SOPHOS

LA VERA STORIA DEL RANSOMWARE

I risultati di uno studio indipendente condotto tra 5.000 responsabili IT in 26 paesi

White paper Sophos maggio 2020

Introduzione

Nelle notizie di IT security continuano a comparire storie di organizzazioni messe in ginocchio dal ransomware e le richieste di riscatto a sette cifre non sono una rarità. Ma si può affermare che questi articoli forniscano un quadro completo della realtà?

Per capire cosa si nasconde dietro a questi titoli, Sophos ha sponsorizzato un sondaggio indipendente a cui hanno partecipato 5.000 responsabili IT in 26 paesi. Dai risultati emergono nuovi approfondimenti su quello che accade veramente quando il ransomware colpisce le vittime. Questo studio rivela la percentuale di attacchi che riescono a cifrare i dati, il numero delle vittime che pagano il riscatto, l'impatto dei pagamenti dei riscatti sui costi di disinfezione totali, nonché il ruolo svolto dalle assicurazioni per la cybersecurity. Preparatevi a rimanere meravigliati.

Informazioni sul sondaggio

Sophos ha incaricato l'azienda Vanson Bourne, specializzata nelle ricerca, di intervistare 5.000 responsabili IT, per scoprire di più sulle loro esperienze con il ransomware. Sophos non è intervenuta in alcun modo nella selezione dei partecipanti e tutte le risposte sono state fornite in maniera anonima. Il sondaggio è stato svolto nei mesi di gennaio e febbraio 2020.

I partecipanti erano situati in 26 paesi e 6 continenti:

PAESE	NUM. PARTECIPANTI
Australia	200
Belgio	100
Brasile	200
Canada	200
Cina	200
Colombia	200
Repubblica Ceca	100
Francia	300
Germania	300
India	300
Italia	200
Giappone	200
Malaysia	100

PAESE	NUM. PARTECIPANTI
Messico	200
Paesi Bassi	200
Nigeria	100
Filippine	100
Polonia	100
Singapore	200
Sud Africa	200
Spagna	200
Svezia	100
Turchia	100
EAU	100
Regno Unito	300
Stati Uniti	500

In ciascun paese, il 50% dei partecipanti faceva parte di organizzazioni con un numero di dipendenti compreso tra 100 e 1.000, mentre il restante 50% si trovava in organizzazioni con 1.001-5.000 dipendenti. I partecipanti appartenevano a vari settori diversi, sia pubblici che privati.

SETTORE	NUM. PARTECIPANTI	% PARTECIPANTI
Tecnologie IT e telecomunicazioni	979	20%
Vendita al dettaglio, distribuzione e trasporto	666	13%
Industria manifatturiera e produzione	648	13%
Servizi finanziari	547	11%
Settore pubblico	498	10%
Servizi commerciali e professionali	480	10%
Edilizia e immobili	272	5%
Fonti di energia, petrolio/gas e utenze	204	4%
Mass media, tempo libero e intrattenimento	164	3%
Altro	542	11%

Riepilogo

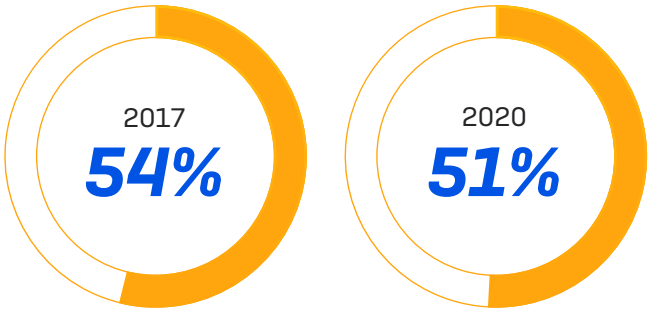
Il sondaggio offre nuovi approfondimenti sulle esperienze delle organizzazioni che sono state colpite dal ransomware. Sono emerse le seguenti informazioni:

- **Quasi tre quarti degli attacchi di ransomware sono riusciti a cifrare i dati.** Il 51% delle organizzazioni è stato colpito dal ransomware negli ultimi 12 mesi. Per questi attacchi, i cybercriminali sono riusciti a cifrare i dati nel 73% dei casi.
- **Il 26% delle vittime del ransomware ha recuperato i dati pagando il riscatto.** Un ulteriore 1% ha pagato il riscatto ma non è riuscito a recuperare i dati.
- **Il 94% delle organizzazioni che sono cadute vittima della cifratura non autorizzata dei dati ha recuperato le informazioni.** Il recupero è avvenuto principalmente tramite backup, con una percentuale doppia (56%) rispetto al recupero tramite pagamento del riscatto (26%).
- **Pagare il riscatto raddoppia i costi di un attacco di ransomware.** Il costo medio delle operazioni necessarie per rimediare all'impatto dell'attacco di ransomware più recente (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali, somma pagata per il riscatto ecc.) ammonta a 732.520 $ per le organizzazioni che non pagano il riscatto e raggiunge la somma di 1.448.458 $ per le organizzazioni che decidono di pagarlo.
- **Nonostante le notizie in primo piano, il settore pubblico è meno colpito di quello privato.** Il 45% delle organizzazioni del settore pubblico è stato colpito dal ransomware l'anno scorso. La media globale è del 51%, con un picco del 60% per i mass media e i settori dell'intrattenimento e del tempo libero.
- **Un'organizzazione su cinque presenta gravi lacune in termini di assicurazione per la cybersecurity.** L'84% dei partecipanti ha stipulato una polizza assicurativa per la cybersecurity, ma solo nel 64% dei casi è incluso anche il ransomware.
- **È l'assicurazione per la cybersecurity a pagare il riscatto.** Nelle organizzazioni assicurate contro il ransomware, il 94% dei pagamenti di un riscatto per ottenere la restituzione dei dati viene effettuato dalla società di assicurazione.
- **Gli attacchi con maggiore possibilità di successo includono dati nel cloud pubblico.** Nel 59% dei casi, i dati che sono stati cifrati in maniera non autorizzata si trovavano nel cloud pubblico. Sebbene sia probabile che gli intervistati abbiano interpretato in modo più ampio il concetto di cloud pubblico, includendo anche servizi basati sul cloud come Google Drive e Dropbox e opzioni di backup nel cloud come Veeam, è evidente che i cybercriminali tendono ad attaccare i dati, indipendentemente da dove siano archiviati.

Parte 1: la prevalenza del ransomware

L'anno scorso, la metà delle organizzazioni è stata colpita dal ransomware

Il 51% dei partecipanti ha confermato di aver subito un attacco di ransomware negli ultimi 12 mesi. Le organizzazioni hanno registrato un leggero calo nel numero di attacchi rispetto agli anni precedenti. In un sondaggio di alcuni anni fa, sponsorizzato da Sophos e pubblicato nel 2017 (dimensioni del campione: 1.700 organizzazioni), la percentuale degli intervistati che erano stati colpiti dal ransomware nei 12 mesi precedenti era pari al 54%.



La vostra organizzazione è stata colpita dal ransomware negli ultimi 12 mesi? Base: 5.000 partecipanti (2020), 1.700 partecipanti (2017).

Sebbene sia ben accetto, questo calo è probabilmente dovuto a un cambiamento delle tattiche dei cybercriminali, piuttosto che a una minore diffusione del ransomware. Dai dati raccolti dai SophosLabs nel 2017 era emerso che il ransomware per desktop del mercato di massa (che tendeva ad agire "sparando alla cieca") era molto comune. Questo tipo di attacco veniva sferrato in maniera estesa e indiscriminata, pertanto il numero di organizzazioni colpite risultava elevato.

Nel 2020 la tendenza predominante sono gli attacchi basati su server. Si tratta di attacchi estremamente mirati e sofisticati, che richiedono un impegno notevole per essere implementati, e questo spiega la riduzione del numero di attacchi. Tipicamente sono però molto più pericolosi, perché puntano a cifrare le risorse di maggior valore che, se compromesse, possono mettere in ginocchio le aziende colpite, con richieste di riscatto che ammontano a vari milioni di dollari.

Nelle domande successive, se l'organizzazione intervistata aveva subito attacchi di ransomware multipli nell'anno precedente, abbiamo chiesto di fornire risposte basate *solamente sull'attacco più significativo degli ultimi 12 mesi.*

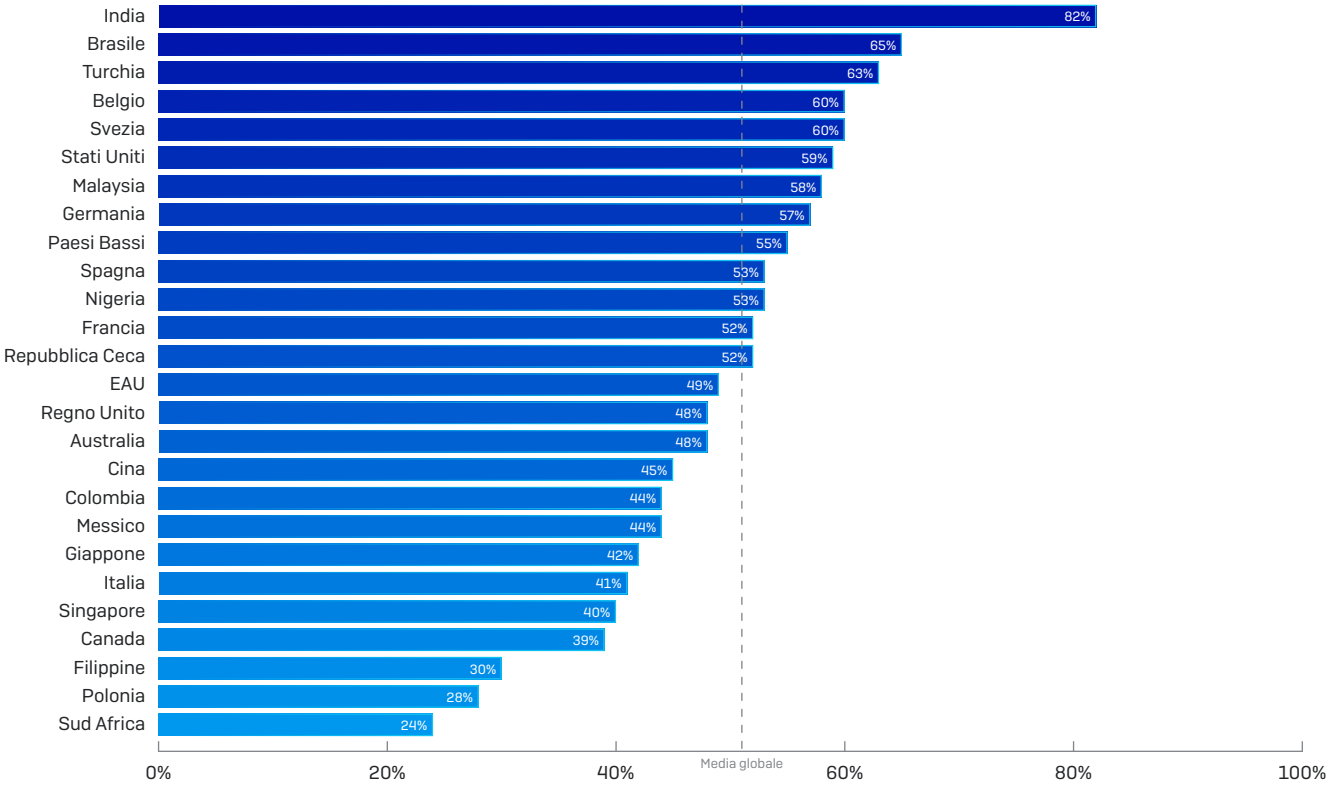
Le dimensioni non contano

Osservando le dimensioni delle organizzazioni, si nota una differenza minima nelle percentuali di attacco del ransomware. Le organizzazioni di piccole dimensioni (100-1.000 dipendenti) che sono state colpite erano poco meno della metà (47%), mentre quelle di dimensioni più estese (1.001-5.000 di dipendenti) erano poco più della metà (54%).

I livelli di attacco variano da paese a paese

L'analisi delle statistiche relative agli attacchi di ransomware a livello globale rivela variazioni interessanti. Con molta probabilità, questo è dovuto al fatto che i criminali dedicano maggiore impegno alle opportunità che considerano più favorevoli; inoltre i livelli di protezione contro il ransomware variano a seconda del paese.

Percentuale delle organizzazioni colpite dal ransomware negli ultimi 12 mesi



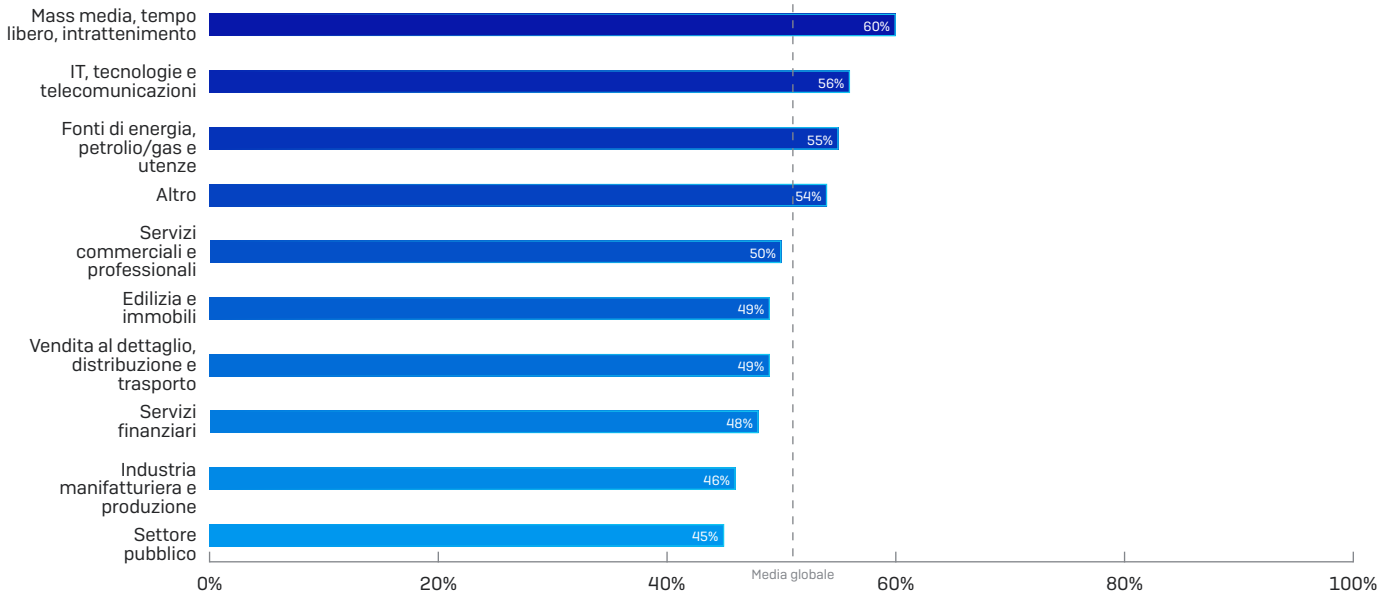
La vostra organizzazione è stata colpita dal ransomware negli ultimi 12 mesi? Base: 5.000 partecipanti.

- **L'India** (300 intervistati) è il paese maggiormente colpito, con l'82% delle organizzazioni che dichiara di aver subito un attacco di ransomware negli ultimi 12 mesi. Questa statistica non sorprende. La sicurezza informatica in India è generalmente molto debole e le tecnologie illegali abbondano. Questo scenario favorisce la presenza di vulnerabilità nelle difese informatiche, indebolendo le organizzazioni di fronte agli attacchi.
- **Filippine, Polonia e Sud Africa** segnalano i minori livelli di attacchi informatici. Come già indicato, i cybercriminali hanno cambiato tattica e adesso, invece di "sparare alla cieca" con attacchi di ransomware per desktop indiscriminati, utilizzano attacchi più mirati e basati su server, che colpiscono una quantità minore di organizzazioni ma esigono riscatti più elevati. I loro obiettivi si trovano in paesi che presentano maggiori opportunità di lucro. I tre paesi meno colpiti hanno un PIL inferiore a molti dei paesi che occupano posizioni più alte in questa classifica, e questo potrebbe spiegare perché tendono a essere maggiormente ignorati dai cybercriminali.
- Il passaggio da attacchi che "sparano alla cieca" ad attacchi mirati, rivolti a bersagli con maggiore opportunità di lucro ha contribuito ampiamente al calo degli attacchi di ransomware in **Sud Africa**. Nel nostro sondaggio precedente (2017), il 54% degli intervistati dichiarava di essere stato colpito dal ransomware nei 12 mesi precedenti, ma questa statistica è ora scesa al 24%, con una diminuzione di più del 50%.
- **In Canada** (200 partecipanti) si sono inaspettatamente registrati pochi attacchi di ransomware. Un paese occidentale economicamente avanzato come il Canada dovrebbe essere considerato un bersaglio che presenta ampie opportunità di lucro, eppure solo il 39% degli intervistati dichiara di essere stato colpito dal ransomware. La differenza è di ben 20 punti percentuali rispetto al paese confinante degli Stati Uniti, dove il ransomware è stato riscontrato dal 59% dei partecipanti. Una possibile spiegazione potrebbe essere il vantaggio di vivere all'ombra degli USA, per quanto riguarda gli attacchi. Allo stesso tempo, i partecipanti situati in Canada si sono dimostrati consci del problema, nonché preparati ad affrontarlo: il 68% delle organizzazioni che non sono state colpite dal ransomware prevede attacchi futuri.

Il settore pubblico è quello meno colpito dagli attacchi di ransomware

Sì, avete letto bene: il settore pubblico ha riscontrato meno attacchi rispetto a tutti gli altri. Sono infatti mass media, intrattenimento e tempo libero i settori che segnalano i livelli di attacco più elevati (60%), seguiti da IT, tecnologie e telecomunicazioni (56%).

Percentuale delle organizzazioni colpite dal ransomware negli ultimi 12 mesi



La vostra organizzazione è stata colpita dal ransomware negli ultimi 12 mesi? Base: 5.000 partecipanti.

A prima vista queste statistiche possono sorprendere: nei notiziari si continuano a vedere storie di ospedali ed enti pubblici minacciati dalle richieste di riscatto dei cybercriminali. Tuttavia, dal sondaggio emerge che queste notizie rappresentano una realtà distorta.

In molti paesi le organizzazioni del settore pubblico hanno l'obbligo legale di segnalare gli attacchi di ransomware. Tuttavia è raro che il settore privato debba attenersi a tali disposizioni, pertanto può decidere di non segnalare eventuali attacchi; questa strategia è probabilmente dovuta al desiderio di non suscitare preoccupazioni tra i clienti, di prevenire danni alla reputazione e di evitare di essere considerati un bersaglio facile da altri cybercriminali.

La veridicità dei risultati è confermata dalla ricerca svolta da Sophos sul ransomware SamSam. Sophos, in collaborazione con Neutrino (un'organizzazione esperta nel monitoraggio delle criptovalute), ha seguito la pista del denaro, identificando vari pagamenti e vittime di cui precedentemente non si sapeva nulla. In base al presupposto che vi sia un numero ancora più elevato di vittime ignote, sembrerebbe che sia stato il settore privato a subire maggiormente l'impatto di SamSam.

Parte 2: l'impatto del ransomware

Tre quarti degli attacchi di ransomware riescono a cifrare i dati

Tradizionalmente, il successo degli attacchi di ransomware viene valutato in base a tre elementi principali: la cifratura dei dati, la ricezione del pagamento e la decifrazione dei dati. In quasi tre quarti (73%) degli attacchi di ransomware, i cybercriminali sono riusciti a cifrare i dati.

Tuttavia, un dato rassicurante è che in poco meno di un quarto (24%) dei casi l'attacco è stato bloccato prima che i dati potessero essere cifrati. Sembrerebbe che le tecnologie antiransomware stiano cominciando a incidere sul tasso di successo degli attacchi di ransomware.

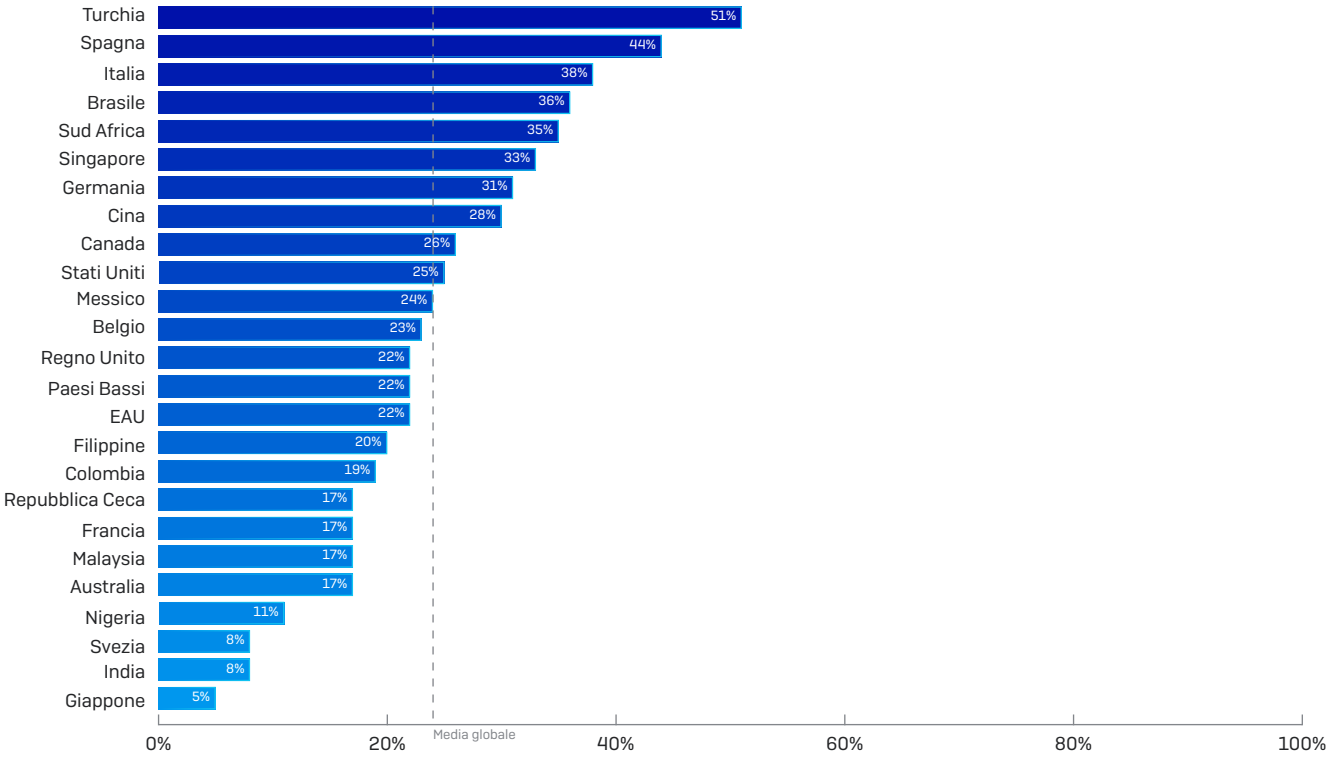
Un dato interessante emerso dal sondaggio è che il 3% delle organizzazioni ha dichiarato di aver ricevuto richieste di riscatto anche senza che i loro dati fossero stati cifrati. Questo tipo di attacco si è rivelato predominante in particolar modo in Nigeria, Colombia, Sud Africa, Cina, Polonia, Belgio e nelle Filippine.

Si potrebbe argomentare che in realtà si tratti di estorsione, piuttosto che di ransomware. Definizioni a parte, il concetto più importante è che ci troviamo comunque di fronte a un vettore di attacco da monitorare attentamente, in quanto i criminali sono sempre alla ricerca di nuovi modi per arricchirsi, senza dover fare lo sforzo di cifrare e decifrare file.

In Giappone gli attacchi hanno maggiore probabilità di andare a segno

Analizzando le statistiche in base ai paesi, il Giappone è quello che ha mostrato la minore capacità di bloccare gli attacchi in quanto nel 95% dei casi i tentativi di cifratura dei dati sono andati a segno. Una tendenza opposta si è osservata invece in Turchia, dove la metà degli attacchi (51%) è stata bloccata prima che i dati venissero cifrati. Questa variazione a livello globale potrebbe essere dovuta a motivi diversi, inclusi livelli non omogenei di consapevolezza sulla prevalenza del ransomware e sulla probabilità di esserne colpiti; questa tendenza potrebbe, a sua volta, causare un'eterogeneità nell'efficacia della protezione antiransomware.

Percentuale di attacchi bloccati prima che i dati venissero cifrati

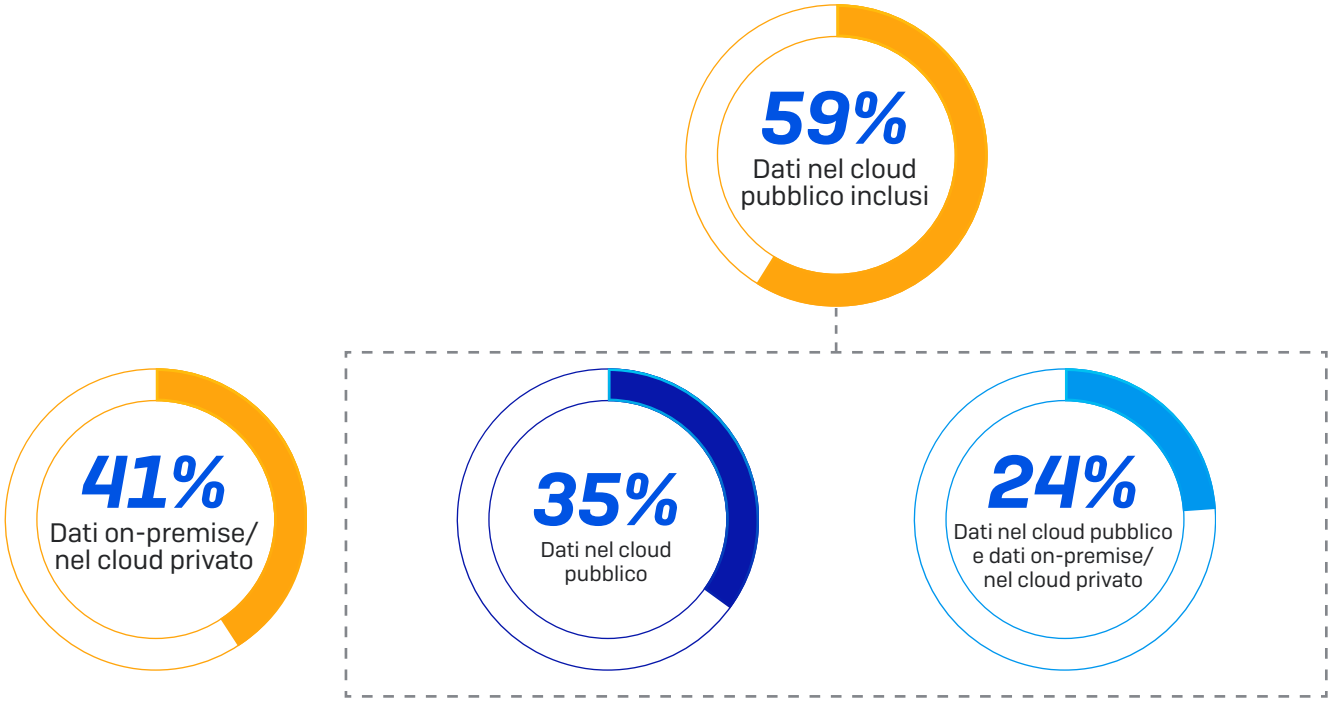


Percentuale degli intervistati che hanno risposto "No,l'attacco è stato bloccato prima che i dati potessero essere cifrati" alla domanda: Nell'attacco di ransomware più grave, i cybercriminali sono riusciti a cifrare i dati dell'organizzazione? Domanda rivolta solamente ai partecipanti la cui organizzazione aveva subito un attacco di ransomware nei 12 mesi precedenti. Base: 2.538 partecipanti.

La Polonia non è stata inclusa in questo grafico, in quanto presentava una base di partecipanti inferiore a 30; lo stesso vale per le Filippine, la cui base era di soli 30 partecipanti.

I dati nel cloud pubblico sono un obiettivo dominante

Al 73% degli intervistati che hanno dichiarato di aver subito la cifratura dei propri dati nell'attacco di ransomware più recente abbiamo chiesto quali dati sono stati cifrati. Il 41% ha risposto che i dati cifrati erano archiviati localmente e/o in un cloud privato, mentre il 35% ha dichiarato che si trattava solamente di dati nel cloud pubblico. Il 24% ha risposto che i dati erano situati in una combinazione delle due opzioni. Facendo le dovute somme, si deduce che quasi sei attacchi su 10 (59%) che sono andati a segno includevano dati nel cloud pubblico.



Nell'attacco di ransomware più grave, i cybercriminali sono riusciti a cifrare i dati dell'organizzazione? Risposte dei partecipanti la cui organizzazione ha subito la cifratura non autorizzata dei dati nell'attacco di ransomware più recente. Base: 1.849 partecipanti.

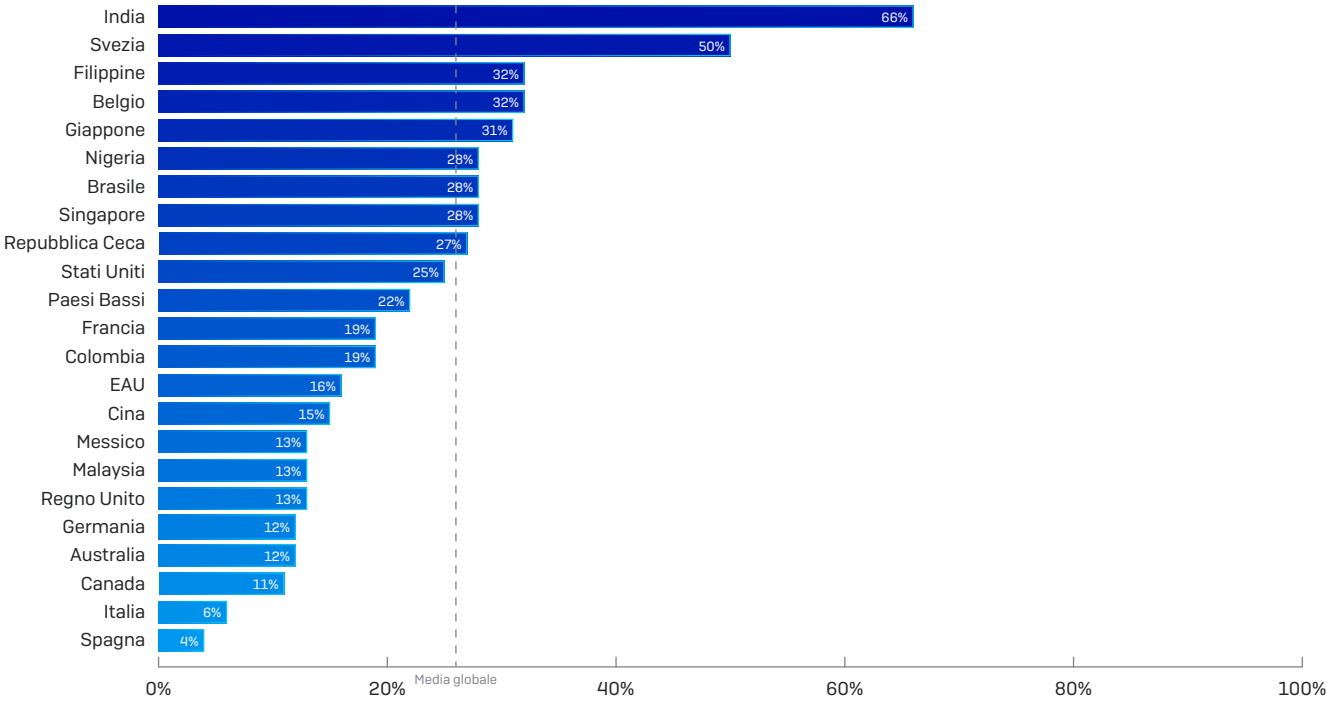
Una premessa: è probabile che gli intervistati abbiano interpretato in modo più ampio il concetto di cloud pubblico, includendo anche servizi basati sul cloud come Google Drive e Dropbox e opzioni per il backup nel cloud come Veeam, piuttosto che considerare solamente AWS, Azure e servizi cloud come Alibaba. Ciononostante, la conclusione più importante è che nessun tipo di dati è al sicuro e che pertanto occorre verificare che i dati archiviati nel cloud siano protetti con lo stesso livello di sicurezza di quelli che si trovano nelle strutture locali.

Il 26% delle vittime del ransomware ha recuperato i dati pagando il riscatto

Il 26% delle organizzazioni che hanno subito la cifratura dei dati li ha recuperati pagando il riscatto. Un ulteriore 1% delle organizzazioni che hanno subito la cifratura dei dati ha pagato il riscatto ma non è riuscito a recuperare i dati. Di conseguenza, nel 95% dei casi le organizzazioni che hanno pagato il riscatto sono riuscite a ripristinare i dati (473 delle 496 organizzazioni che avevano pagato il riscatto).

La tendenza a pagare o meno il riscatto presenta visibili variazioni regionali. In India due organizzazioni su tre (66%) hanno pagato il riscatto per recuperare i dati, mentre il 29% ha utilizzato i propri backup. La Spagna mostra una tendenza opposta, in quanto il riscatto è stato pagato solo nel 4% dei casi, mentre il 72% delle vittime ha ripristinato i dati dai backup.

Percentuale delle organizzazioni che hanno pagato il riscatto



Percentuale degli intervistati che hanno risposto "Sì, abbiamo pagato il riscatto" alla domanda: Nell'attacco di ransomware più grave, l'organizzazione ha recuperato i dati? Domanda rivolta solamente ai partecipanti la cui organizzazione aveva subito un attacco di ransomware nel quale i dati sono stati cifrati. Base: 1.849 partecipanti.

Nota: il grafico non include Filippine, Sud Africa, Polonia e Turchia, poiché per questa domanda le basi di partecipanti di questi paesi erano pari o inferiori a 30.

Nel 94% dei casi, le organizzazioni riescono a recuperare i dati

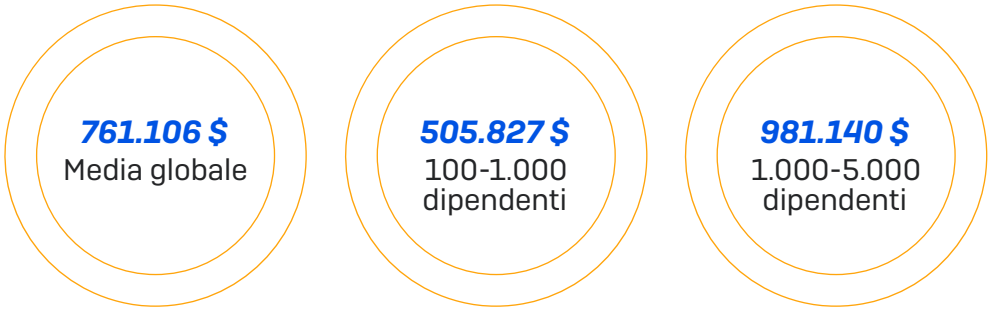
Sebbene nel 73% degli attacchi di ransomware i dati siano stati cifrati, la buona notizia è che nel 94% dei casi le organizzazioni colpite sono riuscite a recuperare i dati.

Come abbiamo visto, il 26% delle vittime ha recuperato i dati pagando il riscatto. Tuttavia, più del doppio di questa percentuale (56%) ha ripristinato i dati dai propri backup. Il restante 12% ha dichiarato di aver recuperato i dati in modi diversi.

Le dimensioni dell'organizzazione influiscono sui costi di riparazione dei danni

Come prevedibile, il sondaggio ha confermato che i costi di riparazione dei danni causati da un attacco di ransomware sono più elevati per le organizzazioni più grandi.

Costo medio delle attività di riparazione dei danni di un attacco di ransomware



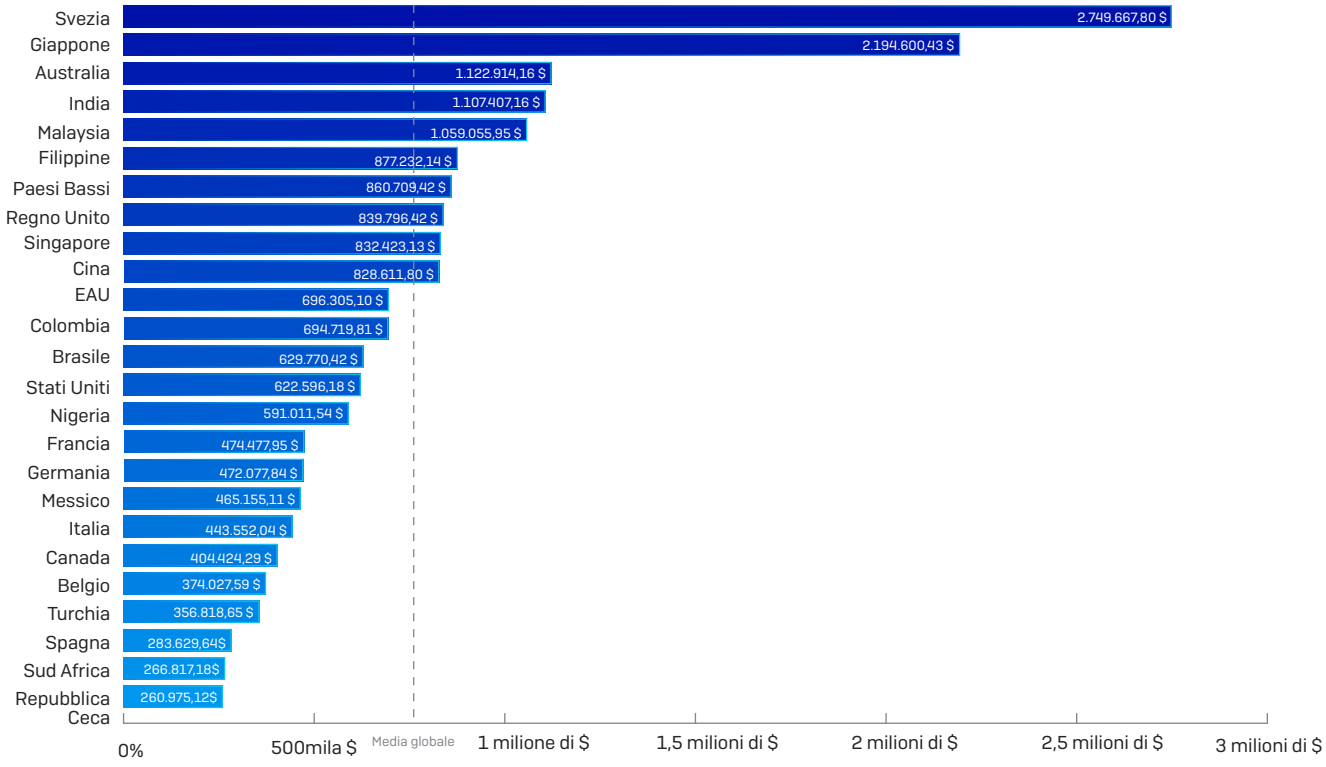
Qual è stato approssimativamente il costo sostenuto dall'organizzazione per rimediare ai danni provocati dall'attacco di ransomware più recente (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali, somma pagata per il riscatto ecc.)? Domanda rivolta solamente ai partecipanti la cui organizzazione aveva subito un attacco di ransomware nei 12 mesi precedenti. Base: 2.538 partecipanti.

Il costo medio sostenuto dall'organizzazione per rimediare ai danni provocati dall'attacco di ransomware più recente (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali, somma pagata per il riscatto ecc.) è pari a 761.106 $. Per le organizzazioni con un numero di dipendenti compreso tra 100 e 1.001 il costo medio è stato di 505.827 $, mentre per quelle con 1.001-5.000 dipendenti il costo medio ha raggiunto i 981.140 $.

L'impatto finanziario del ransomware varia a seconda del paese

Il fatto più sorprendente, tuttavia, è la variazione dei costi di riparazione dei danni riscontrata nei diversi paesi analizzati. Svezia e Giappone si contraddistinguono da tutti gli altri paesi per via degli elevati costi segnalati. All'estremo opposto, Sud Africa e Repubblica Ceca mostrano i minori costi di riparazione dei danni. La Polonia è stata esclusa dal grafico poiché presentava una base di partecipanti inferiore a 30.

Costo medio per la riparazione dei danni causati dal ransomware, in base al paese



Qual è stato approssimativamente il costo sostenuto dall'organizzazione per rimediare ai danni provocati dall'attacco di ransomware più recente (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali, somma pagata per il riscatto ecc.)? Domanda rivolta solamente ai partecipanti la cui organizzazione aveva subito un attacco di ransomware nei 12 mesi precedenti. Base: 2.538 partecipanti.

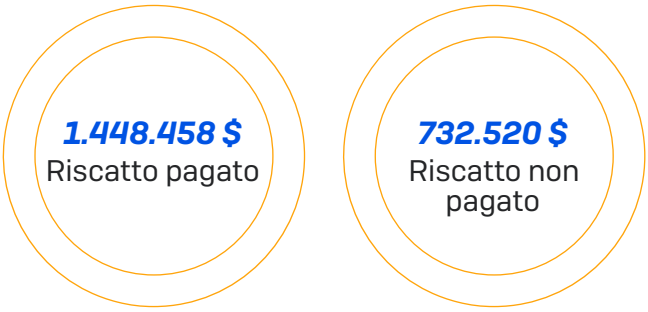
Uno dei motivi di questa variazione potrebbero essere i costi associati alle risorse umane nei vari paesi. Svezia e Giappone sono paesi in cui la media degli stipendi è generalmente alta, pertanto i costi delle ore di lavoro necessarie per rimediare ai danni si accumulano facilmente. Sud Africa e Repubblica Ceca mostrano invece statistiche opposte, in quanto sono paesi in cui i salari sono tendenzialmente bassi.

Come già osservato, la Svezia si classifica al secondo posto tra le più elevate percentuali di pagamento del riscatto, superata solamente dall'India. Tuttavia, a differenza dell'India, la Svezia è anche caratterizzata da salari molto elevati e questo contribuisce doppiamente a rincarare la dose quando si tratta di rimediare ai danni causati dal ransomware.

Pagare il riscatto raddoppia i costi

Uno dei risultati più interessanti emersi dal sondaggio è il fatto che pagare il riscatto incrementa i costi di riparazione, portandoli a quasi il doppio della cifra necessaria per ripristinare i dati tramite backup o altri metodi, senza effettuare pagamenti ai cybercriminali. Non pagare il riscatto non ha solamente un effetto positivo sul morale, in quanto si evita di dare soldi a dei criminali, ma implica anche risparmi a lungo termine.

Costo medio delle attività di riparazione dei danni di un attacco di ransomware



Nell'attacco di ransomware più grave, l'organizzazione ha recuperato i dati? I dati rappresentano solamente le risposte dei partecipanti la cui organizzazione aveva subito la cifratura non autorizzata dei dati durante l'attacco di ransomware più recente. Base: 1.849 partecipanti. **Riscatto pagato** rappresenta la somma delle risposte "Sì, abbiamo pagato il riscatto" e "No, anche se abbiamo pagato il riscatto". **Riscatto non pagato** rappresenta le risposte "Sì, abbiamo utilizzato backup per recuperare i dati", "Sì, abbiamo utilizzato altri metodi per recuperare i dati" e "No, non abbiamo pagato il riscatto".

Potrebbe sembrare un controsenso: se il riscatto è stato pagato, perché i costi sono più elevati? Il fatto è che anche dopo aver pagato un riscatto rimane comunque molto lavoro da fare per recuperare i dati. Ripristinare i dati e ritornare alle normali modalità operative potrebbe infatti avere lo stesso impatto finanziario sia che i dati vengano recuperati dai cybercriminali che dai propri backup. Tuttavia, pagando il riscatto si affronta un ulteriore costo molto ingente.

Parte 3: il ruolo delle polizze assicurative

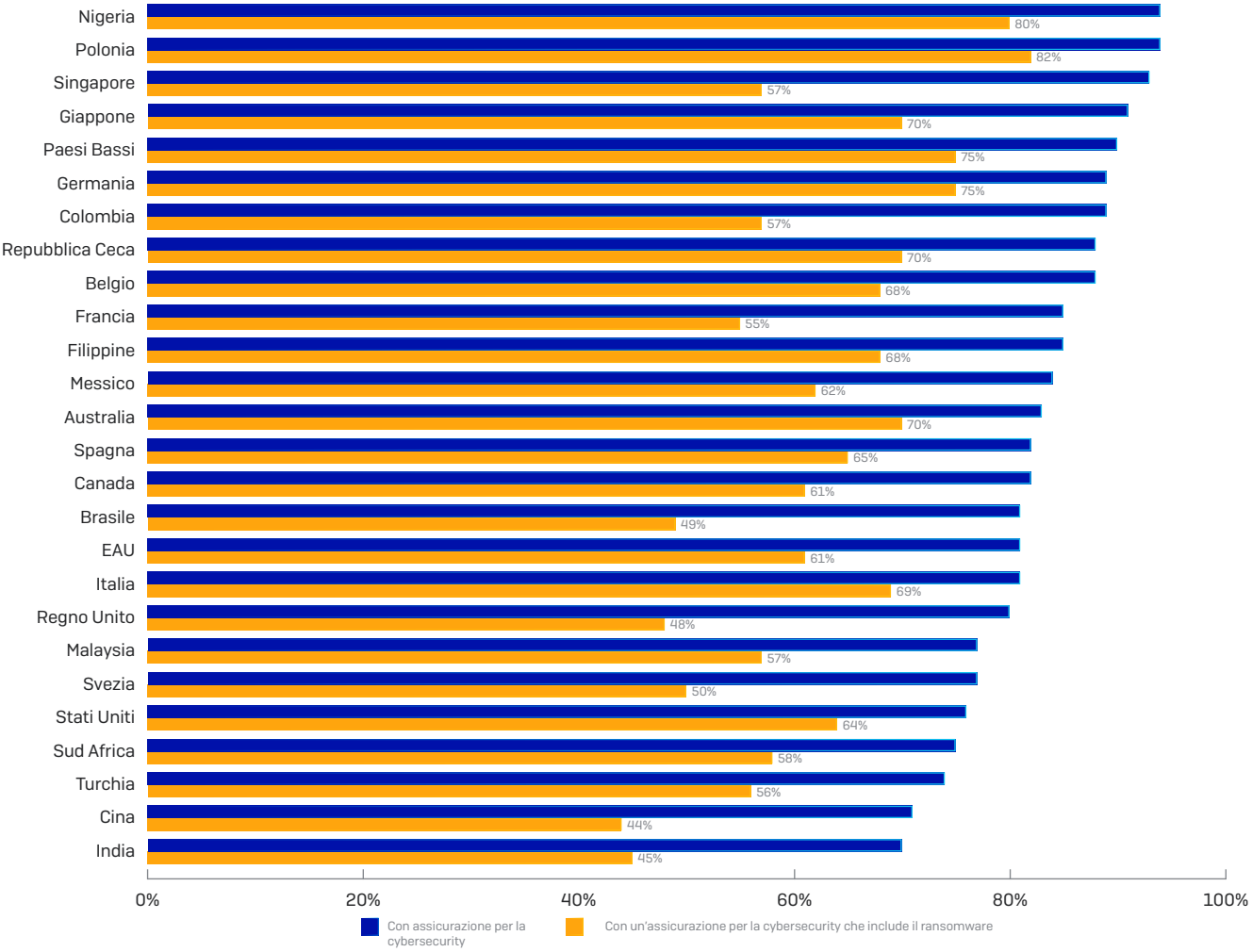
Un'organizzazione su cinque presenta gravi lacune in termini di assicurazione per la cybersecurity

Stipulare una polizza assicurativa per la cybersecurity è ormai una prassi comune e l'84% delle organizzazioni dichiara di averlo fatto. Tuttavia, solo nel 64% dei casi l'assicurazione per la cybersecurity include il ransomware. Questo significa che fino a un'organizzazione su cinque (20%) paga un'assicurazione per la cybersecurity che non la tutela contro il ransomware.

L'organizzazione ha stipulato una polizza assicurativa che la tutelerebbe se dovesse essere colpita dal ransomware? Base: 5.000 partecipanti.

Poiché, come abbiamo visto, il 51% delle organizzazioni ha subito un attacco di ransomware negli ultimi 12 mesi e poiché i costi medi di riparazione dei danni ammontano a 761.106 $, le organizzazioni dovrebbero mettere in discussione il valore di una polizza che esclude il ransomware.

Assicurazione per la cybersecurity, in base al paese



L'organizzazione ha stipulato una polizza assicurativa che la tutelerebbe se dovesse essere colpita dal ransomware? Base: 5.000 partecipanti.

In questo grafico possiamo osservare le percentuali a seconda dei paesi. La barra blu indica la percentuale di organizzazioni che hanno stipulato polizze assicurative per la cybersecurity, mentre quella arancione indica la percentuale delle organizzazioni con un'assicurazione che include il ransomware. I dati da valutare in questo grafico sono sia le quantità assolute che la differenza tra le due barre per ciascun paese.

L'india domina la classifica delle organizzazioni con una polizza assicurativa, occupando il secondo posto per la percentuale più elevata (80%) di organizzazioni con un'assicurazione che include gli attacchi di ransomware. Visto che l'India è anche il paese con la maggiore probabilità di essere colpito dal ransomware, si tratta di una correlazione comprensibile.

La Turchia ha registrato la terza percentuale più elevata di attacchi di ransomware. Tuttavia, nonostante si trovi al terzo posto tra i paesi che hanno un'assicurazione per la cybersecurity (93% delle organizzazioni), presenta anche una delle maggiori divergenze tra le due barre, in quanto solamente il 57% delle organizzazioni ha polizze che le tutelano contro il ransomware.

Anche se la Cina presenta una percentuale di attacchi di ransomware inferiore alla media (45% di aziende colpite negli ultimi 12 mesi), presenta anche la percentuale più elevata (94% a pari merito) di aziende con un'assicurazione per la cybersecurity, nonché il livello più alto di polizze assicurative che includono il ransomware (82%). Presenta infatti la divergenza minore tra tutti e 26 i paesi presi in esame.

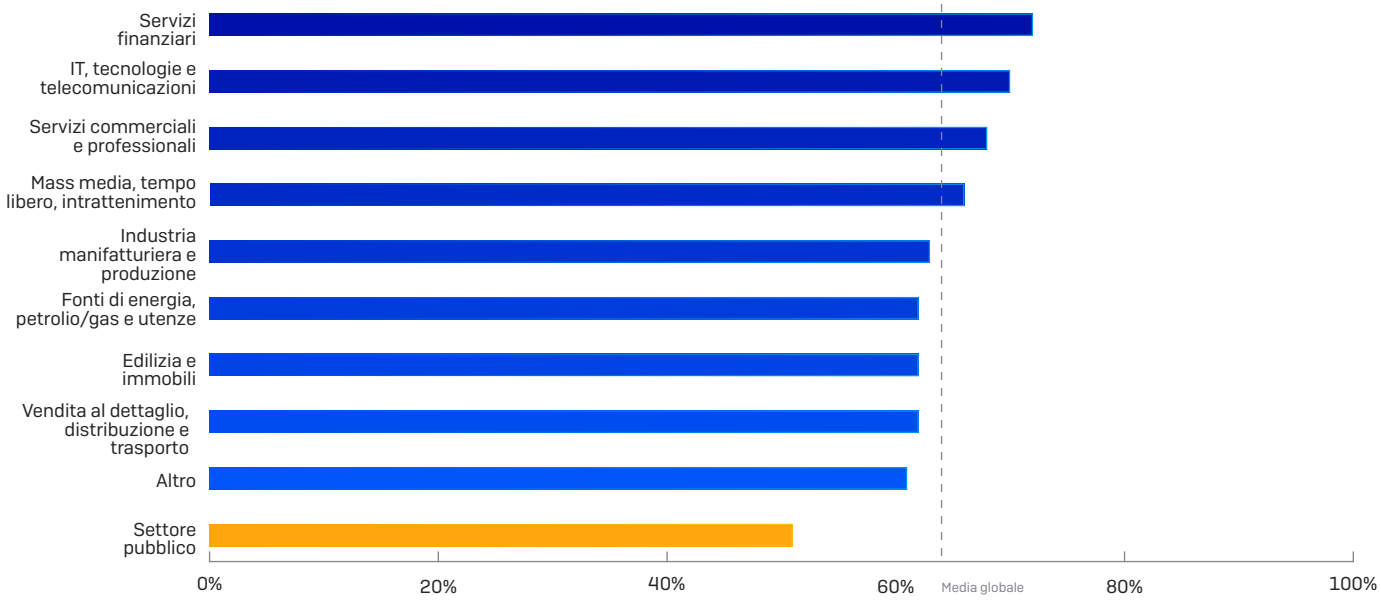
Un'eccezione interessante è quella della Germania. Inaspettatamente, si osserva come un paese con un'economia avanzata presenti una percentuale relativamente bassa di organizzazioni con polizze assicurative (77%), nonché una delle percentuali minori di assicurazioni che includono il ransomware (50%). La Germania ha registrato livelli di ransomware superiori alla media (il 57% delle organizzazioni è stato colpito negli ultimi 12 mesi) e questa statistica rende ancora più inattesi i dati relativi alle polizze assicurative.

Il settore pubblico è quello più esposto all'impatto finanziario del ransomware

Sebbene il settore pubblico sia quello meno esposto al ransomware, è tuttavia quello maggiormente esposto al pieno impatto finanziario di un attacco.

In media, il 64% delle organizzazioni dispone di una polizza assicurativa che le tutela contro il ransomware. I servizi finanziari presentano la percentuale più elevata di assicurazioni (72%), probabilmente per via della natura stessa di questo settore, che lo rende un bersaglio molto allettante per i cybercriminali. IT, telecomunicazioni e tecnologie seguono a distanza ravvicinata, con il 70%.

Polizze assicurative per la cybersecurity che includono il ransomware



L'organizzazione ha stipulato una polizza assicurativa che la tutelerebbe se dovesse essere colpita dal ransomware? Base: 5.000.

Tuttavia, le organizzazioni del settore pubblico si trovano notevolmente indietro rispetto a quelle del settore privato. Solo il 51% dispone di polizze assicurative che prevedono protezione contro l'impatto finanziario del ransomware, ben 10 punti percentuali meno dell'ultimo settore prima di loro. Questa bassa percentuale di protezione potrebbe essere dovuta ai costi. I finanziamenti per il settore pubblico sono tradizionalmente limitati e si tratta di una tendenza globale. Di conseguenza, il budget di queste organizzazioni potrebbe non essere sufficiente per stipulare una polizza assicurativa. In ogni modo, questi risparmi sono a breve termine e verrebbero resi vani qualora un attacco dovesse riuscire a superare le linee di difesa.

Polizze assicurative per la cybersecurity e pagamento dei riscatti

Analizziamo ora il ruolo che svolge la cybersecurity nel pagamento dei riscatti. Come abbiamo visto, nel 73% degli attacchi di ransomware i dati vengono cifrati. Delle organizzazioni i cui dati sono stati cifrati, il 26% dichiara di aver pagato il riscatto per poter recuperare i dati.

Tuttavia, esaminando i fatti in maniera più approfondita, emerge che in quasi tutti i casi (94%) in cui è stato pagato un riscatto, in realtà la somma è stata pagata dall'assicurazione per la cybersecurity. Inoltre, come osservato, il pagamento di un ricatto raddoppia il costo complessivo della riparazione dei danni.

Parte 4: le tecniche di attacco del ransomware

Abbiamo chiesto alle organizzazioni che hanno confermato di essere state colpite dal ransomware negli ultimi 12 mesi di descrivere come ha fatto l'attacco a infiltrarsi nell'organizzazione. In cima alla classifica troviamo i download di file e le e-mail con allegati malevoli, che ammontano al 29% degli attacchi. Al secondo posto ci sono gli attacchi remoti sui server, che rappresentano il 21% degli attacchi.

COME HA FATTO IL RANSOMWARE A INFILTRARSI NELL'ORGANIZZAZIONE	Nº INCIDENTI	% INCIDENTI
Tramite il download di un file o un'e-mail contenente un link malevolo	741	29%
Tramite attacco remoto sul server	543	21%
Tramite e-mail contenente un allegato malevolo	401	16%
Istanze di cloud pubblico configurate in maniera errata	233	9%
Tramite il nostro Remote Desktop Protocol (RDP)	221	9%
Tramite un fornitore di servizi che collabora con la nostra organizzazione	218	9%
Tramite un dispositivo USB/supporto rimovibile	172	7%
Altro	0	0%
Non lo so	9	0%
Totale	2.538	100%

Com'è riuscito l'attacco di ransomware a infiltrarsi nell'organizzazione? Domanda rivolta ai partecipanti la cui organizzazione aveva subito un attacco di ransomware nei 12 mesi precedenti. Base: 2.538 partecipanti.

Il dato più evidente che emerge da queste statistiche è che non esiste un unico vettore di attacco principale. I cybercriminali utilizzano piuttosto una vasta gamma di tecniche, sfruttando qualsiasi vulnerabilità delle difese per infiltrarsi nei sistemi. Se una tecnica non dovesse risultare efficace, ne provano un'altra, fino a quando non trovano un punto debole.

I dati dimostrano la necessità di un sistema di difesa efficace e a livelli multipli, in grado di proteggere endpoint, server, istanze sul cloud pubblico, e-mail, gateway di rete e catene di distribuzione. Concentrarsi su un'unica tecnologia è una formula che non può fare altro se non favorire le infezioni.

Raccomandazioni

Il sondaggio ha confermato che il ransomware rimane a tutt'oggi una minaccia concreta per le organizzazioni. Inoltre, ha anche fornito approfondimenti utili su come ridurre al minimo il rischio di diventarne vittima:

1. **Partire dal presupposto che si verrà colpiti**. Il ransomware non discrimina: tutte le organizzazioni sono un potenziale bersaglio, indipendentemente da dimensioni, settore o posizione geografica. Occorre pianificare la propria strategia di cybersecurity in base al presupposto che prima o poi si verrà colpiti da un attacco.
2. **Investire in tecnologie antiransomware in grado di prevenire la cifratura non autorizzata dei file.** Il 24% delle organizzazioni che hanno partecipato al sondaggio e che sono state colpite dal ransomware sono riuscite a bloccare l'attacco prima che i dati fossero cifrati.
3. **Proteggere i dati, ovunque siano memorizzati.** In quasi sei casi su 10 degli attacchi di ransomware che sono riusciti a cifrare i dati, l'obiettivo era il cloud pubblico. La strategia di difesa deve includere la protezione dei dati nel cloud pubblico, nel cloud privato e on-premise.
4. **Effettuare regolarmente backup dei dati e conservarli off-site e off-line.** L'anno scorso, nel 56% dei casi le organizzazioni i cui dati sono stati cifrati sono riuscite a recuperare le informazioni grazie ai propri backup. Utilizzare backup per il ripristino dei dati riduce notevolmente i costi associati agli attacchi, rispetto ai casi nei quali viene pagato il riscatto.
5. **Accertarsi che la propria polizza assicurativa per la cybersecurity includa il ransomware.** Verificare di essere completamente tutelati, qualora dovesse succedere il peggio.
6. **Implementare un sistema di difesa a livelli multipli.** I cybercriminali che utilizzano il ransomware sfruttano un'ampia gamma di tecniche per eludere le strategie di difesa; quando ne viene bloccata una passano a quella successiva, fino a quando non riescono a trovare il tallone d'Achille. Occorre proteggere i sistemi contro tutti i vettori di attacco.

Sophos Intercept X Endpoint

I cybercriminali che utilizzano il ransomware sfruttano una combinazione tra sofisticate tecniche di attacco e hackeraggio partecipativo. Sophos Intercept X Endpoint offre le tecnologie di protezione avanzata necessarie per neutralizzare l'intera catena di attacco, tra le quali:

- **Ripristino dei file cifrati**: CryptoGuard blocca la cifratura non autorizzata dei file, ripristinando questi ultimi al loro stato sicuro pre-attacco nel giro di pochi secondi.
- **Protezione contro gli exploit**: rilevamento e blocco di più di una trentina di tecniche di exploit utilizzate per scaricare e installare il malware, per impedire agli hacker di infiltrarsi nella rete.
- **Protezione contro le minacce basata sull'intelligenza artificiale**: il motore di deep learning di Sophos blocca predittivamente un maggior numero di attacchi e presenta tassi di falsi positivi inferiori rispetto a qualsiasi altro software di sicurezza.
- **Protezione contro il furto di credenziali**: impedisce agli hacker di accedere alle preziosissime credenziali degli utenti, bloccando sia l'accesso non autorizzato ai sistemi che i tentativi di ottenere privilegi più elevati.

Per maggiori informazioni e per una demo on-line immediata, visitare: www.sophos.it/intercept-x

Informazioni su Vanson Bourne

Vanson Bourne è un'azienda indipendente, specializzata negli studi di mercato per il settore delle tecnologie. La sua reputazione, garanzia di analisi valide, attendibili e basate sulla ricerca, è fondata sui suoi rigorosissimi princìpi di ricerca e sulla sua abilità di ottenere i pareri dei principali decision maker in ruoli tecnici e commerciali, in tutti i settori e tutti i mercati più importanti. Visitate www.vansonbourne.com

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

200427 WPIT (DD)

SOPHOS