SOPHOS
Cybersecurity evolved.

# La Vera Storia Del Ransomware 2021

Il sondaggio annuale condotto da Sophos sugli attacchi ransomware fornisce approfondimenti esclusivi e un'analisi delle esperienze vissute da aziende di piccole e medie dimensioni in tutto il mondo. Esplora cosa succede durante un attacco, l'impatto che ha sulle vittime e confronta le tendenze emerse rispetto all'anno precedente. Quest'anno, per la prima volta, il sondaggio rivela anche le somme effettive versate dalle vittime come riscatto (ransom) e la percentuale di dati che sono riuscite a recuperare dopo il pagamento.

*Whitepaper Sophos. Aprile 2021*

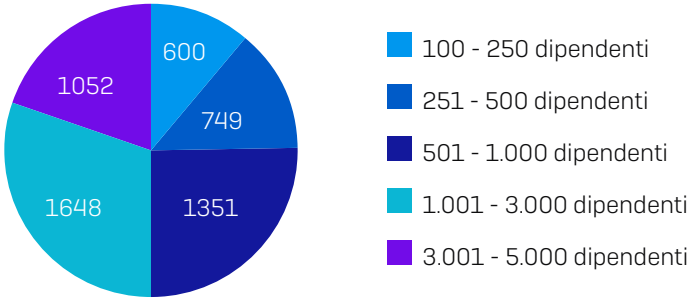
# Informazioni sul sondaggio

Sophos ha incaricato l'azienda Vanson Bourne, specializzata nelle ricerche di mercato, di intervistare 5.400 responsabili IT in 30 paesi. Il sondaggio è stato svolto tra gennaio e febbraio 2021.

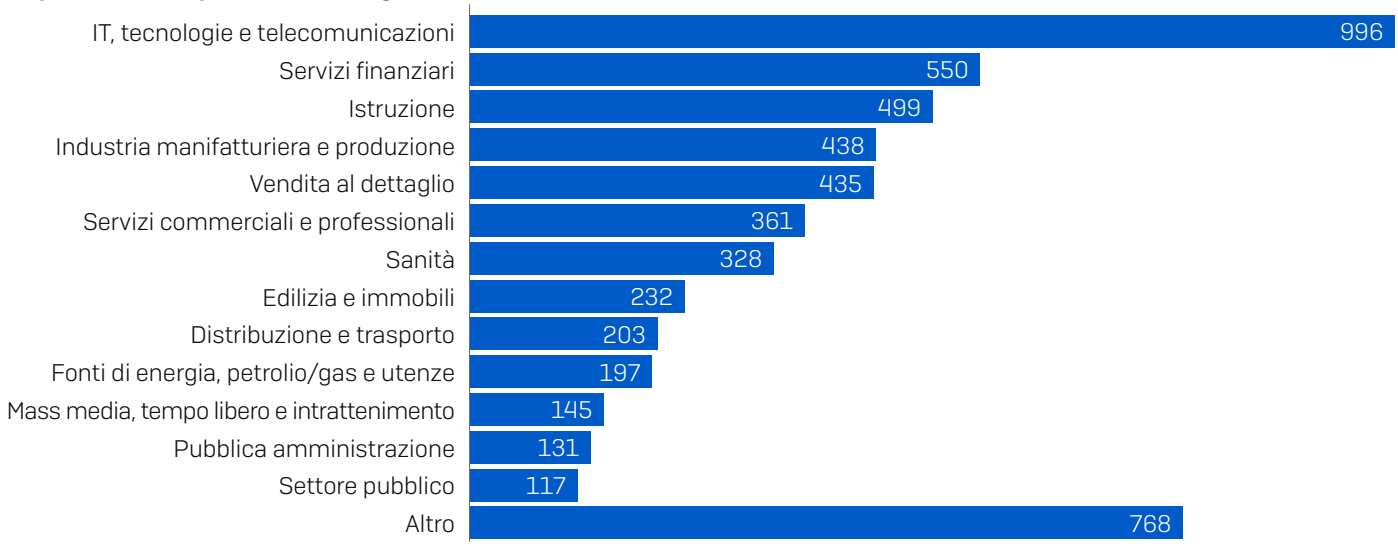
| PAESE | NUM. PARTECIPANTI | PAESE | NUM. PARTECIPANTI | PAESE | NUM. PARTECIPANTI |
|---|---|---|---|---|---|
| Australia | 250 | India | 300 | Arabia Saudita | 100 |
| Austria | 100 | Israele | 100 | Singapore | 150 |
| Belgio | 100 | Italia | 200 | Sud Africa | 200 |
| Brasile | 200 | Giappone | 300 | Spagna | 150 |
| Canada | 200 | Malaysia | 150 | Svezia | 100 |
| Cile | 200 | Messico | 200 | Svizzera | 100 |
| Colombia | 200 | Paesi Bassi | 150 | Turchia | 100 |
| Repubblica Ceca | 100 | Nigeria | 100 | EAU | 100 |
| Francia | 200 | Filippine | 150 | Regno Unito | 300 |
| Germania | 300 | Polonia | 100 | Stati Uniti | 500 |

Come negli anni passati, il 50% dei partecipanti faceva parte di organizzazioni con un numero di dipendenti compreso tra i 100 e i 1.000, mentre il restante 50% si trovava in organizzazioni dai 1.001 ai 5.000 dipendenti. I partecipanti appartenevano a settori diversi.

### Quanti dipendenti ha la vostra organizzazione a livello globale?




### In quale settore opera la vostra organizzazione?



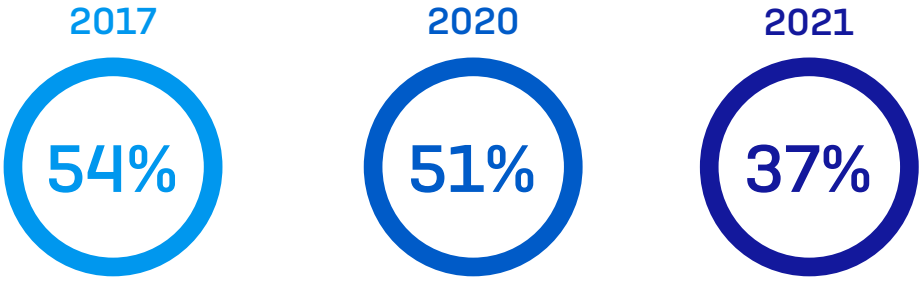
# I risultati più salienti

- Il **37%** delle organizzazioni intervistate **è stato colpito dal ransomware l'anno scorso**
- Il **54%** delle organizzazioni colpite dal ransomware durante l'anno passato sostiene che **i cybercriminali sono riusciti a cifrare i dati** nell'attacco di maggiore impatto
- Il **96%** dei partecipanti che hanno subito la cifratura dei dati **è riuscito a recuperare i dati** sottratti nell'attacco di maggiore impatto
- La **somma media dei pagamenti di riscatto** delle organizzazioni di medie dimensioni ammonta a **170.404 USD**
- Tuttavia, in media, solo il **65% dei dati cifrati è stato recuperato** dopo il pagamento del riscatto
- Il **costo medio necessario per rimediare ai danni di un attacco ransomware** (considerando tempi di inattività, ore di lavoro del personale, costi associati a dispositivi e rete, perdita di opportunità commerciali, somma pagata per il riscatto) è pari a **1,85 milioni di USD**
- Gli **attacchi con tentativi di estorsione** che non prevedono la cifratura dei dati, ma che ricattano la vittima **sono più che raddoppiati** rispetto all'anno scorso, passando dal 3% al 7%
- La presenza di **personale tecnico qualificato, in grado di bloccare gli attacchi** è il motivo più comune per il quale alcune organizzazioni sono convinte che non cadranno vittima del ransomware in futuro

# La prevalenza del ransomware

## Il ransomware continua a essere una minaccia molto grave

L'anno scorso, il 37% delle organizzazioni (più di un terzo delle 5.400 intervistate) è stato colpito dal ransomware, ciò significa che **vari computer sono stati attaccati, anche se non tutti sono stati cifrati**. Sebbene si tratti di una percentuale elevata, la buona notizia è che questo rappresenta un calo rispetto all'anno precedente, quando le vittime dichiarate erano il 51%.

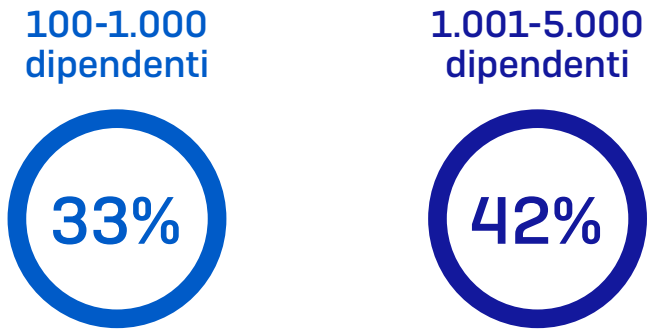



*La vostra organizzazione è stata colpita dal ransomware negli ultimi 12 mesi? Sì [2021=5.400; 2020=5.000; 2017=2.700], alcune opzioni di risposta sono state omesse, suddivisione in base all'anno*

I cambiamenti nei comportamenti dei cybercriminali che sono stati osservati dai SophosLabs e dal team Sophos di Managed Threat Response indicano che la diminuzione della quantità di attacchi potrebbe essere in parte dovuta a un'evoluzione degli approcci di attacco. Per esempio, gli hacker stanno velocemente migrando verso tecniche di attacco meno rilevabili, frutto di un mix tra automazione e manualità. Sebbene la quantità totale degli attacchi sia inferiore, abbiamo osservato che il potenziale disastroso di questi attacchi mirati è molto più elevato.

## Le organizzazioni di grandi dimensioni hanno una maggiore probabilità di essere colpite

Analizzando il numero di incidenti in base alle dimensioni dell'organizzazione, si nota che le organizzazioni più grandi segnalano una maggiore prevalenza degli attacchi, con il 42% delle aziende con 1.001-5.000 dipendenti che ammette di essere stato colpito, rispetto al 33% delle imprese più piccole.

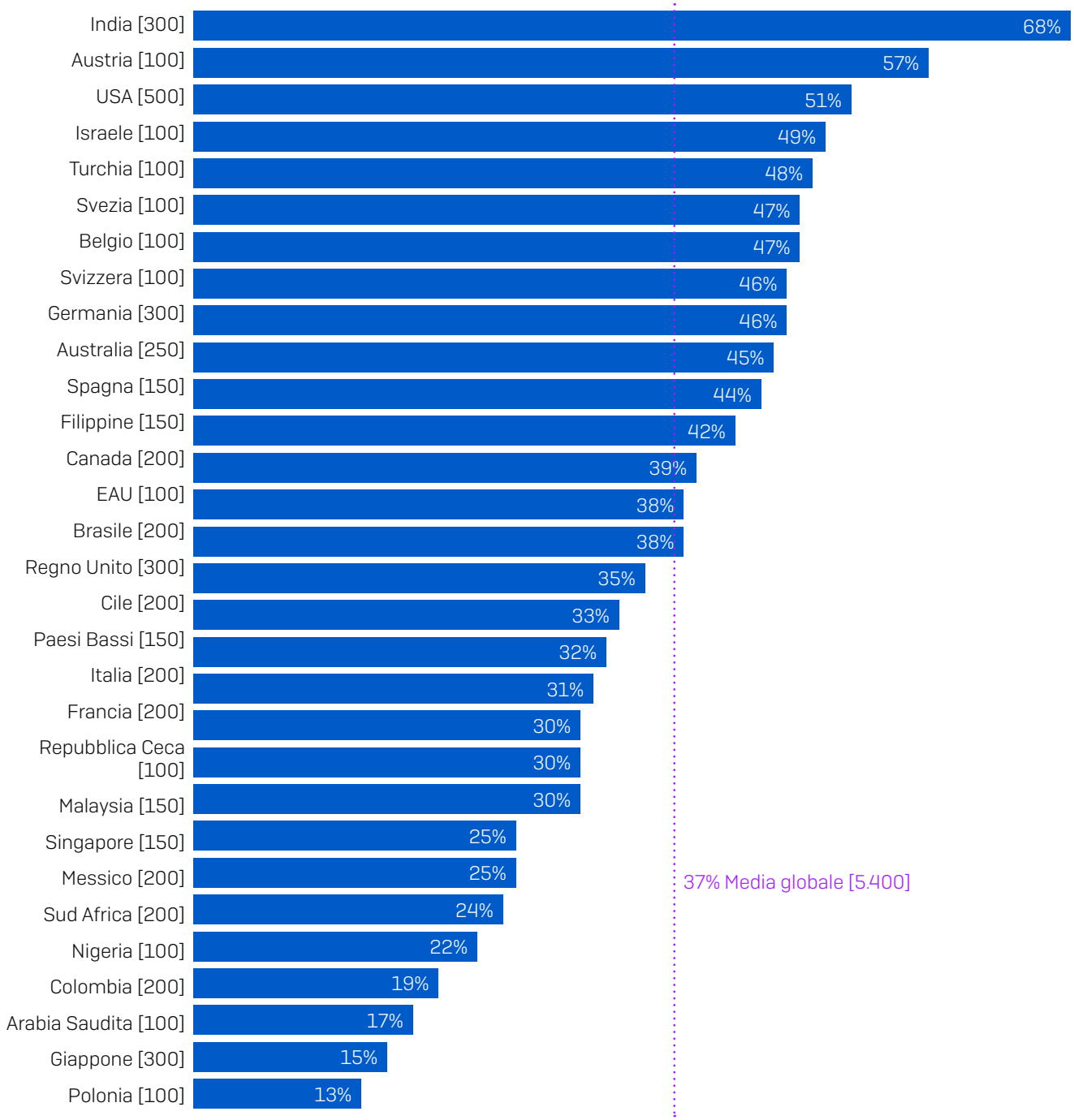



*La vostra organizzazione è stata colpita dal ransomware negli ultimi 12 mesi? Sì [5.400], alcune opzioni di risposta sono state omesse, suddivisione in base alle dimensioni dell'organizzazione*

Quest'anno anche il divario tra le organizzazioni più piccole e quelle più grandi è aumentato, passando dal 7% del 2020 al 9% di oggi. Il fatto che gli hacker abbiano deciso di focalizzarsi maggiormente sulle organizzazioni di grandi dimensioni non sorprende: queste imprese hanno infatti più risorse economiche e offrono quindi maggiori opportunità di lucro. Detto questo, un'organizzazione di piccole dimensioni su tre è stata colpita dal ransomware l'anno scorso, confermando che questi tipi di aziende sono ancora oggetto di grande interesse da parte degli autori degli attacchi. È una battaglia che non ha vincitori.

## I livelli di attacco variano da paese a paese

L'analisi dei dati in base al paese in cui hanno sede i partecipanti rivela statistiche molto interessanti.




*La vostra organizzazione è stata colpita dal ransomware negli ultimi 12 mesi? Sì [base di partecipanti indicata nel grafico], alcune opzioni di risposta sono state omesse, suddivisione in base al paese*

L'**India** ha il discutibile onore di trovarsi in cima alla classifica, con il 68% degli intervistati che dichiara di essere stato colpito dal ransomware l'anno scorso. Spesso nei titoli dei giornali vengono citati cybercriminali che sferrano i loro attacchi dalla Cina, Corea del Nord, Russia e altri paesi dell'Est Europa. In realtà i SophosLabs hanno osservato che i più elevati livelli di ransomware domestico, ovvero hacker che attaccano aziende, arrivano dall'India. Quindi hacker indiani che attaccano aziende indiane.

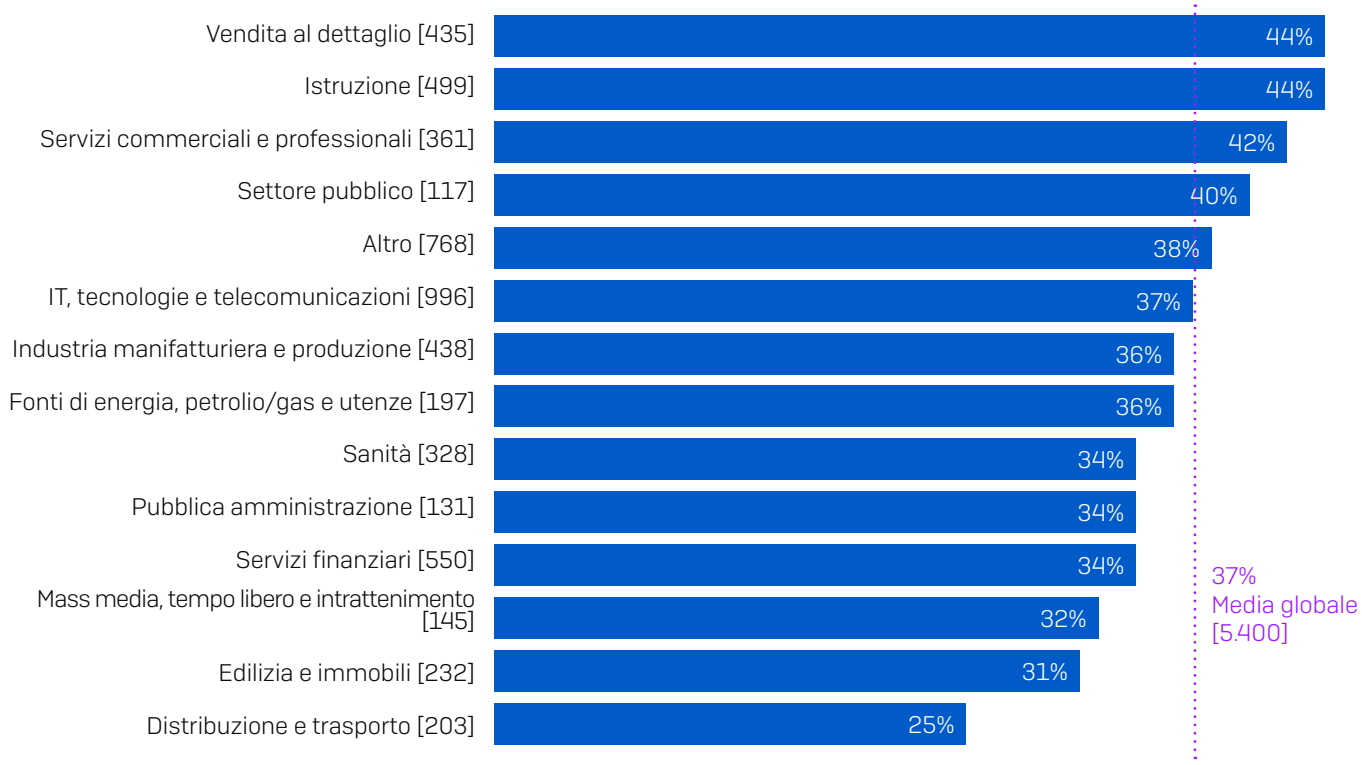
Gli **U.S.A.** sono un bersaglio molto frequente per i cybercriminali, a causa del potenziale percepito di poter esigere pagamenti di riscatto molto elevati; poco più della metà (51%) dei partecipanti negli U.S.A. ha dichiarato di essere stato colpito l'anno scorso.

**Polonia, Colombia, Nigeria, Sud Africa** e **Messico** registrano i livelli di attacco più bassi, il che probabilmente è dovuto a un PIL meno alto rispetto agli altri paesi e di conseguenza a un potenziale di riscatto inferiore per gli autori degli attacchi.

I risultati del **Giappone** spiccano tra i paesi con un'economia sviluppata, in quanto presentano livelli molto bassi di ransomware: solo il 15% degli intervistati ha dichiarato di essere stato colpito dal ransomware l'anno scorso. Il Giappone di solito registra livelli di ransomware molto bassi nei nostri sondaggi annuali. Questo potrebbe essere dovuto al fatto che le organizzazioni giapponesi hanno investito molto nelle difese antiransomware. Un altro motivo potrebbe essere la natura unica della lingua giapponese, che complica il processo di attacco per i cybercriminali.

## La vendita al dettaglio e l'istruzione sono i settori più colpiti dagli attacchi di ransomware

Analizzando i livelli di attacco in base al settore operativo, si osservano variazioni notevoli nella propensione a cadere vittima di un attacco di ransomware.




*La vostra organizzazione è stata colpita dal ransomware negli ultimi 12 mesi? Sì [base di partecipanti indicata nel grafico], alcune opzioni di risposta sono state omesse, suddivisione in base al settore*

*Quelli della* **vendita al dettaglio** e dell'**istruzione** sono i settori che registrano i più alti livelli di attacco, con il 44% dei partecipanti che dichiara di essere stato colpito.

La **sanità**, che solitamente domina i titoli delle notizie relative agli attacchi di ransomware, segnala livelli di attacco appena sotto la media, con il 34% delle organizzazioni intervistate che sostiene di esserne caduto vittima. La frequenza elevata con cui questo settore viene rappresentato nelle news è probabilmente dovuta agli obblighi normativi che impongono alle organizzazioni che operano nell'ambito sanitario di comunicare gli attacchi subiti, mentre molte organizzazioni commerciali possono mantenere la riservatezza.

# L'impatto del ransomware

## Diminuisce la cifratura non autorizzata, aumentano i tentativi di estorsione.

Abbiamo chiesto alle organizzazioni colpite dal ransomware se i cybercriminali sono riusciti a cifrare i loro dati. Il 54% ha risposto di sì. Il 39% è riuscito a bloccare l'attacco prima che venissero cifrati i dati, mentre il 7% ha dichiarato che i dati non sono stati cifrati, ma che hanno comunque ricevuto una richiesta di riscatto.

Mettendo a confronto queste statistiche con i risultati del nostro sondaggio del 2020, emerge una narrativa molto interessante.

| 2020 | 2021 | |
|---|---|---|
| 73% | 54% | I cybercriminali sono riusciti a cifrare i dati |
| 24% | 39% | Attacco bloccato prima che i dati potessero essere cifrati |
| 3% | 7% | Richieste di riscatto anche se i dati non erano stati cifrati |

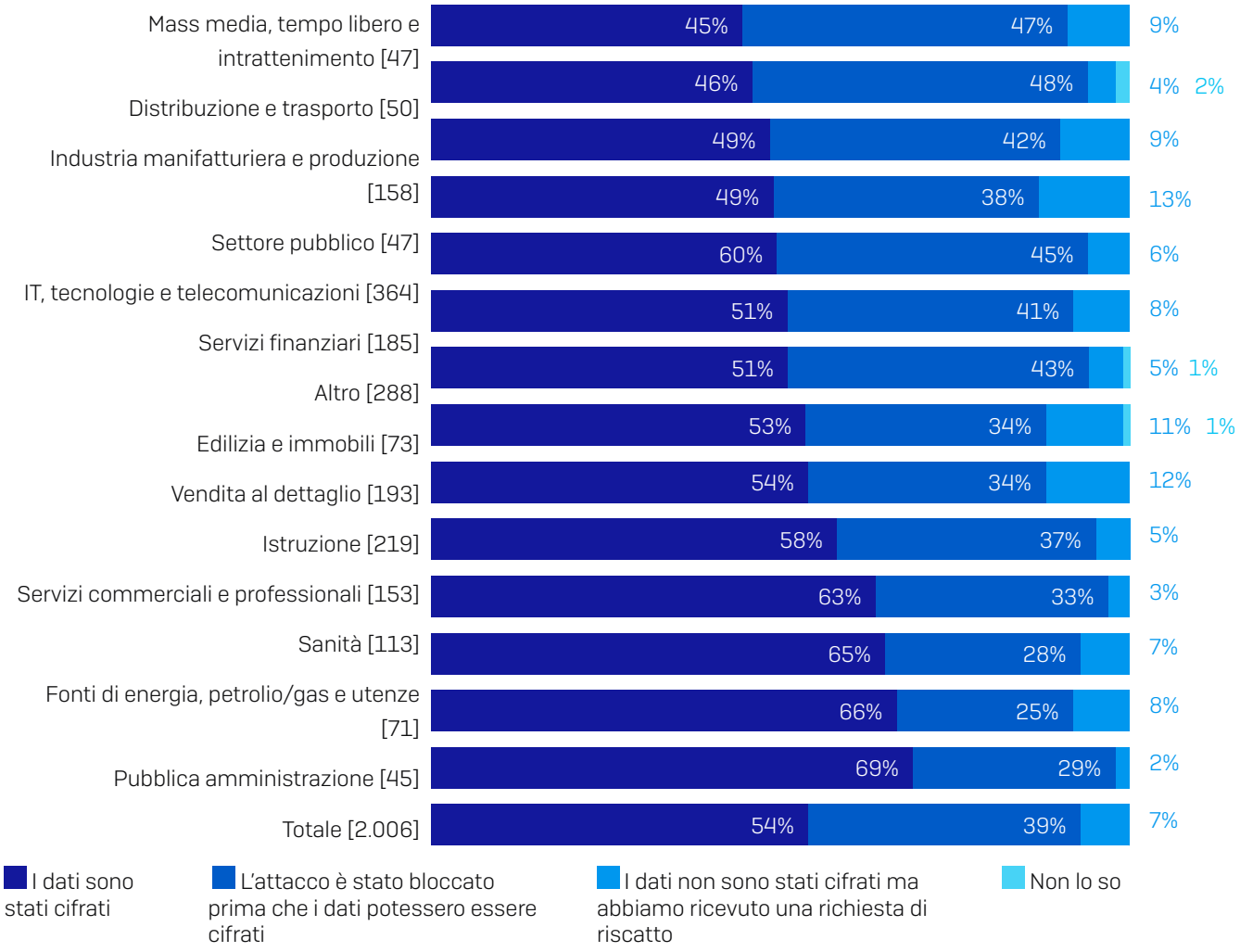
*Nell'attacco ransomware più grave, i cybercriminali sono riusciti a cifrare i dati dell'organizzazione? [2021=2.006, 2020=2.538] organizzazioni che hanno subito un attacco di ransomware l'anno scorso*

In primo luogo, l'anno scorso si è verificato un calo significativo della percentuale degli attacchi durante i quali i cybercriminali sono riusciti a cifrare i dati: sono infatti scesi dal 73% al 54% e sono ora molto più numerose le organizzazioni in grado di bloccare un attacco prima che vengano cifrati i dati. Questo indica che l'implementazione delle tecnologie antiransomware sta dando i suoi frutti.

Tuttavia, si nota anche che la percentuale degli attacchi che prevedono una richiesta di riscatto senza cifrare i dati è raddoppiata. Alcuni hacker stanno infatti adottando un approccio diverso, basato sull'estorsione, con il quale i file, invece di essere cifrati, vengono prelevati illecitamente con la minaccia di una loro pubblicazione, a meno che non venga pagato il riscatto specificato.  Questi attacchi richiedono un impegno minore: non implicano operazioni di cifratura o decifratura dei dati. Nelle richieste di riscatto, i cybercriminali spesso cercano di indurre le vittime a pagare, puntando sulle pesanti sanzioni previste per i casi di violazione dei dati.

## La capacità di bloccare la cifratura dei dati varia notevolmente in base al settore

Nel bloccare la cifratura dei file, alcuni settori riscontrano tassi di successo superiori rispetto ad altri.




*Nell'attacco di ransomware più grave, i cybercriminali sono riusciti a cifrare i dati dell'organizzazione? [base di partecipanti indicata nel grafico] organizzazioni che hanno subito un attacco di ransomware l'anno scorso*

Quello della **distribuzione e trasporto** è il settore con la maggiore percentuale di successo nel blocco dei cybercriminali prima che possano cifrare i file (48%), seguito a distanza ravvicinata dal settore dei **mass media, tempo libero e intrattenimento** (47%).

Una tendenza opposta si è osservata invece nel settore della **pubblica amministrazione**, che presenta la maggiore probabilità di non riuscire a evitare la cifratura dei dati in un attacco di ransomware (69%). Questa statistica è probabilmente dovuta alla combinazione di due fattori molto importanti:

- Difese più deboli: generalmente le organizzazioni della pubblica amministrazione hanno budget IT molto bassi e personale tecnico limitato e/o oberato di lavoro.
- Maggiore interesse da parte dei cybercriminali: per via delle loro dimensioni e della possibilità di accedere a fondi pubblici, le organizzazioni della pubblica amministrazione vengono spesso considerate bersagli molto lucrativi e pertanto vengono colpite con attacchi più sofisticati.
  Inoltre (come vedremo in seguito), quello della pubblica amministrazione è anche al secondo posto tra i settori più propensi a pagare il riscatto.

Il settore **pubblico** è quello maggiormente soggetto a tentativi di estorsione (13%).

La **sanità**, come abbiamo visto, registra un numero medio di attacchi inferiore alla media. Tuttavia, i cybercriminali sono riusciti a cifrare i file in quasi due terzi (65%) degli incidenti, una statistica nettamente superiore alla media.

## Le vittime che pagano il riscatto sono più numerose

Abbiamo chiesto alle organizzazioni i cui dati sono stati cifrati (1.086) se sono riuscite a recuperarli e in tale eventualità come.

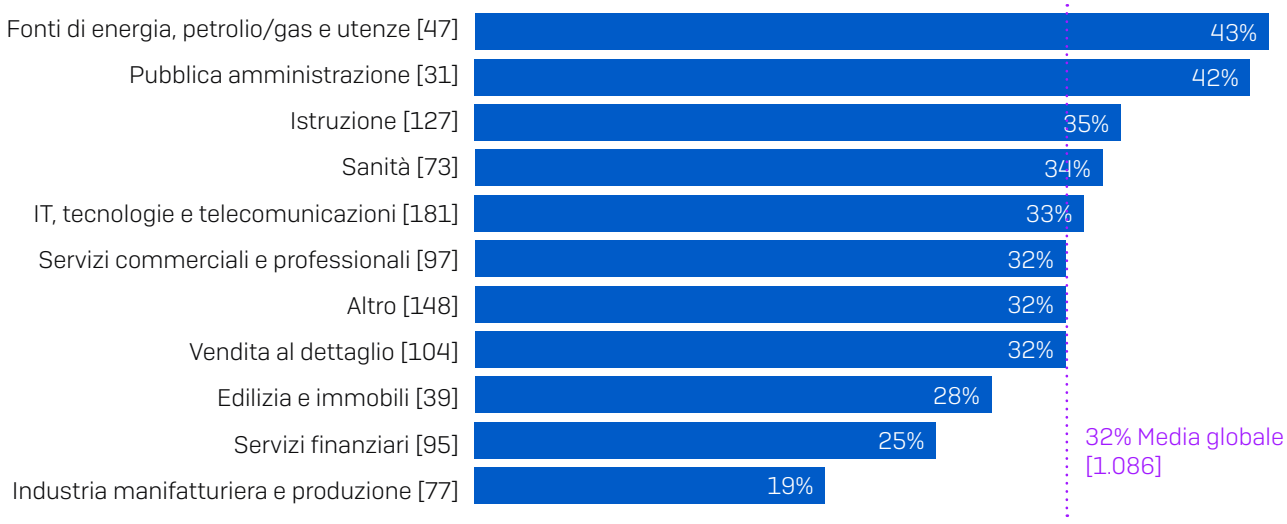
| 2020 | 2021 | |
|---|---|---|
| 26% | 32% | Percentuale delle organizzazioni che hanno pagato il riscatto per recuperare i dati |
| 56% | 57% | Percentuale delle organizzazioni che hanno utilizzato il backup per recuperare i dati |
| 12% | 8% | Percentuale delle organizzazioni che hanno utilizzato altri mezzi per recuperare i dati |
| 94% | 96% | Totale delle organizzazioni che hanno recuperato dei dati |

*Nota: Siccome i dati sono stati arrotondati, ci sono occasioni in cui la somma dei totali non è equivalente alla somma delle cifre individuali*
*Nell'attacco ransomware più grave, l'organizzazione ha recuperato i dati?*
*[2021=1.086, 2020=1.849] organizzazioni i cui dati sono stati cifrati*

Come si può osservare nel grafico riportato sopra, il 32% delle organizzazioni ha pagato il riscatto per recuperare i dati, con un aumento del 26% rispetto alla ricerca dell'anno scorso. Il 57% delle organizzazioni è stata in grado di utilizzare i backup per ripristinare i dati, in linea con i risultati dell'anno scorso. Complessivamente, quasi tutte le organizzazioni (96%) hanno recuperato almeno parte dei dati.

## La propensione a pagare il riscatto varia in base al settore

Tra i vari settori, si nota un divario significativo nel pagamento del riscatto.




*Nell'attacco ransomware più grave, l'organizzazione ha recuperato i dati? Sì, abbiamo pagato il riscatto [base di partecipanti indicata nel grafico] organizzazioni nelle quali i cybercriminali sono riusciti a cifrare i dati nell'attacco ransomware più grave, alcune opzioni di risposta sono state omesse, suddivisione in base al settore*

Quello delle **fonti di energia, petrolio/gas e utenze** è il settore con la maggiore propensione a pagare il riscatto, con il 43% degli intervistati di queste organizzazioni che dichiara di aver ceduto alla richiesta di riscatto. Questo settore è caratterizzato dalla presenza di molte infrastrutture difficili da aggiornare, per cui le vittime possono sentirsi costrette a pagare il riscatto per garantire che l'erogazione dei servizi non venga interrotta.

La **pubblica amministrazione** si trova al secondo posto nella classifica dei settori più propensi a pagare il riscatto (42%). È interessante analizzare questa statistica alla luce di quella discussa precedentemente, secondo la quale il settore della pubblica amministrazione è quello con la maggiore probabilità di cadere vittima della cifratura non autorizzata dei dati. È possibile che l'alta propensione delle organizzazioni della pubblica amministrazione a effettuare il pagamento stia inducendo i cybercriminali a focalizzarsi su questo settore per sferrare attacchi più complessi ed efficaci.

Sembra che ci sia una connessione tra la capacità di un'organizzazione di ripristinare i dati dai backup e la probabilità che paghi il riscatto. Il settore dell'**industria manifatturiera e della produzione** è quello con la minore probabilità di effettuare un pagamento, nonché quello con la maggiore capacità di ripristinare i dati dai backup (68%). Analogamente, l'**edilizia e gli immobili** e i **servizi finanziari** mostrano entrambi livelli inferiori alla media in termini di pagamenti di riscatto e livelli superiori alla media per la capacità di ripristinare i dati dai backup.

Gli **enti governativi e pubblici** non sono stati inclusi nel grafico, in quanto la base di partecipanti era troppo limitata per essere statisticamente significativa. A titolo informativo, delle 23 organizzazioni di questo settore i cui dati sono stati cifrati, il 61% ha dichiarato di aver potuto ripristinare i dati dai backup e solo il 26% ha pagato il riscatto. Questi risultati indicativi potrebbero spiegare perché questo settore è oggetto di particolare attenzione da parte degli attacchi che sfruttano l'estorsione.

### Il pagamento del riscatto aiuta a recuperare solo parte dei dati

**65%**

**Percentuale di dati ripristinati dopo il pagamento di un riscatto**

*Quantità media dei dati recuperati nell'attacco di ransomware più grave [344] organizzazioni che hanno pagato il riscatto per riappropriarsi dei dati*

Quello che i cybercriminali non dicono quando inviano una richiesta di riscatto è che, anche pagando, le probabilità di recuperare tutti i dati sono poche. In media, le organizzazioni che hanno pagato il riscatto sono riuscite a riavere solo il 65% dei file cifrati, mentre un terzo dei dati è rimasto inaccessibile. Il 29% dei partecipanti ha dichiarato di aver recuperato il 50% o meno dei file e solo l'8% si è riappropriato di tutti i dati.

## Il costo del ransomware

### I pagamenti di riscatto variano significativamente

Dei 357 intervistati che dichiarano di aver pagato il riscatto, 282 hanno anche condiviso la somma versata. In questo gruppo, la **somma media versata è stata 170.404 USD**. Tuttavia, i singoli pagamenti di riscatto variano notevolmente. La somma più comunemente versata è stata di 10.000 USD (pagata da 20 organizzazioni intervistate), mentre il pagamento più alto ammonta a 3,2 milioni di USD (cifra esorbitante pagata da due intervistati).

Queste somme sono molto diverse dai pagamenti a otto cifre di cui si sente parlare nei notiziari e i motivi sono vari.

1. **Dimensioni dell'organizzazione.** Le organizzazioni che hanno partecipato al nostro sondaggio sono piccole e medie imprese con un numero di utenti compreso tra 100 e 5.000. In genere, questo tipo di organizzazioni ha a disposizione risorse finanziarie molto più limitate rispetto a quelle delle aziende più grandi. I cybercriminali che utilizzano il ransomware modificano le richieste di riscatto in base al capitale a disposizione della vittima e di solito accettano pagamenti più bassi da aziende più piccole. Le statistiche lo confermano, in quanto il pagamento di riscatto medio delle organizzazioni con 100-1.000 dipendenti ammonta a 107.694 USD, mentre quello delle organizzazioni con 1.000-5.000 dipendenti è di 225.588 USD.
2. **Natura dell'attacco.** I cybercriminali che utilizzano il ransomware sono molti, così come lo sono i tipi di attacco di ransomware esistenti: è possibile trovare hacker abilissimi che utilizzano tattiche, tecniche e procedure (TTP) estremamente sofisticate per colpire individualmente i propri bersagli, così come ci sono anche operatori con competenze tecniche limitate che utilizzano ransomware "preconfezionato" e "sparano alla cieca", augurandosi che l'attacco vada a segno. Gli hacker che investono molto in un attacco mirato esigeranno riscatti molto alti per compensare l'impegno, mentre gli operatori che sferrano attacchi generici spesso accettano un ritorno sull'investimento minore.
3. **Posizione geografica.** Gli autori degli attacchi inviano le richieste di riscatto più elevate ai paesi occidentali caratterizzati da un'economia sviluppata, motivati dal potenziale percepito di poter esigere somme più alte. I pagamenti di riscatto più alti sono stati registrati da due organizzazioni intervistate in Italia. Inoltre, il pagamento di riscatto versato in media in U.S.A., Canada, Regno Unito, Germania e Australia è stato di 214.096 USD, ovvero il 26% in più rispetto alla media globale (base: 101 partecipanti). In India invece il pagamento di riscatto medio è stato di 76.619 USD, meno della metà della media globale (base: 86 partecipanti).

## I costi di riparazione dei danni del ransomware sono più che raddoppiati rispetto all'anno precedente

Il pagamento del riscatto è solo parte della spesa necessaria per rimediare ai danni di un attacco. Sebbene sia il numero di attacchi ransomware che la percentuale degli attacchi che sono riusciti a cifrare i dati abbiano registrato un calo rispetto all'anno precedente, il costo complessivo di riparazione dei danni di un attacco di ransomware è aumentato.

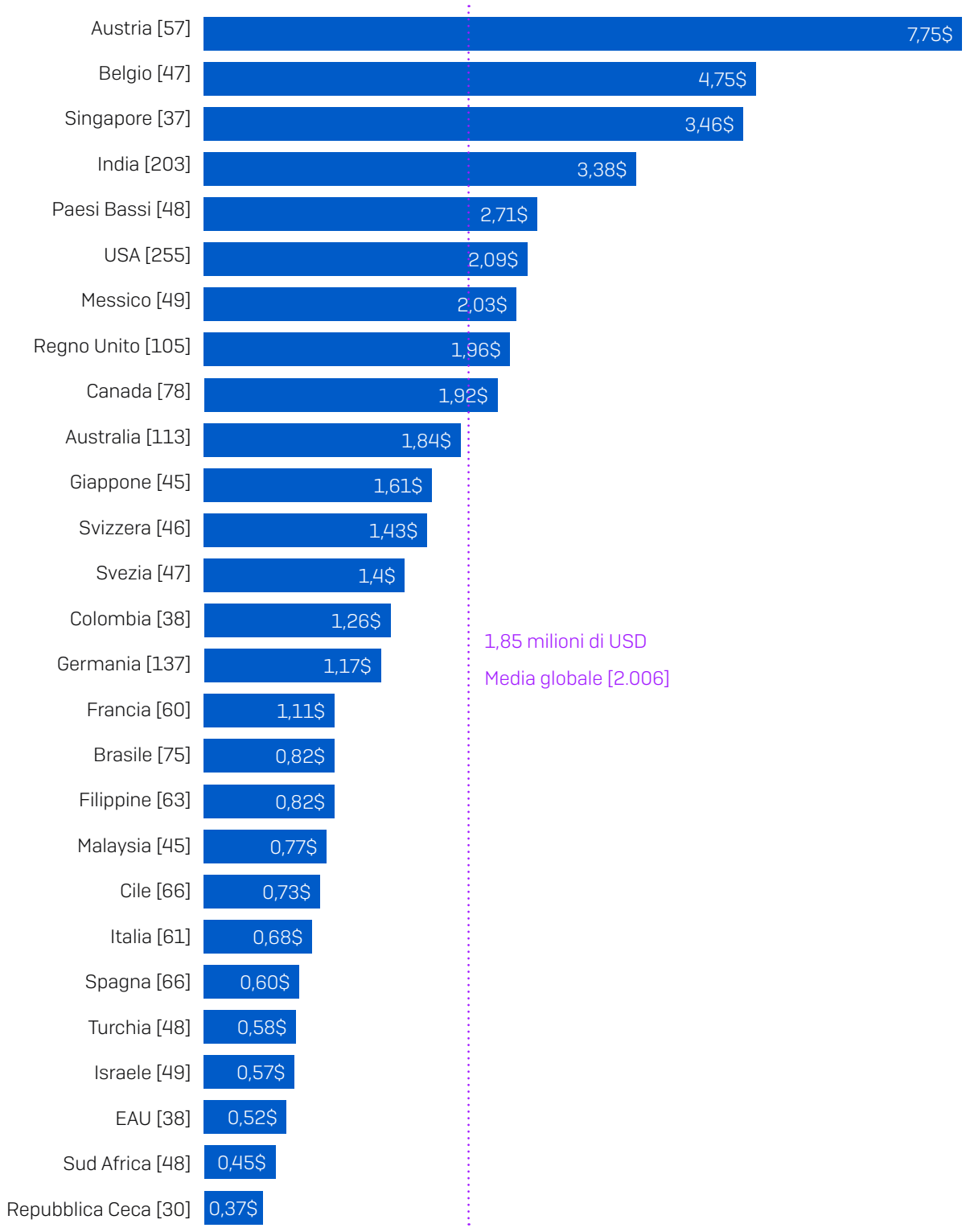
I partecipanti hanno dichiarato che la spesa media per rimediare all'impatto dell'attacco di ransomware più recente (considerando tempi di inattività, ore di lavoro del personale, costi associati a dispositivi e rete, perdita di opportunità commerciali, somma pagata per il riscatto) è pari a 1,85 milioni di USD, più del doppio rispetto ai 761.106 USD dell'anno precedente.


*Costo medio approssimativo sostenuto dalle organizzazioni per rimediare ai danni provocati dall'attacco di ransomware più recente (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi associati a dispositivi e rete, perdita di opportunità, riscatto versato, ecc.) [2021=2.006, 2020=2.538] partecipanti la cui organizzazione ha subito in attacco di ransomware l'anno scorso, suddivisione in base all'anno*

L'anno scorso, gli esperti di ransomware di Sophos hanno notato un incremento significativo nella quantità degli attacchi di ransomware avanzato che utilizzano la combinazione tra automazione e manualità con intervento umano.  Questi attacchi estremamente complessi richiedono processi di ripresa più complicati e questo potrebbe essere un fattore determinante per i costi necessari per rimediare ai danni del ransomware.

## I costi di riparazione dei danni variano in base alla posizione geografica

Osservando i costi di riparazione dei danni del ransomware in base ai paesi, si osservano variazioni notevoli.




*Costo medio approssimativo sostenuto dalle organizzazioni per rimediare ai danni provocati dall'attacco di ransomware più recente (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi associati a dispositivi e rete, perdita di opportunità, riscatto versato) [base di partecipanti indicata nel grafico] partecipanti la cui organizzazione ha subito in attacco di ransomware l'anno scorso, suddivisione in base al paese, in milioni di USD*

*Whitepaper Sophos. Aprile 2021*

L'Austria è il paese che si distingue per i più alti costi di riparazione dei danni causati dal ransomware. L'anno scorso si sono verificati diversi attacchi informatici che hanno colpito organizzazioni austriache di alto profilo. Stando alle informazioni fornite, il ministero degli affari esteri austriaco è stato colpito da hacker che colpiscono gli enti governativi: la gang di ransomware Netwalker, che ha comunicato su Twitter di aver rubato dati dall'amministrazione comunale della città austriaca di Weiz. Si noti che, anche escludendo l'Austria dai risultati, il costo medio di riparazione scende solo a 1,68 milioni di USD, comunque più del doppio rispetto all'anno precedente.

Generalmente, i paesi in cui gli stipendi sono più alti (Belgio, Singapore, Paesi Bassi e U.S.A.) registrano i costi complessivi più elevati, mentre i paesi dove gli stipendi sono più bassi (Repubblica Ceca, Sud Africa) presentano costi complessivi minori. Queste tendenze riflettono la fatica manuale richiesta per rimediare ai danni di un attacco. Il costo totale di riparazione dei danni di un attacco di ransomware è in realtà 10 volte superiore alla somma di riscatto richiesta.

Israele è tra i paesi con i costi di riparazione dei danni del ransomware più bassi, nonostante abbia un'economia sviluppata. Per motivi geopolitici, Israele è un bersaglio molto frequente per gli attacchi informatici (non solo di ransomware) e di conseguenza l'intero paese è caratterizzato da livelli elevati di cybersecurity, preparazione e competenze per la riparazione. L'insieme di questi fattori contribuisce a ridurre l'impatto finanziario di un attacco.

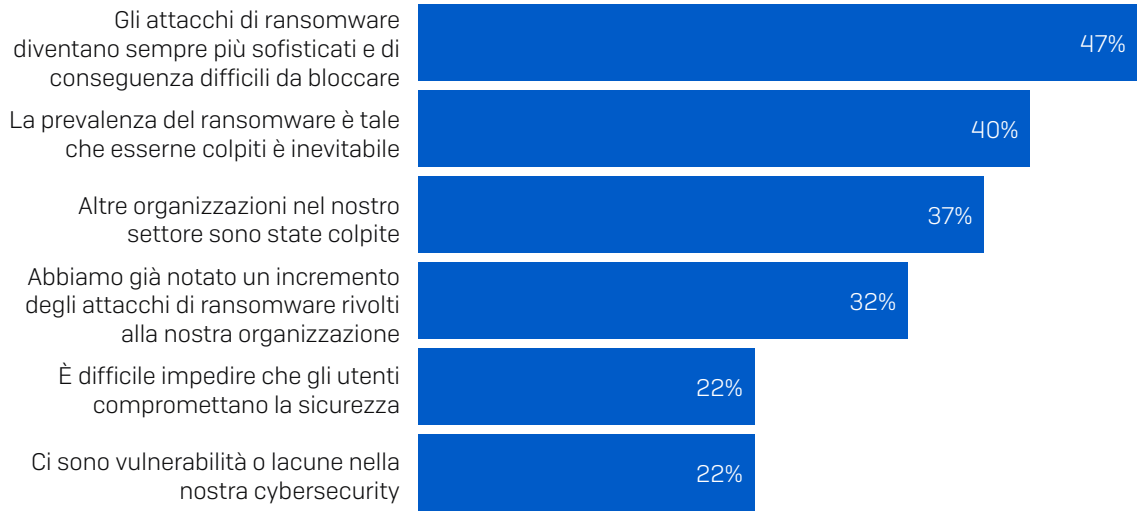
# Il futuro

## Le aspettative per il ransomware possono variare

Il 62% delle organizzazioni che hanno partecipato al sondaggio (3.353) ha dichiarato di non aver subito un attacco di ransomware l'anno scorso. All'interno di questo gruppo si osservano variazioni significative in termini di attitudine verso il ransomware e di fiducia nelle proprie capacità di affrontarlo. Il 65% dei partecipanti prevede che sarà colpito dal ransomware in futuro, mentre il 35% non si aspetta un attacco.

## I motivi per cui le organizzazioni prevedono che saranno colpite dal ransomware

Tra le 2.187 organizzazioni intervistate che non sono state colpite dal ransomware l'anno scorso, ma che ritengono che saranno attaccate in futuro, il motivo più comune per cui prevedono di subire un attacco è che "gli attacchi di ransomware diventano sempre più sofisticati e di conseguenza difficili da bloccare", menzionato dal 47% dei partecipanti in questo gruppo.



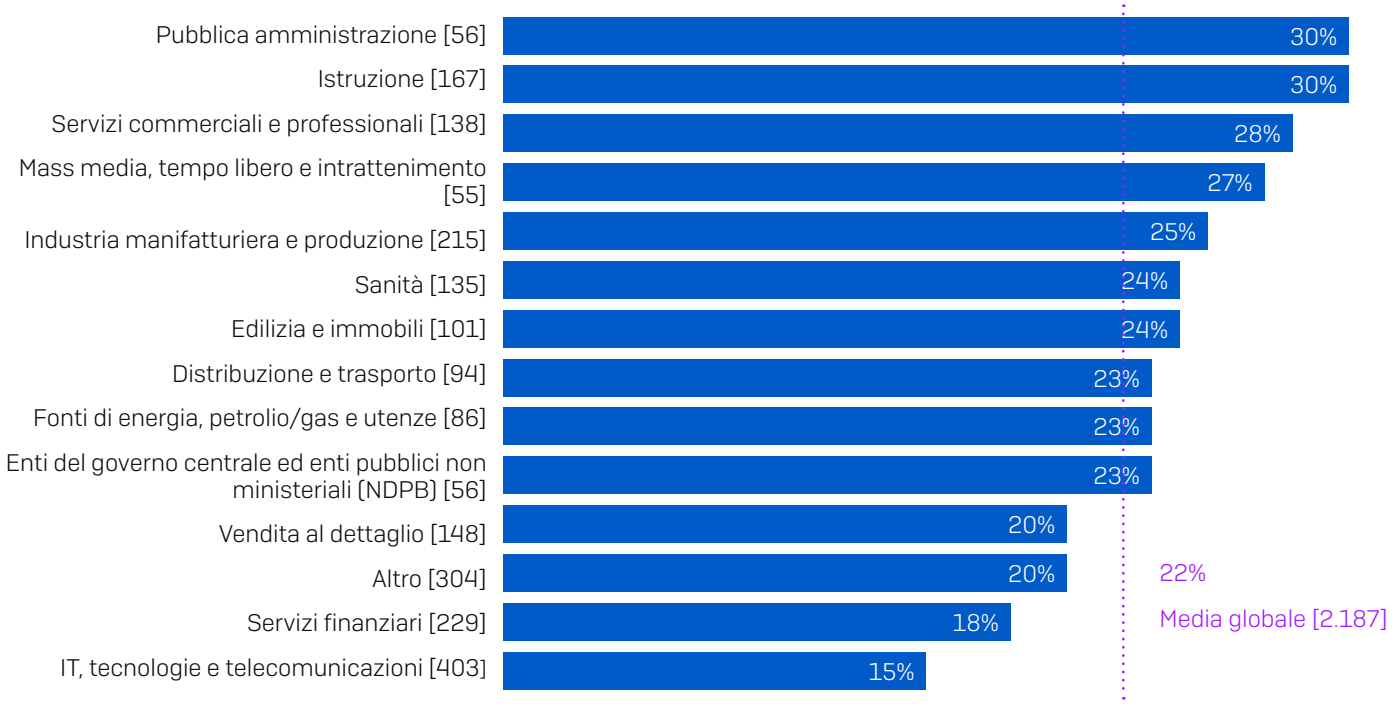

*Perché prevedete che la vostra organizzazione sarà colpita dal ransomware in futuro? [2.187] organizzazioni che non sono state colpite dal ransomware l'anno scorso ma che ritengono che ne cadranno vittima in futuro, alcune opzioni di risposta sono state omesse*

Sebbene si tratti di cifre molto alte, è sicuramente positivo che le organizzazioni siano consce della costante evoluzione del ransomware e questo potrebbe essere uno dei fattori che ha permesso loro di bloccare i potenziali attacchi di ransomware l'anno scorso.

Il 22% dei partecipanti identifica la compromissione della sicurezza da parte degli utenti come uno dei principali fattori di rischio legati a un potenziale attacco di ransomware in futuro. È certamente promettente osservare come, di fronte alla minaccia di hacker sempre più sofisticati, la maggior parte dei team tecnici abbia scelto di non dare semplicemente la colpa ai propri utenti.

Analogamente, il 22% ammette di avere vulnerabilità o lacune nella propria struttura di cybersecurity. Anche se naturalmente non è un bene che esistano lacune di sicurezza, riconoscere la presenza di questi problemi è un primo passo verso il potenziamento delle proprie difese.

Approfondendo ulteriormente le analisi, si nota che i settori della pubblica amministrazione e dell'istruzione sono quelli più propensi ad ammettere di avere lacune di sicurezza (30% ciascuno).




*Perché prevedete che la vostra organizzazione sarà colpita dal ransomware in futuro? Ci sono vulnerabilità o lacune nella nostra cybersecurity [base di partecipanti indicata nel grafico] organizzazioni che non sono state colpite dal ransomware l'anno scorso, ma che ritengono che ne cadranno vittima in futuro, alcune opzioni di risposta sono state omesse, suddivisione in base al settore*

Anche se le organizzazioni che hanno risposto a questa domanda non sono state direttamente colpite dal ransomware l'anno scorso, è probabile che siano state influenzate dalle esperienze in materia di ransomware di altre aziende nei loro settori:

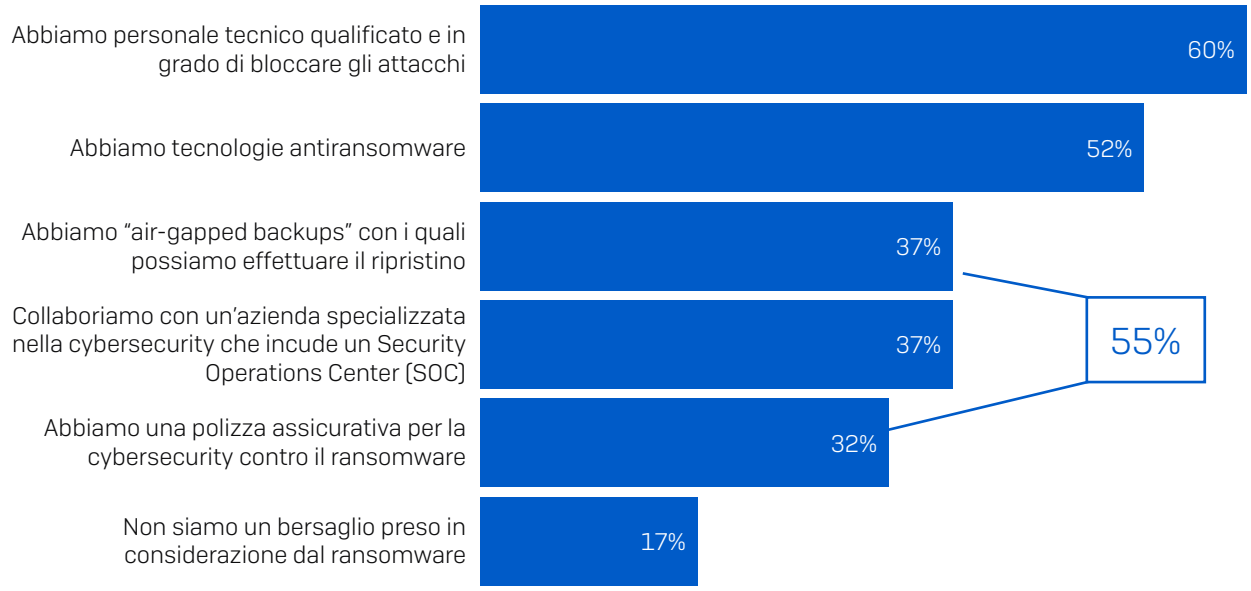
- **La pubblica amministrazione** è il settore con la maggiore probabilità che un hacker riesca a cifrare i dati della vittima
- **L'istruzione** (a pari merito con la vendita al dettaglio) è il settore che ha registrato la percentuale più alta di organizzazioni colpite dal ransomware l'anno scorso

Inoltre, entrambi i settori devono affrontare il problema della mancanza di fondi da dedicare alle tecnologie e alle risorse informatiche, il che causa la presenza di lacune di sicurezza.

**IT, telecomunicazioni e tecnologie** (15%) e **servizi finanziari** (18%) hanno invece la percentuale più bassa di lacune di sicurezza, secondo i dati forniti dai partecipanti. Si tratta di settori che sono generalmente pronti ad adottare rapidamente nuove tecnologie e che possono contare su budget più elevati; di conseguenza, hanno anche maggiori opportunità di correggere eventuali punti deboli.

## La presenza di personale tecnico qualificato aumenta la sicurezza di poter contrastare il ransomware

1.166 partecipanti dichiarano di non essere stati colpiti dal ransomware l'anno scorso e non prevedono di subire un attacco in futuro. Il motivo principale alla base di questa sicurezza è la presenza di personale tecnico qualificato e in grado di bloccare gli attacchi.




*Perché prevedete che la vostra organizzazione non sarà colpita dal ransomware in futuro? [1.166] organizzazioni che non sono state colpite dal ransomware l'anno scorso e che ritengono che non ne cadranno vittima in futuro, alcune opzioni di risposta sono state omesse*

Anche se la presenza di tecnologie avanzate e automatizzate è essenziale per l'efficacia di un sistema di difesa antiransomware, per bloccare gli attacchi manuali occorre anche un monitoraggio coordinato da una mente umana, nonché l'intervento di professionisti dotati di competenze adeguate. Sia che ci si affidi a dipendenti aziendali o a professionisti esterni, gli esperti hanno competenze esclusive che li rendono in grado di identificare eventuali segnali che indicano la presenza di hacker pronti a sferrare un attacco di ransomware al momento giusto.

Il 37% delle organizzazioni che ritengono che non saranno colpite dal ransomware collaborano con un'azienda specializzata nella cybersecurity che include un Security Operations Center (SOC). Solo pochi anni fa, i SOC erano presenti solamente nelle imprese più grandi, per cui questo rappresenta un cambiamento radicale nella fornitura dei servizi di cybersecurity per le organizzazioni di medie dimensioni.

Ma non ci sono solo buone notizie. Alcuni dei risultati sono preoccupanti:

- Il 55% degli intervistati, che ritengono che non saranno colpiti da un attacco, adottano approcci che non offrono alcuna protezione contro il ransomware:
  - Il 37% dei partecipanti al sondaggio è convinto che non cadrà vittima del ransomware perché ha "air-gapped backups'". Come abbiamo osservato, i backup sono strumenti importanti per ripristinare i dati dopo un attacco, ma non offrono prevenzione.
  - Il 32% degli intervistati sostiene di essere protetto contro il ransomware perché ha una polizza assicurativa per la cybersecurity. Anche in questo caso, una polizza assicurativa può aiutare a risolvere le conseguenze di un attacco, ma non a prevenirlo.

**Nota: alcuni dei partecipanti hanno selezionato entrambe le opzioni, il 55% ha selezionato almeno una di queste due opzioni.**

- Inoltre, il 17% dei partecipanti sostiene di non essere un bersaglio preso in considerazione dal ransomware. Purtroppo, questa affermazione non è vera. Nessuna organizzazione è al sicuro.

## I piani di emergenza in caso di attacco di malware sono uno standard essenziale

Rispondere a un attacco informatico critico può essere estremamente stressante. Sebbene non esista un rimedio in grado di alleviare lo stress derivato dal dover affrontare un attacco, la presenza di un piano di emergenza efficace è un metodo infallibile per ridurne l'impatto.

È promettente osservare che il 90% degli intervistati dichiara che la propria organizzazione ha un piano di emergenza in caso di attacco di malware. Tra questi, poco più della metà (51%) ha realizzato un piano dettagliato e il 39% un piano parzialmente sviluppato.

I piani di emergenza in caso di malware sono simili a quelli progettati per affrontare i disastri naturali: in entrambi i casi devono permettere di ripartire da zero. Le Filippine, una nazione frequentemente colpita da inondazioni e terremoti, è il paese più preparato in caso di incidenti di malware, con l'83% dei partecipanti che dichiara di avere un piano di emergenza completo e dettagliato in caso di malware.

## Quello della pubblica amministrazione è il settore meno preparato a rispondere a un attacco di malware

Nella maggior parte dei casi, le organizzazioni appartenenti ai vari settori sono adeguatamente preparate ad avviare un ripristino dei sistemi dopo un incidente di malware. Tuttavia, è emerso che gli enti governativi sono quelli maggiormente caratterizzati da una mancanza di preparazione: solo il 73% delle organizzazioni della **pubblica amministrazione** e l'81% degli **enti governativi e pubblici** hanno un piano di emergenza in caso di attacco di malware.

Sono statistiche preoccupanti, poiché questi settori sono tra quelli più colpiti dal ransomware: la pubblica amministrazione è il settore con maggiore probabilità di cadere vittima di un attacco di cifratura non autorizzata dei dati, mentre gli enti governativi e pubblici hanno probabilità più elevate di subire attacchi di estorsione.

L'assenza di un piano di emergenza in caso di malware potrebbe essere uno dei fattori alla base dei risultati che vedono la pubblica amministrazione al secondo posto nella classifica dei settori con maggiore probabilità di pagare il riscatto richiesto.

# Raccomandazioni

Alla luce di questi risultati, gli esperti di Sophos consigliano di seguire alcune Best Practice:

1. **Presumere di essere colpiti.** Il ransomware è tutt'ora una minaccia molto pericolosa e diffusa. Nessun settore, nessun paese e nessun tipo di organizzazione è immune al rischio. È meglio essere preparati e non subire un attacco, piuttosto che il contrario.

2. **Effettuare i backup.** I backup sono il metodo più sicuro con il quale le organizzazioni riescono a recuperare i dati dopo un attacco. Come abbiamo visto, anche se si paga il riscatto non è garantito che sarà possibile recuperare tutti i dati, per cui i backup sono essenziali in ogni caso.

3. **Implementare una protezione a livelli multipli.** Di fronte al notevole incremento degli attacchi basati sull'estorsione, è ora più importante che mai assicurarsi che gli hacker non riescano a infiltrarsi nell'ambiente informatico dell'organizzazione. Occorre utilizzare una protezione a livelli multipli per bloccare i cybercriminali ovunque possibile all'interno dell'ambiente

4. **Utilizzare una combinazione tra competenze umane e tecnologie antiransomware.** Per bloccare il ransomware, occorre una difesa in profondità che sia il risultato della combinazione tra tecnologie antiransomware dedicate e threat hunting con supervisione umana. Le tecnologie offrono la scalabilità e i livelli di automazione necessari, mentre gli esperti sono in grado di individuare tattiche, tecniche e procedure che indicano che un hacker molto abile sta cercando di infiltrarsi nell'ambiente informatico. Chi non ha alle dipendenze personale dotato competenze tecniche adeguate può avvalersi dei servizi di un'azienda specializzata nella cybersecurity: i SOC sono ora un'opzione alla portata delle organizzazioni di qualsiasi dimensione.

5. **Evitare di pagare il riscatto.** Sappiamo quanto sia facile a dirsi, ma tutt'altro che semplice da mettere in pratica quando un'organizzazione rimane completamente bloccata per colpa di un attacco di ransomware. Indipendentemente dalle potenziali considerazioni etiche, pagare il ransomware è un modo inefficace per recuperare i dati. Se decidete di pagare il riscatto, non dimenticate di includere un'analisi costi-benefici che tenga conto della previsione che gli hacker ripristineranno, in media, solo due terzi dei file.

6. **Realizzare un piano di emergenza in caso di malware.** Il modo migliore per impedire che un attacco informatico diventi un vero e proprio caso di violazione è prepararsi in anticipo. Spesso le organizzazioni che cadono vittima di un attacco si rendono conto che avrebbero potuto evitare tutti i costi, i problemi e i disagi subiti, se solo avessero avuto un piano strategico di risposta.

## Ulteriori risorse

La Guida Alla Incident Response di Sophos aiuta le organizzazioni a definire il quadro strutturale per la strategia di risposta agli incidenti di cybersecurity ed esplora i 10 passaggi principali da includere.

Ai responsabili IT potrebbero interessare anche i Quattro Suggerimenti Chiave Per Gestire Al Meglio l'Incident Response, che mettono in evidenza le lezioni che tutti dovrebbero apprendere per poter rispondere adeguatamente agli incidenti di sicurezza.

Entrambe le risorse si basano sull'esperienza maturata sul campo dal nostro team Sophos di Managed Threat Response e di Rapid Response, che sono intervenuti e hanno risolto migliaia di incidenti di cybersecurity.

Scoprite di più sul ransomware e su come Sophos può aiutarvi a proteggere la vostra 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.


19/04/2021 (SB-NP)

SOPHOS