SOPHOS
Cybersecurity evolved.

La Vera Storia Del Ransomware Per Gli Enti Governativi 2021

Un'emergenza nazionale

Questo report svela le più recenti scoperte ed i nuovi aggiornamenti sugli attacchi ransomware che colpiscono **gli enti governativi e della pubblica amministrazione**. Esplora la prevalenza del ransomware tra gli enti governativi, il suo impatto sulle vittime, i costi di riparazione ai danni di un attacco e la percentuale di organizzazioni governative che sono riuscite a recuperare i loro dati dopo aver pagato il riscatto.

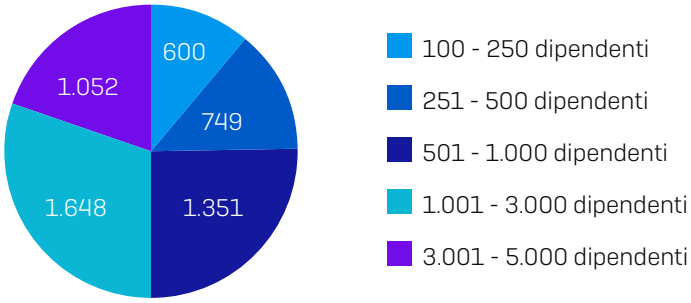
Inoltre, il sondaggio riporta i risultati emersi dal confronto tra il settore della pubblica amministrazione e gli altri settori, fornendo informazioni sulle aspettative future e sul grado di preparazione degli enti governativi ad affrontare questo tipo di attacchi.

Whitepaper Sophos. Giugno 2021

Informazioni sul sondaggio

Sophos ha affidato a Vanson Bourne, un'azienda di ricerca indipendente, l'incarico di intervistare 5.400 IT Manager presenti in 30 paesi. I partecipanti provengono vari settori, incluse 117 organizzazioni del settore pubblico e 131 della pubblica amministrazione. Il sondaggio è stato svolto nei mesi di 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 117 IT Manager operanti nel settore pubblico e i 131 nella pubblica amministrazione provengono da tutte le aree geografiche che hanno partecipato al sondaggio: Nord e Sud America, Europa, Medio Oriente, Africa e Asia Pacifico.

Area geografica	N° partecipanti nel settore pubblico	N° partecipanti nella pubblica amministrazione
Nord e Sud America	29	39
Europa	52	57
Medio Oriente e Africa	16	18
Asia Pacifico	20	17
TOTALE	**117**	**131**

117 IT Manager operanti nel settore pubblico; 131 nella pubblica amministrazione

I risultati più salienti per il settore pubblico

- Il **40%** dei partecipanti appartenenti a organizzazioni del settore pubblico **è stato colpito dal ransomware l'anno scorso**
- Il **49%** degli intervistati in organizzazioni colpite dal ransomware l'anno scorso sostiene che **i cybercriminali sono riusciti a cifrare i dati** nell'attacco di maggiore impatto
- Il **13%** delle organizzazioni colpite dal ransomware l'anno scorso riporta che i dati non sono stati cifrati, ma che si sono comunque **ricevute richieste di riscatto**; per gli attacchi basati sull'estorsione, si tratta della **percentuale maggiore tra tutti i settori**
- Il **61%** degli intervistati che hanno subito la cifratura dei dati **ha recuperato i dati grazie ai backup**
- L'**81%** delle organizzazioni del settore pubblico dispone di un **piano di risposta in caso di un attacco malware: la seconda percentuale più bassa tra tutti i settori** analizzati
- 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) è pari a **1,37 milioni di USD**

I risultati più salienti per la pubblica amministrazione

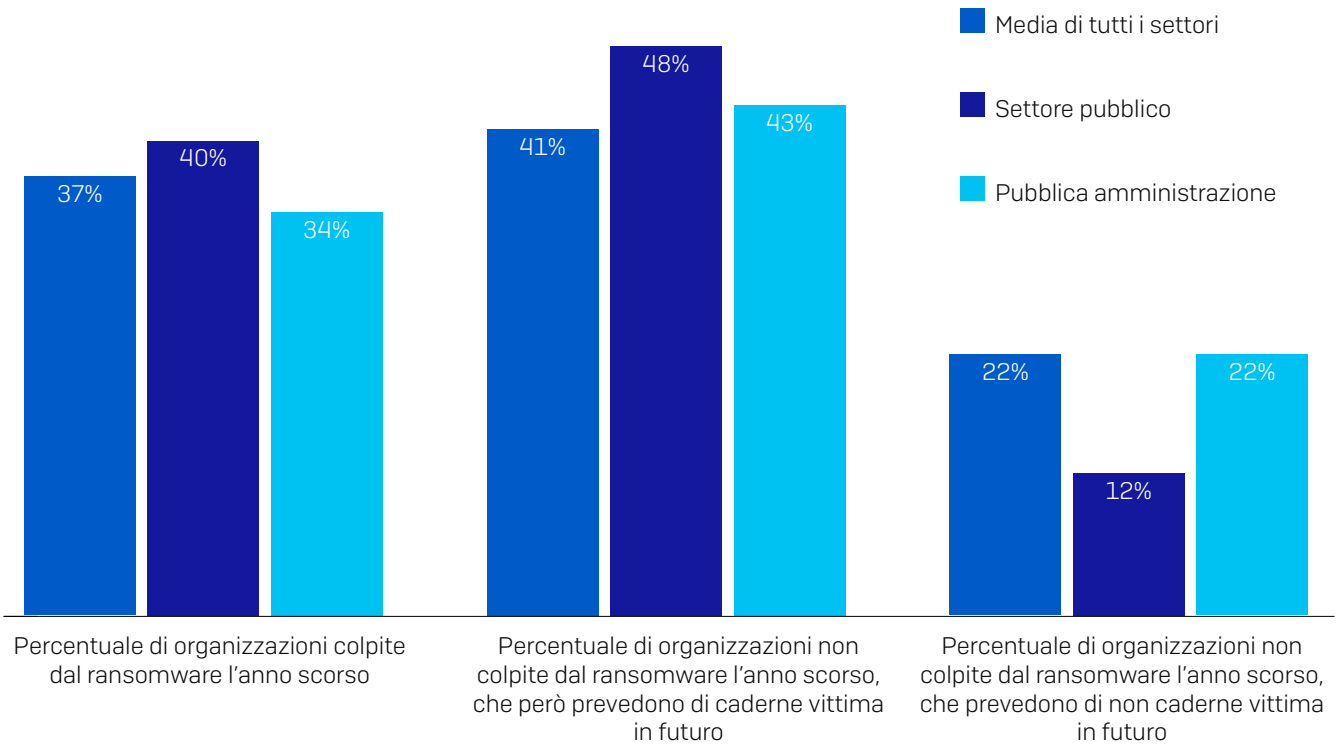
- Il **34%** delle organizzazioni della pubblica amministrazione **è stato colpito dal ransomware l'anno scorso,** una percentuale leggermente inferiore rispetto al settore pubblico
- Il **69%** degli intervistati appartenenti a organizzazioni colpite dal ransomware l'anno scorso sostiene che **i cybercriminali sono riusciti a cifrare i dati** nell'attacco di maggiore impatto: ben 20 punti percentuali in più rispetto al settore pubblico
- Il **42%** dei partecipanti al sondaggio la cui organizzazione ha subito la cifratura dei dati **ha pagato il riscatto per recuperare i dati sottratti** nell'attacco di maggiore impatto
- Il **42%** delle organizzazioni che hanno subito la cifratura dei dati **ha recuperato i dati grazie ai backup**
- Il **73%** delle organizzazioni della pubblica amministrazione dispone di un **piano di risposta in caso di un attacco malware**: la **percentuale più bassa tra tutti i settori** analizzati
- 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) è pari a **1,64 milioni di USD**

La prevalenza del ransomware negli enti governativi

Il settore pubblico è un obiettivo colpito più frequentemente rispetto alla pubblica amministrazione

Abbiamo chiesto ai partecipanti che lavorano in enti governativi se l'anno scorso la loro azienda è stata colpita dal ransomware (ovvero se vari computer dell'organizzazione hanno subito le conseguenze di un attacco di ransomware, inclusi i casi in cui i dati non sono stati cifrati). Il 40% degli intervistati nel settore pubblico e il 34% nella pubblica amministrazione ha risposto Sì. La media di tutti i settori è del 37%.

% di partecipanti colpiti dal ransomware negli ultimi 12 mesi



La vostra organizzazione è stata colpita dal ransomware negli ultimi 12 mesi? [Tutti i settori: 5.400; settore pubblico: 117; pubblica amministrazione: 131]

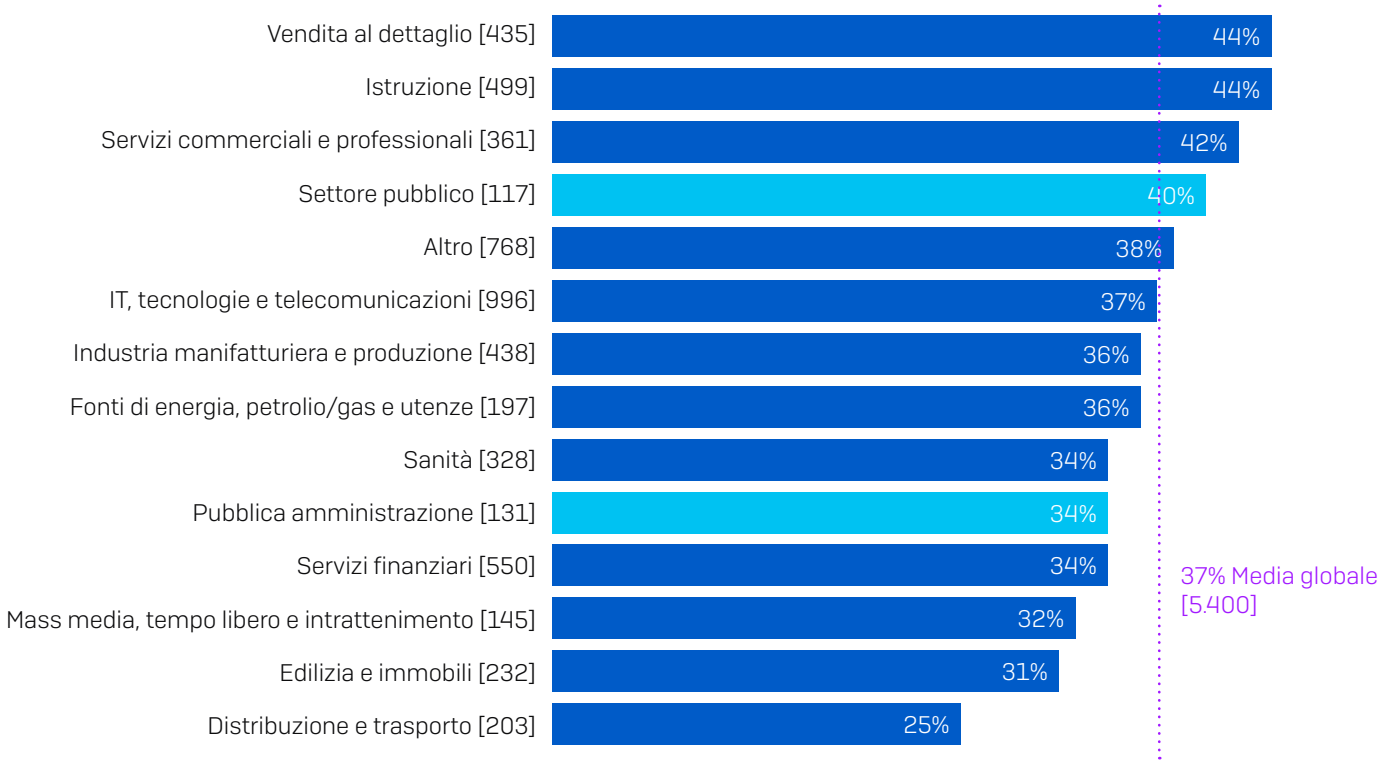
Allo stesso tempo, il 48% degli intervistati che operano nel settore pubblico e il 43% nella pubblica amministrazione ha dichiarato che la propria organizzazione non è caduta vittima dal ransomware l'anno scorso, ma prevede che subirà un attacco in futuro. In entrambi i casi, queste statistiche superano la media di tutti i settori (41%), il che indica una maggiore consapevolezza sul ransomware tra gli enti governativi.

Per quanto riguarda la proporzione di partecipanti al sondaggio la cui organizzazione non è stata colpita dal ransomware e che prevede che non ne cadrà vittima in futuro, il settore pubblico è in linea con la media di tutti i settori (22%), ma la pubblica amministrazione sembra avere molta meno fiducia, in quanto questa opzione è stata selezionata solamente dal 12% degli intervistati. 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.

Le esperienze in tema di attacchi ransomware degli enti governativi rispetto agli altri settori

Tra tutti i settori analizzati per il sondaggio, quelli della **vendita al dettaglio** e dell'**istruzione** riportano il livello più elevato di attacchi, con il 44% degli intervistati di questi settori che indica di essere stato colpito, mentre **distribuzione e trasporto** è il settore con la minore probabilità di cadere vittima di un attacco.

% 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

Complessivamente, la percentuale di organizzazioni che dichiara di essere stata colpita dal ransomware mostra un calo netto rispetto all'anno scorso, quando il 51% degli intervistati aveva ammesso di esserne caduta vittima. Sebbene questo calo sia 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. 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. Di conseguenza, sebbene la quantità totale degli attacchi sia inferiore, abbiamo osservato che il potenziale di arrecare danno di questi attacchi mirati è molto più elevato.

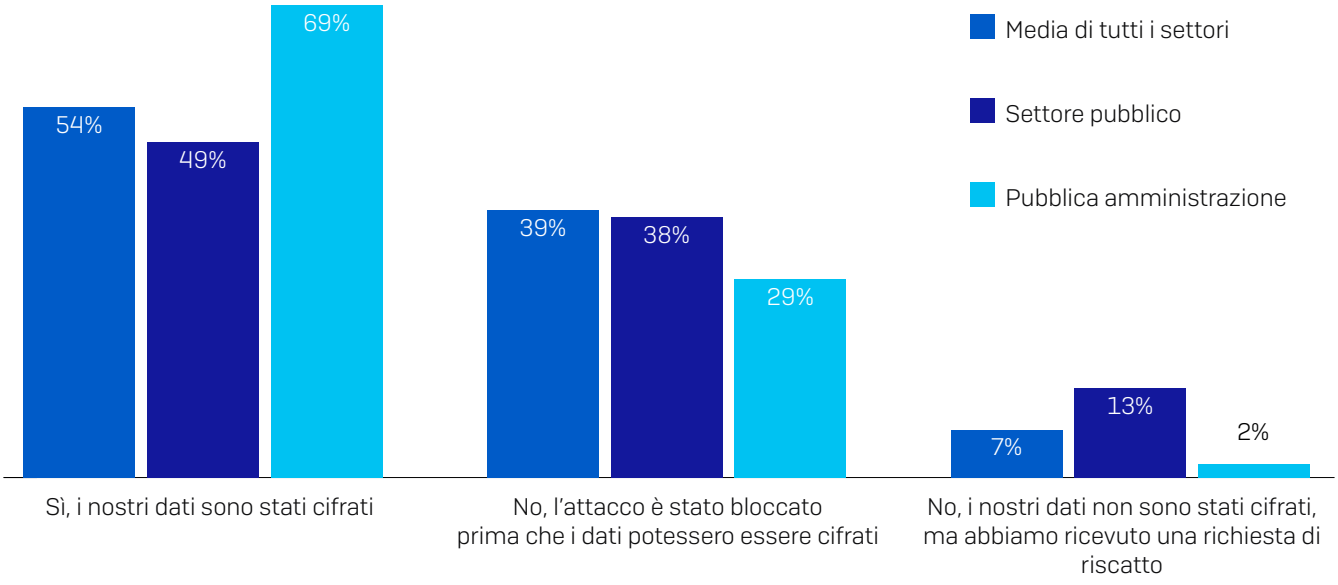
L'impatto del ransomware

I cybercriminali riescono a cifrare i dati degli enti governativi

Abbiamo chiesto alle organizzazioni colpite dal ransomware se i cybercriminali sono riusciti a cifrare i loro dati.

Nelle organizzazioni della **pubblica amministrazione**si è registrato un esito peggiore rispetto a molti altri settori per quanto riguarda il blocco degli attacchi: il 69% dichiara infatti che i cybercriminali sono riusciti a cifrare i dati, mentre la media globale è del 54%. Una tendenza inversa si osserva invece nelle organizzazioni del **settore pubblico**, che mostrano una capacità superiore alle media di bloccare gli attacchi: poco meno della metà (49%) degli attacchi hanno avuto come risultato la cifratura dei dati.

La capacità degli enti governativi di bloccare il ransomware



Nell'attacco di ransomware più grave, i cybercriminali sono riusciti a cifrare i dati dell'organizzazione? [Partecipanti di tutti i settori: 2.006; del settore pubblico: 47; della pubblica amministrazione: 45]

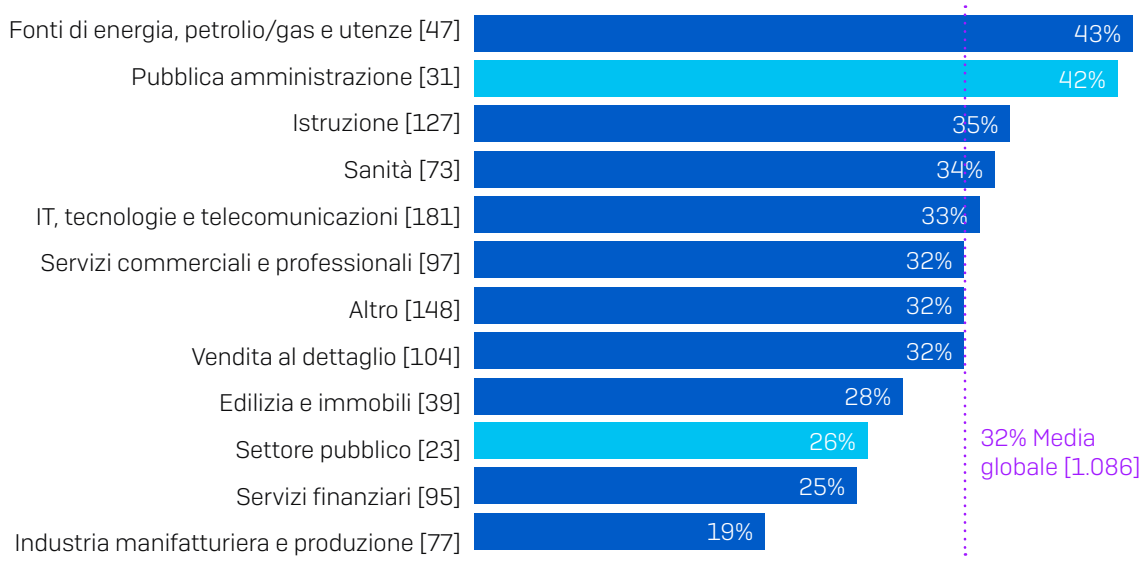
Gli elevati tassi di cifratura registrati nella **pubblica amministrazione** potrebbero essere in parte dovuti alle sfide in termini di fondi e risorse umane disponibili per i team IT di questo settore. I budget sono molto limitati, i team hanno pochi dipendenti e le organizzazioni non possono liberamente destinare alla cybersecurity fondi che potrebbero essere investiti nel miglioramento dei servizi pubblici.

Sebbene, come già osservato, il **settore pubblico** abbia subito una quantità di attacchi superiore alla media, ha anche riportato una delle percentuali più basse di attacchi in cui i dati sono stati cifrati. In parte, questo è dovuto a un investimento mirato nell'assunzione di personale IT qualificato e all'utilizzo di Security Operations Center (SOC), di cui parleremo in maniera più approfondita in un'altra sezione di questo documento.

Tuttavia, per questo settore gli hacker adottano tecniche di attacco leggermente diverse. Tra tutti i settori analizzati, il settore pubblico ha riportato la quantità più elevata di attacchi in cui i dati non sono stati cifrati (quasi il doppio rispetto alla media). Tuttavia queste organizzazioni hanno comunque ricevuto una richiesta di riscatto, con la minaccia di rendere pubblici i dati sottratti.

Una differenza abissale nella propensione a pagare il riscatto

% 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

Le organizzazioni della **pubblica amministrazione** non sono solo quelle con il maggiore tasso di cifratura dei dati, ma riportano anche la seconda percentuale più alta di pagamento del riscatto (42%) tra tutti i settori. 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. Parallelamente, uno dei fattori determinanti alla base della maggiore propensione a pagare il riscatto potrebbe essere la pressione sui team della pubblica amministrazione, che sono tenuti a garantire continuità nell'erogazione dei servizi pubblici.

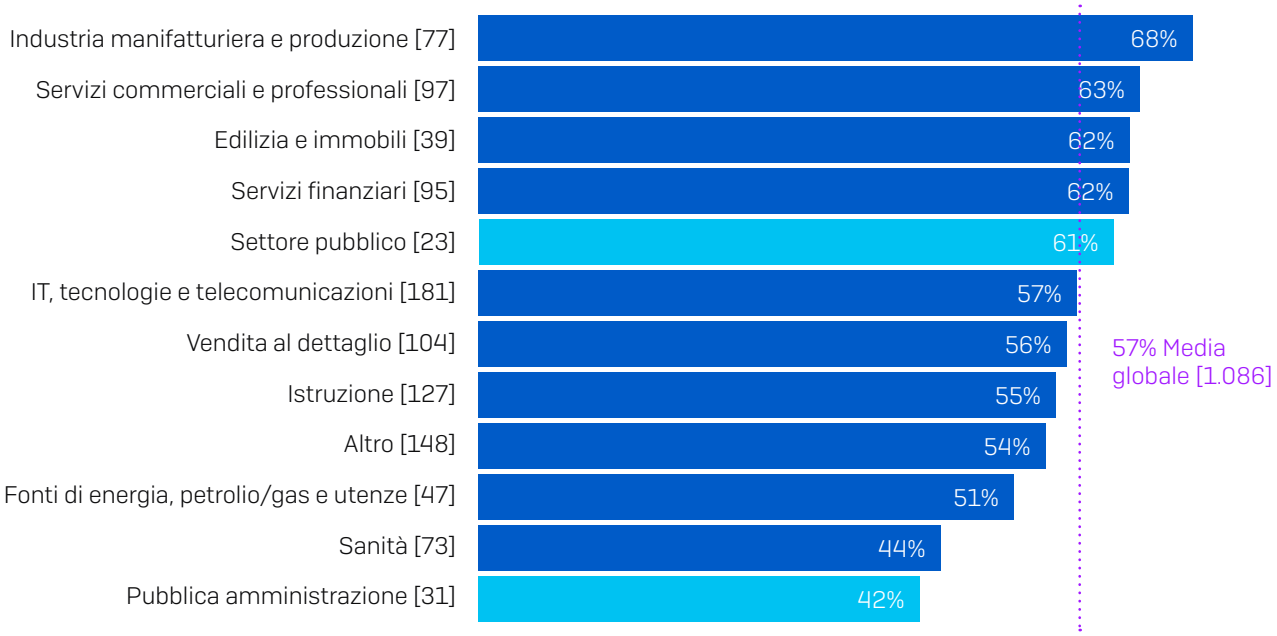
Il **settore pubblico** si trova invece vicino al fondo della classifica, con solo il 26% degli intervistati che dichiara di aver pagato il riscatto per recuperare i dati: una percentuale di gran lunga inferiore rispetto alla media di tutti i settori (32%). Come vedremo a breve, questo settore può contare su altri metodi per ripristinare i dati. È importante tenere presente che i numeri relativi al settore pubblico si basano su 23 partecipanti e che pertanto il campione non può essere ritenuto significativo a fini statistici.

Tra tutti, il settore delle **fonti di energia, petrolio/gas e utenze** è quello più propenso 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.

Capacità di ripristinare i dati utilizzando i backup

C'è decisamente una correlazione tra la propensione di un'organizzazione a pagare il riscatto e la sua capacità di ripristinare i dati dai backup.

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



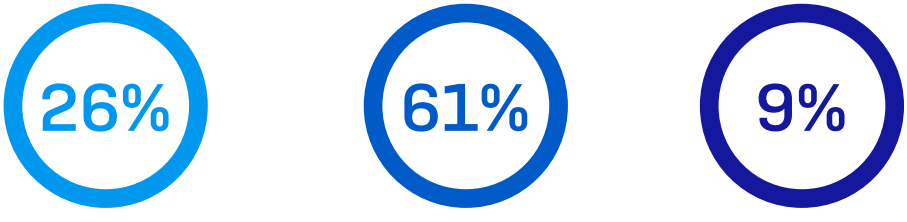
Nell'attacco di ransomware più grave, l'organizzazione ha recuperato i dati?

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

La **pubblica amministrazione** è tra tutti i settori quello con la minore capacità di ripristinare i dati dai backup. A livello globale, il 57% delle organizzazioni colpite dalla cifratura non autorizzata dei dati è riuscito a recuperarli con l'aiuto dei backup, ma questa statistica raggiunge solo il 42% nella pubblica amministrazione. Tuttavia, più di sei organizzazioni su dieci (61%) nel **settore pubblico** sono riuscite a ripristinare i dati dai backup, con una percentuale superiore alla media globale.

Nel 96% dei casi le organizzazioni del settore pubblico sono riuscite a recuperare i dati cifrati

Vediamo ora le percentuali relative alle organizzazioni che sono riuscite a recuperare i dati dopo la loro cifratura. La base di partecipanti nel settore pubblico era di 23 intervistati, per cui i dati acquisiti non sono significativi dal punto di vista statistico. Tuttavia, a titolo informativo, nel 96% dei casi le organizzazioni del **settore pubblico** sono riuscite a recuperare i dati cifrati. Tra queste, il 61% ha recuperato i dati grazie ai backup, il 26% ha pagato il riscatto per recuperare i dati e il 9% ha utilizzato altri metodi.



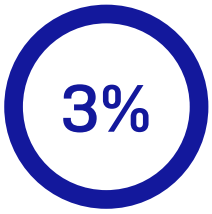
Nell'attacco di ransomware più grave, l'organizzazione ha recuperato i dati? [23] organizzazioni nel settore pubblico hanno risposto.

L'87% delle organizzazioni della pubblica amministrazione è riuscito a recuperare i dati cifrati

L'87% dei partecipanti appartenenti a organizzazioni della **pubblica amministrazione** che sono cadute vittima della cifratura non autorizzata dei dati ha recuperato le informazioni sottratte. In questo settore si sono osservate quantità equivalenti di intervistati che dichiarano di aver pagato il riscatto (42%) e di avere utilizzato i backup (42%) per recuperare i dati. Solo il 3% ha utilizzato altri metodi per recuperare i dati.

Ha pagato il riscatto per recuperare i dati

Ha utilizzato i backup per recuperare i dati



Ha utilizzato altri mezzi per recuperare i dati

Nell'attacco di ransomware più grave, l'organizzazione ha recuperato i dati?
[31] organizzazioni nella pubblica amministrazione hanno risposto.

Pagare il riscatto non ripaga

Quello che i cybercriminali non dicono quando inviano una richiesta di riscatto è che, anche pagando, le probabilità di recuperare tutti i dati sono poche. In media, le organizzazioni che hanno pagato il riscatto sono riuscite a riavere solo il 65% dei dati, mentre un terzo è rimasto inaccessibile.

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

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

La base degli intervistati provenienti da organizzazioni nel settore pubblico e nella pubblica amministrazione era inferiore a 30, per cui i dati di questi partecipanti non possono essere considerati validi a fini statistici. Tuttavia, a titolo informativo, gli intervistati del **settore pubblico** hanno dichiarato di aver recuperato in media il 63% dei propri dati, mentre nella **pubblica amministrazione** la percentuale sale al 70%: una statistica leggermente migliore rispetto alla media globale, ma che lascia pur sempre un'elevata quantità di dati che sono rimasti inaccessibili. In tutti i settori, il 29% delle organizzazioni ha recuperato il 50% o meno dei dati e solo l'8% è riuscito a recuperare tutti i dati.

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. La base di partecipanti nel **settore pubblico** era troppo bassa per essere inclusa. Tuttavia, a titolo informativo, 11 partecipanti appartenenti a organizzazioni della **pubblica amministrazione** sostengono di aver versato in media 296.136 USD, ovvero quasi 126.000 USD in più rispetto alla somma media di riscatto.

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

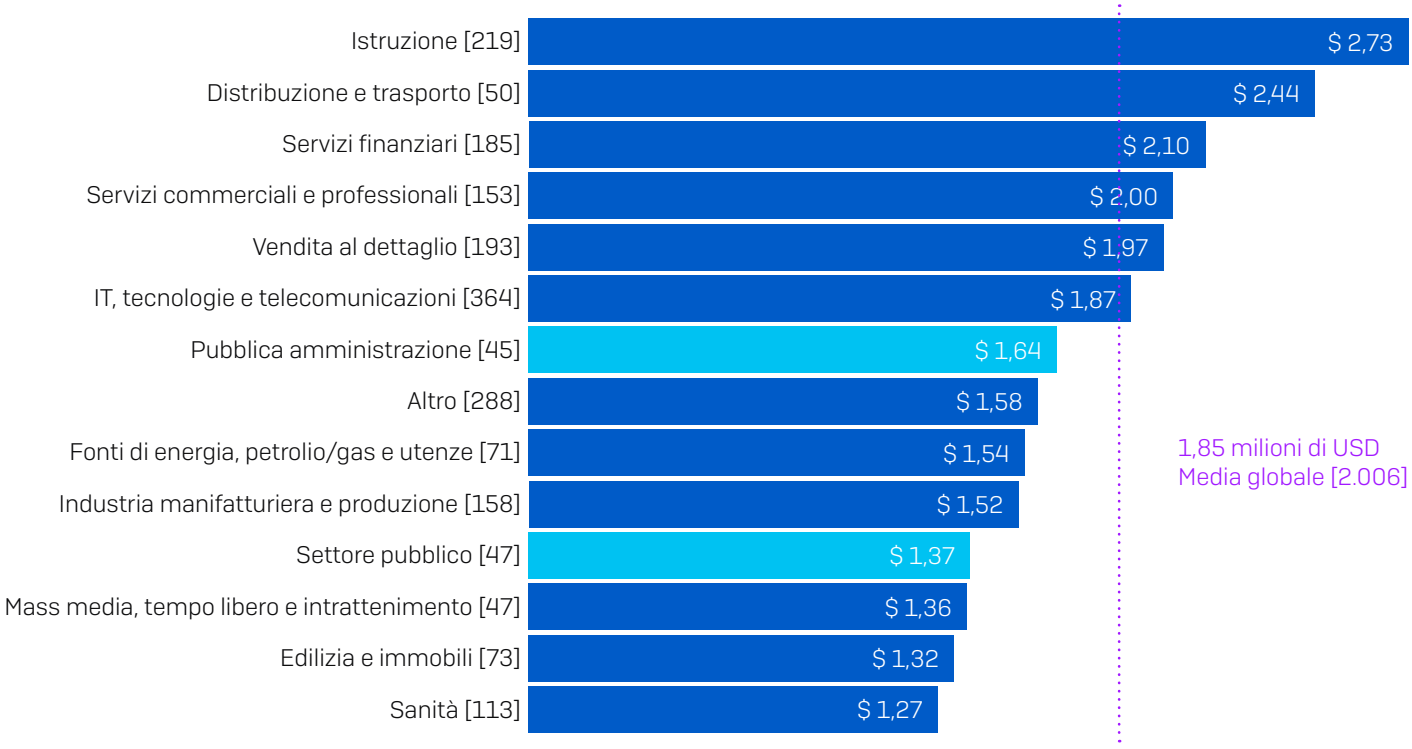
1. **Dimensioni dell'organizzazione.** A partecipare al nostro sondaggio sono state organizzazioni di medie dimensioni con un numero di utenti compreso tra 100 e 5.000. In genere, questo tipo di organizzazioni ha a disposizione risorse finanziarie molto più limitate rispetto alle aziende più grandi. I cybercriminali che utilizzano il ransomware modificano le richieste di riscatto in base al capitale a disposizione della vittima e di solito accettano pagamenti più bassi da aziende più piccole. Le statistiche 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).

I costi necessari per rimediare ai danni causati dal ransomware

Valutando nel complesso i costi necessari per rimediare ai danni causati dal ransomware, quando si osserva la somma media approssimativa che le organizzazioni hanno dovuto versare per fronteggiare l'impatto dell'attacco di ransomware più recente (considerando tempi di inattività, ore di lavoro del personale, costi associati a dispositivi e rete, perdita di opportunità commerciali, somma pagata per il riscatto e così via), si nota che la **pubblica amministrazione** presenta costi di correzione complessivi pari a 1,64 milioni di USD, mentre la media di tutti i settori è di 1,85 milioni di USD.



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, in milioni di USD

A giustificare il costo medio inferiore alla media globale vi è probabilmente il fatto che spesso le organizzazioni della pubblica amministrazione hanno budget più limitati e di conseguenza meno fondi da investire nel rimediare ai danni. Inoltre, i costi correlati ai danni alla reputazione e alla perdita di opportunità per gli enti pubblici sono generalmente inferiori a quelli delle organizzazioni private.

Per il **settore pubblico** si sono riscontrati costi di riparazione (1,37 milioni di USD) molto inferiori rispetto alla media globale; questa statistica è probabilmente correlata alla maggiore capacità di questo settore di utilizzare i backup per recuperare i dati e di conseguenza alla minore dipendenza dai pagamenti di riscatto.

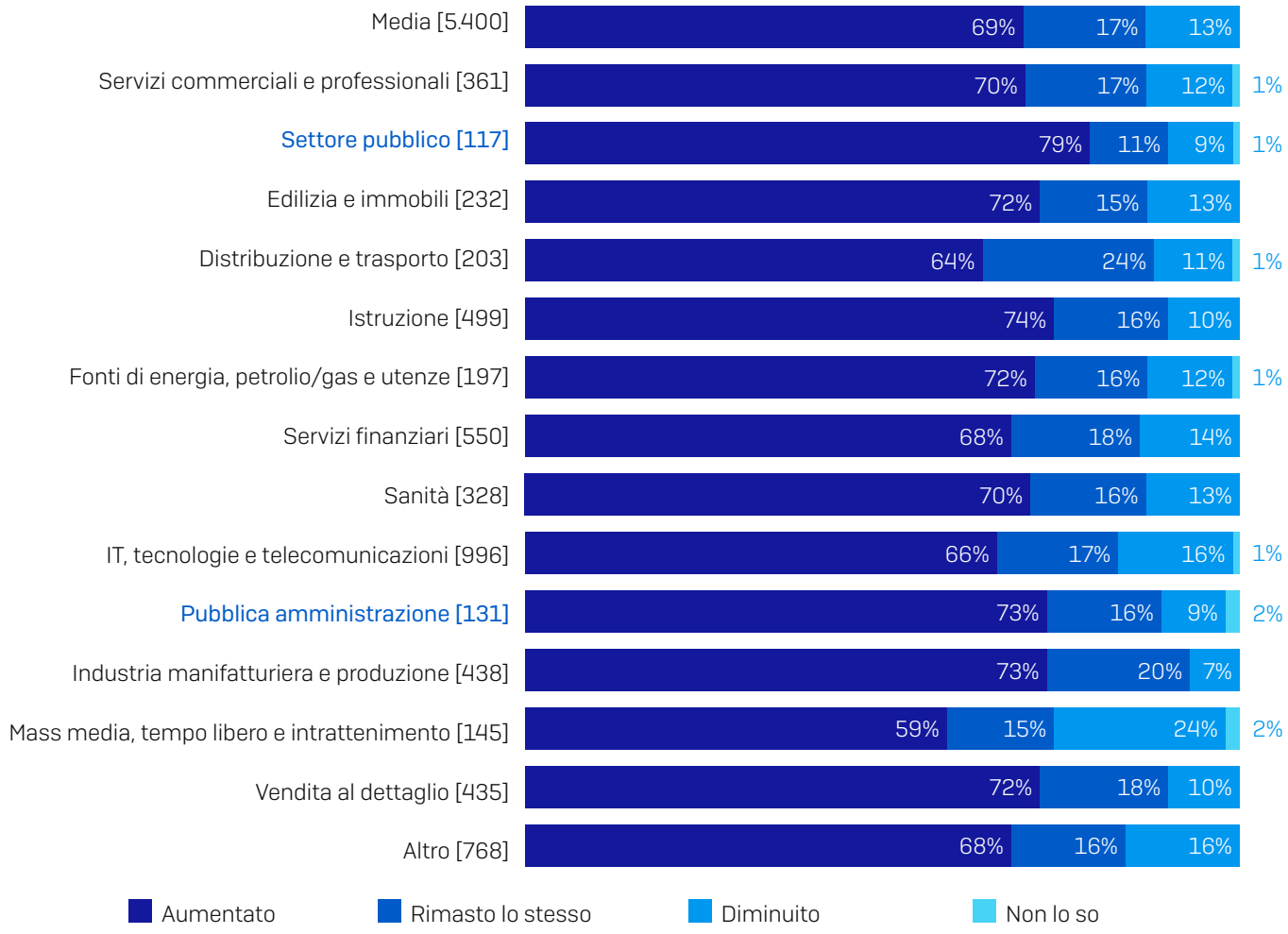
Il ransomware è solo una delle tante sfide di cybersecurity

Il ransomware è un problema di sicurezza molto serio per gli enti governativi, 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

Abbiamo chiesto ai partecipanti al sondaggio quale cambiamento hanno notato nel carico di lavoro di cybersecurity durante il 2020. Il **settore pubblico** ha riportato l'incremento più elevato tra tutti i settori, con quasi un intervistato su cinque (79%) che sostiene di aver osservato un aumento del carico di lavoro. La **pubblica amministrazione** segue a distanza relativamente ravvicinata, con il 73% degli intervistati che dichiara di aver notato un incremento. La media di tutti i settori è del 69%.

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



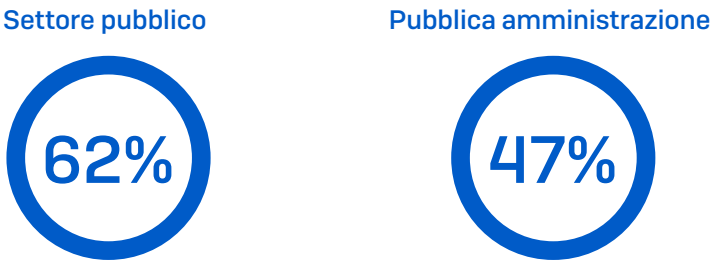
Nel 2020 il nostro carico di lavoro di cybersecurity è aumentato/diminuito/rimasto lo stesso [5.400]

Con molta probabilità, questo aumento del carico di lavoro può essere per la maggior parte attribuito al ruolo fondamentale svolto dagli enti governativi nella risposta alla pandemia: il lavoro del personale IT è stato indispensabile per garantire l'erogazione di servizi essenziali e per aiutare questi enti a soddisfare le esigenze dei cittadini. Verosimilmente, l'incremento del carico di lavoro ha influito sulla capacità dei team IT di monitorare le minacce informatiche e di rispondere in maniera adeguata.

Gli attacchi stanno diventando più difficili da bloccare

Oltre a questo, le minacce diventano sempre più avanzate. Gli hacker utilizzano innumerevoli tecniche, tattiche e procedure (TTP) di attacco, spesso basate sulla combinazione tra automazione e utilizzo di strumenti IT legittimi per eludere le difese delle organizzazioni. Affrontare questi attacchi in continua evoluzione sta diventando sempre più problematico e per più della metà dei partecipanti al sondaggio (54%), gli attacchi informatici sono ora troppo avanzati per essere risolti dal proprio team IT senza un aiuto esterno.

% che sostiene che gli attacchi informatici sono ora troppo avanzati per essere affrontati dal team IT dell'organizzazione, senza un aiuto esterno



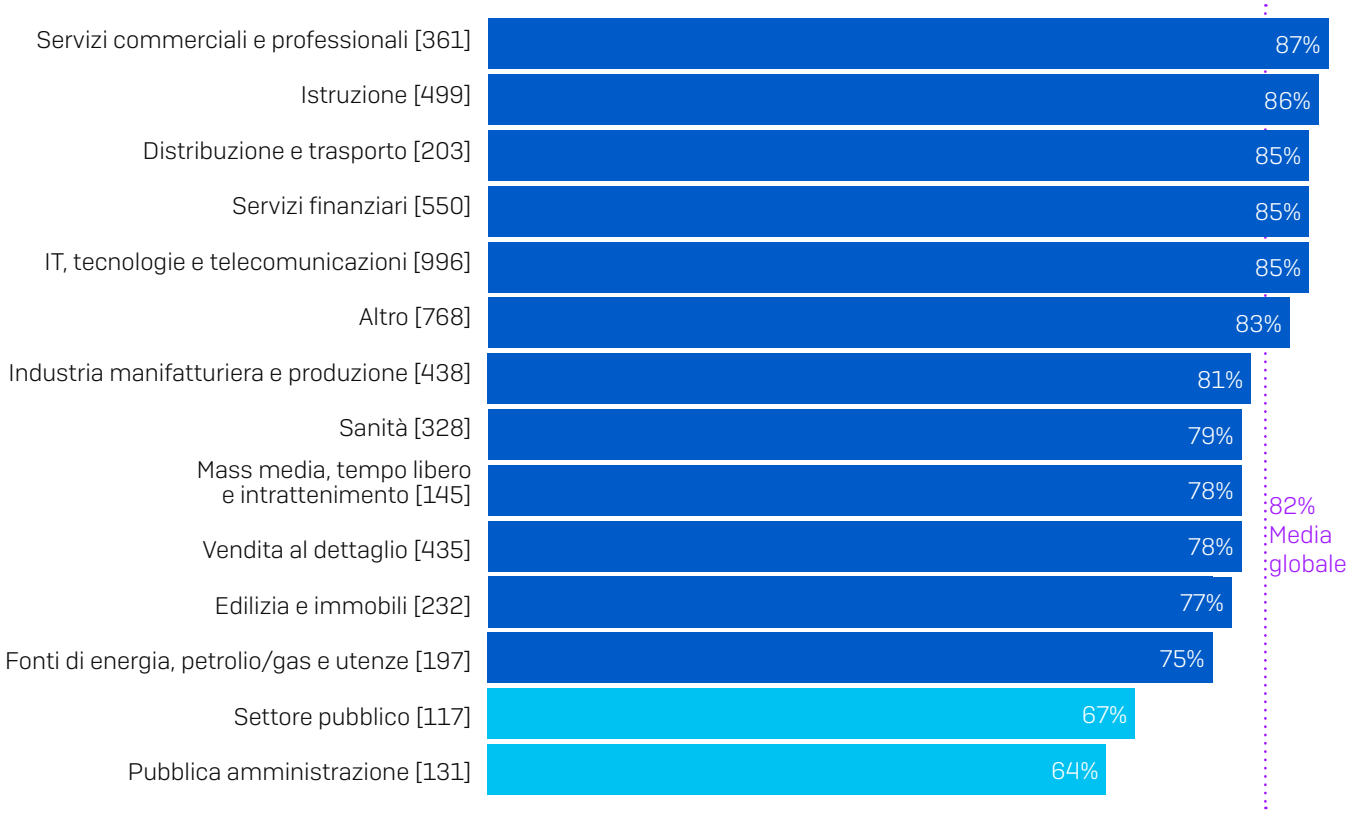
Gli attacchi informatici sono ora troppo avanzati per essere affrontati dal team IT della mia organizzazione, senza un aiuto esterno: Pienamente d'accordo, D'accordo. Alcune risposte sono state escluse [settore pubblico: 117; pubblica amministrazione: 131]

Questa sfida è particolarmente sentita nel **settore pubblico**, con il 62% degli intervistati che ammette che gli attacchi sono troppo avanzati per il personale interno. La **pubblica amministrazione** ha invece riportato la quantità minore di organizzazioni con questa sfida per il personale interno, con una percentuale pari al 47% di partecipanti che sostiene che gli attacchi sono troppo complessi per essere gestiti dal team IT senza un aiuto esterno. Il caso della pubblica amministrazione è particolarmente sorprendente, in quanto, come abbiamo visto, in questo settore è più probabile che gli attacchi di ransomware riescano a cifrare i dati.

Preparazione ad affrontare le sfide future

Avere strumenti validi e conoscenze adeguate è fondamentale per poter indagare sulle minacce informatiche e debellarle. È pertanto rassicurante scoprire che, nonostante l'aumento del carico di lavoro e della frequenza degli attacchi, l'82% dei Manager IT intervistati, sostiene di disporre degli strumenti e delle conoscenze necessari per svolgere indagini esaustive sulle attività sospette. Ci sono tuttavia due eccezioni evidenti: il **settore pubblico** e la **pubblica amministrazione**.

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 risposte sono state escluse [5.400]

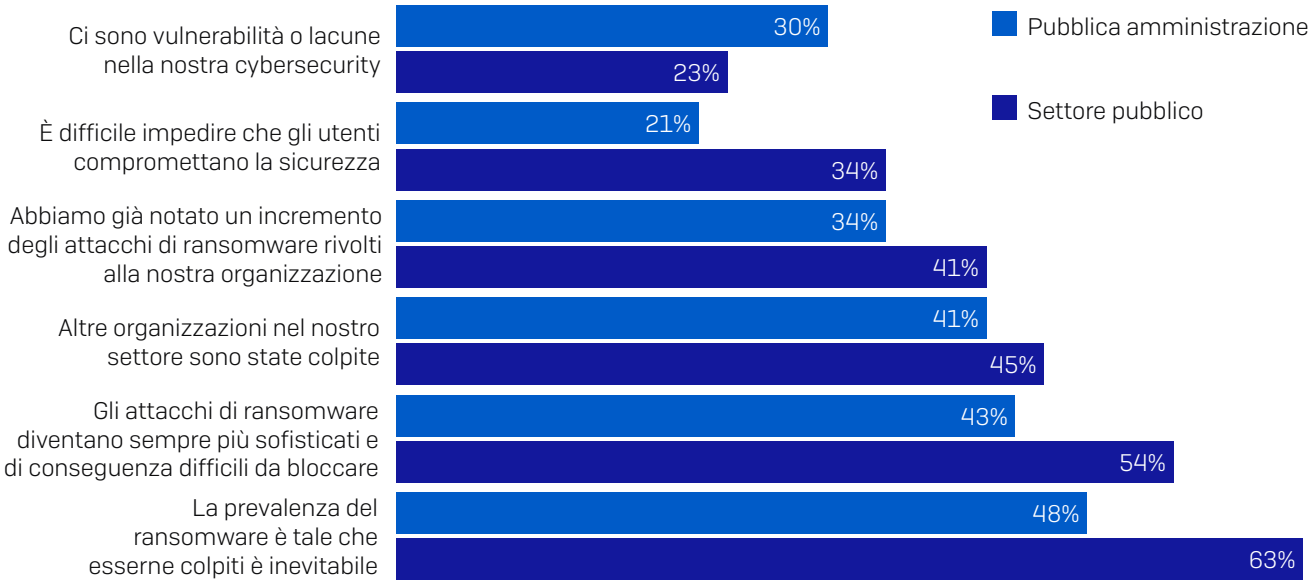
I budget limitati potrebbero essere uno dei fattori alla base di questi risultati, in quanto la mancanza di fondi destinati agli enti pubblici è una sfida costante in molti paesi. In ogni caso, poiché i cybercriminali continuano ad affinare le proprie tecniche di attacco, è essenziale dotare i team IT negli enti governativi delle risorse necessarie per mettersi in pari con gli altri settori.

Il futuro

Come abbiamo visto all'inizio di questo rapporto, quasi la metà dei partecipanti che operano nel settore governativo (48% nel **settore pubblico** e 43% nella **pubblica amministrazione**) e che hanno dichiarato di non avere subito un attacco di ransomware l'anno scorso prevede di caderne vittima in futuro, mentre la media di tutti i settori è del 41%. Il 12% degli intervistati nel **settore pubblico** e il 22% nella **pubblica amministrazione** non si aspettano di essere colpiti da un attacco di ransomware in futuro.

I motivi per cui il settore governativo si aspetta di essere colpito dal ransomware

Tra le organizzazioni che non hanno subito un attacco di ransomware ma prevedono che ne cadranno vittima in futuro (**settore pubblico**: 63%; **pubblica amministrazione**: 48%), il motivo più comune è stato che il ransomware è talmente prevalente da rendere inevitabile l'esserne colpiti. Inoltre, il 54% degli intervistati nel settore pubblico e il 43% nella pubblica amministrazione sostiene che gli attacchi di ransomware stanno diventando sempre più difficili da bloccare, poiché sono molto sofisticati.



Perché prevedete che la vostra organizzazione sarà colpita dal ransomware in futuro? [56/56] organizzazioni 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

Sebbene si tratti di una cifra molto alta, il fatto che queste organizzazioni siano consapevoli che il ransomware continua a evolversi è molto positivo, potrebbe anche essere stato uno dei fattori che hanno contribuito alla loro capacità di bloccare i potenziali attacchi di ransomware l'anno scorso.

Il 45% degli intervistati nel settore pubblico e il 41% nella pubblica amministrazione ritiene che, poiché gli altri settori ne sono caduti vittima, è probabile che anche loro subiranno un attacco.

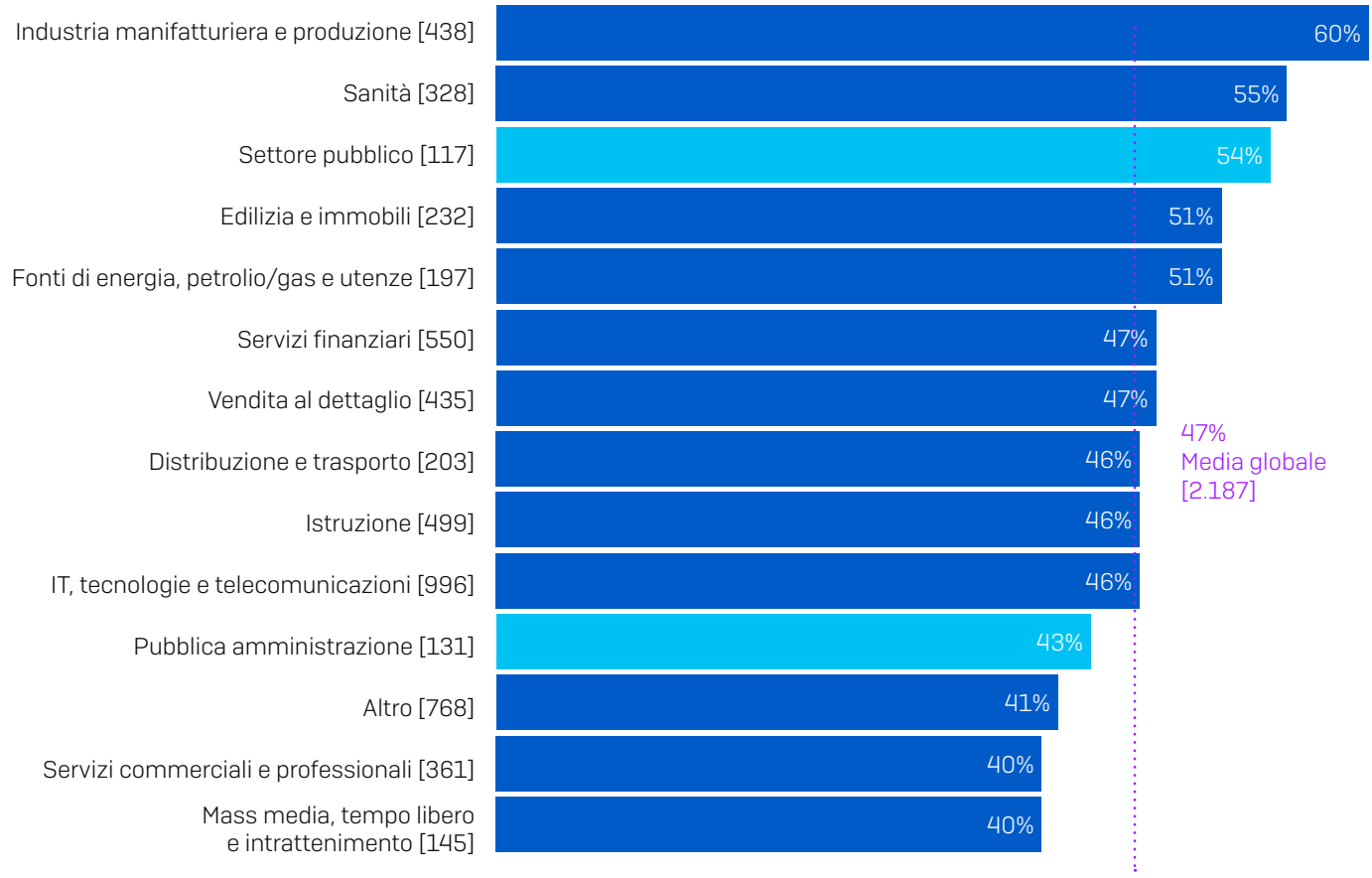
La pubblica amministrazione (30%), insieme all'istruzione, è il settore con maggiore probabilità di ammettere la presenza di vulnerabilità o lacune di cybersecurity. La percentuale scende al 23% per il settore pubblico. Anche se naturalmente non è un bene che esistano lacune di sicurezza, riconoscere la presenza di questi problemi è un primo passo verso il potenziamento delle proprie difese.

Più di un terzo (34%) dei partecipanti al sondaggio nel settore pubblico indica i propri utenti come causa della compromissione della sicurezza e dell'esposizione della propria organizzazione al rischio di ransomware. È una quantità che supera di diversi punti percentuali la media globale del 22% e il 21% del settore della pubblica amministrazione.

Consapevolezza sulla maggiore complessità del ransomware

Analizzando le statistiche in maniera più approfondita, si osserva che il **settore pubblico** è tra quelli maggiormente consci della crescente complessità del ransomware, con il 54% degli intervistati che indica questo fattore come uno dei motivi per cui prevede di subirne un attacco in futuro. La **pubblica amministrazione** (43%), al contrario, si trova appena sotto la media di tutti i settori (47%).

% degli intervistati che riconduce l'aumento degli attacchi al fatto che il ransomware sta diventando più sofisticato



Perché prevedete che la vostra organizzazione sarà colpita dal ransomware in futuro? [2.187] organizzazioni che hanno menzionato il fatto che gli attacchi di ransomware diventano sempre più sofisticati e di conseguenza difficili da bloccare come uno dei motivi per cui si aspettano di esserne colpite in futuro

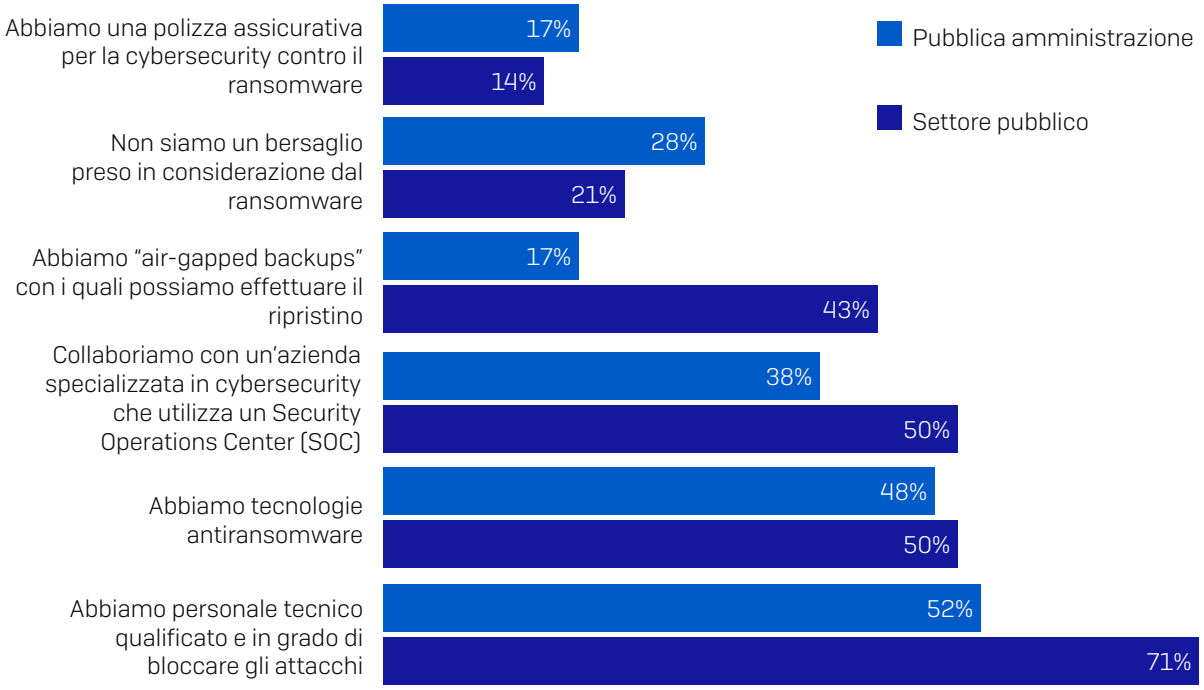
Sebbene i partecipanti al sondaggio che hanno risposto a questa domanda non fossero stati colpiti direttamente dal ransomware l'anno scorso, è probabile che siano stati influenzati delle esperienze riscontrate nei rispettivi settori. Quello degli enti governativi in particolare ha subito maggiormente l'impatto di molti attacchi andati a segno.

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

A rispondere a questa domanda sono stati solo 29 intervistati della pubblica amministrazione e 14 del settore pubblico, pertanto i risultati sono da considerarsi puramente indicativi.

Tra i partecipanti al sondaggio che non sono stati colpiti dal ransomware l'anno scorso e prevedono che non ne cadranno vittima in futuro, il motivo principale di questa fiducia è la disponibilità di personale IT qualificato e in grado di bloccare gli attacchi, seguita dall'utilizzo di tecnologie antiransomware.

I motivi per cui gli intervistati prevedono che non saranno colpiti dal ransomware in futuro



Perché prevedete che la vostra organizzazione non sarà colpita dal ransomware in futuro? [29 nella pubblica amministrazione/14 nel settore pubblico] organizzazioni che non sono cadute vittima del ransomware l'anno scorso e prevedono che non ne saranno colpite in futuro, alcune opzioni di risposta sono state omesse

Una percentuale molto elevata (71%) di partecipanti del **settore pubblico** ha dichiarato di avere investito in personale IT qualificato, mentre questa statistica ammonta al 52% per la **pubblica amministrazione**. La metà (50%) degli intervistati nel settore pubblico e il 38% di quelli che lavorano nella pubblica amministrazione che prevedono di non essere colpiti dal ransomware collaborano con aziende specializzate in cybersecurity che utilizzano un Security Operations Center (SOC).

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

È certamente rassicurante osservare che circa la metà delle organizzazioni che hanno partecipato al sondaggio ha implementato tecnologie antiransomware.

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

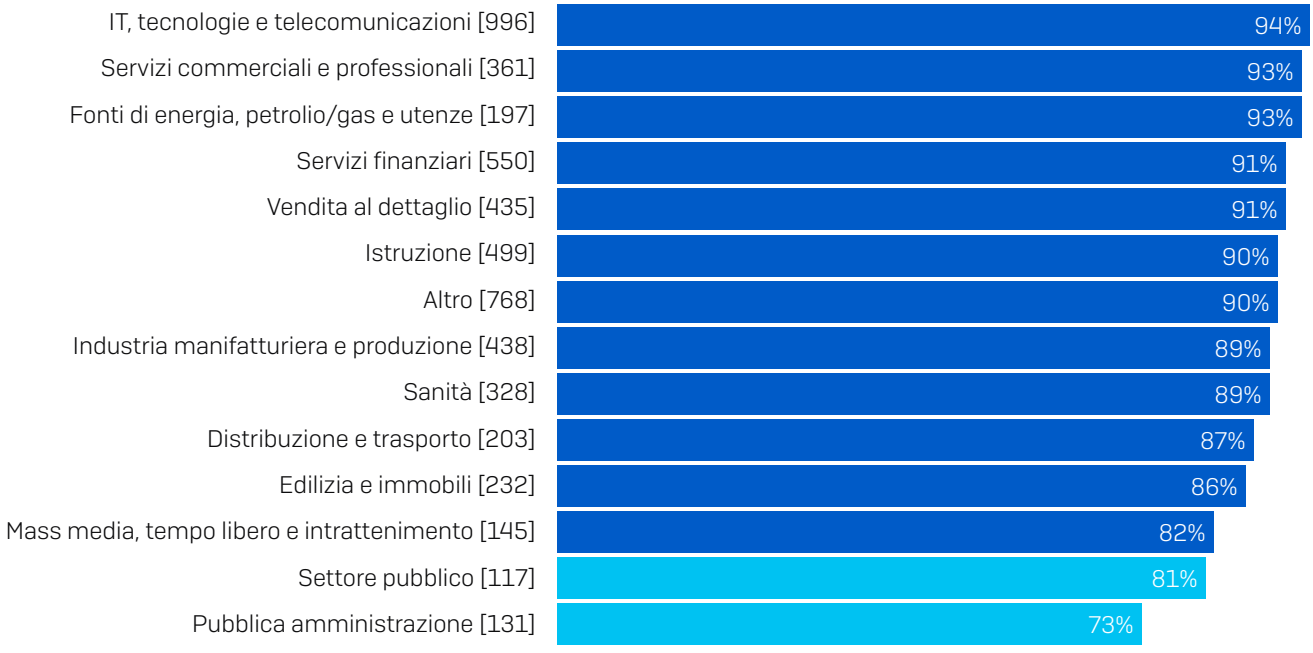
- Il 57% degli intervistati nel settore pubblico che ritengono che non saranno colpiti da un attacco e il 31% nella pubblica amministrazione adottano approcci che non offrono alcuna protezione contro il ransomware.
  - Il 43% dei partecipanti al sondaggio nel settore pubblico è convinto che non cadrà vittima del ransomware perché ha "backup in un air gap", mentre nella pubblica amministrazione la percentuale scende al 17%. Sono statistiche preoccupanti, poiché sebbene i backup (come abbiamo visto) sono strumenti molto utili per ripristinare i dati dopo un attacco, non offrono alcuna prevenzione contro il ransomware.
  - Il 14% degli intervistati nel settore pubblico e il 17% nella pubblica amministrazione ritiene di essere protetto contro il ransomware perché ha una polizza assicurativa per la cybersecurity. Anche in questo caso, una polizza assicurativa può far fronte alle conseguenze di un attacco, ma non svolge alcun ruolo nella prevenzione di tali attacchi. *Nota: alcuni degli intervistati hanno selezionato entrambe le opzioni e il 57%/ 31% ha selezionato almeno una delle due opzioni.*
- Il 21% dei partecipanti nel settore pubblico e il 28% nella pubblica amministrazione ritengono di non essere un bersaglio preso in considerazione dai criminali informatici. Purtroppo, questa affermazione non è vera. Nessuna organizzazione è al sicuro.

Gli enti governativi sono quelli meno preparati in caso di un incidente di malware grave

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.

La maggior parte dei settori è adeguatamente preparata per rimediare ai danni di un incidente di malware grave. Tuttavia, gli enti governativi sono risultati quelli con il minore grado di preparazione: solo l'81% delle organizzazioni nel **settore pubblico** e il 73% di quelle nella **pubblica amministrazione** dispone di un piano per eventi imprevisti in caso di incidenti di malware.

Partecipanti che dispongono di 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

I risultati sono molto preoccupanti, poiché questi settori sono tra quelli maggiormente colpiti dal ransomware. *La* **pubblica amministrazione** è il settore con la maggiore probabilità di subire un attacco di cifratura non autorizzata dei dati, mentre il **settore pubblico** è quello maggiormente soggetto a tentativi di estorsione. L'assenza di un piano di risposta agli incidenti informatici potrebbe essere uno dei motivi per cui la pubblica amministrazione si trova al secondo posto tra i settori più propensi a pagare il riscatto.

Riepilogo

Pubblica amministrazione

Dal sondaggio è emerso che la pubblica amministrazione si trova in un circolo vizioso di attacchi ransomware, che a sua volta è alimentato dall'incapacità di questo settore di difendersi dai cybercriminali. Sebbene questo settore abbia subito una quantità di attacchi inferiore alla media, è anche quello con la minore capacità tra tutti i settori di impedire la cifratura dei dati e di ripristinare i dati dai backup. Di conseguenza, la pubblica amministrazione è uno dei settori maggiormente propensi a pagare il riscatto, il che non fa altro che istigare gli hacker a colpire le organizzazioni della pubblica amministrazione.

Sebbene questo settore sia consapevole delle proprie lacune di cybersecurity, si trova all'ultimo posto per l'implementazione di un piano di emergenza in caso di ransomware. Questo settore deve adottare tempestivamente misure adeguate per porre rimedio alla situazione.

Settore pubblico

Il settore pubblico ha mostrato capacità di blocco del ransomware superiori rispetto alla pubblica amministrazione, grazie all'ampio investimento in professionisti IT qualificati e SOC. Nonostante abbia riscontrato livelli di attacco superiori alla media, ha anche registrato uno dei minori livelli di cifratura non autorizzata dei dati. È anche uno dei settori che ha dimostrato una maggiore capacità di ripristinare i dati dai backup.

Tuttavia, anche se il settore pubblico riesce a proteggersi adeguatamente dal ransomware, gli autori degli attacchi stanno adottando un approccio basato sull'estorsione, nel quali i dati vengono prelevati illecitamente con la minaccia di una loro pubblicazione, a meno che non venga pagato un riscatto. L'anno scorso il settore pubblico è stato quello maggiormente colpito da attacchi di questo genere, con una percentuale quasi doppia rispetto alla media di tutti i settori.

Il settore pubblico deve continuare a mantenere risultati positivi contro il ransomware. Inoltre, deve focalizzarsi sul prevenire gli attacchi prima che i cybercriminali riescano ad accedere ai dati. Lo sviluppo di un piano di risposta agli incidenti di cybersecurity deve essere una delle priorità principali per le organizzazioni che ancora non ne hanno implementato uno.

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

2. **Effettuare 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.

2021-06-10 (SB-NP)

SOPHOS