REPORT

La vera storia del ransomware per il settore dell'istruzione 2026

I risultati di uno studio indipendente a cui hanno partecipato 226 responsabili IT e di cybersecurity che operano nel settore dell'istruzione in 17 paesi e le cui organizzazioni sono state colpite dal ransomware l'anno scorso.

SOPHOS

Introduzione

Benvenuti alla sesta edizione del rapporto annuale Sophos State of Ransomware in Education, che rivela la realtà del ransomware sia per gli istituti di istruzione inferiore (inclusi scuole K-12, primarie e secondarie — tipicamente per studenti sotto i 18 anni) che per gli istituti di istruzione superiore (università, college e istituti equivalenti — tipicamente per studenti sopra i 18 anni) nel 2026.

Il rapporto di quest'anno illumina anche nuove aree precedentemente inesplorate, tra cui dove iniziano gli attacchi nell'ambiente, il ruolo difensivo dell'autenticazione multifattoriale (MFA) e dei firewall, e il legame tra attacchi basati sull'identità e ransomware.

Basandosi sulle esperienze reali di 226 leader IT e di cybersecurity dell'istruzione, 131 provenienti da istituti di istruzione inferiore e 95 da istituti di istruzione superiore colpiti da ransomware nell'ultimo anno, questo report offre approfondimenti unici su:

- Metodi di attacco e di difesa
- Crittografia e recupero dei dati
- Richieste e pagamenti del riscatto
- Impatto sulle aziende e sugli esseri umani

Nota: In questo report, il termine "indagine generale" si riferisce ai risultati ottenuti dai partecipanti in tutti i settori analizzati. I 226 partecipanti nel settore dell'istruzione fanno parte di una coorte più ampia di 2.158 partecipanti in 15 settori industriali.

Informazioni sul sondaggio

Questo report si basa sui risultati di un sondaggio indipendente e vendor-agnostic commissionato da Sophos. Il sondaggio ha posto domande sulle esperienze delle organizzazioni in merito agli attacchi ransomware e alle intrusioni basate sull'identità, monitorando anno su anno i tassi di pagamento del riscatto, i costi di riparazione dei danni, i tempi di recupero dopo un attacco e molte altre metriche. Le risposte sono state raccolte tra gennaio e marzo 2026 e si basano sulle esperienze degli intervistati relative ai 12 mesi precedenti.

I partecipanti provengono da 17 paesi e 15 settori economici, un'ampia varietà di settori pubblici e privati, e includono un campionamento a curva gaussiana di aziende con un numero di dipendenti compreso tra 15 e 100, mantenutosi proporzionalmente coerente nei sette anni di storia del sondaggio. Tutti i dati finanziari sono espressi in dollari U.S.A.

I risultati più salienti

- **Gli attacchi di identità, specialmente quelli basati su e-mail, erano alti nei settori dell'istruzione.**
  - Il 77% delle vittime di istruzione superiore e il 71% di istruzione inferiore hanno confermato che il loro attacco ransomware è stato anche il loro attacco di identità più significativo, entrambi al di sopra della percentuale generale del 67% (tutti i settori).
  - Le e-mail dannose sono state la causa tecnica principale degli attacchi ransomware nell'istruzione inferiore (31%) e nell'istruzione superiore (29%).
  - Gli approcci basati sull'identità (ad esempio, e-mail dannose, phishing, credenziali compromesse o forza bruta) hanno avviato l'85% degli attacchi in tutti gli ambiti dell'istruzione, superando il tasso del 79% per tutti i settori.
- **Le debolezze operative nell'istruzione erano superiori a quelle dell'indagine generale (tutti i settori).**
  - Il principale divario nell'istruzione superiore è stato riscontrato nelle competenze: Il 53% ha dichiarato di non avere le competenze per rilevare e fermare l'attacco in tempo, contro il 35% per l'indagine generale.
  - Le principali cause operative dell'istruzione inferiore erano l'errore umano (52%), la mancanza di protezione (47%), le lacune di sicurezza sconosciute (42%) e la mancanza di personale o capacità (41%).
- **La crittografia dei dati in seguito agli attacchi ransomware è aumentata drasticamente nell'istruzione inferiore.**
  - Il tasso di crittografia dei dati nel settore dell'istruzione inferiore è più che raddoppiato, salendo dal 29% del 2025 al 61% del 2026.
  - Il 58% degli attacchi al settore dell'istruzione ha avuto come risultato dati crittografati, vicino al tasso generale del 56% rilevato nel sondaggio.
- **I fornitori di istruzione facevano grande affidamento sui backup per ripristinare i dati.**
  - Il 77% dei fornitori di istruzione inferiore ha ripristinato dati crittografati dai backup, superiore al tasso medio del 66% dell'indagine.
  - Il 69% dei fornitori di istruzione superiore ha anche ripristinato i dati utilizzando i backup.
- **Il settore dell'istruzione ha pagato meno rispetto all'indagine generale, ma ha riscontrato un maggior numero di pagamenti del riscatto superiori a 5 milioni di $.**
  - La richiesta di riscatto mediana per l'istruzione è stata più alta rispetto all'indagine generale, con 775.200 $ (rispetto a 698.000 $), ma il pagamento del riscatto mediano è risultato inferiore, con 515.000 $ (rispetto ai 769.000 $ dell'indagine generale).
  - In questo settore, le richieste di riscatto mediane sono diminuite per due anni consecutivi, mentre i pagamenti sono aumentati di 15.000 $ dal report del 2025 a quello del 2026.
  - Gli istituti di istruzione sono stati più propensi a pagare 5 milioni di $ o più (23% rispetto al 16% dell'indagine generale).
- **Il costo di riparazione dei danni è stato più elevato e ha richiesto più tempo nel settore dell'istruzione.**
  - I costi medi di riparazione dei danni nell'istruzione hanno raggiunto 2,26 milioni di $, al di sopra degli 1,7 milioni di $ dell'indagine generale.
  - I costi di riparazione dei danni nell'istruzione sono aumentati rispetto al report del 2025, passando da 1,66 milioni a 2,26 milioni di $, con un aumento di oltre 1 milione di $ nell'istruzione superiore.
  - Il 26% dei fornitori di istruzione ha impiegato da uno a tre mesi per riprendersi completamente da un attacco ransomware, circa il doppio del tasso del 14% per tutti i settori.
  - L'istruzione inferiore ha registrato la più alta percentuale di attività di riparazione dei danni durate a lungo: il 31% ha impiegato un mese o più per tornare alla normalità operativa, più di qualsiasi altro settore.
- **L'impatto umano sui team di sicurezza si è intensificato.**
  - Il 53% dei team in organizzazioni dell'istruzione superiore ha segnalato maggiori pressioni dal Senior Management, rispetto al 40% tra tutti i settori.
  - Circa il 39% dei team educativi ha segnalato assenze del personale dovute a stress o problemi di salute mentale, contro il 29% in tutti i settori.

Metodi di attacco e di difesa

Cause all'origine degli attacchi

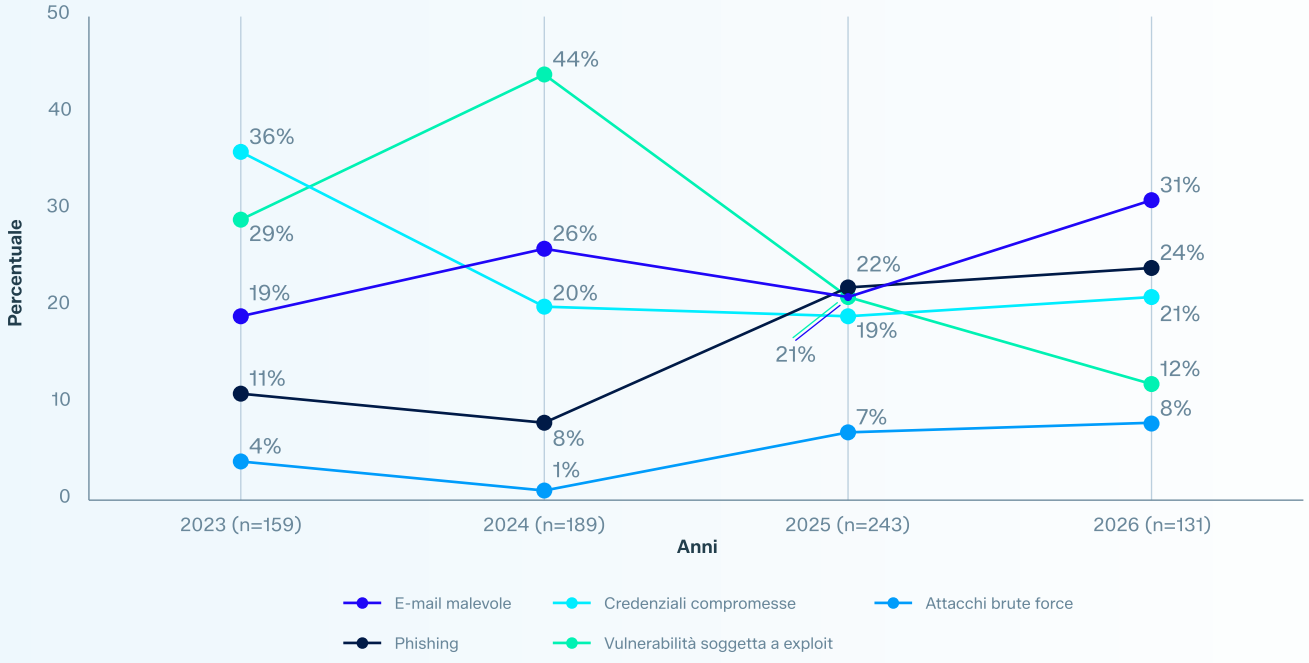
I dati educativi di quest'anno riflettono la stessa tendenza osservata in tutti i settori: gli attacchi basati sull'identità sono in crescita.

Le e-mail dannose sono state la causa tecnica principale nell'istruzione inferiore (31%), seguite da phishing (24%) e credenziali compromesse (21%). Le vulnerabilità soggette a exploit sono scese al 12%, il che riflette il calo complessivo nell'indagine generale (tutti i settori) al 18%.

85%

La percentuale di attacchi rivolti agli istituti di istruzione che sono iniziati con un approccio basato sull'identità (ad es. e-mail dannose, phishing, credenziali compromesse o brute force), superiore al tasso del 79% per l'indagine generale.

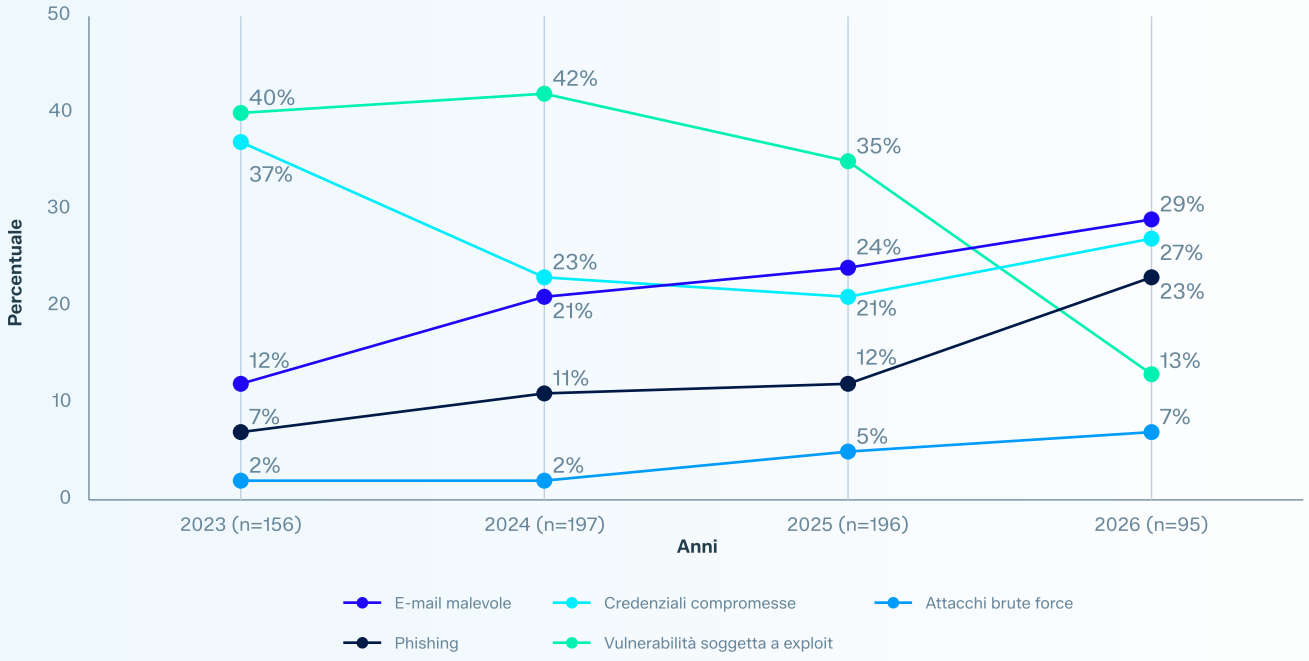
Causa tecnica all'origine degli attacchi ransomware 2023–2026: Istruzione scolastica



Conosci la causa all'origine dell'attacco ransomware subito l'anno scorso dalla tua organizzazione?
I download e le risposte "Non so" sono stati esclusi dal grafico per chiarezza visiva. La somma delle percentuali potrebbe non essere uguale al 100%.
Base di partecipanti indicata nel grafico.

Anche gli istituti di istruzione superiore hanno segnalato una diminuzione delle vulnerabilità soggette a exploit. Questo vettore è sceso al 13% nel report del 2026, in calo rispetto al 35% del 2025. **E-mail dannose (29%) e credenziali compromesse (27%) sono quasi cause principali** con il phishing che segue a 23%. Sia il settore dell'istruzione inferiore che quello superiore riportano attacchi basati su e-mail come cause principali, il che è coerente con l'indagine generale, dove e-mail dannose (26%) e phishing (24%) insieme rappresentano metà di tutti gli incidenti.

Causa tecnica all'origine degli attacchi ransomware 2023–2026: Istruzione superiore

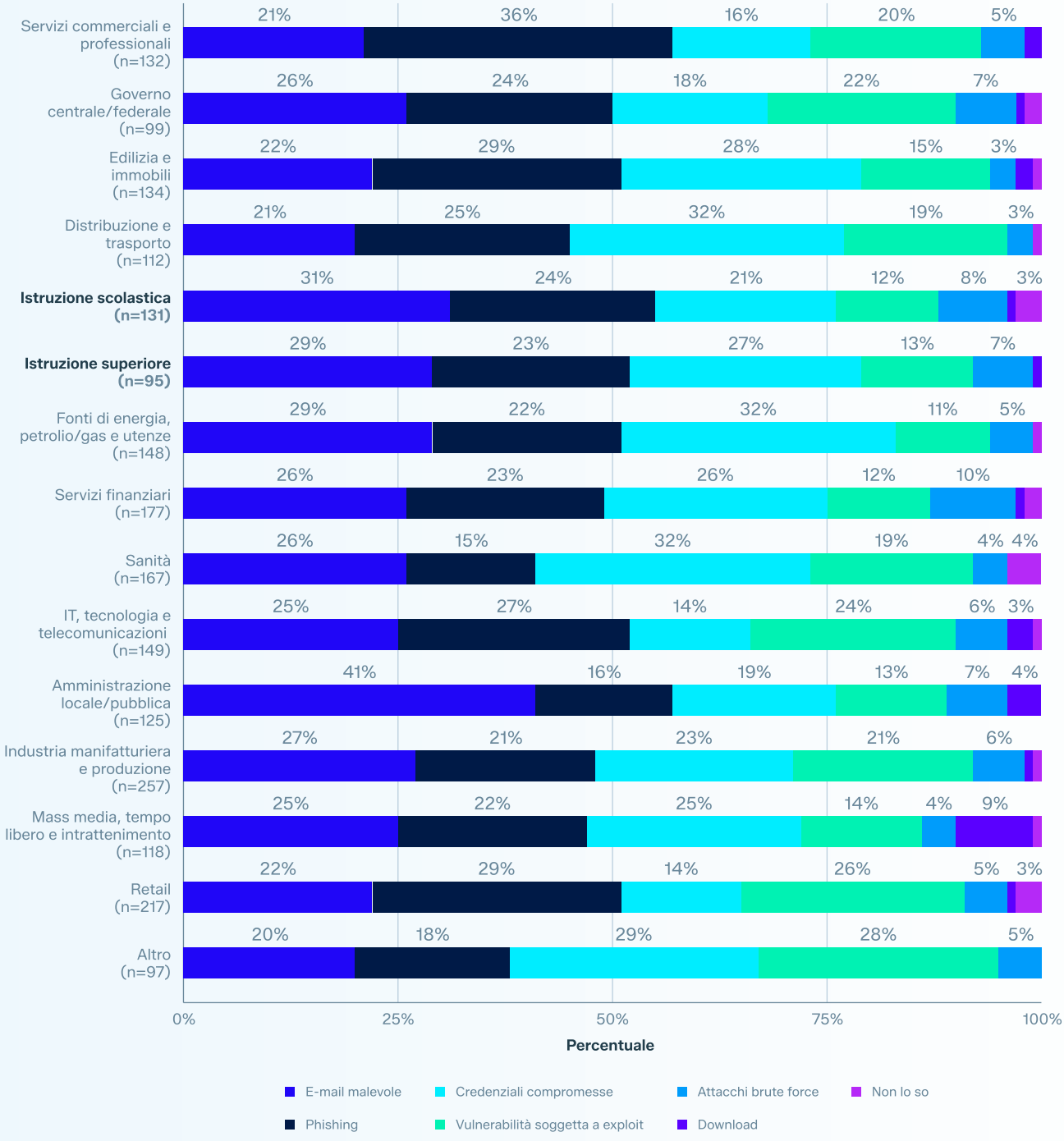


Conosci la causa all'origine dell'attacco ransomware subito l'anno scorso dalla tua organizzazione?
I download e le risposte "Non so" sono stati esclusi dal grafico per chiarezza visiva. La somma delle percentuali potrebbe non essere uguale al 100%.
Base di partecipanti indicata nel grafico.

Nel loro insieme, i vettori basati sull'identità **(ad es. e-mail dannose, phishing, credenziali compromesse e attacchi brute force) hanno rappresentato l'85% degli attacchi agli istituti di istruzione, superando il tasso del 79% dell'indagine generale**. L'istruzione superiore ha registrato la percentuale più alta con l'86%, seguita dall'istruzione inferiore con l'84%. In altre parole, circa sei su sette attacchi contro l'istruzione sono iniziati con un approccio basato sull'identità, rafforzando il motivo per cui la sicurezza dell'identità è centrale nelle difese del settore.

L'istruzione rispecchia la più ampia tendenza intersettoriale verso un aumento degli attacchi veicolati via e-mail e una diminuzione dei casi di vulnerabilità soggette a exploit. Tuttavia, gli esperti Sophos prevedono che gli exploit aumenteranno di nuovo poiché le organizzazioni faticano a stare al passo con le patch per le vulnerabilità scoperte dall'IA di frontiera.

Causa tecnica all'origine per settore (2026)



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

Cosa ha reso vulnerabili le organizzazioni

Gli istituti di istruzione hanno indicato una vasta gamma di sfide relative a protezione, risorse e lacune di sicurezza. Nelle tre categorie consolidate, i problemi di risorse (mancanza di personale o competenze) sono stati citati dal 63% dei fornitori di istruzione, seguiti dai problemi di protezione (62%) e dalle lacune di sicurezza (62%).

Perché ritieni che la tua organizzazione sia caduta vittima dell'attacco ransomware? n=226. Risposte consolidate.

L'insieme dell'istruzione ha riportato un tasso più alto rispetto all'indagine generale su quasi tutte le cause radice operative, con le lacune di sicurezza note come unica eccezione. Dividendo i settori dell'istruzione inferiore e superiore emergono due debolezze diverse.

La debolezza principale dell'istruzione superiore è stata la mancanza di competenze. Il 53% ha dichiarato di non possedere le competenze o le conoscenze per rilevare e fermare l'attacco in tempo, rispetto al 35% per l'indagine generale, un divario di 18 punti percentuali e il più grande in assoluto.

Le debolezze nell'istruzione inferiore si sono concentrate su risorse operative e strumentazione. L'errore umano è stato indicato dal 52% degli istituti di istruzione inferiore (rispetto al 35% di tutti i settori), la mancanza di protezione dal 47% e la mancanza di personale o capacità dal 41% degli istituti.

53%

La quota di vittime dell'istruzione superiore che hanno dichiarato di non avere le competenze o le conoscenze per rilevare e fermare l'attacco in tempo, 18 punti sopra l'indagine generale e la loro singola maggiore debolezza.

Cause operative all'origine degli attacchi: istruzione inferiore e superiore vs tutti i settori

Causa operativa all'origine degli attacchi	Istruzione scolastica (n=131)	Istruzione superiore (n=95)	Tutti i settori (n=2.158)
Mancanza di protezione	47%	36%	36%
Lacuna di sicurezza sconosciuta	42%	38%	36%
Lacuna di sicurezza nota	33%	35%	36%
Mancanza di personale/ capacità	41%	37%	35%
Errore umano	52%	36%	35%
Mancanza di competenze	33%	53%	35%
Protezione di scarsa qualità	38%	39%	33%

Perché ritieni che la tua organizzazione sia caduta vittima dell'attacco ransomware? Risposte multiple consentite. Base di partecipanti indicata nel grafico.

Rispetto agli altri settori, quello dell'istruzione ha incontrato maggiori difficoltà a causa della mancanza di protezione e di competenze. La tabella seguente mostra i settori collocati nella colonna della causa radice operativa che hanno citato più spesso.

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

MANCANZA DI PROTEZIONE	LACUNA DI SICUREZZA SCONOSCIUTA	LACUNA DI SICUREZZA NOTA	MANCANZA DI PERSONALE/ CAPACITÀ	MANCANZA DI COMPETENZE	PROTEZIONE DI SCARSA QUALITÀ	ERRORE UMANO
Non avevamo i prodotti e i servizi di cybersecurity necessari	C'era un punto debole nelle nostre difese di cui non eravamo a conoscenza	C'erano uno o più punti deboli nelle nostre difese di cui eravamo a conoscenza, ma che non avevamo risolto	Non avevamo un numero sufficiente di esperti di cybersecurity che monitoravano i nostri sistemi al momento dell'attacco.	Non avevamo a disposizione le capacità o le conoscenze necessarie per rilevare e bloccare l'attacco in tempo	I nostri prodotti e servizi di cybersecurity non sono stati in grado di bloccare l'attacco	I nostri team hanno commesso un errore/non hanno seguito correttamente le procedure
Servizi commerciali e professionali (44%) Altro (42%) Fonti di energia, petrolio/gas e utenze* (37%)	IT, tecnologie e telecomunicazioni (42%) Edilizia e immobili (41%)	Servizi finanziari (44%) Retail (38%) Fonti di energia, petrolio/gas e utenze* (37%)	Mass media, tempo libero e intrattenimento (43%) Amministrazione locale/pubblica (42%)	**Istruzione superiore (53%)** Sanità (47%) Governo centrale/ federale (43%)	Distribuzione e trasporto (38%)	**Istruzione inferiore (52%)** Industria manifatturiera e produzione (39%)

Perché ritieni che la tua organizzazione sia caduta vittima dell'attacco ransomware? Risposte multiple consentite.
I settori collegati a più cause sono contrassegnati con un asterisco (*). n=2158.

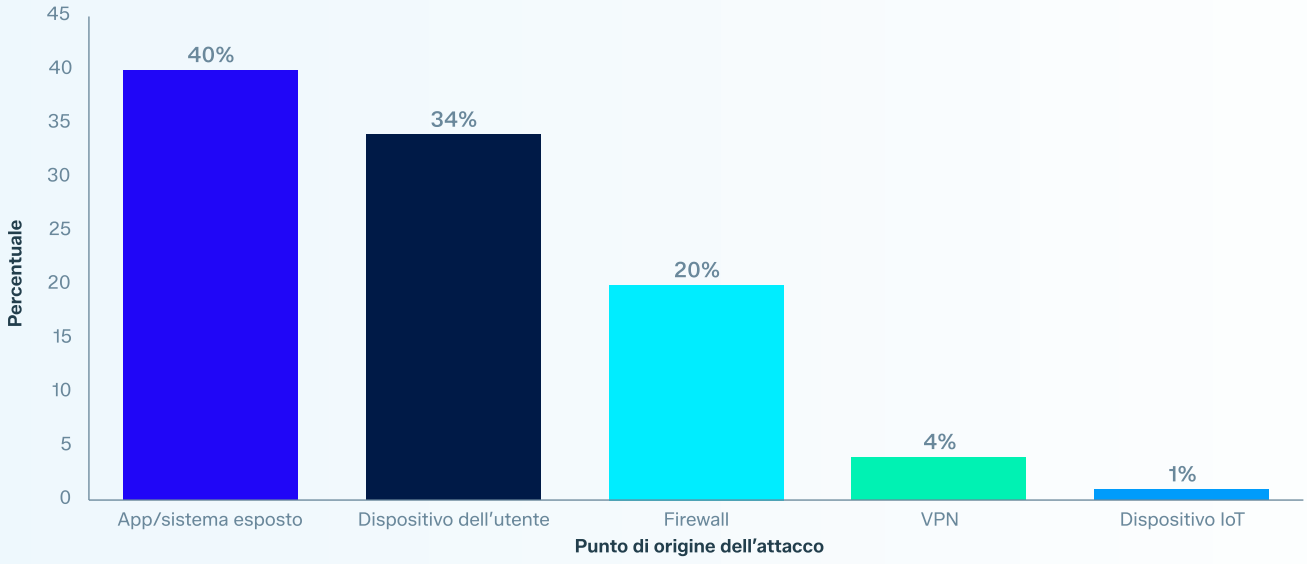
NUOVA RICERCA

Dove iniziano gli attacchi

Nuove ricerche quest'anno aggiungono una domanda su dove nell'ambiente sono iniziati gli attacchi, specificamente tra gli incidenti iniziati con una vulnerabilità sfruttata, credenziali compromesse o un attacco brute force.

Per l'istruzione superiore, le applicazioni e i sistemi esposti sono stati il punto di ingresso più comune (40%), seguiti dai dispositivi utente (34%) e dai firewall (20%). Queste statistiche ricalcano da vicino l'indagine generale (rispettivamente 38%, 30% e 21%), evidenziando come il settore dell'istruzione non presenti scostamenti significativi su questo punto.

Dove iniziano gli attacchi di ransomware: settore dell'istruzione superiore e inferiore combinato



Hai indicato che la causa originaria era una vulnerabilità soggetta a exploit, credenziali compromesse o un attacco brute force. In quale punto del tuo ambiente aziendale si è verificata? Settore dell'istruzione superiore e inferiore combinato. n=99

NUOVA RICERCA

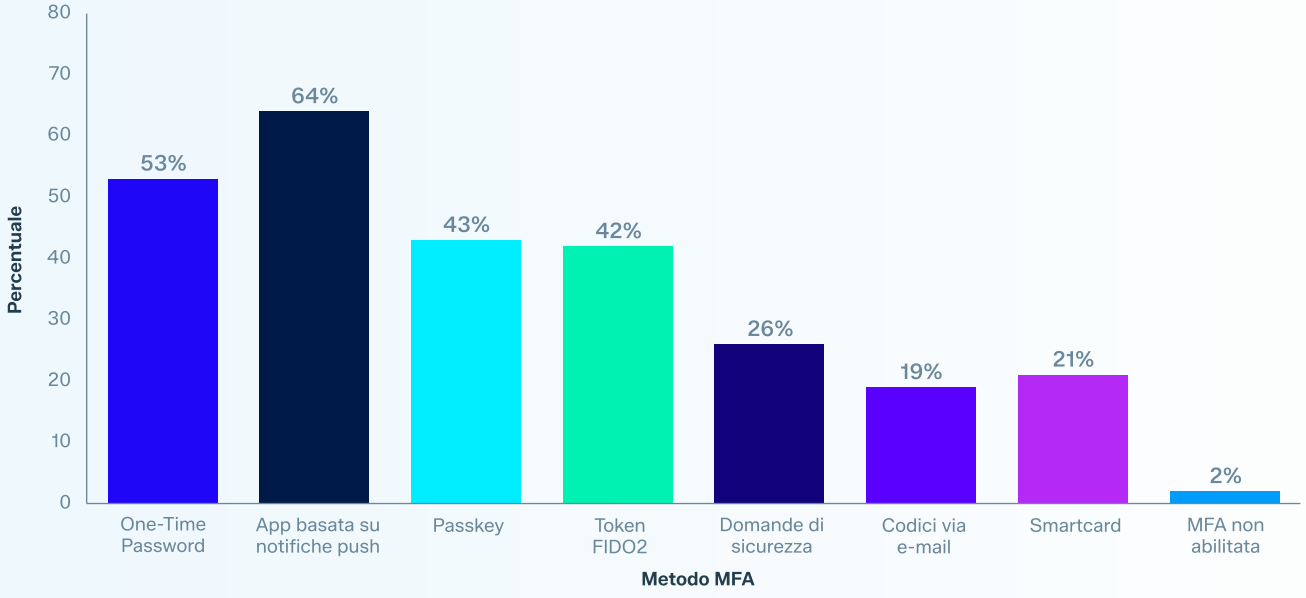
Il ruolo dell'autenticazione multifattoriale (MFA)

Abbiamo anche analizzato i metodi di MFA in uso al momento dell'attacco tra gli istituti di istruzione il cui attacco aveva avuto inizio con credenziali compromesse. Quasi tutte le vittime nel settore dell'istruzione avevano qualche forma di MFA abilitata (98%), riecheggiando il dato generale del sondaggio (97%) secondo cui l'MFA era presente nella maggior parte degli attacchi basati su credenziali.

Tuttavia, tra gli istituti di istruzione interpellati sulla MFA, l'81% aveva comunque subito la crittografia non autorizzata dei dati, nonostante la MFA fosse abilitata. Questo suggerisce che o l'autenticazione multifattoriale (MFA) non è stata implementata in modo completo su tutti i sistemi critici, gli attaccanti hanno trovato modi per aggirare le protezioni MFA, o i vettori di attacco non si basavano esclusivamente sul compromesso delle credenziali.

Le applicazioni con notifiche push (64%) e le One-Time Password (53%) sono stati i metodi più comunemente adottati nel settore dell'istruzione.

Metodi MFA abilitati al momento dell'attacco: settore dell'istruzione superiore e inferiore combinato



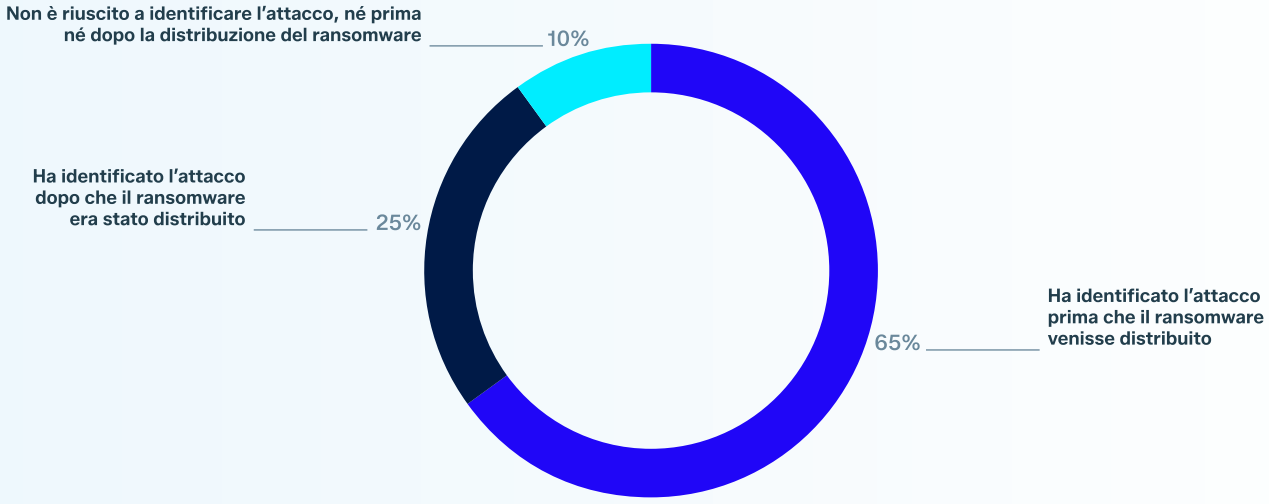
Quale tipo di autenticazione multifattoriale era attiva al momento dell'attacco, se presente? Risposte multiple consentite.
Base: L'attacco si è verificato a causa di credenziali compromesse. Settore dell'istruzione superiore e inferiore combinato. n=53.

NUOVA RICERCA

Il ruolo dei firewall

Nel settore dell'istruzione, i firewall hanno identificato la maggior parte degli attacchi, ma non sono sempre riusciti a fermarli. Il 65% dei fornitori ha dichiarato che il loro firewall ha identificato l'attacco prima che il ransomware venisse distribuito, il 25% ha dichiarato che l'ha identificato dopo, e il 10% ha dichiarato che non l'ha identificato affatto. Questo riflette l'indagine generale (61%, 32% e 7%), con un leggero spostamento verso i due estremi dello spettro.

Quale ruolo ha svolto il tuo firewall nell'identificazione dell'attacco?



Quale ruolo ha svolto il tuo firewall nell'identificazione dell'attacco? Settore dell'istruzione superiore e inferiore combinato. n=226.

Tra i casi di rilevamento tempestivo, le vittime nel settore dell'istruzione avevano comunque subito la crittografia dei dati nel 51% dei casi.

I firewall stanno facendo un buon lavoro nel raccogliere dati per identificare gli attacchi, ma gli attacchi non vengono ancora bloccati alla stessa velocità con cui vengono identificati. I firewall spesso registrano i dati necessari per rilevare e bloccare un attacco, ma potrebbero non essere collegati abbastanza profondamente ad altri sistemi per riconoscere la minaccia e rispondere in tempo.

NUOVA RICERCA

Il legame tra identità e ransomware

Una delle conclusioni più chiare del sondaggio è il legame diretto tra attacchi all'identità e ransomware. In tutti i settori, due terzi delle vittime di ransomware (67%) hanno confermato che l'incidente è stato lo stesso evento del loro attacco di identità più significativo. Tuttavia, il settore dell'istruzione si posiziona al di sopra di quel valore: il 71% nell'istruzione inferiore e il 77% nell'istruzione superiore (73% per il settore dell'istruzione superiore e inferiore combinato).

Sebbene non tutti gli attacchi abbiano portato alla crittografia dei dati, la scoperta mostra una forte sovrapposizione tra attacchi all'identità e ransomware nel settore dell'istruzione.

L'attacco ransomware ne ha rappresentato anche l'attacco più significativo legato all'identità

La vostra organizzazione ha subito un attacco ransomware che è stato anche un attacco di identità? Organizzazioni colpite dal ransomware. Basi riportate nei grafici.

73%

La quota di vittime del settore dell'istruzione il cui incidente ransomware è stato lo stesso evento del loro attacco di identità più significativo, superiore al tasso generale del 67% del sondaggio.

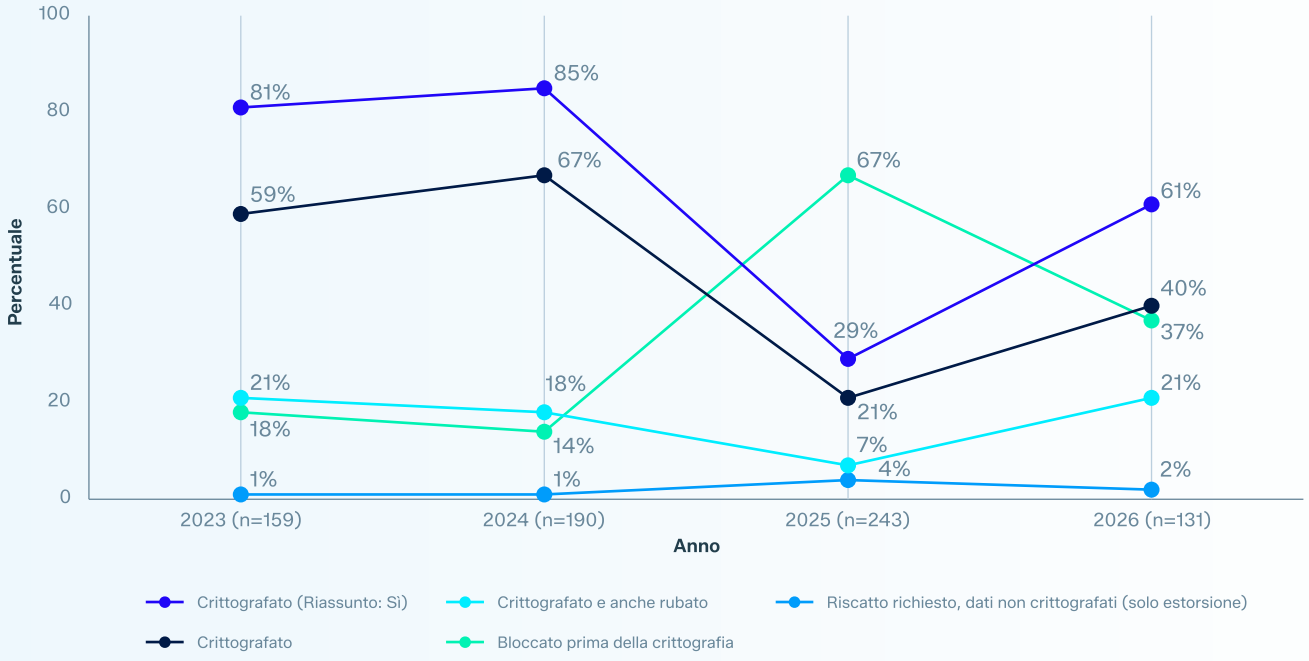
Crittografia e recupero dei dati

Tasso di crittografia dei dati

I risultati del Rapporto sullo Stato del Ransomware nel 2025 nell'istruzione hanno mostrato esiti molto positivi per l'istruzione inferiore. Sfortunatamente, il report di quest'anno mostra un'inversione di tendenza per l'istruzione inferiore, che si riavvicina ai livelli precedenti.

Dopo che il tasso di crittografia non autorizzata dei dati nell'istruzione inferiore è sceso al 29% nel report del 2025 (il più basso di qualsiasi settore quell'anno), **la quota di attacchi rivolto all'istruzione inferiore che sono riusciti a crittografare i dati è più che raddoppiata, raggiungendo il 61% nel 2026** (superando il 56% dell'indagine generale). Quest'anno solo il 37% degli attacchi nell'istruzione inferiore è stato bloccato prima della crittografia, rispetto al 67% nel report dell'anno scorso.

Tasso di crittografia dei dati nel tempo: Istruzione scolastica

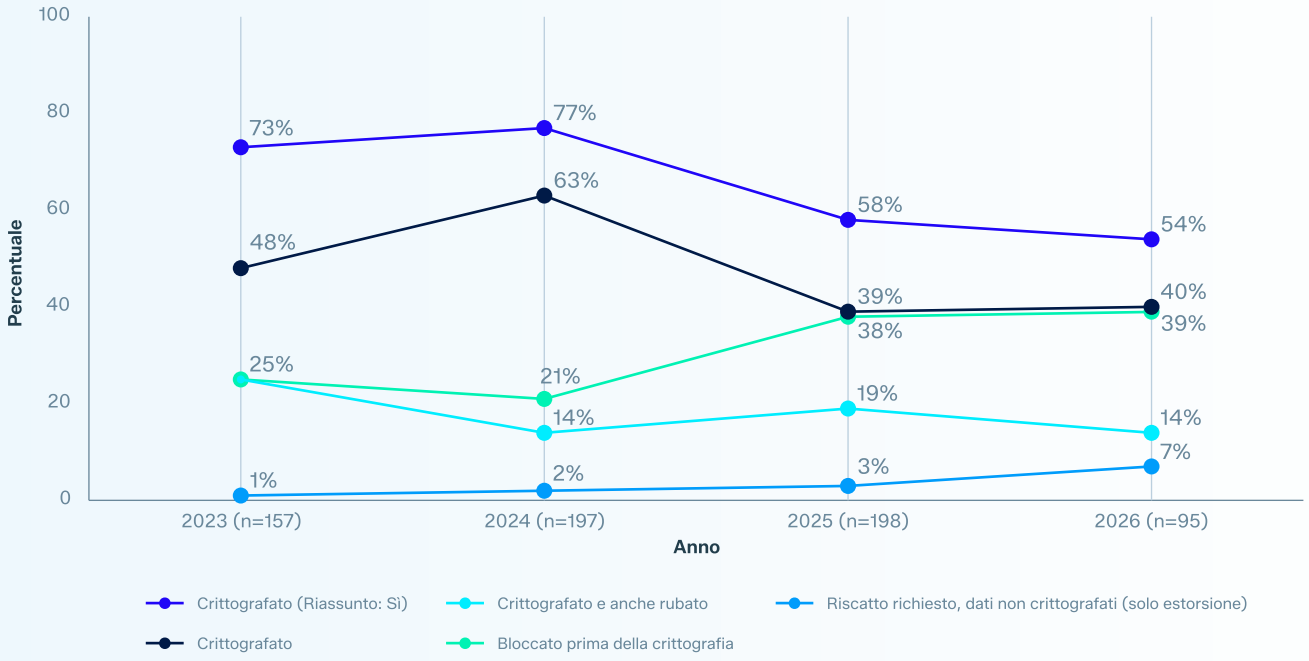


Durante l'attacco ransomware, i cybercriminali sono riusciti a crittografare i dati della tua organizzazione? Base di partecipanti indicata nel grafico. La linea "Crittografati (riepilogo: sì)" in questo grafico rappresenta la somma delle risposte "Crittografati" e "Sia crittografati che esfiltrati".

La doppia estorsione (in cui i dati vengono sia crittografati che esfiltrati) è tornata ad aumentare nell'istruzione inferiore, passando dal 7% del 2025 al 21% del 2026, riallineandosi ai livelli antecedenti al 2025. Questi attacchi offrono ai cybercriminali una seconda leva di ricatto. Gli attacchi di sola estorsione **(soggetti a riscatto senza crittografia)** sono diminuiti leggermente dal 4% al 2% per l'istruzione inferiore.

L’istruzione superiore ha mostrato una maggiore stabilità. Il suo tasso di crittografia è sceso leggermente al 54% nel 2026, rispetto al 58% del 2025, mantenendosi in linea con i dati dell’indagine generale.

Tasso di crittografia dei dati nel tempo: Istruzione superiore



Durante l’attacco ransomware, i cybercriminali sono riusciti a crittografare i dati della tua organizzazione? Base di partecipanti indicata nel grafico. La linea “Crittografati (riepilogo: sì)” in questo grafico rappresenta la somma delle risposte “Crittografati” e “Sia crittografati che esfiltrati”.

Per l'istruzione superiore, gli attacchi di estorsione sono aumentati al 7%, rispetto al 3% nel 2025, il che merita attenzione anche in una piccola percentuale.

Il quadro del 2026 riporta inoltre il settore dell’istruzione al suo andamento di lungo periodo. Nel 2023 e nel 2024, il tasso di crittografia dei dati nell'istruzione inferiore era più alto rispetto a quello dell'istruzione superiore; il 2025 è stata l'eccezione, quando il tasso dell'istruzione inferiore è crollato brevemente. Il tasso di crittografia di quest’anno (pari al 61%) per l’istruzione inferiore, rispetto al 54% per l’istruzione superiore, ripristina la tendenza a lungo termine.

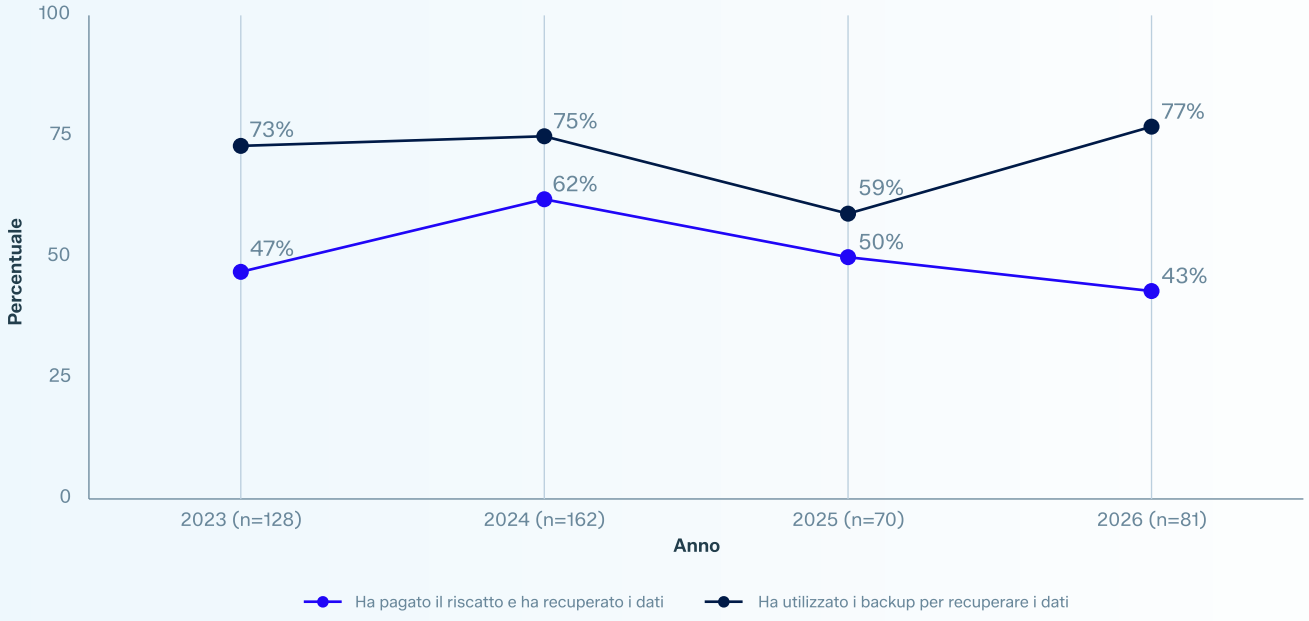
Come le organizzazioni hanno recuperato i dati crittografati

Nel 2026, i backup sono stati la leva di recupero più importante nel settore dell'istruzione. Dopo la flessione registrata nel 2025 (59% nell'istruzione inferiore, 47% nell'istruzione superiore), il recupero basato sui backup è tornato a crescere quest'anno. **Il 77% degli istituti di istruzione inferiore e il 69% degli istituti di istruzione superiore hanno ripristinato i dati dai backup**, entrambi valori al di sopra della percentuale media del 66% dell'indagine generale. Questo incremento suggerisce che il settore dell'istruzione ha rinnovato i suoi investimenti nell'infrastruttura di backup e sta rafforzando la propria resilienza di fronte alle richieste di riscatto.

77%

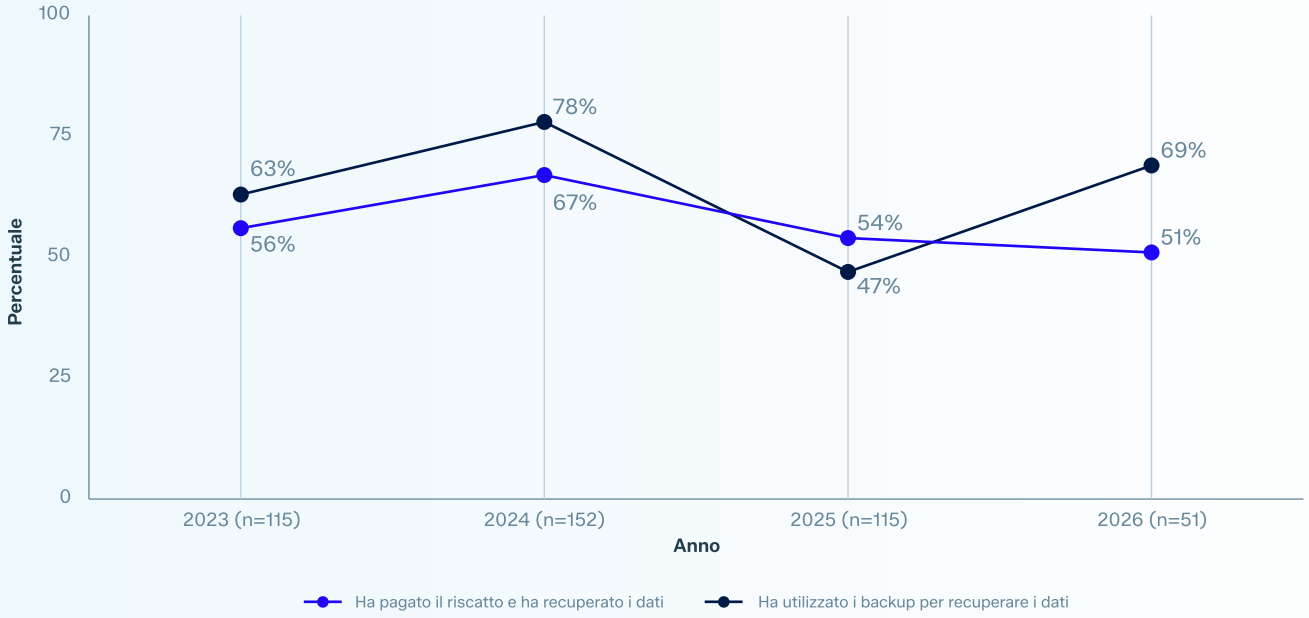
La quota di fornitori di istruzione inferiore che hanno ripristinato dati crittografati dai backup nel 2026, superiore al tasso medio del 66% dell'indagine.

Metodi di recupero dati nel tempo: Istruzione scolastica



In che modo la tua organizzazione ha recuperato i dati? Risposte multiple consentite. Base di partecipanti indicata nel grafico.

Metodi di recupero dati nel tempo: Istruzione superiore



In che modo la tua organizzazione ha recuperato i dati? Risposte multiple consentite. Base di partecipanti indicata nel grafico.

Allo stesso tempo, il settore dell'istruzione paga riscatti con minore frequenza. **La quota di fornitori che hanno pagato il riscatto e hanno recuperato i dati è diminuita per due anni consecutivi**, passando dal 62% (2024) al 50% (2025) al 43% (2026) nell'istruzione inferiore, e dal 67% al 54% al 51% rispettivamente nell'istruzione superiore.

Con l'aumento del ripristino da backup e la diminuzione del recupero basato sul pagamento, il settore dell'istruzione si sta riprendendo grazie alle proprie capacità più che grazie alla cooperazione degli attaccanti.

Richieste e pagamenti del riscatto

Richieste di riscatto

Il settore dell'istruzione ha dovuto affrontare richieste di riscatto più elevate rispetto agli altri settori nell'indagine generale. La richiesta di riscatto mediana avanzata a un istituto di istruzione è stata pari a 775.200 $, superiore alla cifra mediana di 698.000 $ per tutti i settori. Anche la distribuzione si attesta su valori alti: **metà delle richieste di riscatto (50%) è stata pari o superiore a 1 milione di $, e un quarto (25%) è stata pari o superiore a 5 milioni di $**, contro rispettivamente il 46% e il 23% del campione di tutti i settori.

Nota: i valori anomali dei riscatti pari o superiori a 40 milioni di $ sono stati rimossi da questi dati.

Richiesta di riscatto mediana

	2025	2026
Istruzione	0,98 Mio di $ (n=185)	0,78 Mio di $ (n=132)
Tutti i settori	1,32 Mio di $ (n=1700)	0,70 Mio di $ (n=1214)

A quanto ammonta la somma di riscatto richiesta dal o dai cybercriminali? Base: aziende i cui dati sono stati crittografati. Base di partecipanti indicata nel grafico.

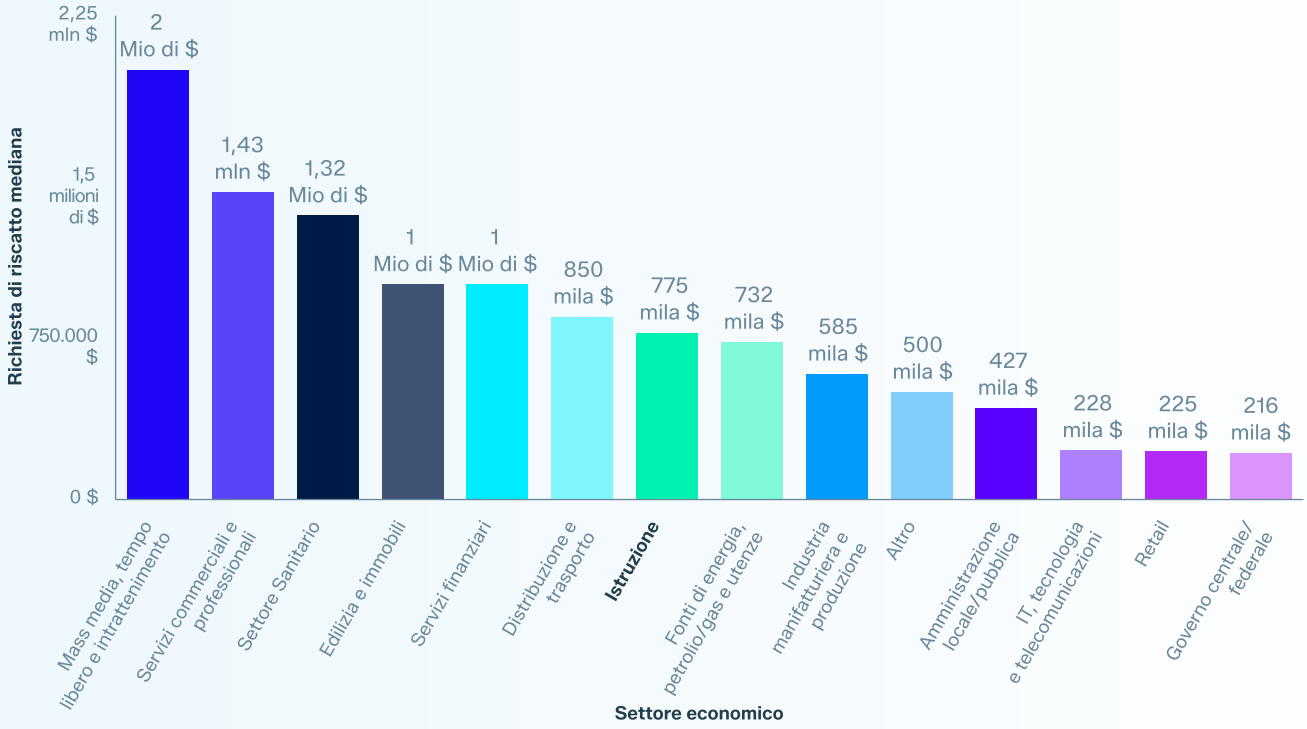
Rispetto ad altri settori, l'istruzione si colloca in una posizione intermedia. Le sue richieste di riscatto mediane si mantengono al di sotto dei settori con le richieste più elevate, come Mass media, tempo libero e intrattenimento (2 milioni di $) e Servizi commerciali e professionali (1,43 milioni di $); tuttavia, risultano nettamente superiori a quelle dei settori con le richieste più basse, come Settore pubblico (216.500 $) e Retail (225.000 $).

775.200 $

La richiesta di riscatto mediana nei confronti degli istituti di istruzione, superiore alla cifra mediana di 698.000 $ dell'indagine generale.

Metà delle richieste di riscatto nel settore dell'istruzione sono state pari a 1 milione di $ o più.

Richieste di riscatto mediane, in base al settore



A quanto ammonta la somma di riscatto richiesta dal o dai cybercriminali? Base: aziende i cui dati sono stati crittografati. n=1141

Le tendenze su base annua evidenziano aspetti sia positivi che negativi. La richiesta di riscatto mediana nel settore dell'istruzione superiore e inferiore combinato è scesa da 976.000 $ nel 2025 a 775.200 $ nel 2026. Questo calo è stato guidato principalmente dall'istruzione inferiore, dove la richiesta di riscatto mediana è scesa da 1,03 milioni di $ a 737.600 $, mentre l'istruzione superiore ha mostrato un andamento opposto, con una richiesta mediana che è aumentata, passando da 697.086 $ a 889.200 $.

Pagamento del riscatto

Le richieste più elevate nel settore dell'istruzione non si sono tradotte in pagamenti più alti. **Sebbene siano state registrate richieste più elevate, il riscatto mediano pagato dal settore dell'istruzione è stato inferiore rispetto ad altri settori nell'indagine generale**. Il pagamento del riscatto mediano effettuato da un istituto di istruzione è stato di 515.000 $, al di sotto della mediana di 769.000 $ dell'indagine generale.

I pagamenti nel settore dell'istruzione si sono concentrati lontano dalla fascia più alta, ma hanno incluso una quota maggiore di pagamenti da oltre 5 milioni di $. Il 39% dei pagamenti nell'istruzione è stato pari o superiore a 1 milione di $, al di sotto del 44% dell'indagine generale. Tuttavia, il 23% consisteva in pagamenti di 5 milioni di $ o più, una statistica superiore al 16% dell'indagine generale. Quando il settore dell'istruzione effettua un pagamento, di solito versa meno rispetto ad altri settori, ma una minoranza significativa paga somme molto elevate.

Pagamento del riscatto mediano

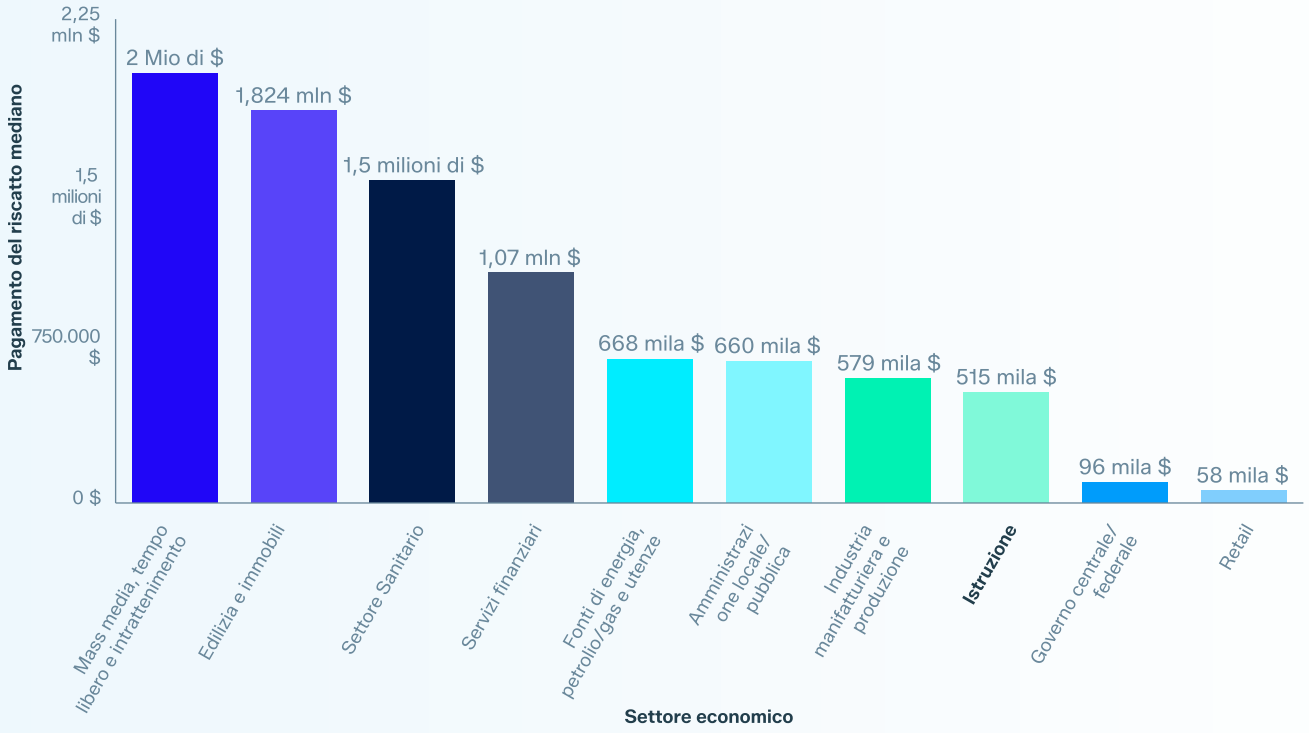
	2025	2026
Istruzione	0,50 Mio di $ (n=100)	0,52 Mio di $ (n=62)
Tutti i settori	1 Mio di $ (n=847)	0,77 Mio di $ (n=587)

A quanto ammonta approssimativamente la somma di riscatto pagata ai cybercriminali?
Base: aziende che hanno pagato il riscatto. Base di partecipanti indicata nel grafico.

515.000 $

Il riscatto mediano pagato dagli istituti di istruzione, inferiore rispetto alla cifra mediana di 769.000 $ rilevata nell'indagine generale, anche se le richieste di riscatto sono più elevate.

Pagamenti del riscatto mediani, in base al settore



A quanto ammonta approssimativamente la somma di riscatto pagata ai cybercriminali? Base: aziende che hanno pagato il riscatto. n=587. Esclude i settori con meno di 30 rispondenti a questa domanda.

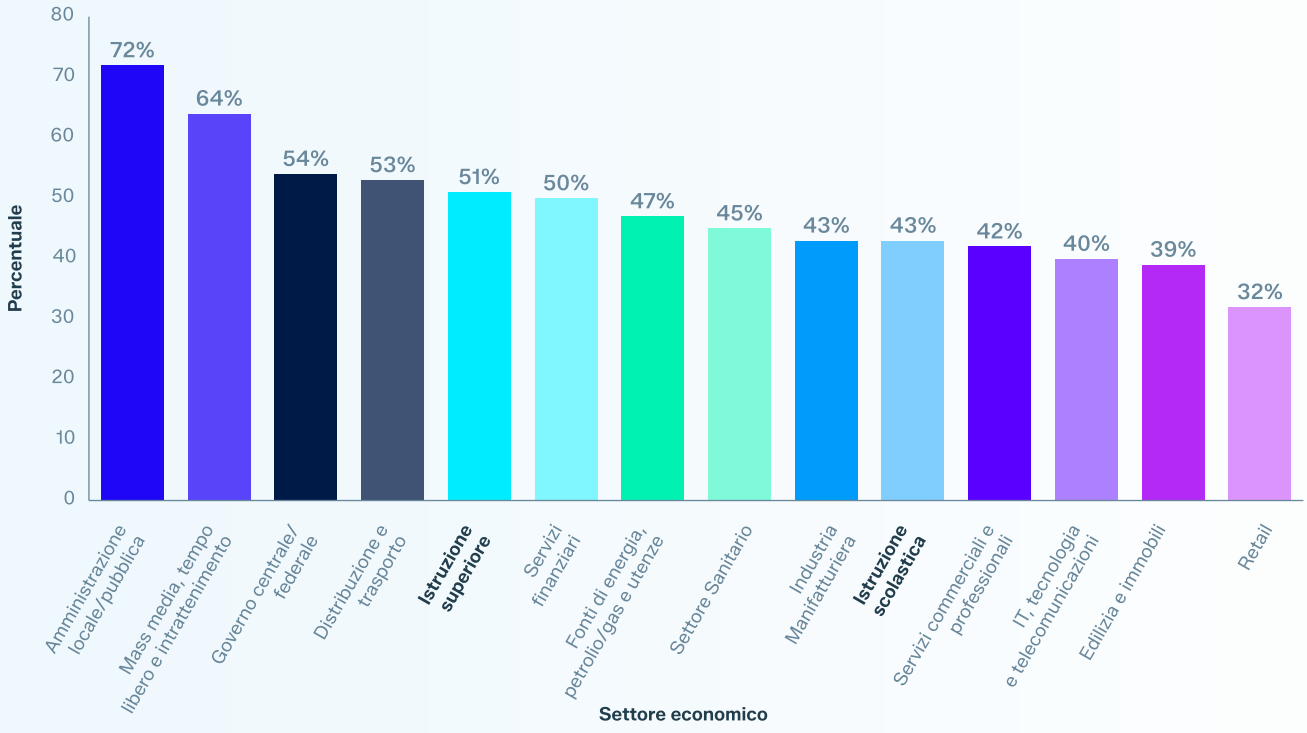
Anche le tendenze anno su anno sono risultate contrastanti per i pagamenti del riscatto. Il pagamento mediano nel settore dell'istruzione superiore e inferiore combinato è rimasto sostanzialmente stabile, registrando un lieve incremento da 500.000 $ nel 2025 a 515.000 $ nel 2026. Il pagamento mediano nell'istruzione inferiore è crollato drasticamente nello stesso periodo, passando da 800.000 $ a 320.000 $. Il leggero aumento a livello combinato è stato quindi guidato dall'istruzione superiore.

Poiché quest'anno meno di 30 istituti di istruzione superiore hanno indicato la cifra del pagamento (n=27), non possiamo mostrare una linea di tendenza autonoma affidabile per i pagamenti nell'istruzione superiore, per cui consigliamo di fare riferimento alle tendenze dei pagamenti per il settore dell'istruzione superiore e inferiore combinato.

Percentuale di aziende che hanno pagato il riscatto, per settore

La propensione a pagare il riscatto è risultata differente tra i due segmenti dell'istruzione. Il riscatto è stato pagato dal 51% delle vittime nel settore dell'istruzione superiore, una statistica che oltrepassa il 48% dell'indagine generale, mentre nell'istruzione inferiore questo tasso è pari al il 43%, mostrando una maggiore resistenza al pagamento più frequentemente rispetto all'indagine generale.

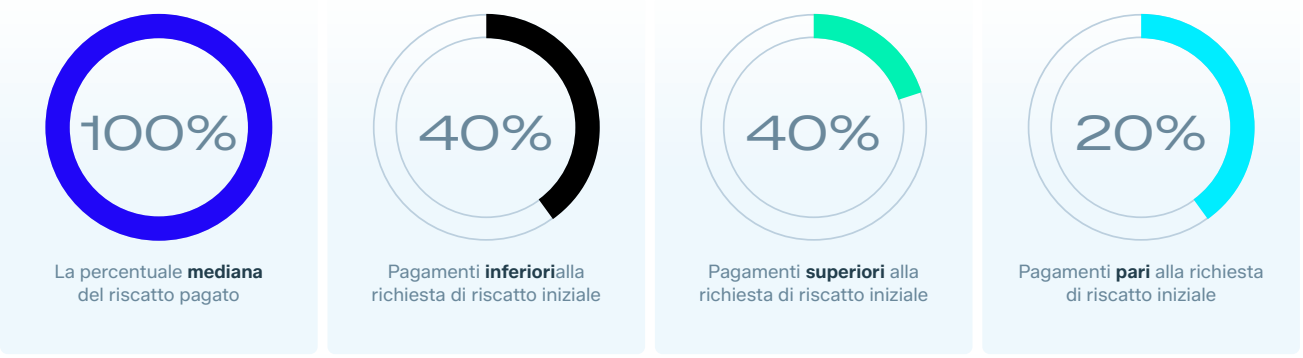
Percentuale che ha pagato il riscatto per settore



In che modo la tua organizzazione ha recuperato i dati? Base: aziende i cui dati sono stati crittografati. n=1.214

Pagamenti effettivi rispetto alle richieste iniziali

Tra le istituzioni del settore dell'istruzione che hanno pagato il riscatto, il 40% ha pagato meno della richiesta iniziale, il 40% ha pagato di più e il 20% ha pagato esattamente quanto richiesto. L'istituzione mediana ha pagato il 100% della somma richiesta, in aumento rispettoall'82% del 2025. Quindi, sebbene una quota consistente di istituzioni sia riuscita a negoziare il pagamento al ribasso, una percentuale equivalente ha finito per pagare più di quanto inizialmente richiesto.



Considerando il pagamento del riscatto effettuato, è stato inferiore, pari o superiore alla richiesta iniziale di riscatto? Escludendo le eccezioni. Settore dell'istruzione superiore e inferiore combinato. n=58.

Impatto sulle aziende e sugli esseri umani

Costi di riparazione dei danni del ransomware

Il settore dell'istruzione ha affrontato costi di riparazione dei danni superiori alla media. **Il costo medio (media aritmetica) di riparazione dei danni causati dal ransomware, escludendo le cifre pagate per il riscatto, è stato di 2,46 milioni di $ nell'istruzione inferiore e di 1,99 milioni di $ in quella superiore**, entrambi al di sopra della media di 1,7 milioni di $ dell'indagine generale.

L'istruzione inferiore ha sostenuto l'onere maggiore per due anni consecutivi. Il suo costo medio di riparazione dei danni è salito da 2,28 milioni di $ nel 2025 a 2,46 milioni di $ nel 2026, confermandosi come il settore più costoso, e ben al di sopra della media dell'indagine generale (1,7 milioni di $).

Costo medio (media aritmetica) di riparazione dei danni

	2025	2026
Istruzione scolastica	2,28 Mio di $ (n=243)	2,46 Mio di $ (n=131)
Istruzione superiore	0,90 Mio di $ (n=198)	1,99 Mio di $ (n=95)
Tutti i settori	1,53 Mio di $ (n=3400)	1,70 Mio di $ (n=2158)

Qual è stato approssimativamente il costo sostenuto dalla tua organizzazione per riparare i danni provocati dall'attacco ransomware più grave? Media (aritmetica), escludendo un eventuale riscatto pagato. Base di partecipanti indicata nel grafico.

L'istruzione superiore è il segmento in cui il divario si è ampliato più nettamente. Il costo medio di riparazione dei danni è più che raddoppiato, passando da 0,90 milioni di $ nel 2025 a 1,99 milioni di $ nel 2026. Nel report del 2025, l'istruzione superiore aveva registrato uno dei costi di riparazione dei danni più bassi di qualsiasi settore. Quest'anno è salita verso l'alto, avvicinandosi all'istruzione inferiore. Entrambi i segmenti dell'istruzione si collocano ora al di sopra della media dell'indagine generale, che a sua volta è cresciuta modestamente da 1,53 milioni di $ a 1,7 milioni di $.

1,09 Mio di $

L'aumento dei costi medi di recupero dai ransomware per l'istruzione superiore dal 2025 al 2026.

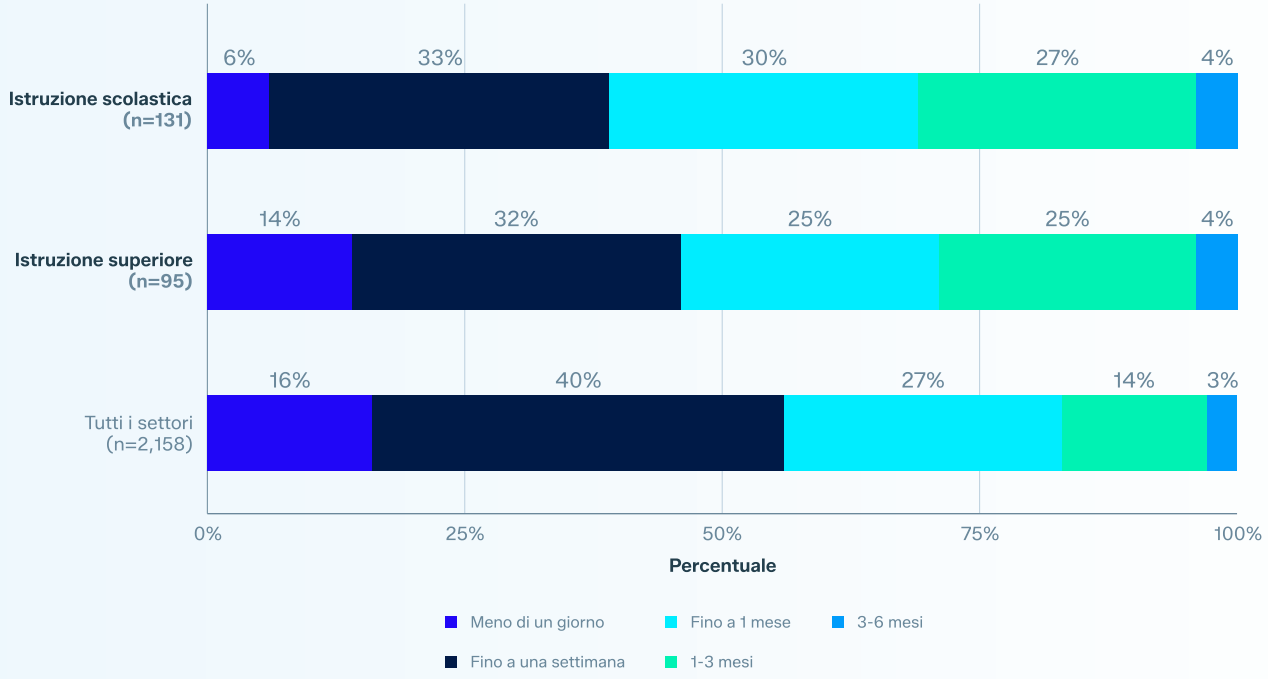
Tempi necessari per riprendere le normali attività

Gli istituti di istruzione non solo hanno pagato di più per riprendere le normali attività, ma hanno anche impiegato più tempo per farlo. La divisione più netta è nella fascia da uno a tre mesi: il 27% delle istituzioni di istruzione inferiore e il 25% di quelle di istruzione superiore hanno avuto bisogno di un tale periodo di tempo per una ripresa completa, a differenza di appena il 14% registrato nell'indagine generale. **Il settore dell'istruzione ha registrato una probabilità quasi doppia di affrontare tempi di recovery della durata di un mese o più.**.

31%

La quota degli istituti di istruzione inferiore che hanno avuto bisogno di almeno un mese per riprendere le normali attività, più di qualsiasi altro settore.

Quanto tempo è stato necessario per riprendere le normali attività operative dopo un attacco ransomware



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.

L'estremità più rapida della scala conferma la stessa dinamica al contrario. Solo il 6% delle istituzioni nell'istruzione inferiore hanno ripreso le normali attività in meno di un giorno, rispetto al 16% dell'indagine generale e al 14% dell'istruzione superiore.

Nessun settore ha registrato una quota di tempi di recovery prolungati più alta dell'istruzione inferiore, dove il 31% degli istituti ha avuto bisogno di almeno un mese per tornare alla piena operatività.

L’impatto umano del ransomware

L’impatto umano sulle persone nell’ambito dell’istruzione è stato maggiore rispetto all’indagine generale, e ogni settore dell’istruzione lo ha avvertito in modo diverso. Per l’istruzione superiore, la pressione determinante è giunta dall’alto: il 53% dei team ha segnalato un aumento delle pressioni da parte del Senior Management, 13 punti percentuali al di sopra del 40% dell’indagine generale. Anche i cambiamenti nel team o nella struttura organizzativa erano più comuni nell'istruzione superiore (43% contro il 32% in tutti i settori).

L’esperienza dell’istruzione inferiore si è concentrata sul riconoscimento e sul carico di lavoro. Quasi metà dei team nell’istruzione inferiore (49%) ha indicato di godere ora di una maggiore stima da parte del Senior Management, al di sopra del tasso del 36% dell’indagine generale. La maggiore stima può anche essere un fattore positivo, ma l’aumento del carico di lavoro non lo è. Il 43% degli intervistati nell’istruzione inferiore ha citato un aumento costante del carico di lavoro, rispetto al 31% riscontrato in tutti i settori. L’attenzione si è rivelata un’arma a doppio taglio: maggiore visibilità, ma anche un carico più pesante e prolungato.

53%

La percentuale di team IT e di sicurezza dell'istruzione superiore che ha affrontato una maggiore pressione da parte dei dirigenti senior dopo un attacco, rispetto al 40% su tutto il sondaggio.

L’impatto umano del ransomware

Ripercussione	Istruzione scolastica (n=81)	Istruzione superiore (n=51)	Tutti i settori (n=1.214)
Maggiore ansia o stress per paura di attacchi futuri	40%	33%	41%
Maggiori pressioni dal Senior Management	48%	53%	40%
Maggiore stima da parte del Senior Management	49%	29%	36%
Cambiamenti della struttura del team/organizzativa	33%	43%	32%
Cambiamenti di priorità/ focalizzazione del team	33%	35%	32%
Sensi di colpa dovuti al fatto che l’attacco non è stato fermato	31%	25%	31%
Aumento costante del carico di lavoro	43%	31%	31%
Assenze del personale dovute a problemi di stress/salute mentale	40%	39%	29%
Cambio di leadership nel team	27%	29%	21%

Quali ripercussioni ha avuto l’attacco ransomware sui membri del tuo team IT/di cybersecurity? Base: organizzazioni che avevano subito la crittografia non autorizzata dei dati. Base di partecipanti indicata nel grafico.

Il benessere del personale ha risentito in entrambi i segmenti. Il 39% dei team di istruzione superiore e il 40% dei team di istruzione inferiore hanno segnalato assenze del personale dovute a stress o problemi di salute mentale, ben al di sopra del tasso generale del 29% del sondaggio.

Anche la rotazione ai vertici delle organizzazioni è risultata elevata, con il 29% dei team nell’istruzione superiore e il 27% di quelli nell’istruzione inferiore che hanno visto la propria leadership sostituita dopo l’attacco, rispetto alla percentuale complessiva del 21%.

Raccomandazioni

Potenzia la sicurezza dell'identità come difesa contro i ransomware. Il 73% delle vittime di ransomware nel settore dell'istruzione ha confermato che il proprio incidente ransomware corrispondeva all'attacco all'identità più significativo, una percentuale superiore al 67% dell'indagine generale, sottolineando il forte legame tra compromissione dell'identità e ransomware in questo settore. Le organizzazioni dovrebbero dare priorità a Threat Detection and Response (ITDR), imporre l'autenticazione multifattoriale su tutti i punti di accesso ed eseguire regolarmente audit delle credenziali di identità sia umane che non umane.

Abilita la MFA in modo completo, in particolare la MFA resistente al phishing. L'indagine ha mostrato che il 98% dei fornitori di servizi educativi con credenziali compromesse aveva abilitato l'autenticazione multifattoriale in qualche misura al momento dell'attacco, ma i loro tassi di crittografia erano comunque elevati. L'autenticazione multifattoriale da sola non è sufficiente a bloccare gli attacchi e deve essere abilitata in modo completo piuttosto che lasciata attiva solo per le app SaaS che la impongono e disattivata per i login VPN, le console di amministrazione del firewall e le app legacy.

Rafforza la protezione endpoint per i modelli di IA di frontiera. Sebbene i report sulle vulnerabilità sfruttate siano diminuiti in questo report, gli esperti Sophos prevedono che gli exploit aumenteranno poiché le aziende faticano a stare al passo con le patch per le vulnerabilità scoperte dall'IA di frontiera. Avere difese potenti per gli endpoint, che siano in grado di bloccare automaticamente gli attacchi basati sugli exploit, è essenziale.

Avvalersi del supporto di uno specialista o di MDR. La mancanza di capacità, competenze ed esperienza è un tema ricorrente nell'ambito dell'istruzione, ed è particolarmente acuta nell'istruzione superiore, dove la carenza di esperti interni con elevate competenze tecniche si è distinta come una debolezza determinante. Affrontare minacce potenziate dall'IA metterà ancora più sotto pressione queste aree, poiché i team di Security Operations cercheranno di rimanere aggiornati con la tecnologia di IA in rapida evoluzione. A meno che tu non sia in grado di formare internamente un team di Security Operations, cerca uno specialista esterno per colmare il divario, sia un vendor MDR 24/7 che un Managed Service Provider. I vendor che risolvono un maggior numero di incidenti end-to-end con l'IA e l'automazione agiscono come un moltiplicatore di forza, aiutando a colmare le lacune in termini di competenze e capacità.

Investi nell'infrastruttura di backup e ripristino. I backup sono stati il metodo di ripristino dominante sia nell'istruzione inferiore che nell'istruzione superiore (77% e 69%, entrambi al di sopra alla media dell'indagine generale). I backup devono essere testati regolarmente, conservati off-line o in formati immutabili e integrati in un piano di incident response documentato, che possa essere eseguito anche sotto pressione.

Mantieni programmi di gestione dell'esposizione. Le vulnerabilità soggette a exploit rimangono un vettore di attacco importante, ed è probabile che aumentino man mano che i modelli di IA di frontiera individuano nuove debolezze più velocemente. Gli istituti di istruzione devono mantenere ritmi di applicazione delle patch serrati e concentrarsi su misure di mitigazione quali l'implementazione di segmentazione, Zero Trust Network Access e MFA/autenticazione continua.

Riduci l'esposizione tramite il firewall e sfrutta la telemetria del firewall per rilevare tempestivamente gli attacchi. I dati del 2026 hanno mostrato che i firewall sono bravi a individuare i segni del ransomware, con il 65% che disponeva di dati sufficienti per identificare un attacco prima che il ransomware venisse attivato. Ma anche in quei casi di rilevamento precoce, le vittime nell'ambito educativo avevano ancora i loro dati crittografati il 51% delle volte, perché il firewall spesso non riesce a confermare o bloccare un attacco senza telemetria da altri punti di controllo. Assicurati che il tuo firewall riceva aggiornamenti rapidi (idealmente automatizzati) e riduci al minimo i servizi esposti a Internet, come gli accessi amministrativi e i portali utenti. Collega i firewall a XDR e MDR in modo che la telemetria del firewall aiuti a rilevare gli attacchi ransomware prima che i payload vengano distribuiti. Un sistema di cyber difesa in cui i controlli condividono i segnali è la risposta.

Le azioni consigliate in sintesi:

1. Segmentazione per rallentare gli autori degli attacchi
2. ZTNA per sostituire le VPN legacy e contenere gli exploit delle app
3. Identity Threat Detection and Response (ITDR) per rafforzare l'infrastruttura di identità
4. MFA resistente al phishing come traguardo, piuttosto che come punto di partenza
5. Patching disciplinato dei dispositivi esposti a Internet
6. Rilevamento e risposta 24/7

Conclusione

Il report "La vera storia del ransomware per il settore dell'istruzione 2026" rivela un panorama delle minacce in fase di transizione.

Ci sono segni di progresso: le richieste di riscatto stanno diminuendo, il ripristino basato sui backup è salito a livelli quasi record e i pagamenti del riscatto effettuati dagli istituti di istruzione sono bassi rispetto ad altri settori.

Allo stesso tempo, le sfide che restano da affrontare sono significative. Oltre la metà degli attacchi ransomware contro il settore dell'istruzione riesce ancora a crittografare i dati, il costo medio di riparazione dei danni ammonta a 2,26 milioni di $ per incidente (una cifra superiore a quella dell'indagine generale), e l'istruzione inferiore ha registrato la più alta percentuale di attività di riparazione dei danni durate un mese o più.

L'ambito dell'identità è dove si concentra la maggiore esposizione del settore dell'istruzione. Una quota maggiore di fornitori di servizi educativi ha confermato che il loro incidente ransomware è stato lo stesso evento del loro attacco di identità più significativo rispetto all'indagine generale. Per un settore in cui la riparazione dei danni è già più lenta e costosa, questo stretto legame rende l'infrastruttura di identità l'ambito a più alto impatto su cui investire.

Gli istituti di istruzione devono anche prepararsi per la sfida di cybersecurity cruciale del prossimo decennio: le minacce potenziate dall'IA. I dati offrono già un'indicazione del perché: Il 62% delle aziende del settore educativo ha citato una lacuna di sicurezza, nota o sconosciuta, come un fattore nel loro attacco, e il 63% ha indicato una mancanza di personale o competenze. Entrambe le lacune diventano più rilevanti man mano che l'IA accelera la velocità e la portata degli attacchi, con i cybercriminali che la utilizzano per individuare più rapidamente i punti deboli e orchestrare attacchi su molteplici punti di controllo alla velocità della macchina.

Nei dati di quest'anno sulle cause all'origine degli attacchi emerge anche un segnale più profondo. La distribuzione delle cause primarie percepite si sta livellando; in tutti i settori, incluso quello dell'istruzione, non esiste un singolo vettore dominante. Questo rende rischioso concentrare le difese troppo strettamente su una singola causa principale, perché gli attaccanti stanno avendo successo attraverso più vettori.

Il modello attraverso i risultati di quest'anno, specialmente nel basso impatto del rilevamento del firewall e dell'abilitazione dell'MFA sugli esiti, punta in una direzione coerente: quando le difese operano in isolamento, non sei protetto. Colmare il divario rispetto agli attacchi dell'era dell'IA dipenderà meno dall'aggiunta di ulteriori strumenti e più dalla capacità di connettere quelli già esistenti, affinché il contesto, il rilevamento e la risposta possano muoversi alla velocità richiesta dalle minacce attualmente in circolazione.

Gli istituti di istruzione che avranno maggiori probabilità di resistere agli attacchi ransomware nei prossimi anni saranno quelle che manterranno alta l'attenzione del Senior Management su questo tema, adottando allo stesso tempo sistemi di difesa integrati e guidati dall'IA, e investendo non solo in tecnologie e processi, ma anche nelle persone che ogni giorno difendono i sistemi da queste minacce.

SOPHOS

Per saperne di più sul ransomware e su come Sophos può aiutarti a proteggere la tua organizzazione, visita il nostro sito web.

Vendite per l'Italia
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

2026-09-12 IT (DD)