SOPHOS

LA VERA STORIA DEL RANSOMWARE IN ITALIA 2026

I risultati di un sondaggio indipendente e vendor-agnostic condotto tra 171 organizzazioni italiane che sono state colpite dal ransomware l'anno scorso.

WHITEPAPER SOPHOS - LUGLIO 2026

Informazioni sul report

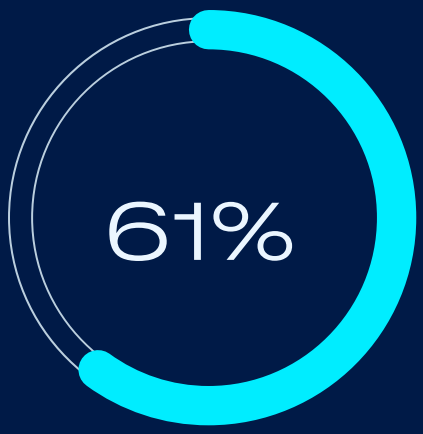
Giunto alla settima edizione, il report La vera storia del ransomware si basa sui risultati di un sondaggio indipendente e vendor-agnostic commissionato da Sophos. Il report globale di quest'anno si basa sulle esperienze di 2.158 IT/Cybersecurity Manager che lavorano in organizzazioni che sono state colpite dal ransomware l'anno scorso, incluse 171 con sede in Italia.

Il sondaggio è stato svolto tra gennaio e marzo 2026. 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. Tutti i dati finanziari sono espressi in dollari U.S.A. i valori anomali dei riscatti pari o superiori a 40 milioni di $ sono stati rimossi da questi dati.

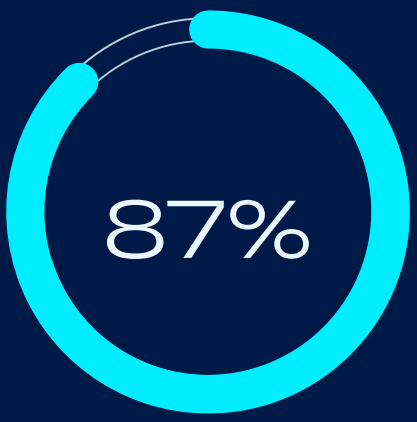
Partecipanti al sondaggio:

171

IT/Cybersecurity Manager che lavorano in organizzazioni con sede in Italia che sono state colpite dal ransomware l'anno scorso.



Percentuale di attacchi in cui sono stati crittografati dei dati.



Percentuale di partecipanti che ha confermato che l'incidente di ransomware dell'anno scorso ha coinciso con il più grave attacco all'identità subito.

Costo medio della riparazione dei danni di un attacco ransomware.

Perché le organizzazioni italiane vengono colpite dal ransomware

- **Gli exploit delle vulnerabilità sono stati la più comune causa tecnica all'origine degli attacchi,** essendo stati utilizzati nel 27,5% degli incidenti, seguiti dalle e-mail malevole (26,9%) e dal phishing (22%). Gli exploit delle vulnerabilità sono scesi dal 35% del report del 2025 al 27,5%.
- **Una lacuna di sicurezza sconosciuta (37,4%) è stata la causa operativa più comune,** seguita dalla mancanza di competenze (36,8%) e dall'errore umano (36%).
- **(NOVITÀ) I dispositivi degli utenti sono stati il più comune punto di ingresso dell'attacco (44%)** per le cause originarie non legate a e-mail o phishing, seguiti da applicazioni e sistemi esposti (29%) e VPN (12%).
- **(NOVITÀ) L'87% dei partecipanti ha confermato che l'incidente di ransomware dell'anno scorso ha coinciso con il più grave attacco all'identità subito.** Una percentuale molto più alta rispetto alla media globale del 67%, nonché il tasso di concomitanza più elevato registrato tra tutti i paesi.

Cosa succede ai dati

- **Nel 61% degli incidenti sono stati crittografati dei dati.** Questa statistica supera la media globale del 56%, e rappresenta un incremento rispetto al 55% registrato in Italia nel report del 2025.
- **Nel 47% degli attacchi, le organizzazioni italiane hanno pagato il riscatto e recuperato dei dati,** una statistica in netto aumento rispetto al 27% dell'anno scorso.
- **Il 98% delle organizzazioni italiane che hanno subito la crittografia non autorizzata dei dati sono riuscite a recuperare le informazioni sottratte,** in linea con la media globale.
- **Il furto dei dati si è verificato anche nel 23% degli attacchi in cui sono state crittografate informazioni,** in aumento rispetto all'11% registrato nel 2025.
- **Nel 65% dei casi, le organizzazioni italiane hanno utilizzato i backup per recuperare i dati crittografati illicitamente,** un dato nettamente superiore al 58% del report del 2025.

Riscatti: richieste e pagamenti

- **La richiesta di riscatto mediana per le organizzazioni con sede in Italia è stata di 1 milione di $,** in calo del 76% rispetto ai 4,12 milioni di $ registrati nel report del 2025.

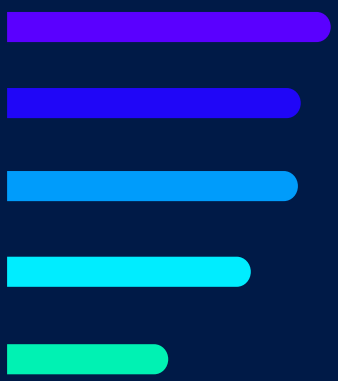
Pagamento del riscatto mediano per le organizzazioni con sede in Italia.

- **Il 48% delle richieste di riscatto era pari ad almeno 1 milione di $,** una diminuzione significativa, se paragonata al 68% del report del 2025.
- **Il pagamento di riscatto mediano per le organizzazioni in Italia è stato di 1.14 milioni di $,** con un calo del 51% rispetto ai 2,32 milioni di $ del report del 2025.
- **Le organizzazioni italiane pagano tipicamente il 97% della somma di riscatto richiesta (cifra mediana),** rispetto al 97% riscontrato nel report del 2025.

L'impatto commerciale del ransomware

- Escludendo eventuali pagamenti del riscatto, **per le organizzazioni italiane il costo medio sostenuto nel report di quest'anno per rimediare ai danni provocati da un attacco ransomware è stato pari a 2,07 milioni di $,** con una riduzione significativa rispetto ai 3,55 milioni di $ dichiarati in media dagli intervistati in Italia nel 2025. La somma include costi relativi a tempi di inattività, ore di lavoro del personale, spese correlate a dispositivi e rete, perdita di opportunità commerciali ecc.
- **Il 64% delle organizzazioni in Italia ha ripreso le normali attività entro una settimana dall'attacco ransomware,** un aumento significativo rispetto al 46% indicato nel report del 2025. Nel 17% dei casi, i partecipanti hanno avuto bisogno di un periodo compreso tra uno e sei mesi per tornare alla normalità operativa, una diminuzione notevole rispetto al 26% del report del 2025.

Impatto umano del ransomware sui team IT/di cybersecurity nelle organizzazioni che hanno subito la crittografia non autorizzata dei dati



Il 39% ammette di aver subito maggiori pressioni dal Senior Management.

Il 36% dichiara di godere di una maggiore stima da parte del Senior Management.

Il 36% indica di aver osservato un cambiamento di priorità/ focalizzazione del team.

Il 30% ha riscontrato cambiamenti della struttura del team/ organizzativa. Una statistica in calo rispetto al 39% del 2025.

Il 20% segnala un cambio di leadership nel team.

Raccomandazioni

Potenzia la sicurezza dell'identità come difesa contro i ransomware. L'ampia maggioranza delle vittime del ransomware in Italia ha confermato che l'incidente di ransomware ha coinciso con il più grave attacco all'identità subito. Le organizzazioni devono dare priorità all'Identity Threat Detection and Response (ITDR), imporre l'autenticazione multifattoriale a tutti i punti di accesso ed eseguire regolarmente audit delle credenziali delle identità sia umane che non umane.

Rafforza la protezione degli endpoint per i modelli di IA di frontiera. L'IA di frontiera sta accelerando l'individuazione e lo sfruttamento delle vulnerabilità. Avere difese potenti per gli endpoint, che siano in grado di bloccare automaticamente gli attacchi basati sugli exploit, è essenziale.

Dai la priorità alla sicurezza delle e-mail. Poiché in Italia phishing ed e-mail malevole rappresentano quasi la metà delle cause originarie dei ransomware, le organizzazioni devono implementare filtri e-mail avanzati, applicare protocolli DMARC/DKIM/SPF e investire in corsi di formazione periodici di consapevolezza sul phishing.

Investi nell'infrastruttura di backup e ripristino. Le organizzazioni che hanno mantenuto sistemi di backup solidi hanno recuperato i dati crittografati a tassi quasi record nell'ultimo anno. 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.

Per scoprire come Sophos può aiutarti a ottimizzare le tue difese antiransomware, parla con un consulente o visita **sophos.it/ransomware2026**

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.

2026-08-05 IT-WP (TA) CRE-6009