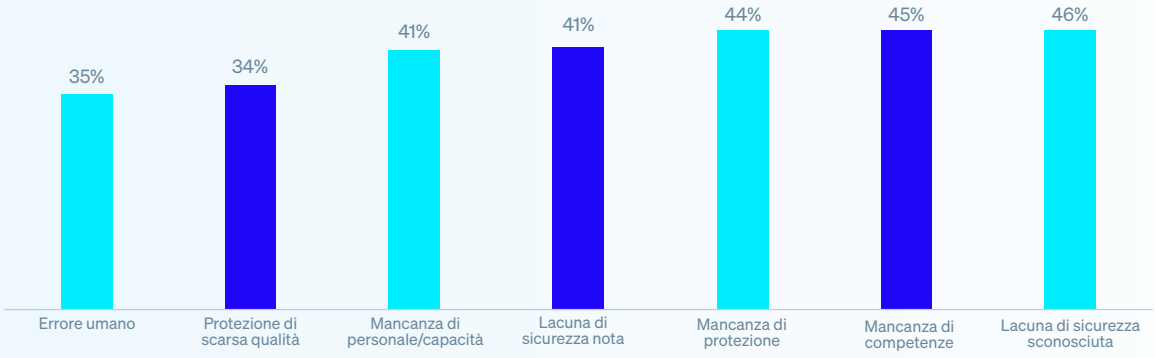
Lacuna di sicurezza

Lacune note o sconosciute nelle proprie difese

Perché ritieni che la tua organizzazione sia stata vittima dell'attacco ransomware? n=361. Risposte consolidate.

Le **lacune di sicurezza sconosciute** (ovvero vulnerabilità nelle difese di cui l'organizzazione non era a conoscenza) sono il singolo motivo principale indicato, in quanto sono state citate dal 46% degli intervistati nel retail. A distanza ravvicinata segue la **mancanza di competenze** (ovvero capacità o conoscenze insufficienti per bloccare l'attacco in tempo), che ha contribuito al 45% degli attacchi, ovvero la percentuale più elevata registrata tra tutti i settori per questa causa originaria specifica. Al terzo posto si trova la mancanza di protezione (ovvero non avere i prodotti e i servizi di cybersecurity necessari), che ha contribuito al 44% degli attacchi.

Grafico 3: Causa operativa all'origine degli attacchi ransomware nelle organizzazioni retail



Perché ritieni che la tua organizzazione sia caduta vittima dell'attacco ransomware? n=361.

Causa all'origine dell'attacco inerente a fattori organizzativi, in base al settore

La più comune causa all'origine dell'attacco inerente a fattori organizzativi varia anche a seconda del settore, il che riflette le diverse tipologie di sfide affrontate dalle aziende. È importante sottolineare che nessuno dei settori ha segnalato l'"errore umano" come motivo principale per cui l'organizzazione ha subito l'attacco ransomware.

Grafico 4: Principale causa operativa all'origine degli attacchi ransomware, in base al settore

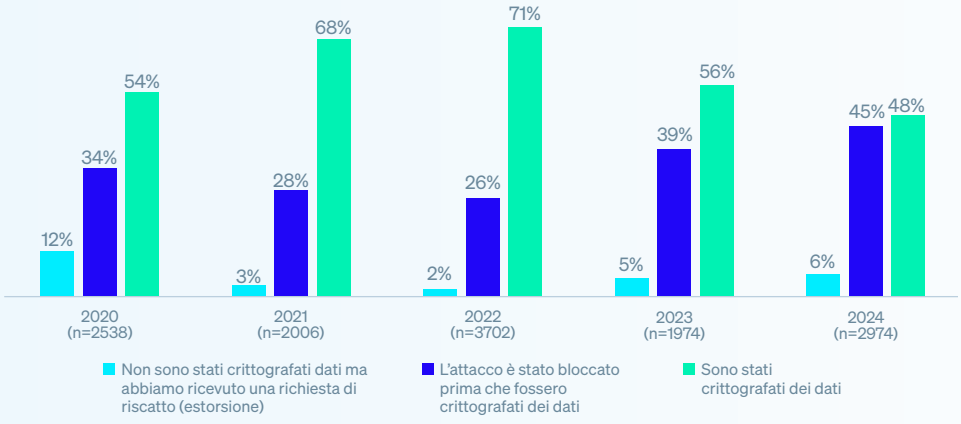
Perché ritieni che la tua organizzazione sia statavittima dell'attacco ransomware? n=3.400. Risultati suddivisi in base al settore.

Cosa succede ai dati

La crittografia dei dati nel retail

Un dato incoraggiante è che il tasso di crittografia non autorizzata dei dati nel retail è stato il più basso tra quelli registrati nei cinque anni di questo studio di ricerca, in quanto i dati sono stati crittografati in poco meno della metà (48%) degli attacchi. Negli ultimi due anni si è registrata una diminuzione significativa della percentuale di attacchi che hanno portato alla crittografia non autorizzata dei dati, pari al 71% in meno rispetto al nostro sondaggio del 2023. Questo suggerisce che le organizzazioni mostrano una maggiore capacità di bloccare gli attacchi prima che riescano a crittografare i dati.

Grafico 5: Tasso di crittografia dei dati negli attacchi ransomware subiti dalle organizzazioni retail, 2021-2025



Durante l'attacco ransomware, i cybercriminali sono riusciti a crittografare i dati della tua organizzazione? Base di partecipanti indicata nel grafico.

Tassi di crittografia dei dati, in base al settore

Le organizzazioni nel settore **distribuzione e trasporto** sono quelle con maggiore probabilità di subire la crittografia dei dati (64%), il che indica che sono meno frequentemente in grado di bloccare le attività di crittografia non autorizzata e/o ripristinare i file allo stato pre-attacco. Gli intervistati che operano nel settore dell'**istruzione** hanno invece registrato il minore tasso di crittografia dei dati, con appena il 29%: una percentuale nettamente al di sotto della media del 50% per tutti i settori.

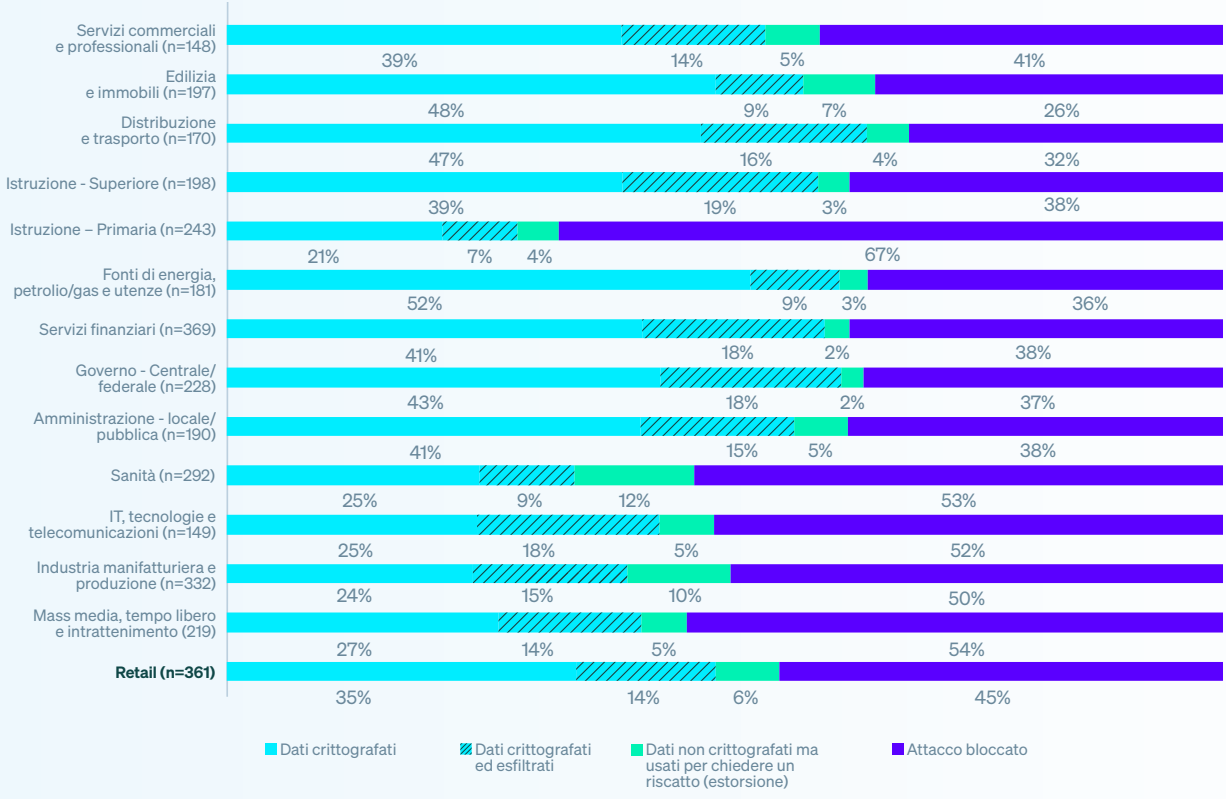
Furto dei dati

I cybercriminali non si limitano solo a crittografare i dati, ma se ne appropriano anche illecitamente. Nel settore del retail, il 14% di tutte le organizzazioni attaccate dal ransomware e il 29% di quelle i cui dati erano stati crittografati sono anche cadute vittima del furto dei dati. Analizzando le statistiche in base al settore, si osserva che:

- In cima alla classifica, il 42% delle organizzazioni del settore **IT, tecnologie e telecomunicazioni** hanno subito sia la crittografia che il furto dei dati.
- In netto contrasto, solo il 15% delle organizzazioni che operano nei settori dell'edilizia, immobiliare **fonti di energia, petrolio/gas e utility** ha dovuto affrontare sia il furto che la crittografia non autorizzata dei dati.

Nonostante ci sia la possibilità che le organizzazioni più piccole abbiano una maggiore capacità di prevenire il furto dei dati rispetto a quelle più grandi, la differenza potrebbe essere dovuta al fatto che è molto più probabile che gli autori degli attacchi cerchino di esfiltrare dati dalle organizzazioni di grandi dimensioni, nonché alla possibilità che le aziende più piccole siano meno in grado di determinare se siano stati sottratti dati.

Grafico 6: Crittografia e furto dei dati, in base al settore



Durante l'attacco ransomware, i cybercriminali sono riusciti a crittografare i dati della tua organizzazione? Base di partecipanti indicata nel grafico.

Attacchi di estorsione

Come indicato nel Grafico 5, l'anno scorso la percentuale di organizzazioni in ambito retail che non ha subito la crittografia dei dati ma ha comunque ricevuto una richiesta di riscatto (estorsione) è risultata la più alta in tre anni, essendo triplicata dal 2% degli attacchi nel 2023, al 6% nel 2025.

Analizzando le statistiche in base al settore, si osserva che i **fornitori di servizi sanitari** hanno dovuto affrontare la maggior parte degli attacchi di estorsione (12%). Molto probabilmente questo è dovuto all'alta sensibilità dei dati medici (cartelle cliniche, ecc.). In netto contrasto, sia i fornitori di **servizi finanziari** che le organizzazioni **governative** hanno registrato la minore quantità di questi tipi di attacchi, con appena il 2%.

Complessivamente, **gli istituti scolastici** i sono quelli che si sono dimostrati maggiormente abili nel prevenire le ripercussioni di un attacco ransomware (ovvero sono riusciti a impedire che i dati venissero crittografati o esfiltrati, e ad evitare i tentativi di estorsione). Questo suggerisce che gli istituti scolastici dimostrano una sorprendente capacità di rilevamento e intervento, nonostante le limitazioni di budget.

Recupero dei dati crittografati nel retail

Il 98% delle organizzazioni del retail i cui dati erano stati crittografati è stato in grado di recuperarli.

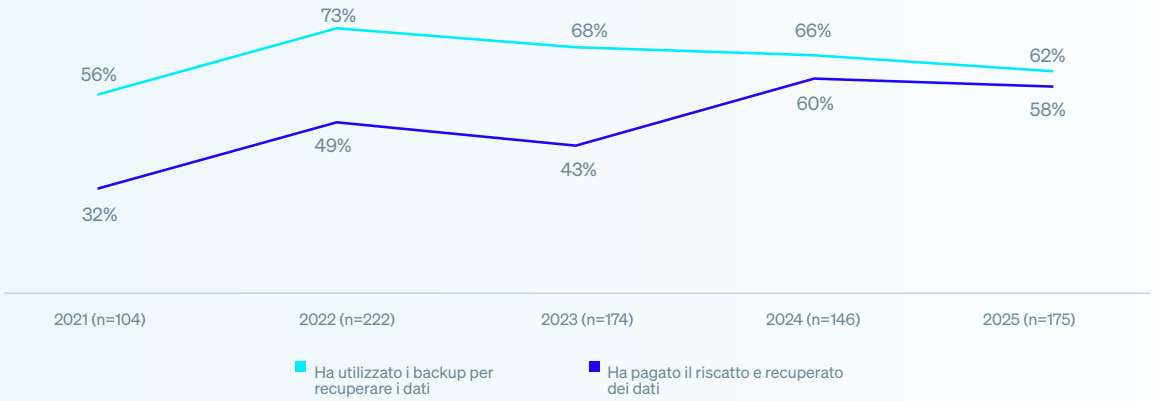
Il 62% delle organizzazioni che operano nel retail è riuscito a recuperare le informazioni sottratte grazie all'**uso di backup**: la percentuale più bassa riscontrata negli ultimi quattro anni; tuttavia, questo rimane uno dei tre settori che utilizzano maggiormente i backup.

Il 58% degli intervistati di questo settore sostiene di **aver pagato il riscatto e aver recuperato i dati in questo modo**. Anche se si tratta di un leggero calo rispetto al 60% dell'anno scorso, è pur sempre il secondo più alto tasso di pagamento del riscatto riscontrato nel settore retail negli ultimi cinque anni.

La diminuzione del divario tra gli intervistati nel retail che hanno pagato il riscatto per recuperare i dati e quelli che hanno invece eseguito il ripristino dai backup suggerisce una maggiore tendenza ad affidarsi a metodi di recupero multipli o alternativi.

A dimostrazione di ciò, abbiamo constatato che il 39% delle organizzazioni del retail che aveva subito la crittografia dei dati ha dichiarato di aver **utilizzato più di un metodo per recuperare le informazioni**. Nessun altro settore ha registrato una percentuale così alta.

Grafico 7: Recupero dei dati crittografati nel retail, 2021- 2025



La tua organizzazione è riuscita a recuperare almeno parte dei dati? Sì, abbiamo pagato il riscatto e recuperato dei dati; Sì, abbiamo utilizzato i backup per recuperare i dati. Base di partecipanti indicata nel grafico.

Riscatti

Richieste di riscatto nel retail

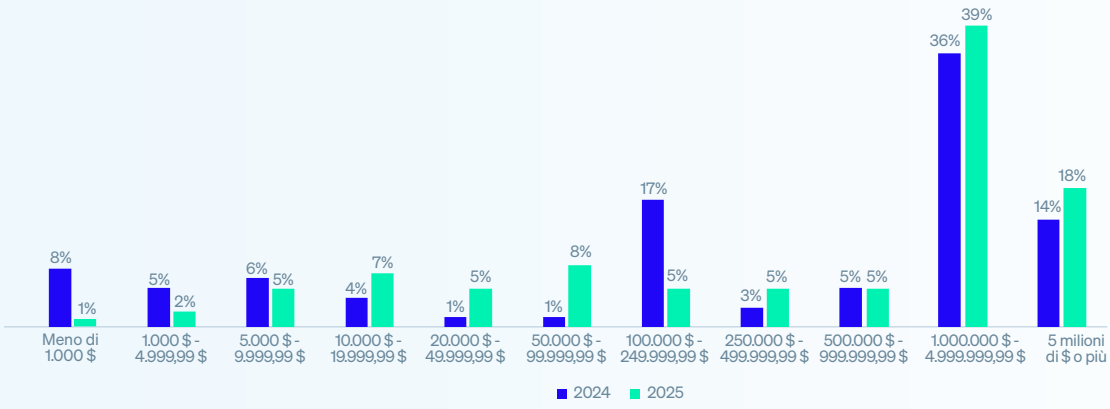
La somma media (mediana) delle richieste di riscatto nei confronti delle organizzazioni del retail è raddoppiata negli ultimi 12 mesi, raggiungendo i 2 milioni di $ nel 2025, in aumento rispetto alla cifra di 1 milione di $ nel 2024. L'incremento delle richieste di pagamento del riscatto tra le organizzazioni retail è dovuto principalmente a un aumento del 59% delle richieste di riscatto pari o superiori ai 5 milioni di $ negli ultimi 12 mesi. Inoltre, il 63% di tutte le richieste di riscatto nei confronti di questo settore ha superato 1 milione di $, in netto aumento rispetto al 50% registrato nel 2024.

La media di tutti i settori è invece scesa di un terzo (34%), passando da 2 milioni di $ nel 2024 a 1,32 milioni di $ nel 2025.

Pagamenti del riscatto nel retail

Nonostante l'impennata della cifra delle richieste di riscatto, la somma media (mediana) pagata dalle organizzazioni del retail è salita di appena il 5%, il che suggerisce che è possibile che le aziende di questo settore stiano diventando sempre più restie a pagare riscatti gonfiati. Ciononostante, sebbene la somma mediana pagata per il riscatto da questi partecipanti sia aumentata moderatamente, la distribuzione mostra una tendenza verso somme di pagamenti del riscatto più alte nel complesso, con un netto calo delle cifre più basse e un incremento delle organizzazioni che hanno pagato oltre 1 milione di $.

Grafico 8: Pagamenti del riscatto | Distribuzione suddivisa in fasce

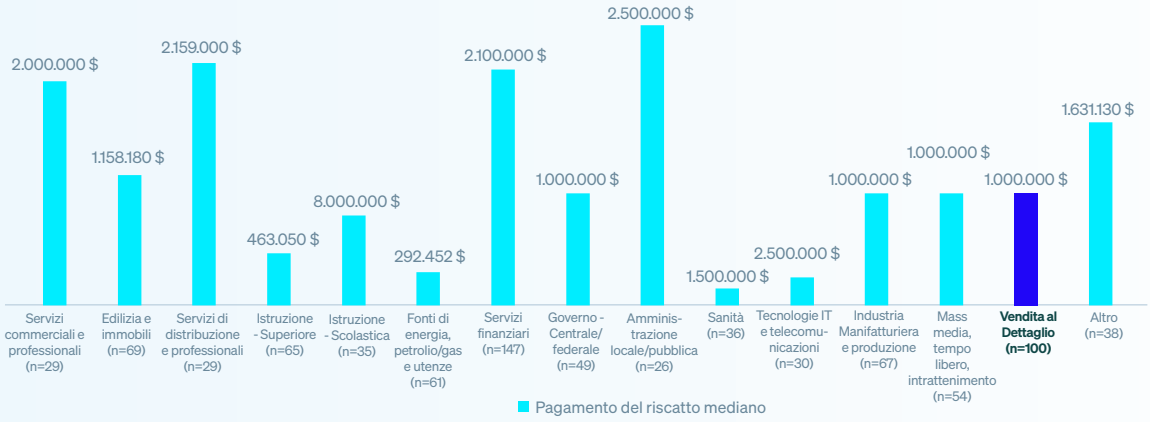


A quanto ammonta la somma di riscatto pagata ai cybercriminali? n=100 (2025), 78 (2024)

Pagamento del riscatto, in base al settore

I pagamenti del riscatto variano notevolmente in base al settore, e a pagare la cifra media più elevata sono state le organizzazioni dell'**amministrazione pubblica e locale**, con 2,5 milioni di $. Questo potrebbe essere dovuto a fattori quali le pressioni dovute all'obbligo di fornire servizi essenziali, la limitata resilienza informatica e il fatto che gli autori degli attacchi sfruttano l'urgenza di riprendere rapidamente le normali attività operative. I fornitori di **servizi sanitari** hanno invece pagato la cifra media minore, ovvero 150,000 $.

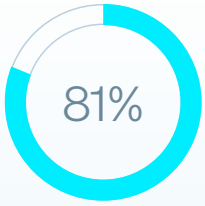
Grafico 9: Pagamento del riscatto, in base al settore



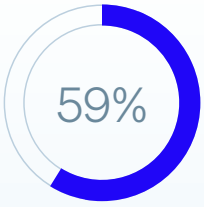
A quanto ammonta la somma di riscatto pagata ai cybercriminali? Base di partecipanti indicata nel grafico. Nota: dato il numero ridotto di partecipanti al sondaggio nei settori Servizi commerciali e professionali e Amministrazione locale/pubblica, i risultati sono da considerarsi puramente indicativi.

Confronto tra pagamenti effettivi e richieste di riscatto iniziali nel retail

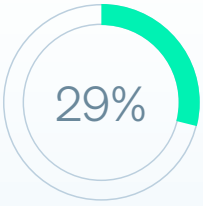
100 delle organizzazioni del retail che hanno pagato il riscatto hanno condiviso sia l'informazione relativa alla richiesta iniziale dei cybercriminali, che quella che concerne la somma effettiva pagata. I risultati rivelano che queste vittime hanno pagato in media l'81% della somma richiesta inizialmente per il riscatto: un calo incoraggiante rispetto all'85% registrato nel 2024. Complessivamente, nel 59% dei casi hanno pagato meno della somma richiesta (ben oltre la media del 53% di tutti i settori), nell'11% dei casi hanno pagato di più e nel 29% degli incidenti si sono attenute alla richiesta iniziale.



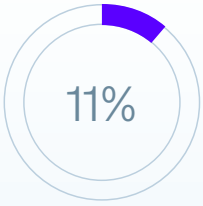
della somma di riscatto richiesta **è stata pagata**, in media



dei pagamenti sono stati **meno** della richiesta di riscatto iniziale



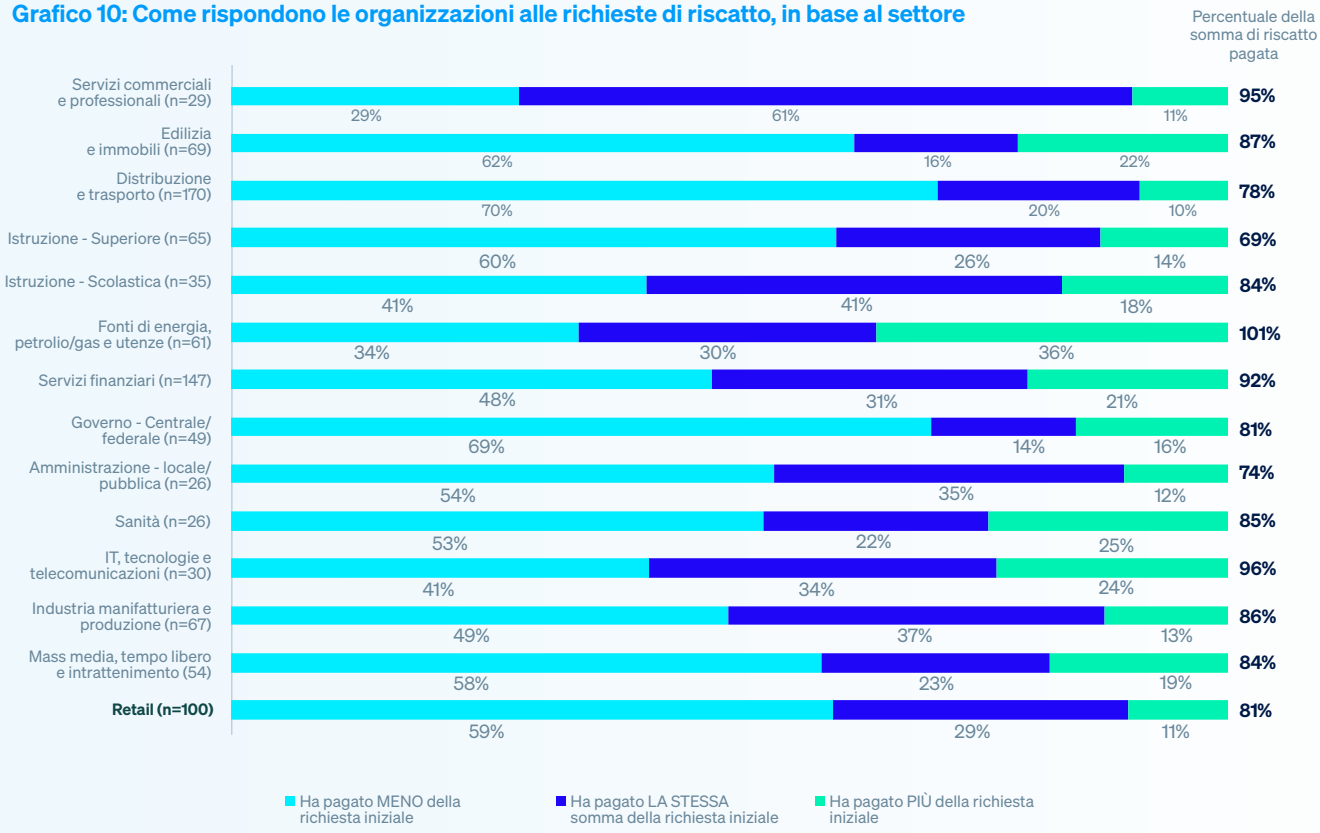
dei pagamenti sono stati **pari** alla richiesta di riscatto iniziale



dei pagamenti sono stati **più** della richiesta di riscatto iniziale

Suddividendo i dati in base al settore, si nota una tendenza incoraggiante: nella maggior parte dei settori è più frequente che venga pagato meno della richiesta di riscatto iniziale. Le organizzazioni del settore **distribuzione e trasporto** sono quelle con più probabilità di pagare meno della richiesta di riscatto iniziale (70%), il che suggerisce una maggiore opposizione a pagare il riscatto. Gli intervistati che operano nell'ambito di **fonti di energia, petrolio/gas e utility** sono quelli che hanno mostrato una maggiore probabilità di pagare più della cifra iniziale richiesta (36%), mentre i **servizi commerciali e professionali** sono stati i più propensi a pagare la somma di riscatto iniziale (61%).

Grafico 10: Come rispondono le organizzazioni alle richieste di riscatto, in base al settore



A quanto ammonta la somma di riscatto pagata ai cybercriminali? Nota: dato il numero ridotto di partecipanti al sondaggio nei settori Servizi commerciali e professionali e Amministrazione locale/pubblica, i risultati sono da considerarsi puramente indicativi. Base di partecipanti indicata nel grafico.

I motivi per cui nella maggior parte dei casi di attacchi al retail si registra una differenza tra la somma di riscatto pagata e quella richiesta inizialmente

Quest'anno abbiamo analizzato per la prima volta i motivi per cui alcune organizzazioni del retail pagano più della richiesta di riscatto iniziale e perché altre pagano meno, offrendo una nuova prospettiva su un ambito importante della gestione degli attacchi ransomware.

11 organizzazioni del retail* che **hanno pagato più** della richiesta iniziale hanno dichiarato quanto segue:

- 45% degli intervistati: i cybercriminali hanno capito che eravamo un bersaglio di alto valore.
- 45% degli intervistati: i cybercriminali si sono infastiditi e hanno aumentato il riscatto.
- 45% degli intervistati: i nostri backup non hanno funzionato o presentavano difetti.
- 36% degli intervistati: i cybercriminali erano convinti che potevamo permetterci di pagare di più.
- 18% degli intervistati: non abbiamo pagato abbastanza rapidamente, quindi la somma è salita.

Tipicamente, le organizzazioni retail hanno indicato due fattori alla base della decisione di pagare di più, rivelando così le molteplici sfide che le vittime si trovano ad affrontare quando cercano di recuperare i propri dati.

*Nota: poiché la base di partecipanti è limitata, i risultati sono da considerarsi puramente indicativi.

60 organizzazioni in ambito retail che hanno **pagato meno** della cifra di riscatto richiesta inizialmente hanno condiviso come sono riuscite a ridurre la somma:

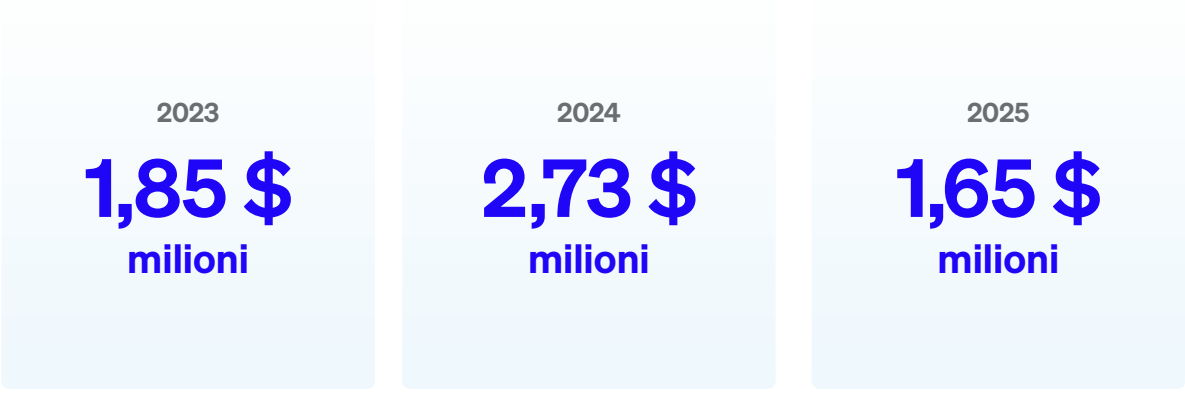
- 60% degli intervistati: i cybercriminali hanno ridotto la richiesta iniziale per via di pressioni esterne (ad es. da parte dei media o delle forze dell'ordine).
- 47% degli intervistati: i cybercriminali hanno diminuito la richiesta per convincerci a pagare.
- 43% degli intervistati: una terza parte ha negoziato con i cybercriminali per ridurre la cifra iniziale.
- 42% degli intervistati: abbiamo pagato il riscatto velocemente, così abbiamo usufruito di uno sconto.
- 35% degli intervistati: abbiamo negoziato una cifra più bassa con i cybercriminali.

Questo campione ha anche indicato, in media, 2 fattori alla base dei pagamenti di una somma minore di riscatto rispetto a quella iniziale, evidenziando ulteriormente la natura complessa e poliedrica della situazione affrontata dalle vittime del ransomware.

Le conseguenze commerciali del ransomware

Costi di recovery dall'attacco nel retail

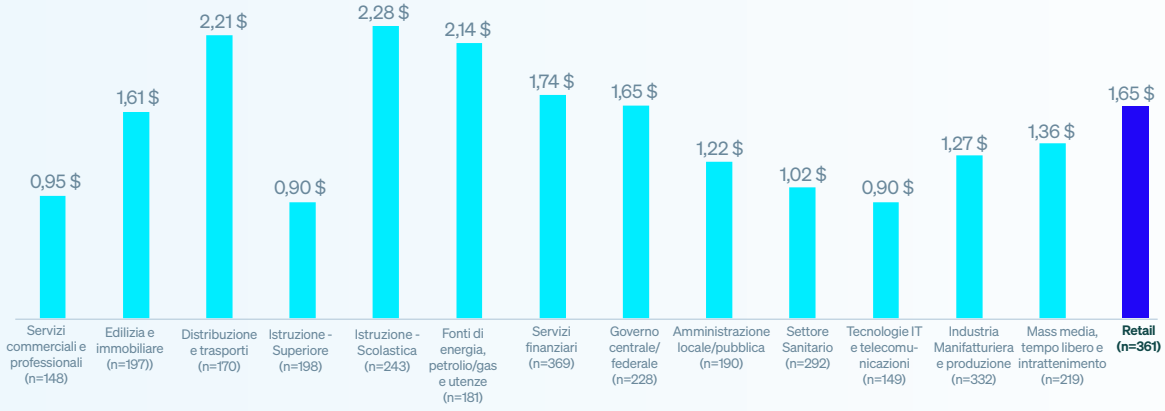
Il costo medio di recovery dall'attaco ransomware nel settore del retail (escludendo eventuali pagamenti del riscatto) ha toccato la cifra più bassa in tre anni, scendendo dal 40% negli ultimi 12 mesi, con 1,65 milioni di $, in calo rispetto ai 2,73 milioni di $ del 2024. Si tratta di 200.000 $ in meno rispetto alla somma registrata nel 2023.



Qual è stato approssimativamente il costo sostenuto dalla tua organizzazione per rimediare ai danni provocati dall'attacco ransomware più grave (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali ecc.), escludendo eventuali pagamenti del riscatto? n=361 (2025), n=261 (2024), n=244 (2023).

Osservando la ripartizione in base al settore, i costi necessari per riprendere le normali attività operative variano in maniera notevole. Gli istituti di **scolastici di livello primario** hanno segnalato il più alto costo medio per riparare ai danni degli incidenti, con 2,28 milioni di $. Gli istituti di **istruzione superiore** e le organizzazioni del settore **IT, tecnologie e telecomunicazioni** hanno invece registrato entrambe il costo più basso, con 0,90 milioni di $.

Grafico 11: Costi di recovery dei danni del ransomware, con risultati suddivisi in base alle dimensioni dell'azienda

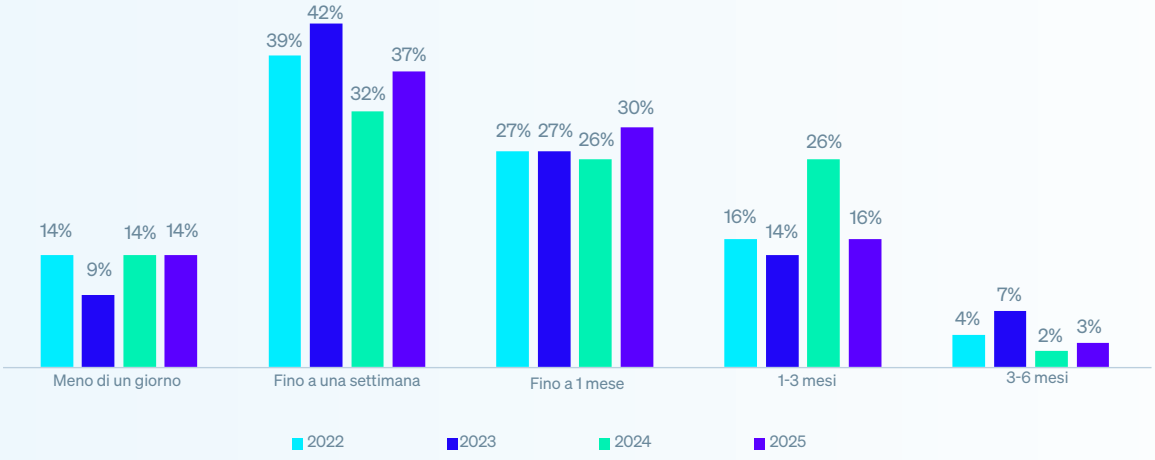


Qual è stato approssimativamente il costo sostenuto dalla tua organizzazione per rimediare ai danni provocati dall'attacco ransomware più grave (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali ecc.), escludendo eventuali pagamenti del riscatto? Base di partecipanti indicata nella tabella.

Tempi necessari per riprendere le normali attività

Dai dati è emerso che nel 2025 le organizzazioni retail hanno mostrato maggiore rapidità di ripresa delle normali attività operative dopo un attacco ransomware. Oltre la metà (51%) dei partecipanti ha ripreso la normalità operativa in meno di una settimana, in aumento rispetto al 46% registrato nel 2024. Allo stesso tempo, la percentuale di intervistati in grado di riprendere le normali attività è diminuita drasticamente, passando dal 26% del 2024 al 16%. Complessivamente, nel 96% dei casi le vittime del retail sono tornate alla normalità operativa entro tre mesi, il che evidenzia una maggiore resilienza e capacità di recupero in questo settore.

Grafico 12: Tempi necessari per tornare alla normalità operativa in seguito a un attacco ransomware per le organizzazioni nel settore retail, 2022-2025



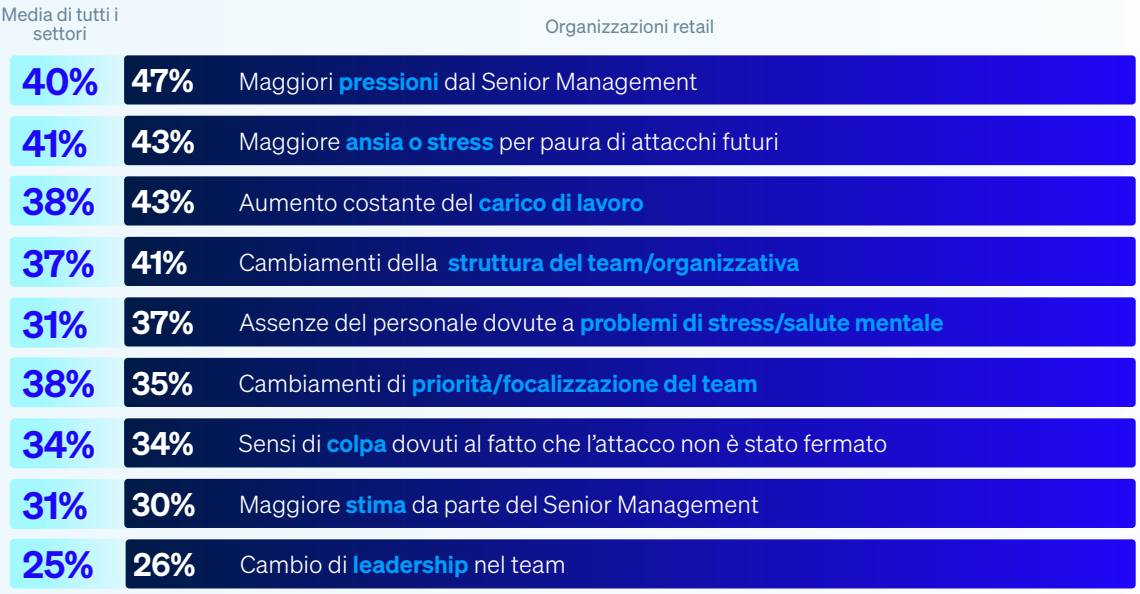
Di quanto tempo ha avuto bisogno la tua organizzazione per riprendere completamente le normali attività operative dopo l'attacco ransomware? Base di partecipanti indicata nel grafico.

Non sorprende il fatto che, tipicamente, le organizzazioni retail che avevano subito la crittografia non autorizzata dei dati sono state più lente a riprendersi rispetto a quelle che erano riuscite a prevenirla: nel 6% dei casi le aziende i cui dati erano stati crittografati sono tornate operative entro un giorno, mentre questa statistica sale al 22% per le organizzazioni che sono riuscite a impedire ai cybercriminali di crittografare i dati.

Le conseguenze a livello umano del ransomware

Il sondaggio mostra chiaramente che subire la crittografia non autorizzata dei dati durante un attacco ransomware implica ripercussioni molto serie per i team IT/di cybersecurity, in quanto tutti gli intervistati nel retail sostengono che il proprio team ne ha risentito in qualche misura.

Grafico 13: Le conseguenze della crittografia dei dati sui team IT/di cybersecurity



Quali ripercussioni (se presenti) ha avuto l'attacco ransomware sui membri del tuo team IT/di cybersecurity? n=175.

Raccomandazioni

Sebbene negli ultimi 12 mesi le organizzazioni retail abbiano notato diversi cambiamenti nelle proprie esperienze con il ransomware, rimane comunque una seria minaccia. Con cybercriminali che continuano a replicare ed evolvere i loro attacchi, è fondamentale che i team di sicurezza e le difese informatiche delle organizzazioni non restino indietro, per poter tener testa al ransomware e ad altre minacce. Utilizza gli approfondimenti di questo report per potenziare le tue difese, ottimizzare le tue attività di risposta alle minacce e limitare l'impatto del ransomware sia sulla tua azienda che sui dipendenti. Concentrati su questi quattro ambiti per tenerti un passo avanti rispetto agli attacchi:

- **Prevenzione**. La difesa più efficace contro il ransomware è quella che lo previene del tutto, perché impedisce ai cybercriminali di compromettere la tua organizzazione. Adotta misure adeguate per eliminare le cause tecniche e operative all'origine degli attacchi indicate in questo report.
- **Protezione**. Avere una solida base di sicurezza è un must. Gli endpoint (server inclusi) sono l'obiettivo iniziale primario per i cybercriminali del ransomware, per cui è importante assicurarsi che vengano difesi adeguatamente, con una protezione anti-ransomware dedicata, in grado di bloccare i tentativi di crittografia non autorizzata e ripristinare i file allo stato pre-attacco.
- **Rilevamento e risposta**. Prima viene bloccato un attacco, migliori saranno i risultati. Un sistema di rilevamento e risposta alle minacce attivo 24/7 è un livello di difesa a cui ormai non è possibile rinunciare. Se non hai le risorse o le competenze necessarie per implementarlo e gestirlo internamente, cerca di collaborare con un fornitore di servizi MDR (Managed Detection and Response).
- **Pianificazione e preparazione**. Poter contare su un piano strategico di incident response con cui hai già acquisito familiarità migliorerà notevolmente i risultati, qualora succedesse il peggio e la tua organizzazione dovesse subire un attacco grave. Assicurati di eseguire backup di alta qualità e svolgi esercitazioni regolari di ripristino dei dati per accelerare il ritorno alla normalità operativa nel caso in cui i tuoi sistemi dovessero essere colpiti.

Per scoprire come Sophos può aiutarti a ottimizzare le tue difese anti-ransomware, parla con un consulente o visita www.sophos.it

Scopri di più sul ransomware e su come Sophos può aiutarti a proteggere la tua organizzazione.

Sophos offre soluzioni di cybersecurity leader di settore, ideali per le aziende di tutte le dimensioni; inoltre, protegge i sistemi in tempo reale contro minacce avanzate quali malware, ransomware e phishing. Grazie alle funzionalità next-gen dall'efficacia comprovata, garantisce una protezione efficace per i dati aziendali, con prodotti basati su tecnologie di intelligenza artificiale e machine learning.

04/08/2025 WP (MP)

SOPHOS