SOPHOS
Cybersecurity evolved.

La Vera Storia Del Ransomware Nel Settore Finanziario 2021

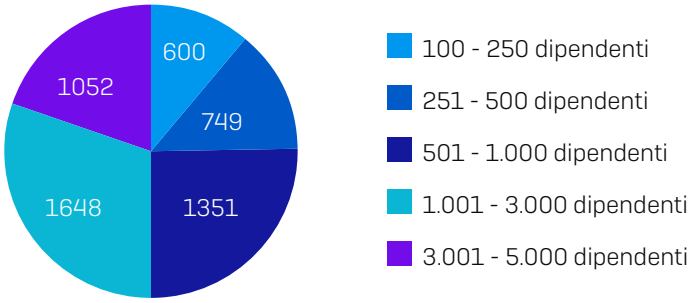
Basato su un sondaggio indipendente a cui hanno partecipato 550 IT Manager, questo report offre nuove prospettive sul panorama attuale del ransomware per il settore dei servizi finanziari. Contiene interessanti approfondimenti sulla prevalenza di questa minaccia nel settore dei servizi finanziari, sull'impatto degli attacchi e sui costi necessari per rimediare ai danni causati dal ransomware. Inoltre, svela i risultati emersi dal confronto tra questo ed altri settori in termini di aspettative future e grado di preparazione contro questi tipi di attacchi.

Whitepaper Sophos. Settembre 2021

Informazioni sul sondaggio

Sophos ha affidato a Vanson Bourne, un'azienda di ricerca indipendente, l'incarico di condurre un sondaggio globale tra 5.400 responsabili IT in 30 paesi. I partecipanti provengono da vari settori, inclusi 550 dipendenti di organizzazioni che operano nel settore dei servizi finanziari. Il sondaggio è stato svolto tra gennaio e febbraio 2021.

Quanti dipendenti ha la vostra organizzazione a livello globale? [5.400]



In quale settore opera la vostra organizzazione? [5.400]

Il 50% dei partecipanti in ogni paese rappresenta organizzazioni con 100-1.000 dipendenti, mentre il restante 50% organizzazioni con 1.001-5.000 dipendenti. I 550 IT Manager che operano nel settore dei servizi finanziari provengono da tutte le aree geografiche che hanno partecipato al sondaggio: Nord e Sud America, Europa, Medio Oriente, Africa e Asia Pacifico.

Area geografica	Num. partecipanti
Nord e Sud America	146
Europa	197
Medio Oriente e Africa	78
Asia Pacifico	129

I 550 IT Manager nel settore dei servizi finanziari

I risultati più salienti per il settore dei servizi finanziari

- Il **34%** delle organizzazioni nel settore dei servizi finanziari **è stato colpito dal ransomware l'anno scorso**
- Il **51%** degli intervistati in organizzazioni colpite dal ransomware l'anno scorso sostiene che nell'attacco di maggiore impatto **i cybercriminali sono riusciti a cifrare i dati**
- Il **25%** dei partecipanti che hanno subito la cifratura dei dati **ha pagato il riscatto per recuperare i dati sottratti** nell'attacco di maggiore impatto
- Il **62%** delle organizzazioni che hanno subito la cifratura dei dati **ha recuperato i dati grazie ai backup**
- In media, dopo aver pagato il riscatto è stato recuperato il **63% dei dati**, il che significa che un terzo dei dati sottratti è rimasto inaccessibile
- Il **91%** delle organizzazioni che operano nel settore dei servizi finanziari ha un **piano per eventi imprevisti in caso di incidenti di malware**
- Il **costo medio necessario per rimediare ai danni di un attacco di 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 e altro) nel settore dei servizi finanziari è pari a **2,10 milioni di USD**

Il ransomware è una realtà molto presente nel settore dei servizi finanziari. L'anno scorso, circa un terzo (34%) di queste organizzazioni è stato colpito dal ransomware. Sebbene si tratti di una percentuale inferiore rispetto alla media globale del 37%, rimane pur sempre un serio motivo di preoccupazione.Un quarto (25%) delle organizzazioni nel settore dei servizi finanziari i cui dati sono stati cifrati ha scelto di pagare il riscatto per recuperare le informazioni sottratte. Anche in questo caso si tratta di una percentuale più bassa rispetto alla media di tutti i settori (32%), il che è probabilmente riconducibile a una capacità superiore alla media di recuperare i dati dai backup. Le statistiche sembrano dimostrare che i servizi finanziari stanno raccogliendo i frutti del proprio investimento in piani di continuità operativa (PCO) e di ripristino in caso di disastro (DRP), grazie ai quali le organizzazioni di questo settore sono pronte ad affrontare situazioni quali gli attacchi di ransomware. Poiché in media le vittime che hanno pagato il riscatto sono riuscite a recuperare solo il 63% dei propri dati, scegliendo di concentrarsi sui backup come metodo principale di recupero, le organizzazioni che operano nei servizi finanziari hanno preso una decisione molto saggia.

Complessivamente, quello dei servizi finanziari è l'unico settore in cui tutte le organizzazioni i cui dati erano stati cifrati sono riuscite a recuperare almeno parte delle informazioni sottratte. Anche in questo caso, è molto probabile che siano stati i loro piani di ripristino in caso di incidenti a prepararle ad affrontare gli attacchi di ransomware.Per quanto riguarda le somme pagate per i riscatti, i servizi finanziari si trovano al di sotto della media: 69.369 USD, rispetto ai 170.404 USD della media di tutti i settori (nota: la base di partecipanti nel settore dei servizi finanziari è troppo bassa per trarre conclusioni definitive).

Purtroppo, le buone notizie finiscono qui. Complessivamente, i costi necessari per rimediare ai danni causati dal ransomware per il settore dei servizi finanziari sono circa un quarto di milione di dollari più alti rispetto alla media globale (2,10 milioni di USD vs 1,85 milioni di USD). Probabilmente la differenza è dovuta agli elevati costi che questo settore deve affrontare, non solo per adottare le misure necessarie a garantire la continuità dei servizi in ogni situazione, ma anche per comunicare la violazione dei dati alle vittime, per rimediare ai danni alla reputazione e per pagare le sanzioni applicabili.

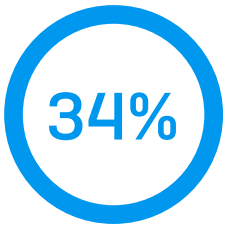
Inoltre, due terzi (68%) dei team tecnici nei servizi finanziari hanno riscontrato un aumento del proprio carico di lavoro di cybersecurity nel 2020, presumibilmente come conseguenza del rapido passaggio allo smart working per via della pandemia. Sebbene tutto questo abbia avuto un impatto significativo sulla capacità dei team tecnici di individuare e rispondere rapidamente ai problemi di cybersecurity, non tutto il male viene per nuocere: il 70% dei team IT ha infatti indicato che la propria capacità di sviluppare maggiori conoscenze e competenze di cybersecurity è aumentata nel 2020, il che ne migliora le prospettive future.

Alle organizzazioni che operano nel settore dei servizi finanziari, consigliamo di continuare a investire nei backup e nei piani di ripristino in caso di disastro, per minimizzare l'impatto di un eventuale attacco. Consigliamo inoltre di estendere la portata delle proprie difese antiransomware con una combinazione tra tecnologie all'avanguardia e threat hunting con supervisione umana, per neutralizzare gli attacchi moderni, solitamente coordinati da hacker che agiscono in tempo reale.

La prevalenza del ransomware nel settore dei servizi finanziari

Il settore dei servizi finanziari è stato colpito dal ransomware l'anno scorso

Dei 550 intervistati nel settore dei servizi finanziari, il 34% è stato colpito dal ransomware l'anno scorso, ovvero *vari computer dell'organizzazione hanno subito le conseguenze di un attacco di ransomware, anche se in alcuni casi i dati delle vittime non sono stati cifrati*.



Percentuale di organizzazioni colpite dal ransomware l'anno scorso

Percentuale di organizzazioni non colpite dal ransomware l'anno scorso, che però prevedono di caderne vittima in futuro

Percentuale di organizzazioni non colpite dal ransomware l'anno scorso, che prevedono di non caderne vittima in futuro

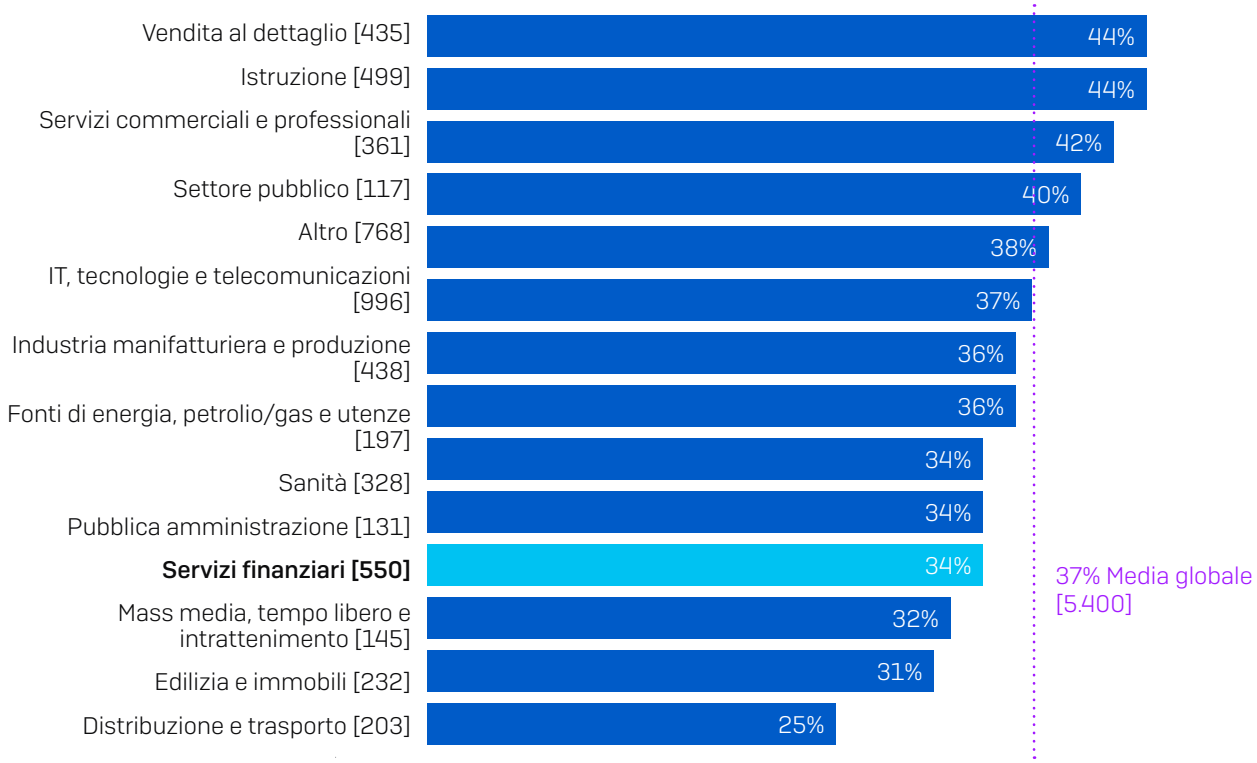
La vostra organizzazione è stata colpita dal ransomware negli ultimi 12 mesi? [550 intervistati nel settore dei servizi finanziari]

Delle organizzazioni che non sono state colpite, il 42% ha dichiarato che si aspetta di subire un attacco di ransomware in futuro, mentre il 22% è convinto di essere adeguatamente protetto contro gli attacchi. I motivi alla base delle aspettative di cadere vittima di un attacco in futuro o di ritenersi al sicuro verranno analizzati in maniera approfondita più avanti in questo documento.

Gli attacchi di ransomware nel settore dei servizi finanziari sono inferiori alla media

Mettendo a confronto i servizi finanziari con altri settori, si osserva un livello di attacco inferiore alla media. Quelli della vendita al dettaglio e dell'istruzione sono i settori che segnalano la quantità più elevata di attacchi di ransomware, con il 44% dei partecipanti che dichiara di essere stato colpito, rispetto alla media globale del 37%.

% di partecipanti colpiti dal ransomware negli ultimi 12 mesi



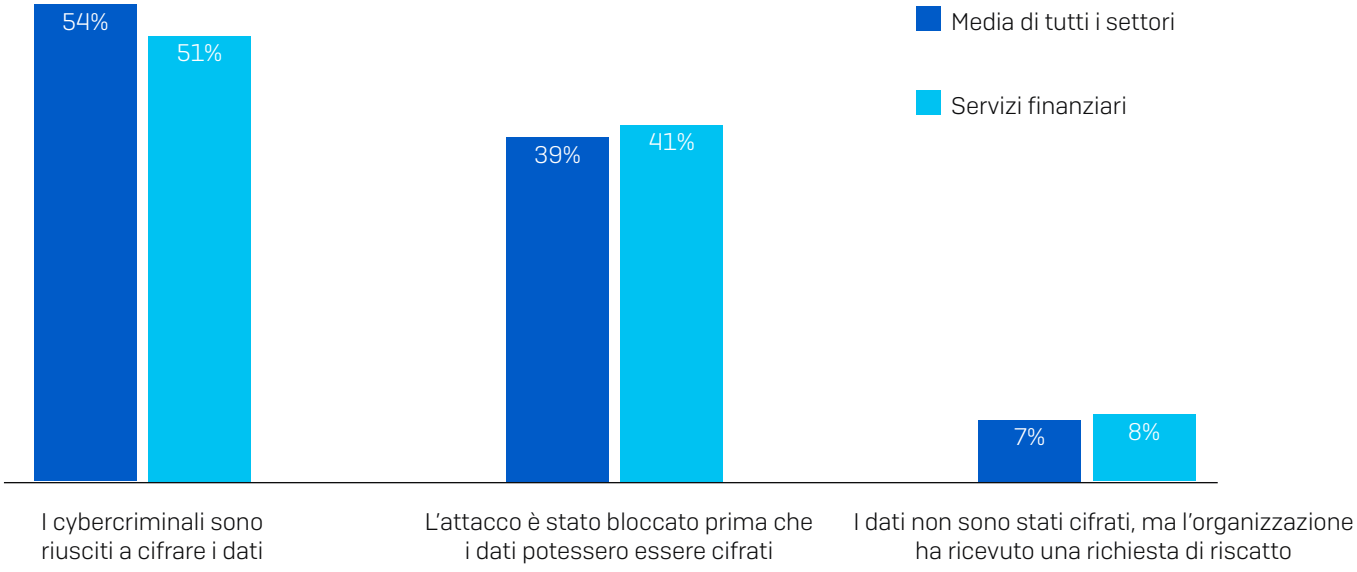
La vostra organizzazione è stata colpita dal ransomware negli ultimi 12 mesi? Sì [base di partecipanti indicata nel grafico], alcune opzioni di risposta sono state omesse, suddivisione in base al settore

Per tutti i settori a livello globale, la percentuale delle organizzazioni colpite dal ransomware negli ultimi 12 mesi ha subito un calo significativo rispetto all'anno precedente, quando il 51% aveva ammesso di esserne caduta vittima. Sebbene questo calo rappresenti una notizia molto positiva, è possibile che sia in parte dovuto all'evoluzione dei comportamenti dei cybercriminali, secondo quanto osservato dai SophosLabs e dal team Sophos Managed Threat Response. Per esempio, molti hacker sono passati dall'utilizzo di attacchi generici e automatizzati, sferrati su vasta scala, all'impiego di attacchi più mirati, che includono hacking di tipo "hands-on-keyboard" con intervento umano diretto. Sebbene la quantità totale degli attacchi sia inferiore, abbiamo osservato che il potenziale di questi attacchi mirati di arrecare è molto più elevato.

L'impatto del ransomware

La capacità del settore dei servizi finanziari di impedire la cifratura dei dati

Abbiamo chiesto agli intervistati le cui organizzazioni erano state colpite dal ransomware l'anno scorso se i cybercriminali fossero riusciti a cifrare i loro dati. Il 51% degli intervistati nel settore dei servizi finanziari ha detto di sì, con una percentuale leggermente inferiore alla media globale del 54%.



Nell'attacco di ransomware più grave, i cybercriminali sono riusciti a cifrare i dati dell'organizzazione? [2006/185 organizzazioni nel settore dei servizi finanziari che sono state colpite dal ransomware l'anno scorso]

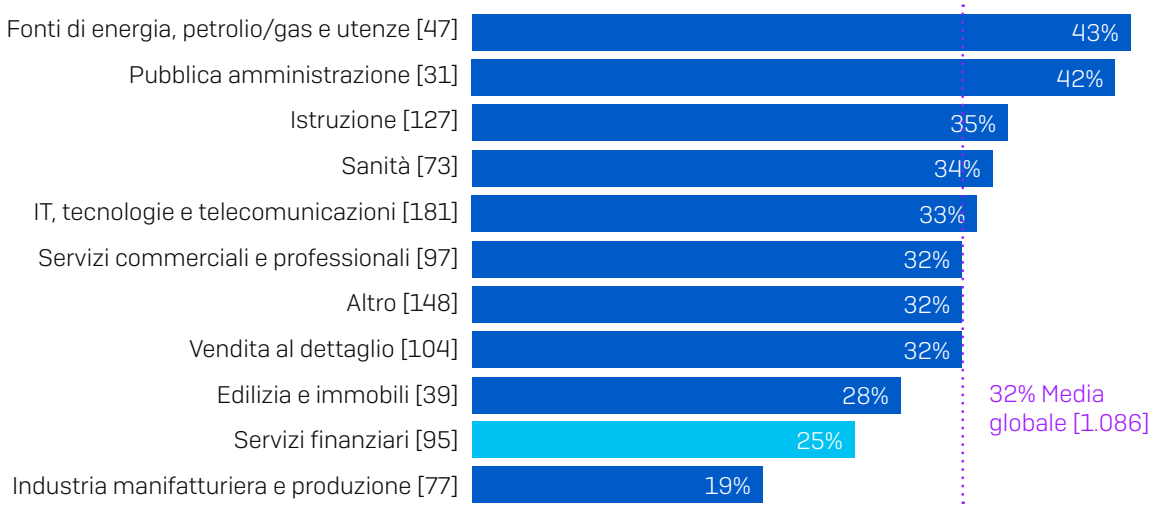
Sebbene le organizzazioni che operano nei servizi finanziari mostrino una capacità superiore alle media di prevenire la cifratura non autorizzata (hanno bloccato il 41% degli attacchi, vs il 39% della media globale), questo settore si è dimostrato vulnerabile a una nuova tendenza in crescita: gli attacchi di estorsione, nei quali i file non vengono cifrati ma prelevati illecitamente, con la minaccia di una loro pubblicazione on-line a meno che non venga pagato il riscatto specificato. L'8% delle organizzazioni nei servizi finanziari che sono state colpite dal ransomware hanno infatti subito un attacco di estorsione.

L'anno scorso i SophosLabs hanno notato un incremento in questo tipo di attacco. Richiede un impegno minore da parte dei cybercriminali, in quanto non implica alcuna azione di cifratura o decifratura dei dati. Spesso gli hacker cercano di indurre le vittime a pagare puntando sulle pesanti sanzioni previste per i casi di violazione dei dati.

Propensione a pagare il riscatto

Dal sondaggio è emerso che i servizi finanziari sono caratterizzati da una propensione a pagare il riscatto molto bassa rispetto agli altri settori. Nei servizi finanziari, tra le organizzazioni i cui dati erano stati cifrati, solo una su quattro (25%) ha accettato di pagare il riscatto, mentre la media globale è del 32%. Come vedremo a breve, uno dei motivi più probabili è l'ottima capacità di questo settore di recuperare i dati cifrati utilizzando i backup.

% di organizzazioni che ha pagato il riscatto per recuperare i dati sottratti



Nell'attacco di 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 di ransomware più grave, alcune opzioni di risposta sono state omesse, suddivisione in base al settore

Tra tutti, il settore delle **fonti di energia, petrolio/gas e utenze** è quello con la maggiore propensione a pagare il riscatto, con

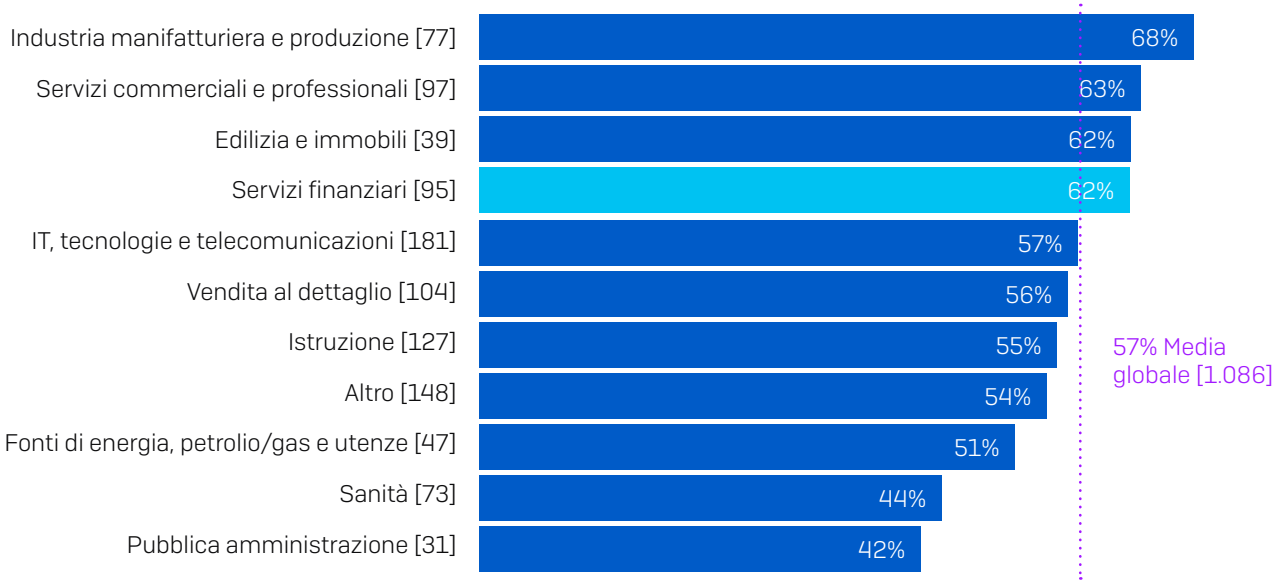
il 43% degli intervistati che dichiara di aver ceduto alla richiesta di riscatto. Questo settore è caratterizzato dalla presenza di molte infrastrutture difficili da aggiornare, per cui le vittime possono sentirsi costrette a pagare il riscatto per garantire che l'erogazione dei servizi non venga interrotta.

La **pubblica amministrazione** si trova al secondo posto nella classifica dei settori più propensi a pagare il riscatto (42%). Questo è anche il settore 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.

Capacità di ripristinare i dati utilizzando i backup

Mettendo a confronto questa sezione con quella precedente, emerge distintamente una correlazione tra la capacità di ripristinare i dati dai backup e la propensione a pagare il riscatto: i settori con maggiore capacità di ripristinare i dati dai backup sono anche quelli con la minore probabilità di pagare il riscatto.

% di organizzazioni che ha utilizzato backup per recuperare i dati cifrati



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

I partecipanti che operano nei servizi finanziari (62%) si sono dimostrati quelli con la maggiore capacità di recuperare i dati cifrati grazie all'uso dei backup. Con molta probabilità, questo è dovuto al fatto che le banche e molte organizzazioni appartenenti ai servizi finanziari sono tenute a implementare piani di continuità operativa (PCO) e di ripristino in caso di disastro (DRP), per prevenire il rischio di enormi perdite finanziarie in caso di violazione dei dati o altra situazione di emergenza. La mancanza di un piano di questo tipo può implicare sanzioni e/o un aumento dei premi assicurativi FDIC. Creare backup e svolgere esercitazioni di ripristino dei dati sono attività essenziali da includere in questi piani.

Tutte le organizzazioni nei servizi finanziari sono riuscite a recuperare i dati cifrati

Nell'attacco di ransomware più grave, l'organizzazione ha recuperato i dati? [95] organizzazioni nei servizi finanziari che hanno dichiarato che, nell'attacco di ransomware più grave, i cybercriminali sono riusciti a cifrare i dati.

La buona notizia per i servizi finanziari è che questo è stato l'unico settore in cui tutte le organizzazioni che hanno subito la cifratura non autorizzata dei dati sono riuscite a recuperare le informazioni sottratte. Come abbiamo visto, il 25% ha pagato il riscatto, il 62% ha utilizzato i backup e il 13% altri metodi per riappropriarsi dei dati.

Il pagamento del riscatto aiuta a recuperare solo parte dei dati

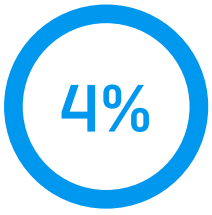
Tuttavia, le vittime che hanno pagato il riscatto non sono riuscite a recuperare tutti i dati. Quello che i cybercriminali non dicono quando inviano una richiesta di riscatto è che, anche pagando, le probabilità di recuperare tutti i dati sono poche.

Percentuale di dati recuperati dopo aver pagato il riscatto **MEDIA DI TUTTI I SETTORI**

Percentuale di dati recuperati dopo aver pagato il riscatto **MEDIA PER IL SETTORE DEI SERVIZI FINANZIARI**

Quantità media di dati che le organizzazioni sono riuscite a recuperare in seguito all'attacco di ransomware di maggiore impatto. [344/24] organizzazioni che hanno pagato il riscatto per recuperare i dati sottratti

La base di partecipanti nel settore dei servizi finanziari è troppo bassa per trarre conclusioni definitive. Tuttavia, a titolo informativo, gli intervistati nel settore dei servizi finanziari hanno dichiarato di aver recuperato in media solo il 63% dei propri dati dopo aver pagato il riscatto, mentre più di un terzo delle informazioni è rimasto inaccessibile. Questa statistica è leggermente inferiore rispetto alla media globale (65%). Con molta probabilità, non si tratta di una strategia deliberata da parte degli hacker, ma piuttosto di una dimostrazione del fatto che i cybercriminali dedicano maggior tempo e impegno allo sviluppo di potenti strumenti di cifratura, trascurando quelli di decifratura.



Percentuale che ha recuperato TUTTI i dati

Percentuale che ha recuperato la metà dei dati o meno

Quantità di dati che le organizzazioni sono riuscite a recuperare in seguito all'attacco di ransomware di maggiore impatto. [24] organizzazioni nel settore dei servizi finanziari che hanno pagato il riscatto per recuperare i dati sottratti

Ne è ulteriore conferma il fatto che solo nel 4% dei casi le organizzazioni nel settore dei servizi finanziari che hanno pagato il riscatto sono riuscite a recuperare **tutti** i dati; il 33% ne ha recuperata la **metà o meno**. È evidente che pagare il riscatto non è un buon investimento. Anche in questo caso, la base di partecipanti nel settore dei servizi finanziari è piuttosto bassa, per cui i risultati sono da considerarsi puramente indicativi.

Il costo del ransomware

Sveliamo il segreto: ecco a quanto ammontano i pagamenti di riscatto

Dei 357 intervistati in tutti i settori che dichiarano di aver pagato il riscatto, 282 hanno anche condiviso la somma versata.

$ 170.404

Somma di riscatto media a livello GLOBALE

A quanto ammonta la somma di riscatto pagata dalla vostra organizzazione nell'attacco di ransomware più grave? [282] organizzazioni che hanno pagato il riscatto per recuperare i dati sottratti

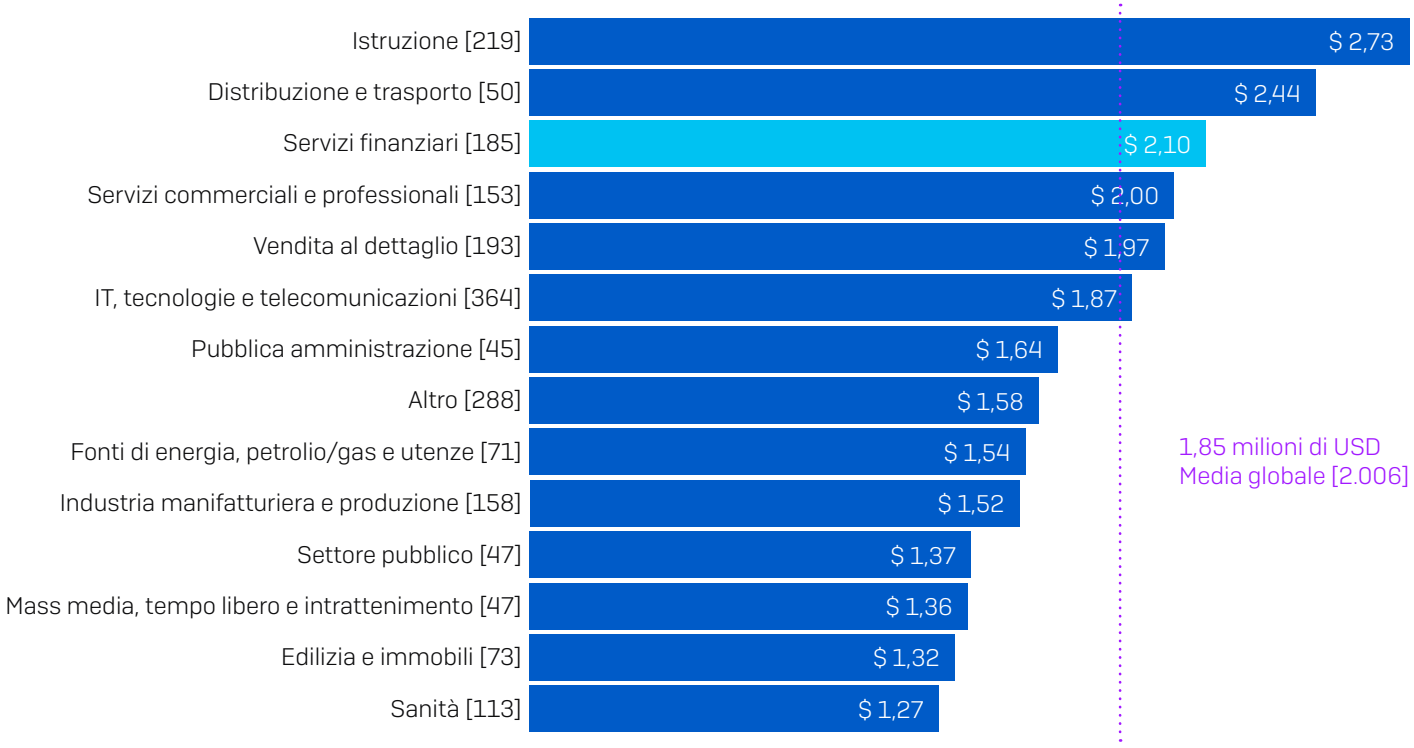
Per **tutti i settori**, la media globale per la somma di riscatto pagata dalle organizzazioni ammonta a 170.404 USD. 13 intervistati appartenenti a organizzazioni che operano nei **servizi finanziari** hanno condiviso le somme di riscatto versate, che ammontano in media a 69.369 USD, ovvero a ben 100.000 USD in meno rispetto alla media globale. La differenza nelle somme pagate è con molta probabilità dovuta all'ottima capacità di questo settore di recuperare i dati con l'uso dei backup. Inoltre, pagare un riscatto può esporre le organizzazioni che operano nei servizi finanziari a un maggiore rischio in termini legali e di conformità alle normative, incluso quello di contravvenzione alle leggi contro il riciclaggio di denaro (AML) e il finanziamento del terrorismo (CFT).

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**. A partecipare al nostro sondaggio sono state organizzazioni di medie dimensioni con un numero di utenti compreso tra 100 e 5.000. In genere, questo tipo di organizzazioni ha a disposizione risorse finanziarie molto limitate rispetto a quelle più grandi. I cybercriminali che sferrano attacchi di 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 confermano questa tendenza, in quanto il pagamento di riscatto medio delle organizzazioni con 100-1.000 dipendenti ammonta a 107.694 USD, mentre quello delle organizzazioni con 1.001-5.000 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**. Come abbiamo osservato prima, questo sondaggio include 30 paesi in tutto il mondo, con livelli di PIL diversi. 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. In India invece il pagamento di riscatto medio è stato di 76.619 USD, meno della metà della media globale (base: 86 partecipanti).

Costo medio per rimediare ai danni causati dal ransomware nel settore dei servizi finanziari

Il riscatto costituisce solamente una parte minima dei costi necessari per rimediare ai danni causati da un attacco di ransomware. Le vittime devono affrontare varie spese aggiuntive, incluse quelle relative alla ricostruzione completa dei sistemi informatici e alla loro protezione, oltre a pubbliche relazioni e indagini sull'accaduto.



Costo medio approssimativo sostenuto dalle organizzazioni per ammortizzare l'impatto dell'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.) [base di partecipanti indicata nel grafico] partecipanti la cui organizzazione ha subito un attacco di ransomware l'anno scorso, suddivisione in base al settore

Dal sondaggio è emerso che per il settore dei servizi finanziari il costo medio per rimediare ai danni del ransomware è pari a 2,10 milioni di USD (considerando tempi di inattività, ore di lavoro perse, costi associati a dispositivi e rete, perdita di opportunità commerciali, somma pagata per il riscatto, sanzioni legali e normative e così via), che è nettamente superiore rispetto alla media globale (1,85 milioni di USD).

I potenziali fattori alla base di queste cifre sono diversi. Prima di tutto, le organizzazioni che operano nei servizi finanziari gestiscono un'enorme quantità di dati di natura sensibile relativi a persone fisiche, aziende ed enti pubblici, per cui, nell'ambito delle attività necessarie per rimediare ai danni, devono sostenere costi più elevati per la comunicazione dei casi di violazione dei dati. In secondo luogo, un'interruzione delle normali attività lavorative per le organizzazioni che operano in questo settore rischierebbe di seminare scompiglio in tutto il mondo. Sulle aziende grava pertanto la pressione di dover tornare operative il più rapidamente possibile ed a qualunque costo.

Inoltre, quello dei servizi finanziari è uno dei settori che prevede le regole più rigide a livello internazionale. Le organizzazioni devono attenersi a moltissime normative (incluse SOX, GDPR e PCI DSS), che prevedono tutte sanzioni molto pesanti in caso di inosservanza. Le salatissime multe in caso di violazione dei dati come conseguenza di un attacco di ransomware contribuiscono a far aumentare i costi necessari per rimediare ai danni.

Infine, poiché i clienti possono passare con molta facilità a un competitor, le organizzazioni che operano nel settore dei servizi finanziari sono completamente esposte all'impatto sul business di eventuali danni alla reputazione, incluse la perdita di clienti e la chiusura dei conti.

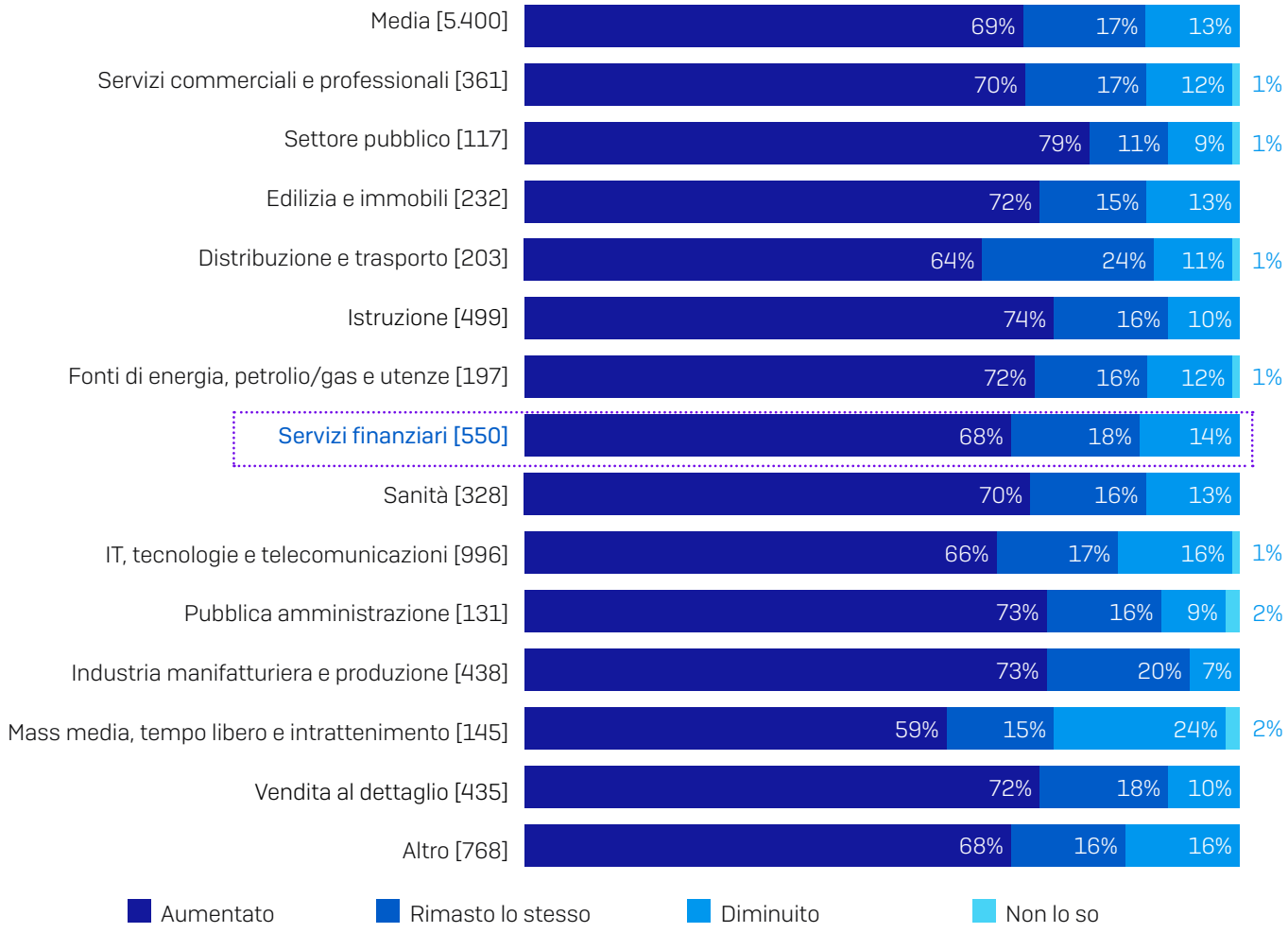
Il ransomware è solo una delle tante sfide di cybersecurity

Il ransomware è un problema di cybersecurity molto serio per le organizzazioni nel settore dei servizi finanziari, ma non è di certo l'unico. I team IT si trovano ad affrontare una grande quantità di richieste e la pandemia non ha fatto altro che aggravare la situazione.

Il carico di lavoro di cybersecurity è aumentato nel 2020

Il personale IT che opera nel settore dei servizi finanziari è tra quelli che hanno avvertito maggiormente l'impatto della pandemia, con il 68% degli intervistati che dichiara di aver notato un aumento del carico di lavoro relativo alla cybersecurity nel corso del 2020. Anche se l'incremento è stato segnalato dalla maggior parte dei partecipanti al sondaggio in tutti i settori, il settore pubblico è quello che ha riscontrato maggiormente un aumento nel carico di lavoro.

Com'è cambiato il carico di lavoro di cybersecurity nel 2020



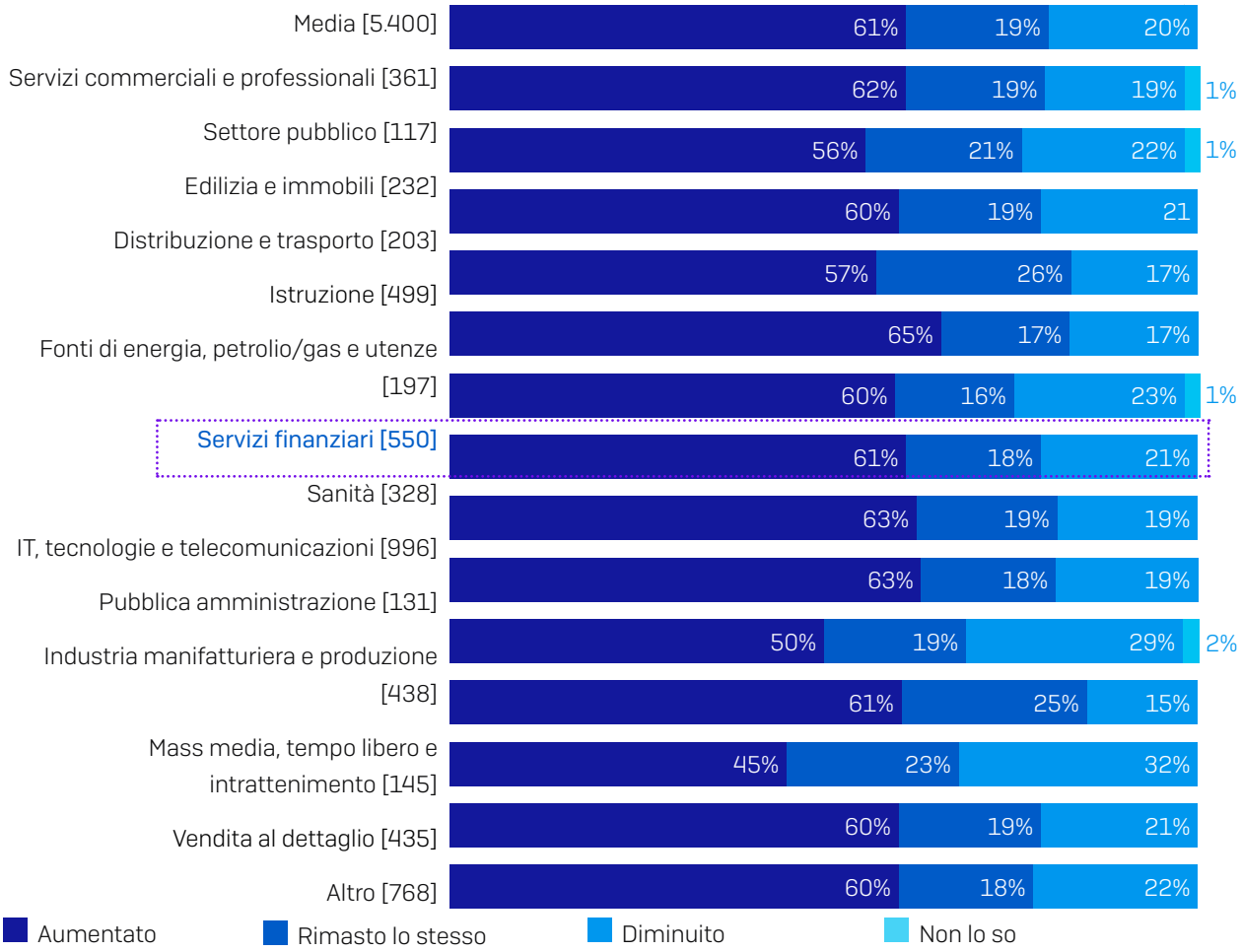
Nel 2020 il nostro carico di lavoro di cybersecurity è aumentato/diminuito/rimasto lo stesso [base di partecipanti indicata nel grafico], suddivisione in base al settore

La rapida adozione dello smart working e l'esigenza di implementare nuovi servizi e soluzioni sia per i dipendenti che per i clienti al fine di garantire la continuità dei servizi è stato uno dei principali fattori alla base dell'aumento del carico di lavoro per il personale IT. Con molta probabilità, le capacità di monitoraggio e risposta alle minacce di ransomware dei team IT è stata limitata dalla necessità di dedicare maggiore attenzione alla protezione di nuove piattaforme on-line.

Il maggiore carico di lavoro ha incrementato i tempi di risposta

Una delle conseguenze dell'aumento del carico di lavoro di cybersecurity nel 2020 è stato il rallentamento dei tempi di risposta ai casi IT. Per il settore dei servizi finanziari l'impatto è stato molto elevato, con il 61% degli intervistati che segnala di aver osservato un aumento dei tempi di risposta l'anno scorso.

Cambiamenti nei tempi di risposta ai casi IT nel 2020



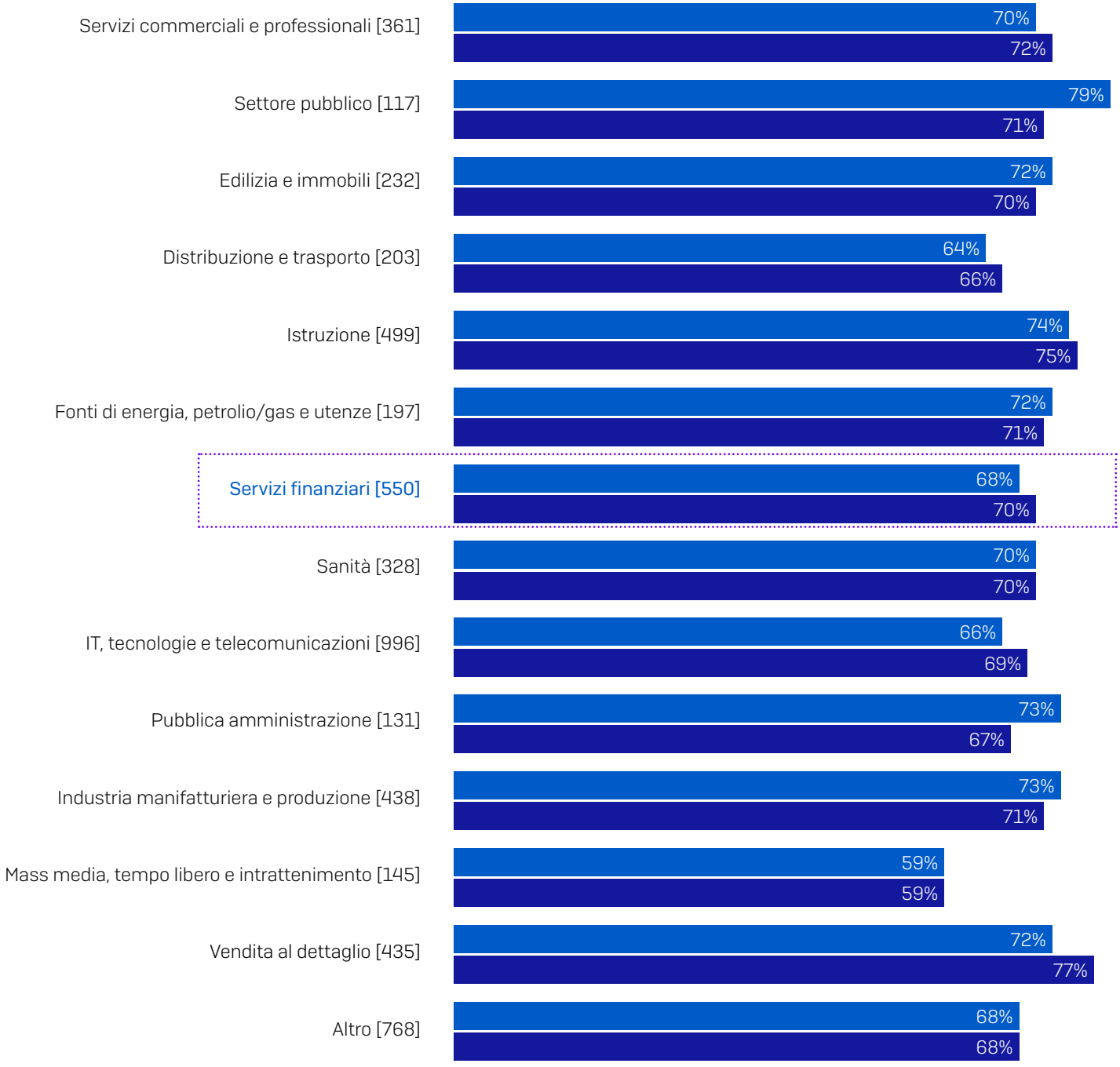
Nel 2020 i nostri tempi di risposta ai casi IT sono aumentati/diminuiti/rimasti gli stessi. [base di partecipanti indicata nel grafico], suddivisione in base al settore

Quando un cybercriminale riesce a infiltrarsi in un ambiente informatico, è essenziale bloccarlo il prima possibile. Più tempo ha a disposizione per esplorare la rete e accedere ai dati, maggiore sarà l'impatto finanziario e operativo dell'attacco. L'allungamento dei tempi di risposta è pertanto motivo di allarme.

L'aumento del carico di lavoro ha portato a sviluppare conoscenze e competenze

Non tutto il male vien per nuocere. Esiste anche una connessione diretta tra l'aumento del carico di lavoro di cybersecurity e lo sviluppo di maggiori conoscenze e competenze di cybersecurity.

Aumento del carico di lavoro di cybersecurity e sviluppo di maggiori conoscenze e competenze di cybersecurity



Nel 2020 il nostro carico di lavoro di cybersecurity/la nostra capacità di sviluppare maggiori conoscenze e competenze di cybersecurity è aumentato/a [base di partecipanti indicata nel grafico], suddivisione in base al settore

Il 70% dei team IT nel settore dei servizi finanziari sostiene che la propria capacità di sviluppare maggiori conoscenze e competenze di cybersecurity è aumentata durante il 2020.

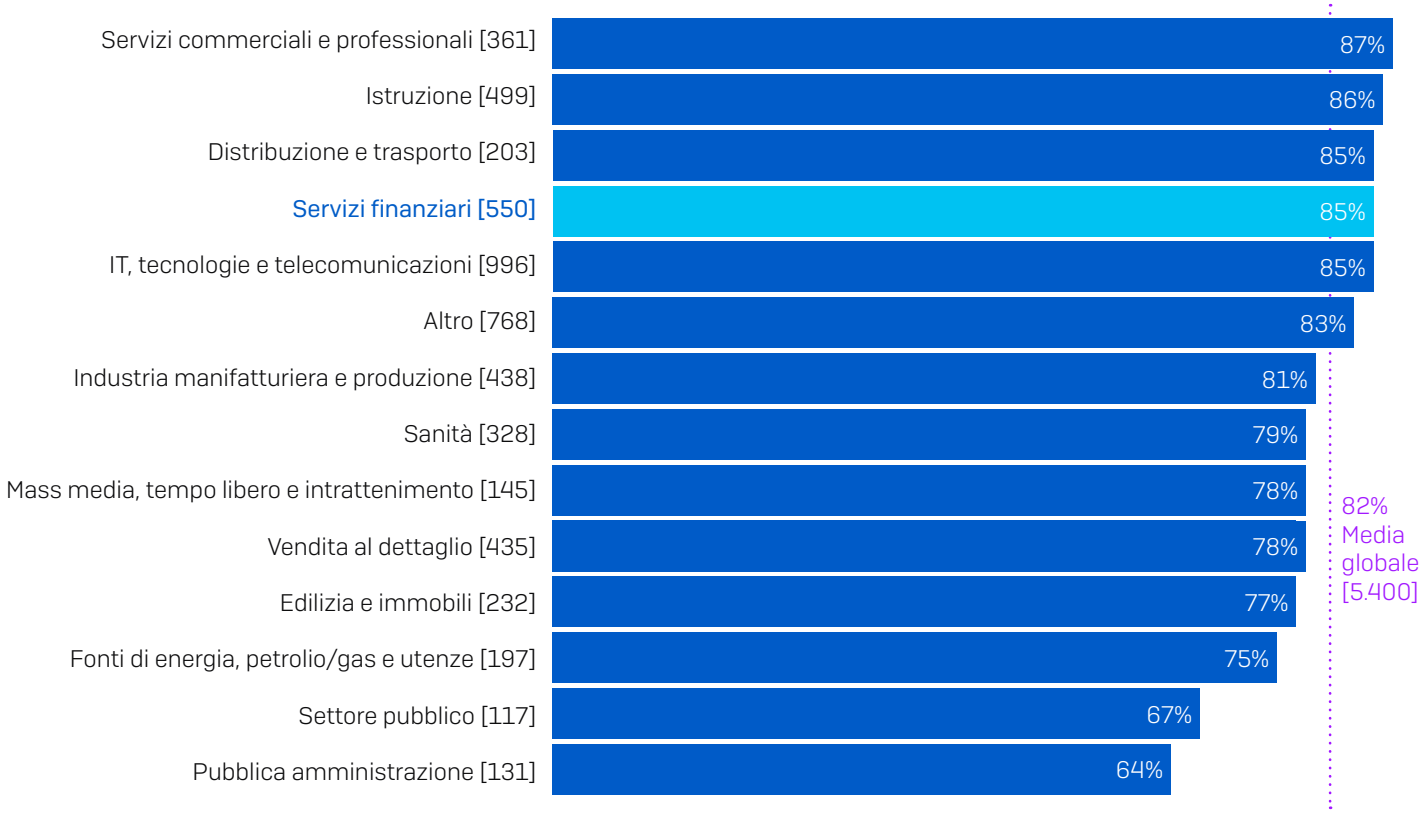
Whitepaper Sophos. Settembre 2021

Se da un lato il maggiore carico di lavoro mette i team sotto pressione, dall'altro offre anche nuove opportunità per espandere le competenze. Inoltre, è probabile che le circostanze eccezionali della pandemia abbiano spinto il personale tecnico a superare i propri limiti, raggiungendo risultati che altrimenti non sarebbero stati richiesti.

Preparazione ad affrontare le sfide future

L'85% degli intervistati nel settore dei servizi finanziari concorda di avere gli strumenti e le conoscenze necessari per svolgere indagini esaustive, se vengono rilevate attività sospette nell'organizzazione: una percentuale superiore alla media globale dell'82%. È sicuramente un'ottima notizia per questo settore, considerando l'aumento del carico di lavoro di cybersecurity riscontrato. Avere strumenti validi e conoscenze adeguate è fondamentale per poter indagare sulle minacce informatiche e debellarle.

Intervistati che sostengono di avere gli strumenti e le conoscenze necessari per svolgere indagini sulle attività sospette



Se vengono rilevate attività sospette nella mia organizzazione, ho a disposizione gli strumenti e le conoscenze necessari per svolgere indagini esaustive: Pienamente d'accordo, D'accordo. Alcune opzioni di risposta sono state omesse [base di partecipanti indicata nel grafico], suddivisione in base al settore

Il futuro

Le aspettative del settore dei servizi finanziari verso gli attacchi futuri

Prevede che subirà un attacco di ransomware in futuro

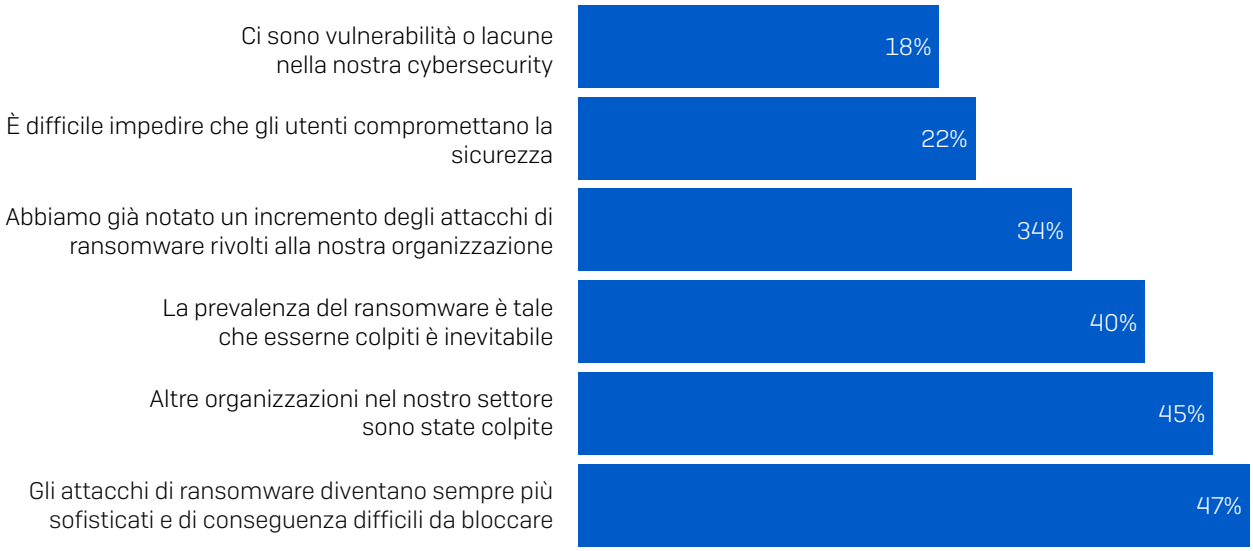
Prevede che non subirà un attacco di ransomware in futuro

[550] intervistati nel settore dei servizi finanziari che hanno risposto "No" alla domanda "La vostra organizzazione è stata colpita dal ransomware negli ultimi 12 mesi?"

Come abbiamo già visto in questo rapporto, il 63% dei partecipanti al sondaggio appartenenti al settore dei servizi finanziari non è stato colpito dal ransomware l'anno scorso. Il 42% prevede che subirà un attacco di ransomware in futuro. Il 22% invece non si aspetta un attacco.

I motivi per cui il settore dei servizi finanziari si aspetta di essere colpito dal ransomware

Tra le organizzazioni nel settore dei servizi finanziari che non sono state colpite dal ransomware ma che ritengono che saranno attaccate in futuro, il motivo più comune (47%) per cui prevedono di subire un attacco è che gli attacchi di ransomware stanno diventando sempre più sofisticati e di conseguenza difficili da bloccare. Sebbene si tratti di percentuali molto alte, il fatto che queste organizzazioni siano consapevoli che il ransomware continua a evolversi è molto positivo. Ciò potrebbe anche essere stato uno dei fattori che hanno contribuito alla loro capacità di bloccare i potenziali attacchi di ransomware l'anno scorso.



Perché prevedete che la vostra organizzazione sarà colpita dal ransomware in futuro? [229 organizzazioni nel settore dei servizi finanziari che non sono cadute vittima del ransomware l'anno scorso ma prevedono che ne saranno colpite in futuro, alcune opzioni di risposta sono state omesse]

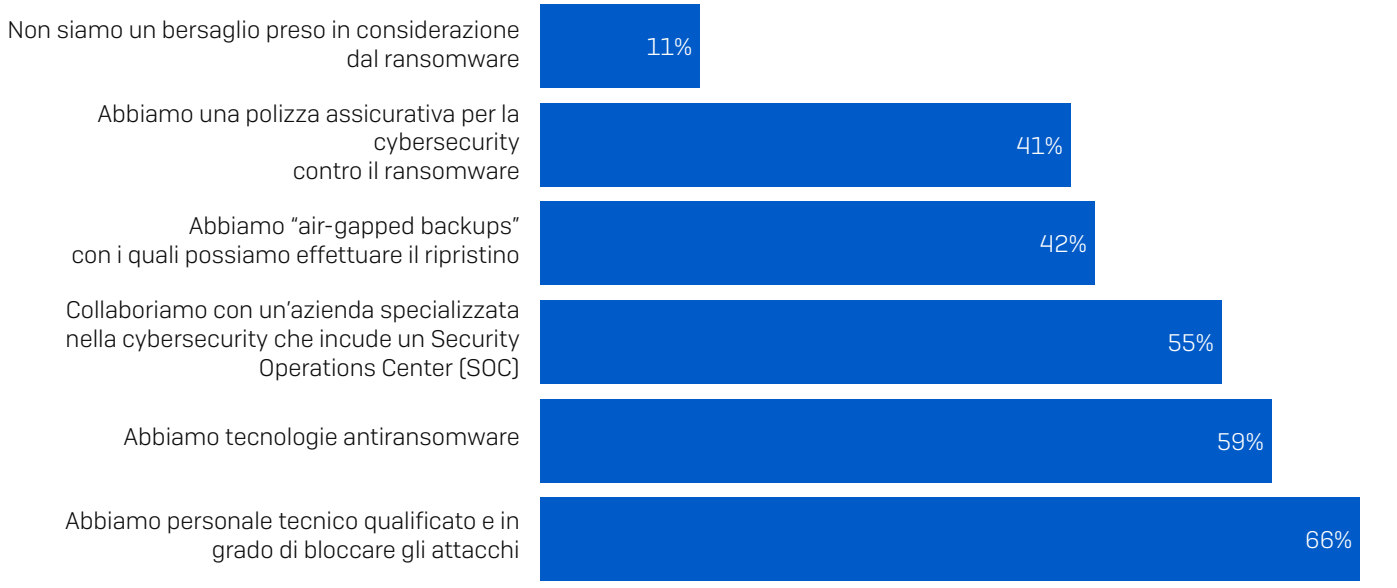
In aggiunta, il 45% degli intervistati sostiene che anche altre organizzazioni nel proprio settore sono state colpite, e questo ne aumenterebbe la probabilità di caderne vittima.

Il 22% degli intervistati ritiene che uno dei motivi principali per cui prevedono di essere colpiti dal ransomware in futuro è il rischio che gli utenti compromettano la sicurezza dei sistemi. 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 18% degli intervistati nel settore dei servizi finanziari ammette di avere vulnerabilità o lacune nella propria struttura di cybersecurity. Sebbene la presenza di lacune di sicurezza sia naturalmente preoccupante, riconoscere che il problema esiste è un primo passo molto importante nel processo di potenziamento delle difese informatiche.

I motivi per cui le organizzazioni nel settore dei servizi finanziari prevedono che non saranno colpite dal ransomware

119 intervistati nel settore dei servizi finanziari hanno dichiarato che la propria organizzazione non è stata colpita dal ransomware l'anno scorso e non si aspettano di caderne vittima in futuro.



Perché prevedete che la vostra organizzazione non sarà colpita dal ransomware in futuro? [119] organizzazioni nel settore dei servizi finanziari che non sono cadute vittima del ransomware l'anno scorso e che prevedono che non ne saranno colpite in futuro, alcune opzioni di risposta sono state omesse

Il motivo principale alla base di questa fiducia è la disponibilità di personale IT qualificato e in grado di bloccare gli attacchi (66%), seguita dall'utilizzo di tecnologie antiransomware (59%). 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 si tratti di dipendenti interni o professionisti esterni, gli esperti umani hanno capacità insostituibili di identificare alcuni degli indizi tipici che rivelano che un'organizzazione si trova nell'occhio del mirino dei cybercriminali del ransomware. Il nostro consiglio per tutte le organizzazioni è sviluppare le competenze tecniche umane a propria disposizione, per affrontare la minaccia costante del ransomware.

Nel 55% dei casi, gli intervistati nel settore dei servizi finanziari che prevedono che non saranno colpiti dal ransomware collaborano con aziende specializzate in cybersecurity che includono un Security Operations Center (SOC). È rassicurante osservare che, quando ne hanno bisogno, le organizzazioni si affidano ai servizi di esperti esterni per migliorare ed estendere la protezione.

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

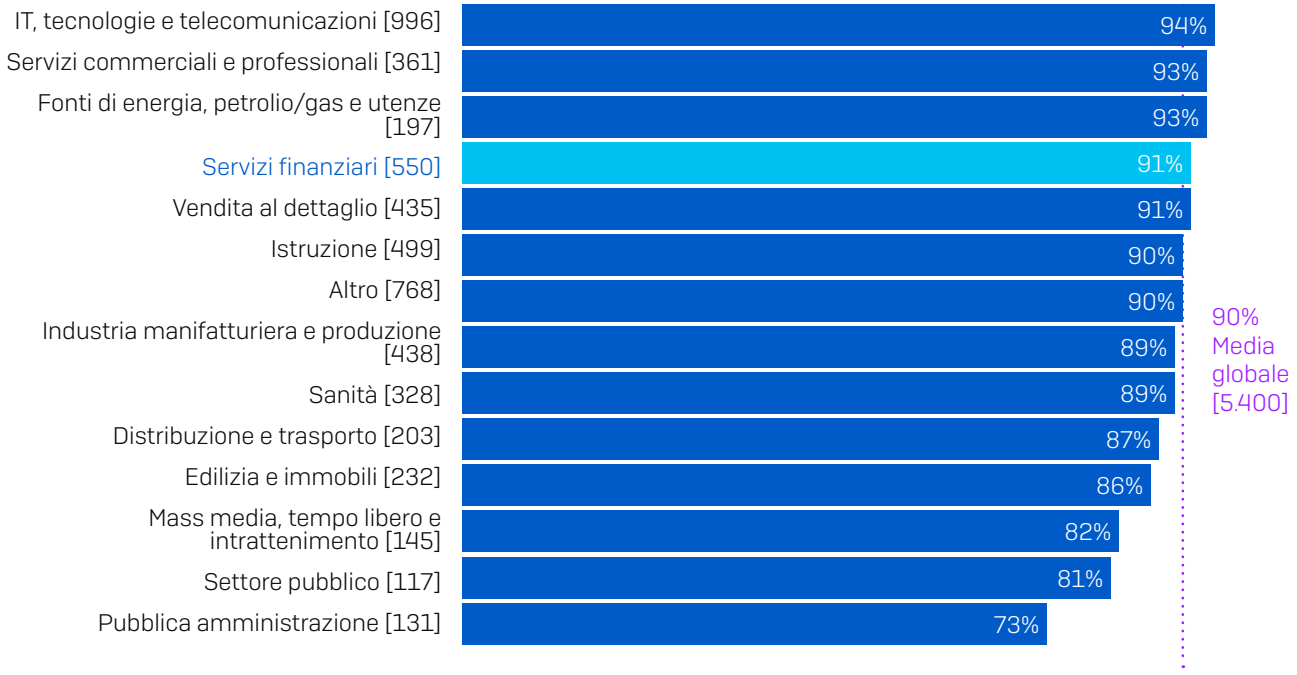
- Il 61% degli intervistati nel settore dei servizi finanziari che ritengono che non saranno colpiti da un attacco adotta approcci che non offrono alcuna protezione contro il ransomware.
  - Il 41% ha indicato di avere una polizza assicurativa per la cybersecurity contro il ransomware. Le assicurazioni aiutano a pagare i costi derivati dagli attacchi, ma non sono in grado di bloccarli.
  - Il 42% ha indicato di disporre di "air-gapped backups". Sebbene i backup siano strumenti importanti per ripristinare i dati in seguito a un attacco, non offrono alcuna prevenzione.

  Nota: alcuni degli intervistati hanno selezionato entrambe le opzioni e il 61% ha selezionato almeno una delle due opzioni.
- L'11% ritiene di non essere un bersaglio preso in considerazione dal ransomware. Purtroppo, questa affermazione non è vera. Nessuna organizzazione è al sicuro.

Le organizzazioni che operano nel settore dei servizi finanziari hanno un livello di preparazione elevato

Rispondere a un attacco informatico critico può essere estremamente stressante. Sebbene non esista un rimedio per alleviare completamente lo stress generato da un attacco, un piano strategico di risposta agli incidenti è un metodo infallibile per minimizzarne l'impatto.

% di partecipanti che hanno un piano per eventi imprevisti in caso di incidenti di malware



Il piano di continuità operativa (PCO)/piano di ripristino in caso di disastro (DRP) della vostra organizzazione include un piano di emergenza per rimediare ai danni di un incidente di malware grave? "Sì, abbiamo un piano completo e dettagliato per eventi imprevisti in caso di malware" e "Sì, abbiamo un piano parzialmente sviluppato per eventi imprevisti in caso di malware" [base di partecipanti indicata nel grafico], alcune opzioni di risposta sono state omesse, suddivisione in base al settore

È pertanto rassicurante osservare che il 91% delle organizzazioni che operano nel settore dei servizi finanziari ha un piano per eventi imprevisti in caso di incidenti di malware. Tra queste, poco più della metà (51%) può contare su un piano completo e dettagliato e il 40% su un piano parzialmente sviluppato. Queste statistiche sono in linea con la media di tutti i settori (90%).

Raccomandazioni

Alla luce dei risultati del sondaggio, gli esperti di Sophos consigliano le seguenti migliori pratiche per tutte le organizzazioni di qualsiasi settore:

1. **Presumere che essere colpiti è inevitabile.** Il ransomware rimane a tutt'oggi una minaccia ad alta prevalenza. 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 backup.** I backup sono il principale metodo utilizzato dalle organizzazioni per recuperare i dati dopo un attacco. Come abbiamo visto, anche se si paga il riscatto, non vi è l'assoluta sicurezza di potere rientrare in possesso di tutti i dati rubati, per cui i backup sono essenziali in ogni caso.
   Un semplice espediente mnemonico per ricordare i backup è "3-2-1". Occorrono almeno **tre** copie diverse (quella che si utilizza, più due di riserva) con almeno **due** sistemi diversi di backup (qualora uno non funzionasse) e almeno **una** copia deve essere memorizzata off-line e preferibilmente off-site (dove i cybercriminali non possono raggiungerla durante un attacco).
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 su più fronti.
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 il livello di scalabilità e automazione necessario, mentre gli esperti umani sono la risorsa migliore per individuare indizi come tattiche, tecniche e procedure che possono rivelare la presenza di un abile cybercriminale in agguato, che cerca solo un'opportunità per infiltrarsi nell'ambiente informatico. In assenza di personale interno con competenze tecniche adeguate, è possibile rivolgersi ad un'azienda specializzata in cybersecurity. I SOC sono ora un'opzione accessibile per le 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. **Stabilire un piano di risposta agli incidenti di cybersecurity**. 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 della protezione dei sistemi 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 dai team Sophos Managed Threat Response e Sophos Rapid Response, che collettivamente sono intervenuti su 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.

2021-09-1 (SB-MP)

SOPHOS