SOPHOS

LA VERA STORIA DEL RANSOMWARE IN ITALIA 2025

I risultati di un sondaggio indipendente e vendor-agnostic condotto tra 254 organizzazioni italiane che sono state colpite dal ransomware l'anno scorso.

WHITEPAPER SOPHOS - GIUGNO 2025

Informazioni sul report

Questo report si basa sui risultati di un sondaggio indipendente e vendor-agnostic, condotto tra 3.400 IT/Cybersecurity Manager che lavorano in organizzazioni che sono state colpite dal ransomware l'anno scorso, incluse 254 con sede in Italia.

Il sondaggio è stato condotto per conto di Sophos da un'azienda specializzata indipendente, tra gennaio e marzo 2025.

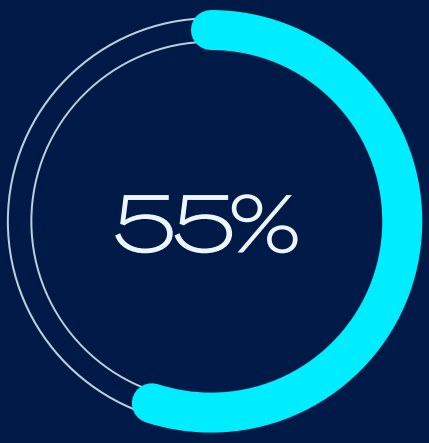
A tutti i partecipanti, che lavorano in organizzazioni con un numero di dipendenti compreso tra 100 e 5.000, è stato chiesto di rispondere tenendo in considerazione le proprie esperienze nei 12 mesi precedenti.

Il report include un confronto con i risultati del nostro sondaggio del 2024. Tutti i dati finanziari sono espressi in dollari U.S.A.

Partecipanti al sondaggio:

254

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.

Pagamento del riscatto mediano per le organizzazioni con sede in Italia l'anno scorso.

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 35% degli incidenti. Segue il phishing, che ha causato il 23% degli attacchi. Le credenziali compromesse. sono state utilizzate nel 16% degli attacchi.
- **La mancanza di competenze è stata identificata come la più comune causa operativa all'origine degli attacchi**, in quanto è stata indicata dal 45% delle organizzazioni italiane che hanno partecipato al sondaggio. Al secondo posto si trovano le lacune di sicurezza note, citate dal 37% delle organizzazioni. Nel 36% dei casi gli intervistati hanno dichiarato che a svolgere un ruolo importante nella compromissione dei sistemi da parte del ransomware è stato un punto debole nelle difese di cui non erano a conoscenza.

Cosa succede ai dati

- **Nel 55% degli incidenti sono stati crittografati dei dati.** Questa statistica supera la media globale del 50%, ma rappresenta un calo significativo rispetto all'85% registrato in Italia nel 2024.
- **In appena l'11% degli attacchi in cui sono state crittografate informazioni si è verificato anche il furto di dati**, meno di un quarto rispetto al 45% osservato l'anno scorso.
- **Il 99% delle organizzazioni italiane che hanno subito la crittografia non autorizzata dei dati sono riuscite a recuperare le informazioni sottratte**, con un tasso che supera la media globale.
- **Nel 27% degli attacchi, le organizzazioni italiane hanno pagato il riscatto e recuperato dei dati**, una statistica nettamente in calo rispetto al 53% dell'anno scorso.
- **Nel 58% dei casi, le organizzazioni italiane hanno utilizzato i backup per recuperare i dati crittografati illecitamente**, con una diminuzione rispetto al 72% dell'anno scorso.

I riscatti: richieste e pagamenti

- **L'anno scorso, la richiesta di riscatto mediana per le organizzazioni con sede in Italia è stata pari a 4,12 milioni di $**, in netto aumento rispetto ai 3,19 milioni di $ del sondaggio del 2024.
- **Il 68% delle richieste di riscatto sono state di 1 o più milioni di $**, in calo rispetto al 78% del 2024.

Richiesta di riscatto mediana per le organizzazioni con sede in Italia l'anno scorso.

- **Il pagamento del riscatto mediano per le organizzazioni con sede in Italia negli ultimi 12 mesi è stato 2,06 milioni di $**, ovvero meno dei 2,20 milioni di $ dichiarati l'anno scorso.
- **Tipicamente, le organizzazioni con sede in Italia hanno pagato il 97% della somma richiesta per il riscatto**, una statistica nettamente al di sopra della media globale dell'85%.
  - Il 62% delle organizzazioni intervistate **hanno pagato MENO della richiesta di riscatto iniziale** (media globale: 53%).
  - Il 14% delle organizzazioni intervistate **hanno pagato LA STESSA somma della richiesta di riscatto iniziale** (media globale: 29%).
  - Il 24% delle organizzazioni intervistate **hanno pagato PIÙ della richiesta di riscatto iniziale** (media globale: 18%).

L'impatto commerciale del ransomware

- Escludendo eventuali pagamenti del riscatto, **per le organizzazioni italiane il costo medio sostenuto l'anno scorso per rimediare ai danni provocati da un attacco ransomware è stato pari a 3,55 milioni di $**, con una riduzione significativa rispetto ai 5,38 milioni di $ dichiarati dagli intervistati in Italia nel 2024. 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.
- **Per le organizzazioni italiane, i tempi necessari per riprendere le normali attività operative dopo un attacco ransomware stanno diventando più brevi**: una ripresa completa entro una settimana si è riscontrata infatti nel 46% delle risposte, il doppio rispetto al 23% dell'anno scorso. Nel 26% dei casi, i partecipanti hanno avuto bisogno di un periodo compreso tra uno e sei mesi per tornare alla normalità operativa, una diminuzione significativa rispetto al 50% dell'anno precedente.

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

Nel 39% dei casi, le organizzazioni che hanno preso parte al sondaggio hanno notato **cambiamenti della struttura del team/organizzativa.**

Nel 36% dei casi, hanno osservato **un aumento costante del carico di lavoro.**

Nel 35% dei casi, hanno provato **maggiore ansia o stress** per paura di attacchi futuri.

Nel 35% dei casi, hanno sperimentato **sensi di colpa** dovuti al fatto che l'attacco non è stato fermato.

Nel 32% dei casi, hanno registrato **assenze del personale dovute a problemi di stress/salute mentale.**

Raccomandazioni

Il ransomware continua a essere una delle minacce più pericolose per le organizzazioni italiane. 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. Le informazioni apprese da questo report mettono in luce importanti ambiti di focalizzazione per il 2025 e in futuro.

- **Prevenzione.** I migliori attacchi ransomware sono quelli che non si verificano, perché i cybercriminali non sono riusciti a infiltrarsi nei sistemi della tua organizzazione. Cerca di ridurre sia le cause tecniche all'origine degli attacchi, che quelle operative, prendendo spunto dai fattori evidenziati 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 antiransomware 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 di svolgere esercitazioni regolari di ripristino dei dati da questi backup.

SOPHOS

Per esplorare come Sophos può aiutarti a ottimizzare le tue difese antiransomware, parla con un consulente o visita **sophos.it/ransomware2025**

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.

© Copyright 2025. Sophos Ltd. Tutti i diritti riservati.
Registrata in Inghilterra e Galles con Nº 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Regno Unito
Sophos è un marchio registrato da Sophos Ltd. Tutti gli altri nomi di società e prodotti qui menzionati sono marchi o marchi registrati dei rispettivi titolari.
2025-07-11 IT-WP (DD)