SOPHOS

La Vera Storia Del Ransomware Per Il Settore Sanitario 2023

I risultati di uno studio indipendente e vendor-agnostic condotto da gennaio a marzo 2023, a cui hanno partecipato 3.000 IT/Cybersecurity Manager (tra cui 233 che lavorano nel settore sanitario) dislocati in 14 paesi del mondo.

Introduzione

Come ogni anno, Sophos ha condotto una ricerca che valuta le esperienze di vita reale degli IT/Cybersecurity Manager in materia di ransomware. I risultati mettono in luce le realtà che le organizzazioni che operano nel settore sanitario si trovano ad affrontare nel 2023. Rivelano le più comuni cause all'origine degli attacchi e offrono nuove prospettive sull'impatto del ransomware in questo settore. Questo report svela inoltre l'impatto commerciale e operativo di quando, invece di servirsi dei backup, le organizzazioni pagano il riscatto per recuperare i dati.

Informazioni Sul Sondaggio

Sophos ha affidato a un'azienda esterna e indipendente l'incarico di condurre un sondaggio vendor-agnostic, coinvolgendo 3.000 IT/Cybersecurity Manager (tra cui 233 che lavorano nel settore sanitario) in organizzazioni con 100-5.000 dipendenti in 14 paesi nelle aree geografiche di Nord e Sud America, EMEA (Europa, Medio Oriente e Africa) e Asia-Pacifico. Il sondaggio è stato svolto da gennaio a marzo 2023 e ai partecipanti è stato chiesto di rispondere tenendo in considerazione le proprie esperienze durante l'anno precedente.

Tasso Di Attacchi Ransomware Nel Settore Sanitario

Il nostro studio del 2023 rivela che il tasso di attacchi ransomware nel settore sanitario è sceso dal 66% dell'anno scorso al 60% di quest'anno. Nonostante questo calo, la percentuale di attacchi registrata nel report del 2023 è pur sempre quasi doppia rispetto a quella del sondaggio condotto nel 2021, che indicava un 34% di organizzazioni del settore sanitario colpite dal ransomware.

Sebbene questo settore sia caratterizzato da una minore frequenza di attacco, con quasi due terzi delle organizzazioni colpite dal ransomware l'anno scorso, è evidente che gli avversari informatici sono in grado di sferrare regolarmente attacchi su larga scala. Si può pertanto affermare che, oggi come oggi, il ransomware è potenzialmente il principale rischio informatico per il settore sanitario.

Sono diversi anni che i cybercriminali sviluppano e affinano il modello ransomware-as-a-service. Questo modello operativo rende l'uso del ransomware molto più accessibile per gli aspiranti hacker; allo stesso tempo, aiuta a conferire agli attacchi dinamiche sempre più sofisticate, in quanto permette ai malintenzionati di specializzarsi in fasi diverse di tali attacchi. Per maggiori informazioni sul ransomware as-a-service, leggi il Sophos 2023 Threat Report.

2021	2022	2023
34%	66%	60%

La tua organizzazione è stata colpita dal ransomware l'anno scorso? Sì. n=233 (2023), 381 (2022), 328 (2021)

A differenza del tasso di attacchi ransomware nel settore sanitario, che è in calo, la tendenza globale è rimasta invariata: sia nel sondaggio del 2023 che in quello del 2022, il 66% di tutti i partecipanti ha dichiarato che la propria organizzazione è stata colpita dal ransomware l'anno precedente.

Quello dell'istruzione è stato il settore con maggiore probabilità di essere colpito, con l'80% dei partecipanti nell'istruzione scolastica e il 79% nell'istruzione superiore che dichiarano di avere subito un attacco. Il settore IT, tecnologie e telecomunicazioni ha registrato il più basso livello di attacchi (50%): un risultato che indica maggiore preparazione informatica e la presenza di difese più efficaci.

Cause All'Origine Degli Attacchi Ransomware Nel Settore Sanitario

Le credenziali compromesse (32%) sono stata la causa originaria più comune per gli attacchi ransomware più gravi subiti dal settore sanitario, seguite dalle vulnerabilità soggetta a exploit (29%). Gli attacchi tramite e-mail (e-mail pericolose o phishing) sono stati il punto iniziale di più di un terzo degli attacchi (36%) nelle organizzazioni del settore sanitario, superando la media del 30% per tutti i settori.

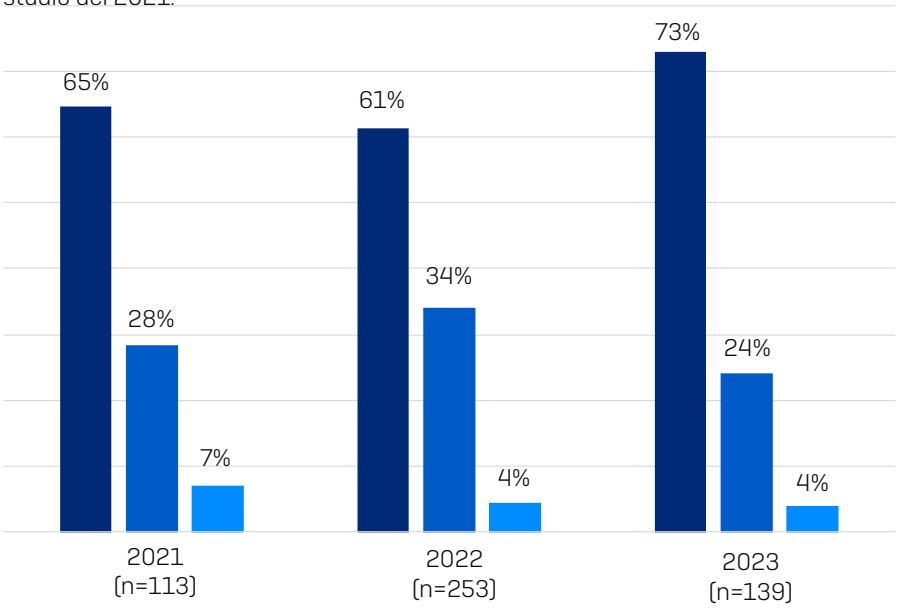
A livello globale, tenendo conto di tutti i settori, l'ordine delle due principali cause originarie è inverso, visto che le vulnerabilità soggette a exploit risultano la root cause più comune (sono infatti state riscontrate nel 36% degli attacchi), seguite dalle credenziali compromesse (nel 29% degli attacchi).

	SETTORE SANITARIO (n=139)	MEDIA DI TUTTI I SETTORI (n=1.974)
Vulnerabilità soggetta a exploit	29%	36%
Credenziali compromesse	32%	29%
E-mail malevole	22%	18%
Phishing	14%	13%
Attacchi brute force	1%	3%
Download	1%	1%

Tasso Di Cifratura Non Autorizzata Nel Settore Sanitario

Il tasso di cifratura non autorizzata dei dati riscontrato nel settore sanitario è stato il più alto negli ultimi tre anni, con quasi tre quarti (73%) di partecipanti nel settore sanitario che dichiara di aver subito questo tipo di attacco: una percentuale in aumento rispetto al 61% del 2022 e al 65% del 2021. Molto probabilmente, queste statistiche riflettono le sempre maggiori capacità tecniche degli antagonisti informatici, che continuano a introdurre innovazioni e ad affinare i propri approcci.

Il tasso di attacchi di sola estorsione nel settore sanitario è pari al 4%: resta dunque invariato rispetto all'anno scorso e risulta in calo rispetto al 7% dello studio del 2021.



- Sì, sono stati cifrati dei dati
- No, l'attacco è stato bloccato prima che fossero cifrati dei dati
- No, non sono stati cifrati dati ma abbiamo ricevuto una richiesta di riscatto (estorsione)

Durante l'attacco ransomware, i cybercriminali sono riusciti a cifrare i dati della tua organizzazione?
Selezione delle opzioni di risposta. Base di partecipanti indicata nel grafico

Sebbene sia alta, la percentuale di attacchi nei quali sono stati cifrati i dati registrata nel settore sanitario è inferiore alla media di tutti i settori, dove il 76% degli attacchi ha portato alla cifratura non autorizzata dei dati. Il tasso più alto di cifratura non autorizzata (92%) è stato registrato dai servizi commerciali e professionali.

Oltre un terzo (37%) degli attacchi al settore sanitario in cui sono stati cifrati i dati è stato caratterizzato anche dal furto di dati. Questo approccio "a doppio impatto" degli avversari informatici sta diventando sempre più diffuso, poiché aiuta i malintenzionati a incrementare le loro possibilità di monetizzazione degli attacchi. La minaccia di divulgare pubblicamente i dati rubati può essere sfruttata per estorcere pagamenti alle vittime; inoltre, queste informazioni possono anche essere vendute a terzi. L'elevata frequenza dei casi di furto dei dati rende ancora più fondamentale la necessità di bloccare gli attacchi tempestivamente, prima che possano essere esfiltrate informazioni importanti.

37%

Percentuale di attacchi ransomware nel settore sanitario in cui sono stati cifrati i dati e che sono stati caratterizzati anche dal furto di dati.

Durante l'attacco ransomware, i cybercriminali sono riusciti a cifrare i dati della tua organizzazione?
Sì/Sì, e sono anche stati rubati dati; n=101/37

Tasso Di Recupero Dei Dati Nel Settore Sanitario

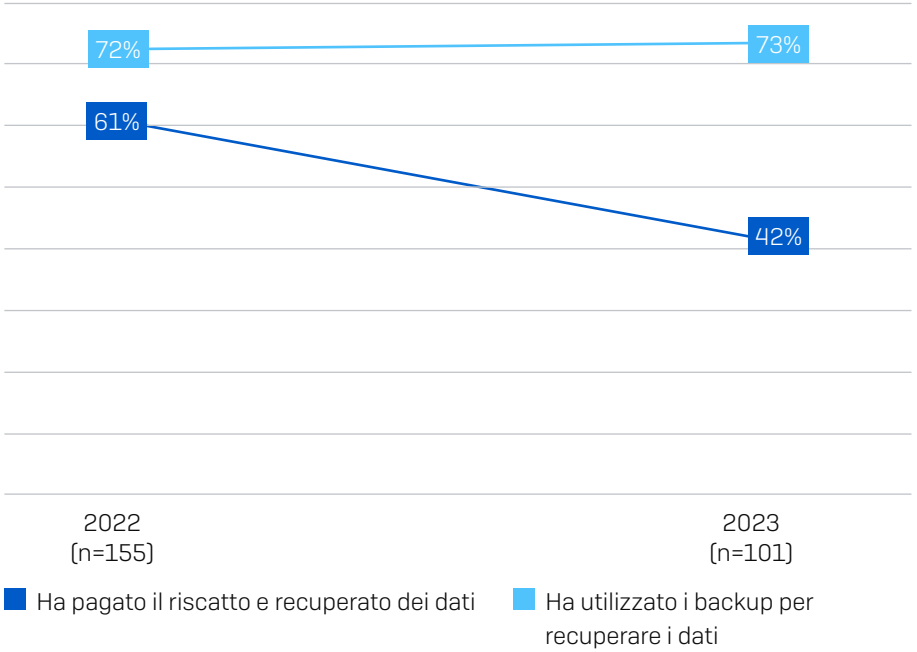
La buona notizia è che tutte le organizzazioni del settore sanitario i cui dati erano stati cifrati è riuscita a recuperare le informazioni, superando la media di tutti i settori (97%).

Il 73% delle organizzazioni del settore sanitario i cui dati erano stati cifrati ha utilizzato i backup per recuperare le informazioni, con una percentuale leggermente superiore al 72% registrato nel sondaggio del 2022. Una statistica molto rassicurante è il calo nella propensione a pagare il riscatto per recuperare i dati cifrati: il 42% degli intervistati nel settore sanitario ha infatti dichiarato di aver pagato il riscatto per riavere le proprie informazioni, in diminuzione rispetto al 61% dell'anno scorso. Il 17% sostiene di essersi servito di più di un solo metodo per recuperare i dati cifrati.

	SETTORE SANITARIO	MEDIA DI TUTTI I SETTORI
Ha recuperato i dati	**100%**	**97%**
Ha utilizzato i backup per ripristinare i dati	**73%**	**70%**
Ha pagato il riscatto per recuperare i dati	**42%**	**46%**
Ha utilizzato altri metodi per recuperare i dati	**2%**	**2%**

La tua organizzazione è riuscita a recuperare almeno parte dei dati? Sì, abbiamo utilizzato i backup per recuperare i dati; Sì, abbiamo pagato il riscatto e recuperato dei dati; Sì, abbiamo utilizzato altri metodi per recuperare i dati. n=1.497 (media di tutti i settori); n=101 (settore sanitario).

Il tasso di pagamento del riscatto nel settore sanitario non è solo stato molto più basso rispetto all'anno precedente, ma è anche risultato inferiore rispetto al 46% della media di tutti i settori. Globalmente, nell'ultimo anno il tasso di pagamento del riscatto è rimasto invariato, mentre l'uso dei backup è sceso dal 73% del report del 2022 al 70% per il 2023.



La tua organizzazione è riuscita a recuperare almeno parte dei dati? Sì, abbiamo pagato il riscatto e recuperato dei dati; Sì, abbiamo utilizzato i backup per recuperare i dati. Base di partecipanti indicata nel grafico

L'Impatto Delle Cyberassicurazioni Sulla Propensione A Pagare Il Riscatto

Sebbene la percentuale complessiva di ripristino dei dati nel settore sanitario sia pari al 100%, i metodi utilizzati per recuperare i dati variano a seconda della copertura assicurativa. Le organizzazioni con polizze cyberassicurative indipendenti hanno mostrato una maggiore propensione a pagare il riscatto, rispetto a quelle dotate di una copertura più completa che include anche l'ambito informatico.

Tra le organizzazioni nel settore sanitario dotate di cyberassicurazione indipendente i cui dati erano stati cifrati, più della metà (53%) ha deciso di pagare il riscatto. La scelta di pagare il riscatto scende al 34% per le organizzazioni con una copertura più completa che include anche l'ambito informatico.

Impatto di un'assicurazione sul pagamento del riscatto nel settore sanitario

La tua organizzazione è riuscita a recuperare almeno parte dei dati? Sì, abbiamo pagato il riscatto e recuperato i dati. n=101 organizzazioni nel settore sanitario colpite l'anno scorso da un attacco ransomware che ne ha cifrato i dati (45 con una polizza cyberassicurativa indipendente, 53 con una copertura più completa che include l'ambito informatico).

Pagamenti del riscatto

Per quanto riguarda la situazione globale di tutti i settori, sebbene generalmente la propensione a pagare il riscatto sia rimasta invariata rispetto al sondaggio dell'anno scorso, i pagamenti hanno subito un'impennata, con somme medie di riscatto che sono quasi raddoppiate, passando da 812.360 $ a 1.542.333 $ nell'ultimo anno. Il pagamento del riscatto mediano è aumentato da 76.500 $ a 400.000 $.

Per quanto riguarda il settore sanitario, 12 organizzazioni che operano in questo settore hanno condiviso la somma esatta del pagamento. La cifra mediana ammonta a 2,5 milioni di $, in netto aumento rispetto ai 30.000 $ del 2022.

Nove organizzazioni del settore sanitario dichiarano di aver pagato riscatti da almeno 1 milione di $, e solo una ha pagato meno di 100.000 $. Sebbene la base limitata di partecipanti che hanno risposto a questa domanda implichi che i dati del report del 2023 non sono da considerarsi significativi dal punto di vista statistico e che devono pertanto essere utilizzati con cautela, i risultati indicano comunque un aumento nella cifra pagata come riscatto nel settore sanitario.

	2022	2023
Media di tutti i settori	812.360 $ (cifra media) 76.500 $ (cifra mediana)	1.542.330 $ (cifra media) 400.000 $ (cifra mediana)
Settore Sanitario	196.749 $ (cifra media) 30.000 $ (cifra mediana)	2.884.167 $ (cifra media) 2.500.000 $ (cifra mediana)

A quanto ammonta la somma di riscatto pagata ai cybercriminali? Le risposte "Non lo so" e le eccezioni sono state omesse. Tutti i settori: n=216 (2023)/965 (2022); settore sanitario: n=12 (2023)/83 (2022).

* Nello studio del 2023 gli intervistati del settore sanitario presentano numeri di base molto bassi, pertanto i risultati sono da considerarsi puramente indicativi.

Costi Di Riparazione Dei Danni

I pagamenti del riscatto sono solo uno dei vari tipi di costi di riparazione dei danni da sostenere quando si viene colpiti dal ransomware. Tra tutti i settori, escludendo le somme di riscatto pagate, le organizzazioni hanno dovuto affrontare un costo medio di riparazione dei danni causati dal ransomware pari a 1,82 milioni di $: un aumento rispetto agli 1,4 milioni di $ del sondaggio del 2022 (che includevano anche il pagamento del riscatto) e agli 1,85 milioni di $ (somma di riscatto inclusa) del 2021.

In linea con la tendenza globale, i costi di riparazione dei danni per le organizzazioni del settore sanitario sono aumentati rispetto all'anno precedente, passando da 1,85 milioni di $ a 2,20 milioni di $. Inoltre, sono quasi raddoppiati rispetto agli 1,27 milioni di $ registrati da questo settore nel sondaggio del 2021. L'incremento dei costi di riparazione dei danni di quest'anno per il settore sanitario è probabilmente dovuto alla maggiore frequenza dell'uso della cifratura non autorizzata dei dati negli attacchi ransomware.

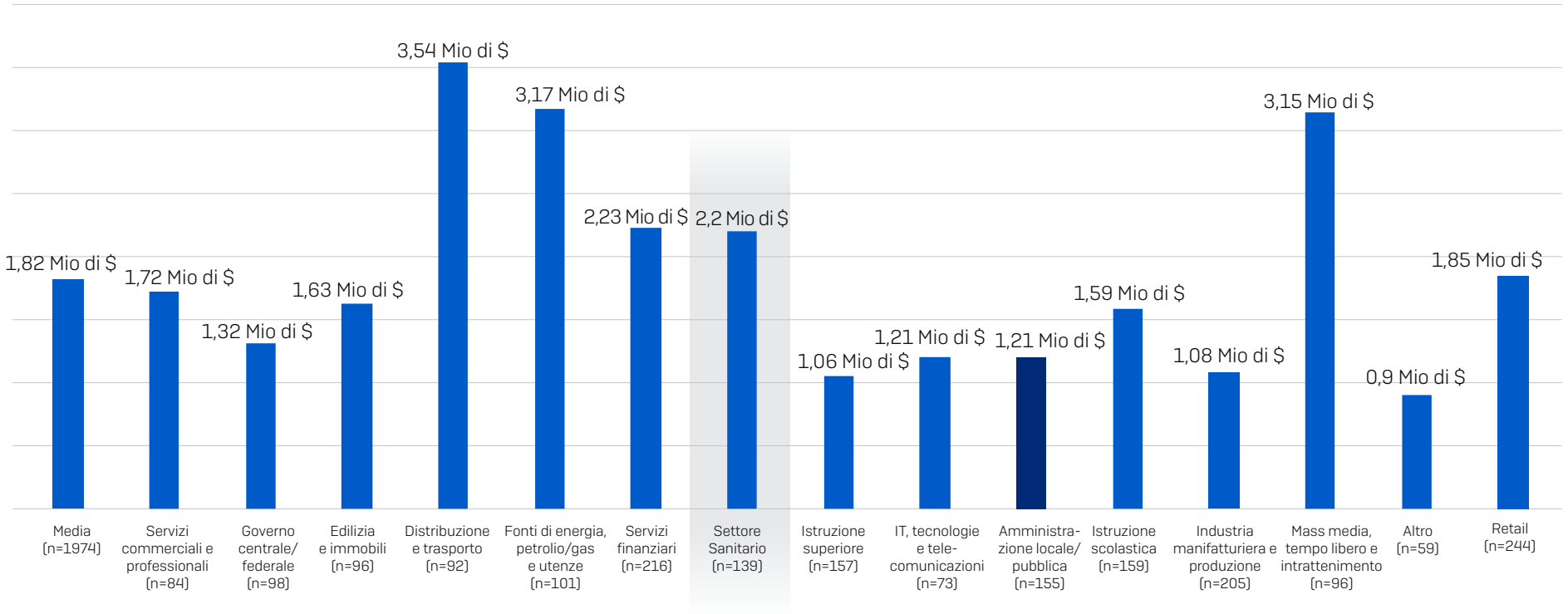
	2021	2022	2023
Media di tutti i settori	1,85 Mio di $	1,4 Mio di $	1,82 Mio di $
Settore Sanitario	1,27 Mio di $	1,85 Mio di $	2,20 Mio di $

Qual è stato approssimativamente il costo sostenuto dalla tua organizzazione per rimediare ai danni provocati dall'attacco ransomware più grave (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali ecc.)? Tutti i settori: n=1.974 (2023)/3.702 (2022)/2.006 (2021); settore sanitario: n=139 (2023)/253 (2022)/113 (2021)

Nota: la domanda formulata per il sondaggio del 2022 e del 2021 includeva anche "pagamento del riscatto"

I costi di riparazione dei danni nelle organizzazioni del settore sanitario sono stati superiori alla media di tutti i settori, che ammonta a 1,82 milioni di $. Distribuzione e trasporto è stato il settore con i più alti costi di riparazione dei danni (3,54 milioni di $), quasi il doppio rispetto alla media globale.

Costi Di Riparazione Dei Danni In Seguito All'Attacco Ransomware Più Grave (In Milioni Di USD)



Qual è stato approssimativamente il costo sostenuto dalla tua organizzazione per rimediare ai danni provocati dall'attacco ransomware più grave (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali ecc.)? Base di partecipanti indicata nel grafico.

Costi Di Riparazione Dei Danni In Base Al Metodo Di Recupero Dei Dati

Lo studio conferma che utilizzare i backup per recuperare i dati cifrati illecitamente implica costi di riparazione dei danni inferiori rispetto a quando si sceglie di pagare il riscatto.

Il costo di riparazione mediano tra tutti i settori per le organizzazioni che hanno utilizzato i backup (375.000 $) è pari alla metà della cifra mediana versata dalle organizzazioni che hanno pagato il riscatto (750.000 $). Analogamente, il costo medio è quasi 1 milione di $ più basso per i partecipanti che hanno optato per i backup, rispetto a chi ha pagato il riscatto.

La stessa tendenza è stata osservata nel settore sanitario, in cui il costo medio di riparazione dei danni per le organizzazioni che hanno utilizzato i backup (2,11 milioni di $) è risultato inferiore alle spese affrontate da chi aveva scelto di pagare il riscatto (2,58 milioni di $).

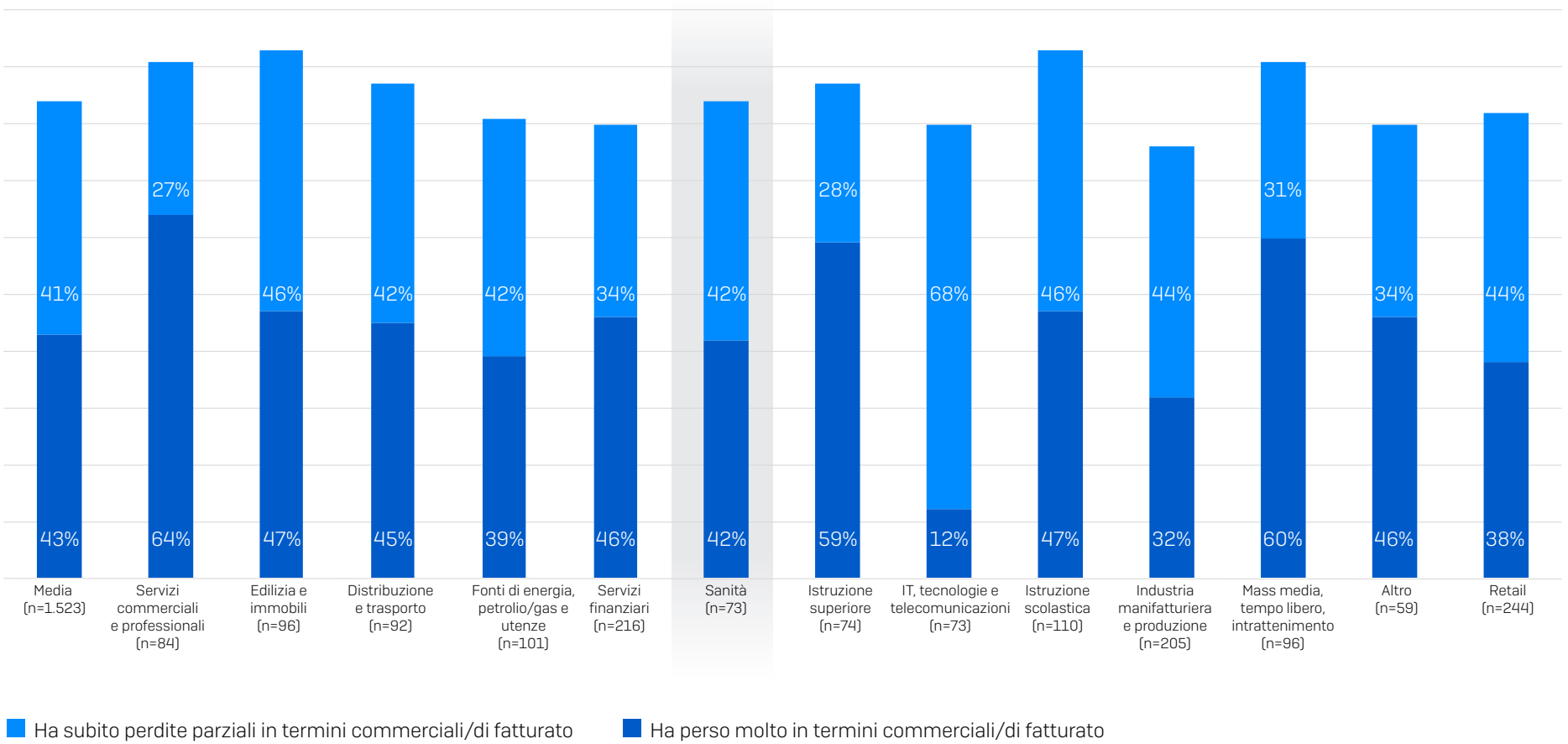
	Ha pagato il riscatto e recuperato dei dati	Ha utilizzato i backup per recuperare i dati
Media di tutti i settori	**750.000 $** Cifra mediana **2,6 Mio di $** Cifra media	**375.000 $** Cifra mediana **1,62 Mio di $** Cifra media
Settore Sanitario	**750.000 $** Cifra mediana **2,58 Mio di $** Cifra media	**750.000 $** Cifra mediana **2,11 Mio di $** Cifra media

Qual è stato approssimativamente il costo sostenuto dalla tua organizzazione per rimediare ai danni provocati dall'attacco ransomware più grave (tenendo in considerazione tempi di inattività, ore di lavoro del personale, costi correlati a dispositivi e rete, perdita di opportunità commerciali ecc.)? Tutti i settori: n=694 organizzazioni che hanno pagato il riscatto e recuperato dei dati e 1.053 che hanno utilizzato i backup per recuperare i dati;

Settore sanitario: n= 42 organizzazioni che hanno pagato il riscatto e recuperato dei dati e n=74 che hanno utilizzato i backup per recuperare i dati.

Impatto Commerciale

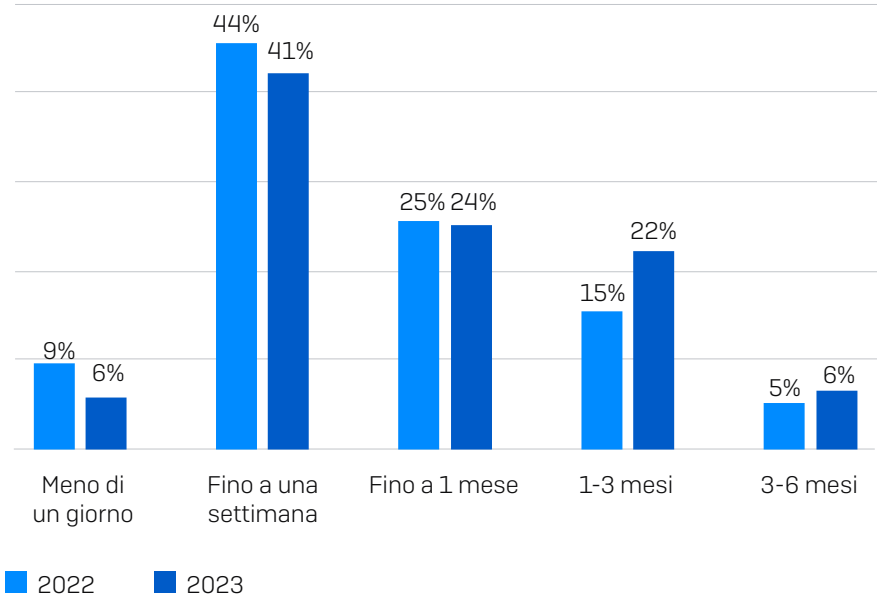
L'85% delle organizzazioni del settore sanitario che sono state colpite dal ransomware sostiene che l'attacco ha provocato perdite commerciali/di fatturato; questa statistica è leggermente superiore alla media globale dell'84% per tutti i settori. Istruzione scolastica (94%) ed edilizia e immobili (93%) sono stati i settori con maggiore propensione a subire parziali perdite commerciali/di fatturato, mentre i servizi commerciali e professionali hanno registrato la maggiore probabilità di segnalare una perdita significativa in termini commerciali/di fatturato (64%). Il settore IT, tecnologie e telecomunicazioni, invece, è quello più preparato, con appena il 12% degli intervistati che indica di aver perso molto in termini commerciali/di fatturato.



L'attacco ransomware è risultato in perdite commerciali/di fatturato per la tua organizzazione? Sì, abbiamo perso molto in termini commerciali/di fatturato, Sì, abbiamo subito perdite parziali in termini commerciali/di fatturato. Organizzazioni del settore privato che sono state colpite dal ransomware, base di partecipanti indicata nel grafico

Tempo Necessario Per Riprendere Le Normali Attività

Le organizzazioni del settore sanitario impiegano più tempo per riprendere le normali attività in seguito a un attacco ransomware, con solo il 47% degli intervistati che tornano operativi entro una settimana, rispetto al 54% del report del 2022. Inoltre, la percentuale delle organizzazioni che hanno avuto bisogno di più di un mese per riprendere le normali attività è aumentata, passando in un anno dal 20% (percentuale arrotondata) al 28% (percentuale arrotondata).



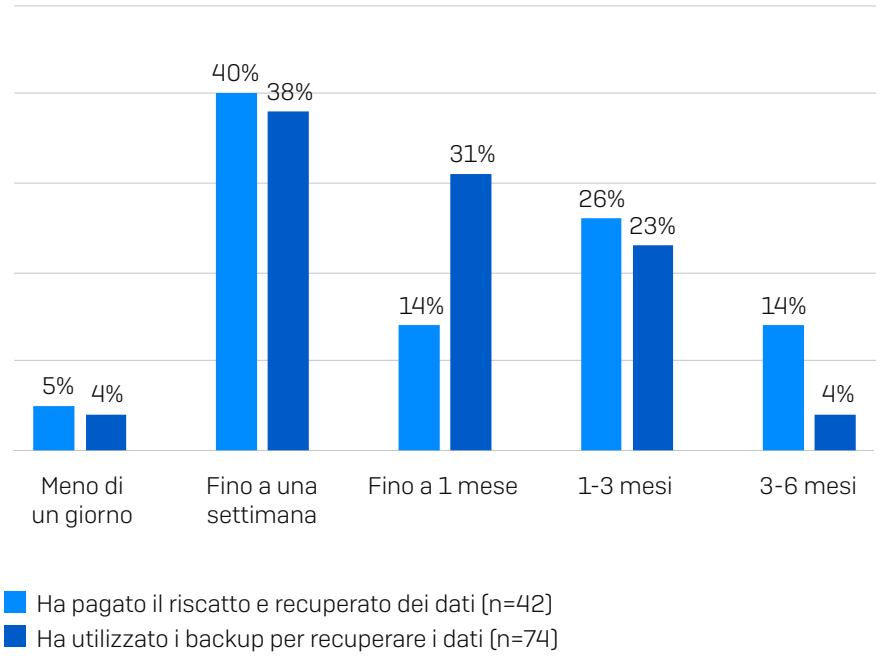
Di quanto tempo ha avuto bisogno la tua organizzazione per riprendere completamente le normali attività operative dopo l'attacco ransomware?
139 (nel 2023)/253 (nel 2022) organizzazioni del settore sanitario che sono state colpite dal ransomware.

Tempo Necessario Per Riprendere Le Normali Attività In Base Al Metodo Di Recupero Dei Dati

Dal sondaggio è emerso che le organizzazioni del settore sanitario che utilizzano i backup per recuperare i dati sono in grado di ripristinare i dati e riprendersi dalle conseguenze dell'attacco più rapidamente, rispetto alle organizzazioni che pagano il riscatto.

Tra i partecipanti al sondaggio che hanno avuto bisogno di più di un mese per recuperare i dati, un quarto (27%, cifra arrotondata) ha utilizzato i backup, mentre il 40% (cifra arrotondata) ha pagato il riscatto.

Anche se queste due opzioni di risposta non si escludono reciprocamente (alcuni intervistati hanno sia pagato il riscatto, sia utilizzato i backup), i vantaggi dei backup in termini di tempi di ripresa delle attività sono evidenti.



Di quanto tempo ha avuto bisogno la tua organizzazione per riprendere completamente le normali attività operative dopo l'attacco ransomware?
Organizzazioni che hanno pagato il riscatto e/o utilizzato backup per recuperare i dati. Base di partecipanti indicata nel grafico

Conclusione

Il ransomware continua a essere una delle minacce più pericolose per le organizzazioni del settore sanitario. Sebbene nello studio di quest'anno la sanità abbia registrato un calo nel tasso di attacchi ransomware, quasi due terzi (60%) degli intervistati sostengono di essere stati colpiti dal ransomware.

Gli avversari informatici continuano ad affinare le proprie tattiche, tecniche e procedure (TTP) di attacco e i team di sicurezza fanno fatica a tenere il passo. Le conseguenze sono un incremento costante dei livelli di attacco e dei tassi di cifratura non autorizzata: quasi tre quarti (73%) delle organizzazioni del settore sanitario colpite dal ransomware hanno subito la cifratura dei dati, in aumento rispetto al 61% dell'anno precedente. Oltretutto, il 37% delle vittime i cui dati erano stati cifrati dichiara di avere subito anche il furto di tali dati.

È comunque rassicurante il fatto che il settore sanitario abbia visto un calo nella propensione a pagare il riscatto per recuperare le informazioni cifrate, che dal 61% dell'anno scorso è scesa al 42% nel 2023.

Allo stesso tempo, l'uso dei backup nel settore sanitario ha subito un leggero incremento, passando in un anno dal 72% al 73%. La buona notizia è che tutte le organizzazioni del settore sanitario i cui dati erano stati cifrati è riuscita a recuperare le informazioni dopo l'attacco, superando il 97% della media di tutti i settori.

I profili assicurativi delle organizzazioni hanno influenzato il metodo scelto per recuperare i dati. Mentre tra le organizzazioni del settore sanitario con polizza cyberassicurativa indipendente il 53% ha optato per pagare il riscatto in seguito alla cifratura non autorizzata dei propri dati, questa statistica ha sfiorato appena il 34% per le organizzazioni che avevano stipulato una copertura più completa che includeva anche l'ambito informatico.

Il costo complessivo di riparazione dei danni per le organizzazioni del settore sanitario è aumentato, passando dagli 1,85 milioni di $ dell'anno scorso ai 2,20 milioni di $ di quest'anno. Con molta probabilità, questo è dovuto (almeno in parte) all'incremento del tasso di cifratura dei dati in seguito a un attacco. I costi di riparazione dei danni per le organizzazioni del settore sanitario sono stati più alti della media di 1,82 milioni di $ per tutti i settori.

Con la crescita del business model del ransomware-as-a-service, Sophos prevede che gli attacchi saranno tutt'altro che in calo nel corso del 2023.

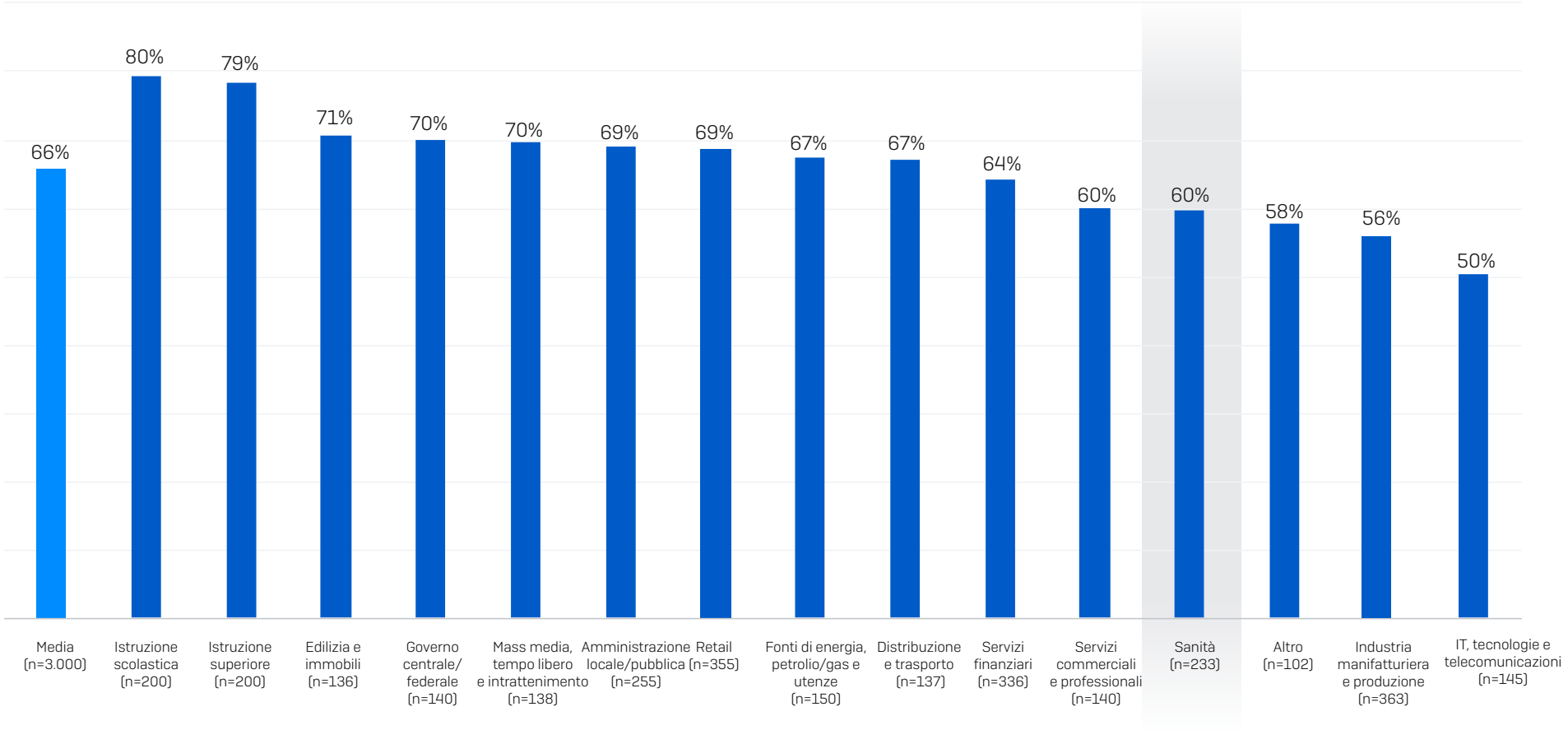
Il nostro consiglio per le organizzazioni è di concentrarsi su quanto segue:

- Potenziamento delle difese, con l'uso di:
  - Strumenti di sicurezza che proteggono i sistemi dai più comuni vettori di attacco (inclusa una protezione endpoint con potenti funzionalità antiexploit per prevenire gli exploit delle vulnerabilità), più Zero Trust Network Access (ZTNA) per sventare i tentativi di utilizzo improprio di credenziali compromesse
  - Tecnologie adattive che rispondono automaticamente agli attacchi, bloccando così gli hacker e regalando ai team di sicurezza tempo prezioso per avviare una risposta adeguata
  - Rilevamento, indagine e risposta alle minacce 24/7, da svolgere internamente oppure in collaborazione con un fornitore di servizi specializzato in Managed Detection and Response (MDR).
- Ottimizzazione della strategia di preparazione per gli attacchi, inclusi backup svolti a intervalli regolari, esercitazioni che prevedono il recupero dei dati dai backup, e compilazione e continuo aggiornamento di un piano di incident response
- Implementazione di una strategia efficace per garantire l'integrità della sicurezza, che deve includere l'applicazione tempestiva delle patch e la revisione a intervalli regolari delle configurazioni degli strumenti di sicurezza

Ulteriori Grafici

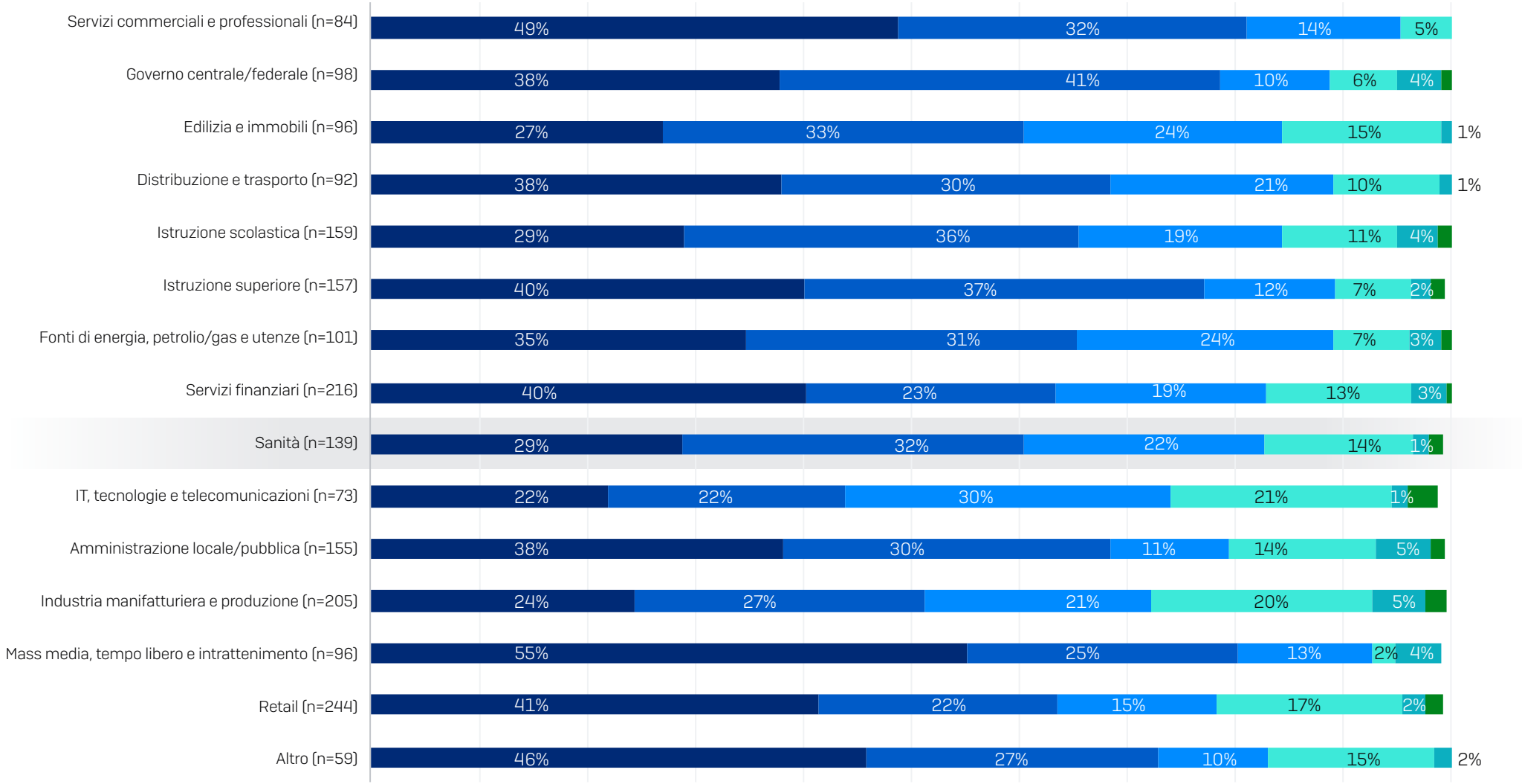
Attacchi Ransomware Per Settore

Percentuale Di Organizzazioni Colpite Dal Ransomware



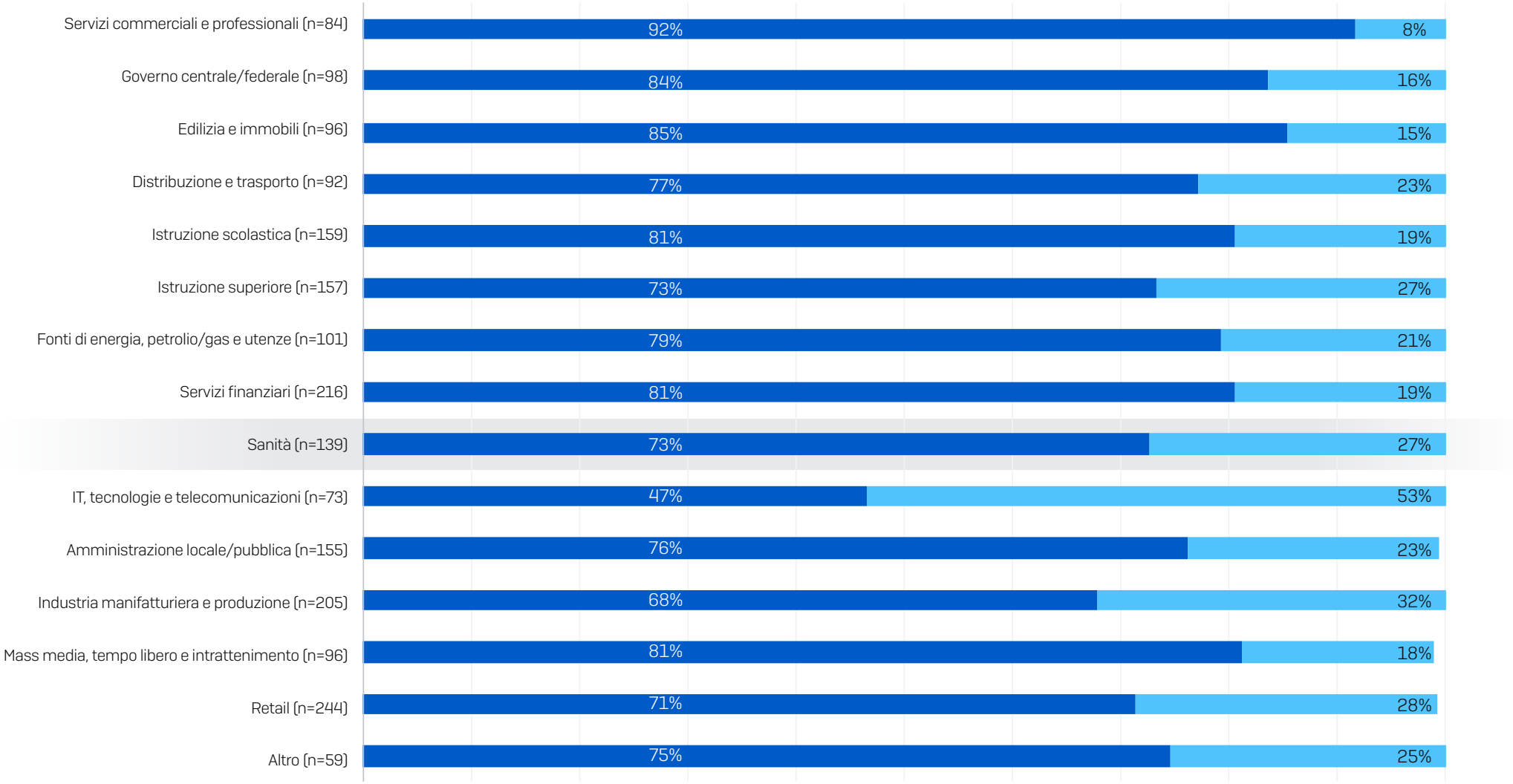
La tua organizzazione è stata colpita dal ransomware l'anno scorso? Base di partecipanti indicata nel grafico

Cause All'Origine Degli Attacchi In Base Al Settore



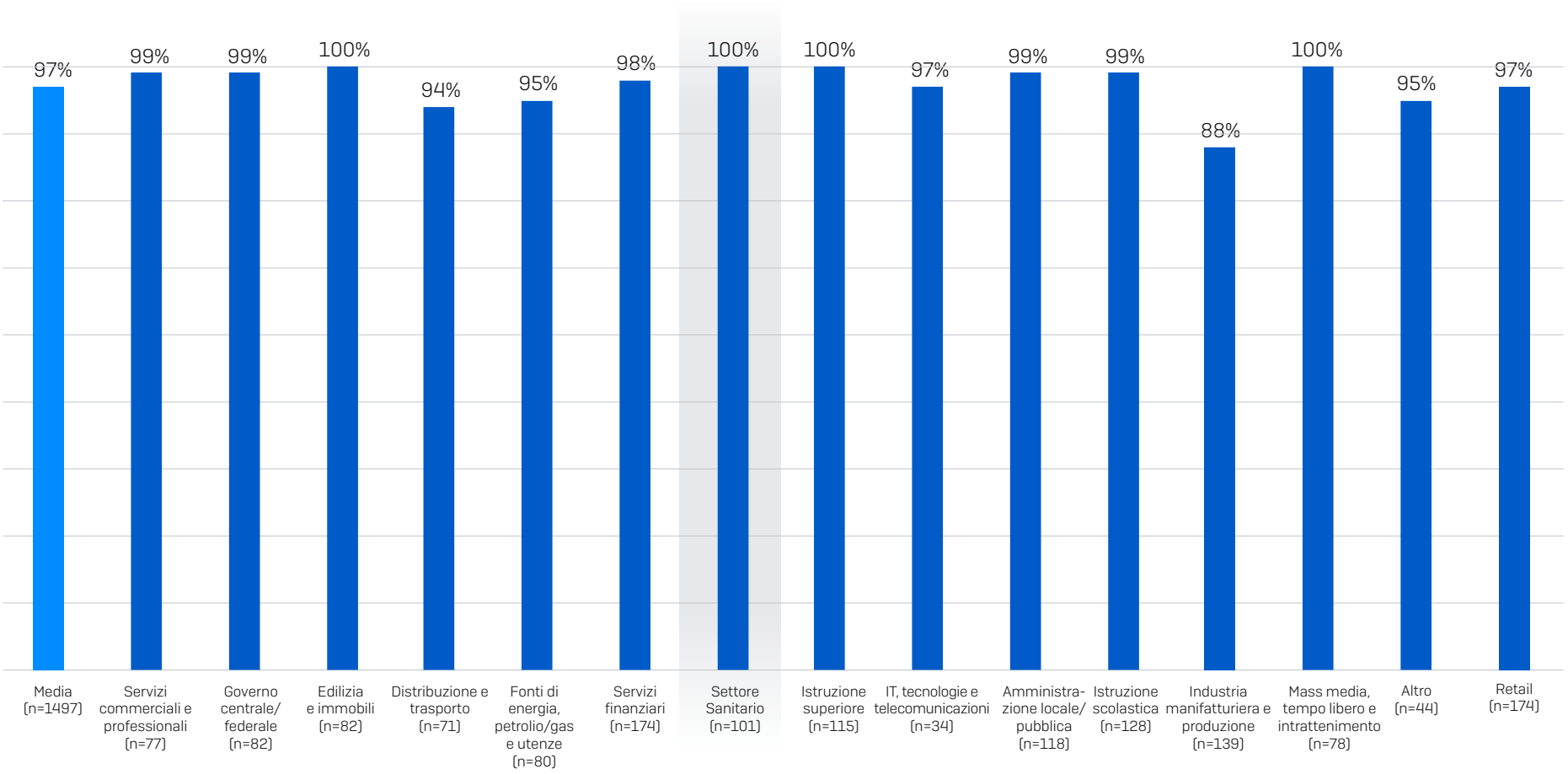
Conosci la causa all'origine dell'attacco ransomware subito l'anno scorso dalla tua organizzazione? Selezione delle opzioni di risposta. Base di partecipanti indicata nel grafico

Cifratura Non Autorizzata Dei Dati In Base Al Settore



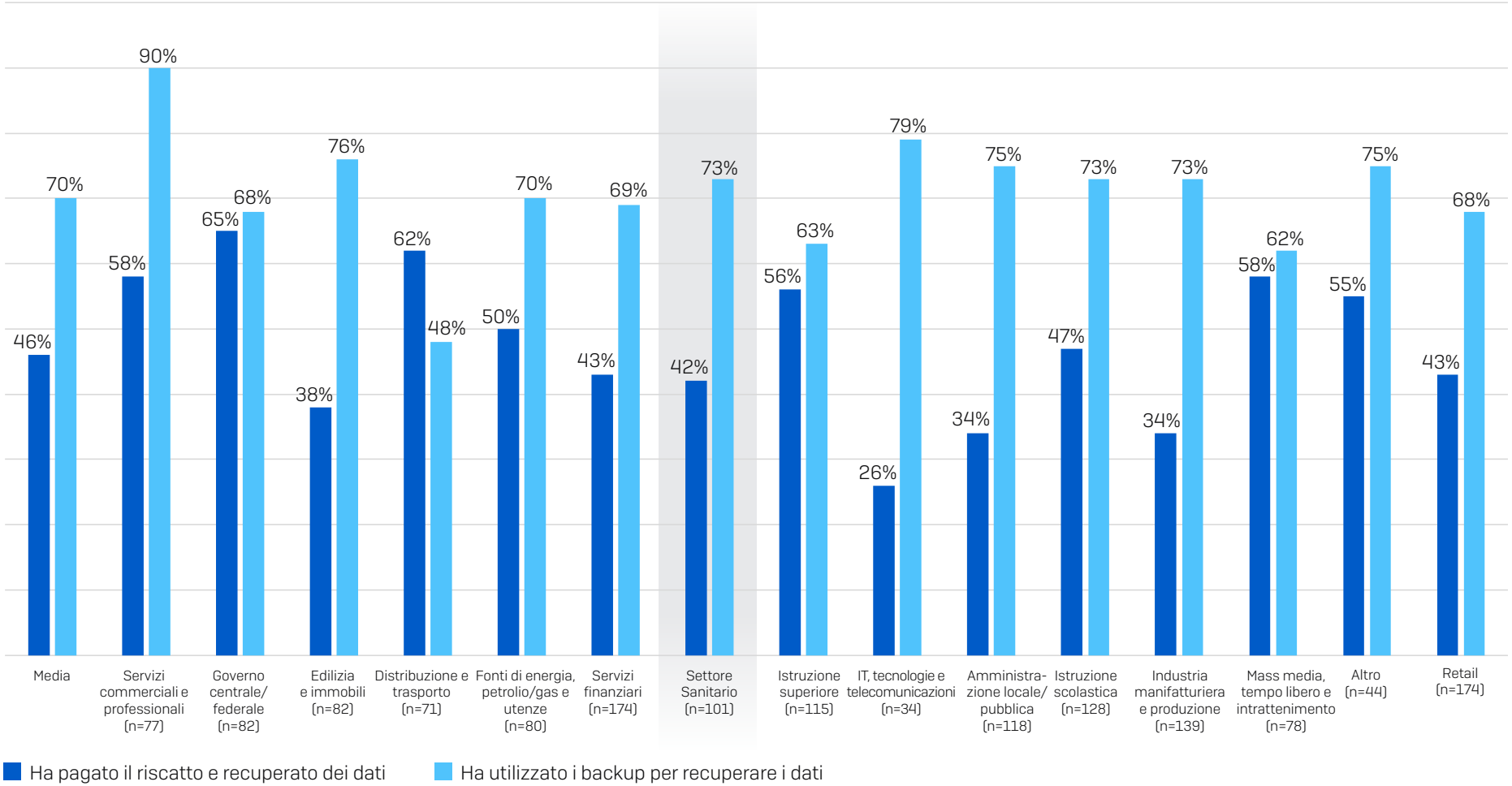
Durante l'attacco ransomware, i cybercriminali sono riusciti a cifrare i dati della tua organizzazione? Alcune opzioni di risposta sono state accorpate. Base di partecipanti indicata nel grafico

Tasso Di Recupero Dei Dati



La tua organizzazione è riuscita a recuperare almeno parte dei dati? n=1.497 organizzazioni colpite da un attacco ransomware che ne ha cifrato i dati

Pagamento Del Riscatto E Utilizzo Dei Backup Per Il Recupero Dei Dati



La tua organizzazione è riuscita a recuperare almeno parte dei dati? n=1.497 organizzazioni colpite da un attacco ransomware che ne ha cifrato i dati

Metodologia Di Ricerca

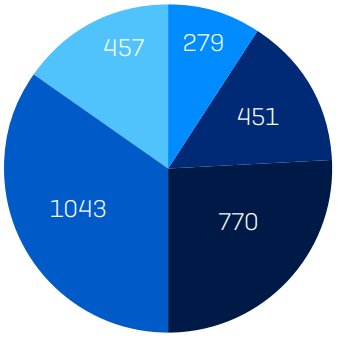
Sophos ha affidato a un'azienda esterna l'incarico di condurre un sondaggio agnostico rispetto ai vendor, coinvolgendo 3.000 Cybersecurity/IT Manager nei mesi di gennaio-marzo 2023. Le persone che hanno partecipato al sondaggio si trovavano in 14 paesi nelle aree geografiche di Nord e Sud America, EMEA (Europa, Medio Oriente e Africa) e Asia-Pacifico.

Tutti gli intervistati lavoravano in organizzazioni con un numero di dipendenti compreso tra 100 e 5.000 (50% in organizzazioni con 100-1.000 dipendenti, 50% in organizzazioni con 1.001-5.000 dipendenti). Nella coorte di ricerca, il fatturato annuo varia da meno di 10 milioni di $ a oltre 5 miliardi di $.

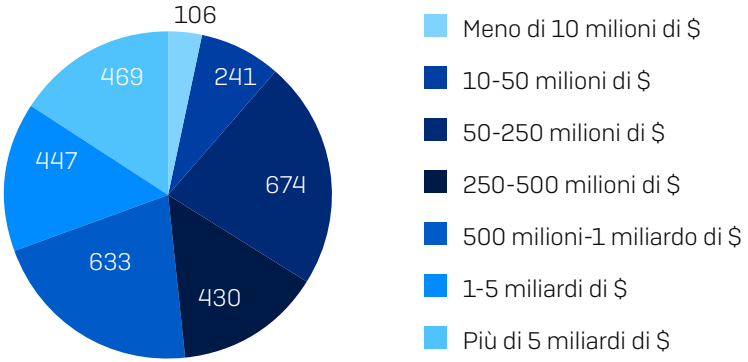
Partecipanti per paese

PAESE	NUMERO DI PARTECIPANTI	PAESE	NUMERO DI PARTECIPANTI
Stati Uniti	500	Regno Unito	200
Germania	300	Sud Africa	200
India	300	Francia	150
Giappone	300	Spagna	150
Australia	200	Austria	100
Brasile	200	Singapore	100
Italia	200	Svizzera	100

Numero Di Intervistati In Base Alle Dimensioni Dell'Organizzazione (Numero Di Dipendenti)



Numero Di Intervistati In Base Alle Dimensioni Dell'Organizzazione (Fatturato Annuo)



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.

03/08/2023 (WP-NP)

SOPHOS